

# **Comparison Study of Industrial Control System Standards Against the Control Systems Protection Framework Cyber-Security Requirements**

Virgil B. Hammond

George A. Shaw

Jeffery E. Dagle

Michael J. Baca

Adam L. Hahn

Kevin D. Robbins

Shabbir A. Shamsuddin

Robert P. Evans

Mark D. Hadley

Roger G. Cox

Robert D. Pollock

Mary L. Young

September 2005

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



# Comparison Study of Industrial Control System Standards Against the Control Systems Protection Framework Cyber-Security Requirements

Virgil B. Hammond<sup>a</sup>  
Shabbir A. Shamsuddin<sup>a</sup>  
George A. Shaw<sup>a</sup>  
Robert P. Evans<sup>b</sup>  
Jeffery E. Dagle<sup>c</sup>  
Mark D. Hadley<sup>c</sup>  
Michael J. Baca<sup>d</sup>  
Roger G. Cox<sup>d</sup>  
Adam L. Hahn<sup>d</sup>  
Robert D. Pollock<sup>d</sup>  
Kevin D. Robbins<sup>d</sup>  
Mary L. Young<sup>d</sup>

<sup>a</sup>Argonne National Laboratory

<sup>b</sup>Idaho National Laboratory

<sup>c</sup>Pacific Northwest Laboratory

<sup>d</sup>Sandia National Laboratories

April 2005

US-CERT Control Systems Security Center  
Idaho Falls, Idaho 83415

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

Control Systems Security Center

**Comparison Study of Industrial Control System Standards against the Control Systems Protection Framework Cyber-Security Requirements**

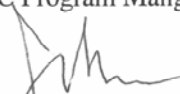
INL/EXT-05-00831

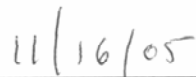
September 2005  
Version 3.2

Approved by:

  
\_\_\_\_\_  
Fred C. Cowart  
CSSC Program Manger

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Julio G. Rodriguez  
Program Lead, SCADA/Power Systems

  
\_\_\_\_\_  
Date



**Control Systems Security Center  
Standards Awareness Team**

# **Comparison Study of Industrial Control System Standards against the Control Systems Protection Framework Cyber- Security Requirements**



**September 2005  
Version 3.2**



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



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.



**NOTICE:** This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors.

## **Contributors**

### **Argonne National Laboratory**

Virgil B. Hammond  
Shabbir A. Shamsuddin  
George A. Shaw

### **Idaho National Laboratory**

Robert P. Evans

### **Pacific Northwest National Laboratory**

Jeffery E. Dagle  
Mark D. Hadley

### **Sandia National Laboratories**

Michael J. Baca  
Roger G. Cox  
Adam L. Hahn  
Robert D. Pollock  
Kevin D. Robbins  
Mary L. Young





# TABLE OF CONTENTS

1.	INTRODUCTION .....	1
1.1	Framework Overview .....	1
1.2	Standards Awareness and Capabilities Task.....	3
1.3	The Comparison Analysis Effort .....	3
1.4	Origin of Common Criteria .....	4
2.	SECTOR STANDARDS REVIEWED .....	8
2.1	Chemical Sector .....	8
2.2	Energy - Natural Gas Sector.....	8
2.3	Energy - Petroleum & Oil Sector.....	9
2.4	Transportation-Rail Sector.....	9
2.5	Cross Sector .....	10
2.6	Energy - Electric Power Sector .....	11
2.7	Telecommunications Sector.....	12
2.8	Water Sector.....	13
3.	COMPARISON RESULTS.....	15
3.1	Common Acronyms .....	16
3.2	Class: Security Audit (FAU) .....	17
3.3	Class: Configuration Management (FCM).....	24
3.4	Class: Cryptographic Support (FCS) .....	28
3.5	Class: User Data Protection (FDP) .....	31
3.6	Class: Event Definition (FEM).....	38
3.7	Class: Identification and Authentication (FIA) .....	41
3.8	Class: Security Management (FMT) .....	47
3.9	Class: Trusted Security Functions (FPT) .....	54
3.10	Class: Resource Utilization (FRU) .....	63
3.11	Class: Target [STOE] Access (FTA) .....	67
3.12	Class: Trusted Path/Channels (FTP) .....	70
4.	CONCLUSIONS .....	100
4.1	Chemical Sector: CIDX Cyber-security Standard .....	100
4.2	Energy - Natural Gas Sector: AGA Report Number 12.....	101
4.3	Energy - Petroleum & Oil Sector: API Standard Number 1164 .....	102
4.4	Transportation-Rail Sector .....	103
4.5	Cross Sector ISA-TR99.01 and 02-2004 .....	103
4.6	Energy - Electric Power Sector: NERC CIP .....	104
4.7	Telecommunications Sector: ANSI T1.276 .....	104
4.8	Water Sector: AWWA .....	105
5.	NEXT STEPS .....	106
6.	REFERENCES .....	107



## EXECUTIVE SUMMARY

Cyber security standards, guidelines, and best practices for control systems are critical requirements that have been delineated and formally recognized by industry and government entities. Cyber security standards provide a common language within the industrial control system community, both national and international, to facilitate understanding of security awareness issues but, ultimately, they are intended to strengthen cyber security for control systems.

This study and the preliminary findings outlined in this report are an initial attempt by the Control Systems Security Center (CSSC) Standard Awareness Team to better understand how existing and emerging industry standards, guidelines, and best practices address cyber security for industrial control systems. The Standard Awareness Team comprised subject matter experts in control systems and cyber security technologies and standards from several Department of Energy (DOE) National Laboratories, including Argonne National Laboratory, Idaho National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories.

This study was conducted in two parts: a standard identification effort and a comparison analysis effort. During the standard identification effort, the Standard Awareness Team conducted a comprehensive open-source survey of existing control systems security standards, regulations, and guidelines in several of the critical infrastructure (CI) sectors, including the telecommunication, water, chemical, energy (electric power, petroleum and oil, natural gas), and transportation - rail sectors and sub-sectors.

During the comparison analysis effort, the team compared the requirements contained in selected, identified, industry standards with the cyber security requirements in “Cyber Security Protection Framework,” Version 0.9 (hereafter referred to as the “Framework”). For each of the seven sector/sub-sectors listed above, one standard was selected from the list of standards identified in the identification effort. The requirements in these seven standards were then compared against the requirements given in the Framework. This comparison identified gaps (requirements not covered) in both the individual industry standards and in the Framework. In addition to the sector-specific standards reviewed, the team compared the requirements in the cross-sector Instrumentation, Systems, and Automation Society (ISA) Technical Reports (TR) 99 -1 and -2 to the Framework requirements.

The Framework defines a set of security classes separated into families as functional requirements for control system security. Each standard reviewed was compared to this template of requirements to determine if the standard requirements closely or partially matched these Framework requirements. An analysis of each class of requirements pertaining to each standard reviewed can be found in the comparison results section of this report. Refer to Appendix A, “Synopsis of Comparison Results,” for a complete graphical representation of the study’s findings at a glance.

Some of the requirements listed in the Framework are covered by many of the standards, while other requirements are addressed by only a few of the standards. In

some cases, the scope of the requirements listed in the standard for a particular industry greatly exceeds the requirements given in the Framework. These additional families of requirements, identified by the various standards bodies, could potentially be added to the Framework. These findings are, in part, due to the maturity both of the security standards themselves and of the different industries' current focus on security. In addition, there are differences in how communication and control is used in different industries and the consequences of disruptions via security breaches to each particular industry that could affect how security requirements are prioritized.

The differences in the requirements listed in the Framework and in the various industry standards are due, in part, to differences in the level and purpose of the standards. While the requirements in the Framework are fairly specific, many of the industry standard requirements are more general in nature. Additionally, the Framework requirements, derived from the "Common Criteria for Information Technology Security Evaluation," are component-based, while most of the industry standards are system-based.

The findings of this study will allow the CSSC Framework Team and the standards organizations responsible for the reviewed standards to quickly grasp the relationship between their requirements and the Framework, as well as the relationship between their standard and other industry sectors. This will help identify areas for future work in developing improved security standards.

## ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AGA	American Gas Association
ANSI	American National Standards Institute
API	American Petroleum Institute
ATIS	Alliance for Telecommunications Industry Solutions
AWWA	American Water Works Association
CC	Common Criteria for Information Technology Security Evaluation
CI	Critical Infrastructure
CIDX	Chemical Industry Data Exchange
CIP	Critical Infrastructure Protection
CS	Cyber Security
CSMS	Cyber-security Management System
CSR	Cyber Security Requirements
CSSC	Control Systems Security Center
DCS	Distributed Control System
DES	Data Encryption Standard
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
FIPS	Federal Information Processing Standards
FRA	Federal Railroad Administration
FY	Fiscal Year
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISA	Instrumentation, Systems, and Automation Society
ISO	International Organization for Standards
ISMS	Information Security Management System
IT	Information Technology
LAN	Local Area Network
M&CS	Manufacturing and Control System
NERC	North American Electric Reliability Council
NIST	U.S. National Institute of Standards and Technology
PCS	Process Control System
PIN	Personal Identification Number
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit

SCADA	Supervisory Control and Data Acquisition
SSL	Secure Socket Layer
STOE	System Target of Evaluation
TCSEC	Trusted Computer Systems Evaluation Criteria
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	Technical Security Functions or Trusted Security Functions
US-CERT	United States – Computer Emergency Readiness Team
VPN	Virtual Private Network
WISE	Water Infrastructure Security Enhancements

# 1. INTRODUCTION

Cyber security standards, guidelines, and best practices (hereafter referred to as “standards”) for control systems are critical requirements that have been delineated and formally recognized by industry and government entities. They are the measure by which organizations are sometimes judged to be operating in a responsible and legal manner. Standards are the result of work performed by industry specific groups that have been judged to be qualified to develop such guidance. They provide *uniform guidance* to control system equipment providers, vendors, and integrators for implementing consistent security approaches and designs into their products, and they provide uniform guidance to system operators to ensure safe and secure operation of their systems. Cyber security standards are also used to provide a *common language* within the industrial control systems community, both national and international, to *facilitate* understanding security awareness issues but, ultimately, they are intended to *strengthen* cyber security for control systems.

The success of the Cyber Security Protection Framework effort of the Control Systems Security Center (CSSC) will depend on its ability to *influence* and *impact* the advancement of cyber security standards for control systems.

This study and the preliminary findings outlined in this report are an initial attempt by the CSSC Standard Awareness Team to better understand how existing and emerging industry standards, guidelines, and best practices address cyber security for industrial control systems and to compare these cyber-related standards against the cyber security requirements delivered as part of the Cyber Security Protection Framework, Version 0.9 deliverable.

## 1.1 Framework Overview<sup>1</sup>

The “Cyber Security Protection Framework, Version 0.9” (hereafter referred to as the “Framework”) provides a methodology for consolidating vulnerability mitigation measures to enhance the security of process control systems against cyber attack. It supports the CSSC’s mission to reduce cyber security vulnerabilities within control systems associated with the nation’s critical infrastructure. It will provide a tool for owner/operators and system vendors to use to assess the security of control systems against a database of categorized cyber security requirements. Each requirement will then be supported by graded recommendations for mitigating vulnerabilities. Figure 1 shows how the Framework will support the CSSC mission to improve cyber security for control systems by involving the control system community.

---

1. Framework description was extracted from the “Framework and Implementation Plan,” Draft – June 8, 2005.

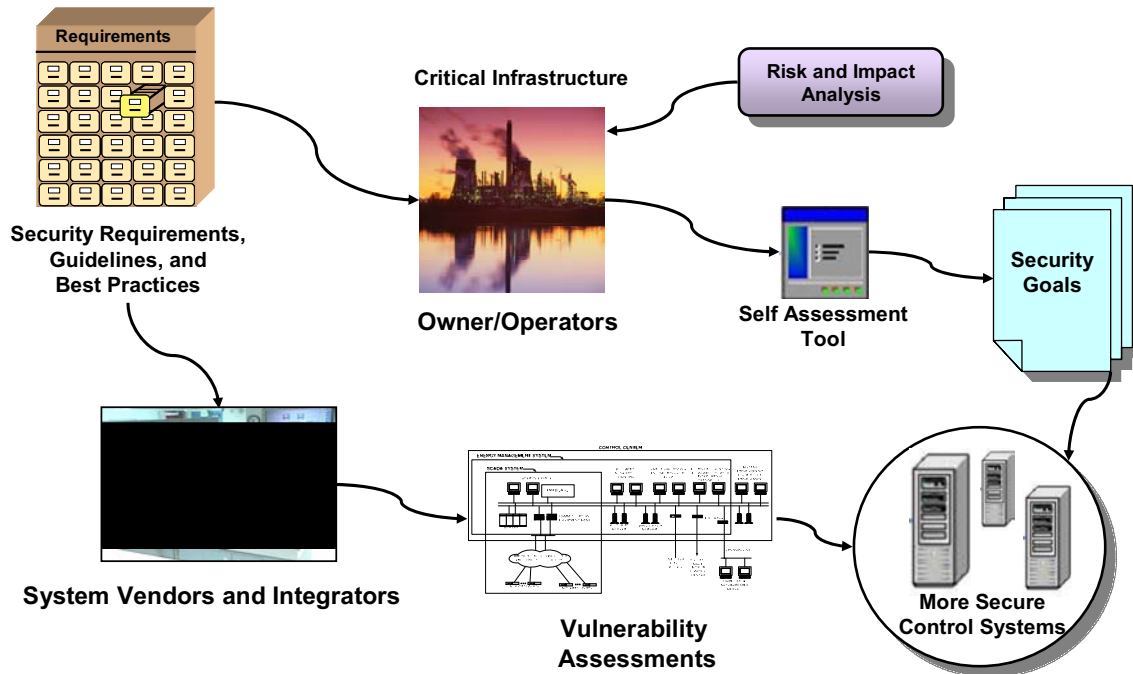


Figure 1. Involving Industry in the Solution.

The Framework tools will help owner/operators identify the details of their control system and the potential consequences of a failure in the system. The system topology and components associated with cyber security are essential to this discovery process. Once the accurate topology is established, the body of knowledge and logic built into the Framework will produce a listing of recommended solutions to meet cyber security requirements, component by component. Requirements are designed to be protective, based on the system architecture; recommended solutions are assigned in a graded manner commensurate with the potential consequences of a successful attack.

The Framework will be used to develop assessment tools to evaluate the current security profile of a system and as a design tool to design or upgrade a system. In time, with the addition of risk data, the Framework will also be used to prioritize the recommendations in terms of greatest risk reduction.

Assessments help owner/operators and vendors identify and prioritize areas where mitigation measures should be applied. Assessments also allow the CSSC to collect system information (market share and sectors) from owners and vendors to assist the US-CERT in communicating emerging information about exploits and vulnerabilities to the user community. Assessment findings also support risk analysis efforts to quantify impacts and security improvement metrics as mitigation measures are implemented.

The Framework cyber security requirements are also linked to industry standards, and the interface tools will allow the user to assess compliance with a given standard. Thus, the protection Framework provides categorized and graded guidance, component by component, for improving control system cyber security.



## **1.2 Standards Awareness and Capabilities Task**

This study was conducted in two parts: a standard identification effort and a comparison analysis effort. During the standard identification effort, the Standard Awareness Team conducted a comprehensive open-source survey of existing control system security standards, regulations, and guidelines in several of the critical infrastructure (CI) sectors, including the telecommunication, water, chemical, energy (electric power, petroleum and oil, natural gas), and transportation - rail sectors and sub-sectors.

During the comparison analysis effort, the team compared the requirements contained in selected, identified, industry standards with the cyber security requirements in the Framework. For each of the seven sectors/sub-sectors listed, one standard was selected from the list of standards identified in the identification effort. The requirements in these seven standards were then compared against the requirements given in the Framework. This comparison identified gaps (requirements not covered) in the individual industry standards. In addition to the sector-specific standards reviewed, the team compared the requirements in the cross-sector Instrumentation, Systems, and Automation Society (ISA) Technical Reports (TR) 99-1 and -2 to the Framework requirements. This effort provides a basic understanding of the relationship between the industry standards and the Framework.

## **1.3 The Comparison Analysis Effort**

The Framework cyber security requirements are arranged hierarchically, first by class, then by family. For example, the class of requirements named Cryptographic Support includes the families Cryptographic Key Management and Cryptographic Operation. Each family contains a number of related cyber security requirements.

Logically, the comparison of a control system security standard to the Framework involves sorting each requirement identified by the standard first into the appropriate Framework class, then into the appropriate Framework family and, finally, noting whether the requirement matches any Framework requirements within that family. In practice, the comparison is not so straightforward.

Frequently, the Framework cyber security requirements do not express complete thoughts or concepts but require further specialization to be precise. For example, one requirement addressing storage of audit files states that, “the TSF shall ensure that [assignment: metric for saving audit records] audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, attack].” To determine that a standard requirement matches this Framework requirement, the analyst must judge that the standard requirement addresses roughly the same issues as the Framework requirement, however it is finally interpreted.

Another difficulty is that some standards that were compared to the Framework are intended to serve as models for organizations developing in-house cyber security programs. These standards tend to provide informative requirements and to designate responsibilities. The Framework requirements, on the other hand, are normative and

prescribe capabilities and behaviors of control system components. Determining a match between such different requirements again involves careful judgment.

Very often standards give words such as “user” a specific meaning not common in everyday speech. For example, American Gas Association Report Number 12 and Federal Information Processing Standards Publication 140-2 define “user” as “an individual or process acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.” However, the Framework defines “user” to be “any entity (human user or external IT entity) outside the TOE [target of evaluation] that interacts with the TOE.” Additionally, American Gas Association Report Number 12 defines the term “operator,” which is not defined in the Framework. Such conflicting definitions and specialized meanings of common words complicate comparison of requirements.

Some of the standards reviewed address cyber security at a higher level than the Framework. And, some standards reviewed are more mature than others or simply differ in scope. For these reasons, and because of the complications just described, the comparison results reported below will differ in the amount of detail provided.

## 1.4 Origin of Common Criteria

The nomenclature and catalog of requirements included in the Idaho National Laboratory’s *Cyber Security Protection Framework for Control Systems* were derived from the document, *System Protection Profile – Industrial Control Systems*<sup>2</sup>. The format used and requirements delineated in *System Protection Profile - Industrial Control Systems* are based on the Common Criteria for Information Technology Security Evaluation” (Common Criteria).

Common Criteria is an international standard that provides:

- A standard nomenclature for describing both security requirements and the security environment of concern.
- A structured format and required content for describing the security environment.
- A taxonomy and catalog of security requirements
- Certified laboratories and processes for evaluating security assurance levels.

The Common Criteria is the result of an effort to develop an internationally accepted framework and criteria for the evaluation of Information Technology (IT) product security. It is a successor to the U.S. Department of Defense (DoD) Orange Book. The Orange Book is one of a series of books published by the National Computer Security Center of the U.S. National Security Agency in the 1980s and 1990s. The series is known as the Rainbow Series<sup>3</sup> because of their colored covers for each topic. The criteria for evaluating trusted computer products were delineated in the Orange Book

---

2. National Institute of Standards, *System Protection Profile – Industrial Control Systems*, Decisive Analytics, Version 1.0, April 14, 2004.

3. <http://csrc.nist.gov/secpubs/rainbow/>

and Red Book. The Orange Book, first published in 1983 and considered the pre-eminent book in the series, contains the “Trusted Computer Systems Evaluation Criteria” (TCSEC), DoD Standard 5200.28. Following publication of the Orange Book, Germany, Britain, and Canada all issued their own version of the Orange Book. These standards were followed by the development of a unified European standard for security evaluations, known as ITSEC. In 1994, an international effort (U.S., Canada, United Kingdom, France, Germany, and the Netherlands) was initiated to develop an international standard for computer system security evaluation criteria. The Common Criteria was the result of this effort. Version 1.0 of Common Criteria was released for public comment in 1996. Version 2.0 was released in 1998. Version 2.0 was adopted by the International Organization for Standards (ISO) and became ISO 15408 in 1999. Common Criteria is currently the pre-eminent international standard for computer system security evaluation criteria. Nations formally agree, by signing the Common Criteria Recognition Arrangement (CCRA), to accept the results of Common Criteria evaluations performed by other CCRA members. The National Information Assurance Partnership administers a security evaluation program in the United States that utilizes the Common Criteria as the standard for evaluation.

The catalog of requirements included in the Common Criteria is divided, at the highest level, into Functional and Assurance requirements. Functional requirements relate to component or system functions that support IT security. Assurance requirements relate to the “strength” level of functional requirements and the rigor with which security functions are implemented and tested.

The taxonomy within which Common Criteria requirements are specified is illustrated in Figure 2. This taxonomy divides both the Functional and Assurance requirements categories into requirements “Classes.” Classes of requirements share a common focus. There are 11 functional classes and 7 assurance classes of requirements. Requirements are further subdivided into Families, Components, and Elements. Figure 3 provides an example of the Common Criteria nomenclature used for the specification of requirements.

Two **Categories** of requirements:

(1) **Functional** – 11 **classes** of security functions; e.g., cryptographic support, user data protection, access

(2) **Assurance** – 7 assurance **classes**; e.g., life cycle support, tests, vulnerability assessment

The members of a class are termed **Families**. A family is a grouping of sets of security requirements that share security objectives but may differ in emphasis or rigor.

**Elements** are members of a component and cannot be selected individually. Elements are explicit "shall" statements.

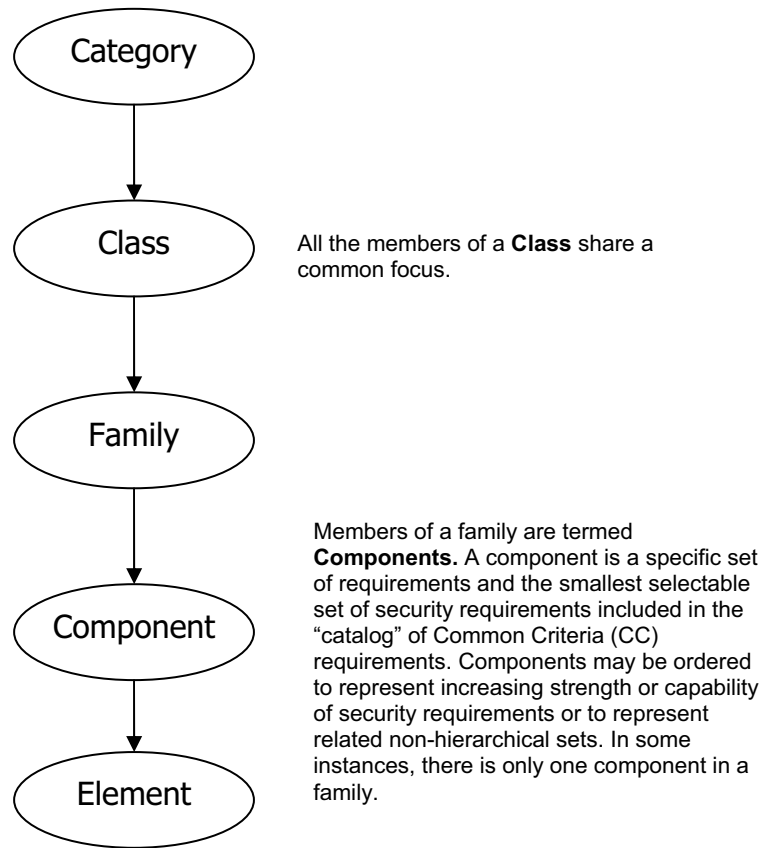


Figure 2. Common criteria requirements taxonomy.

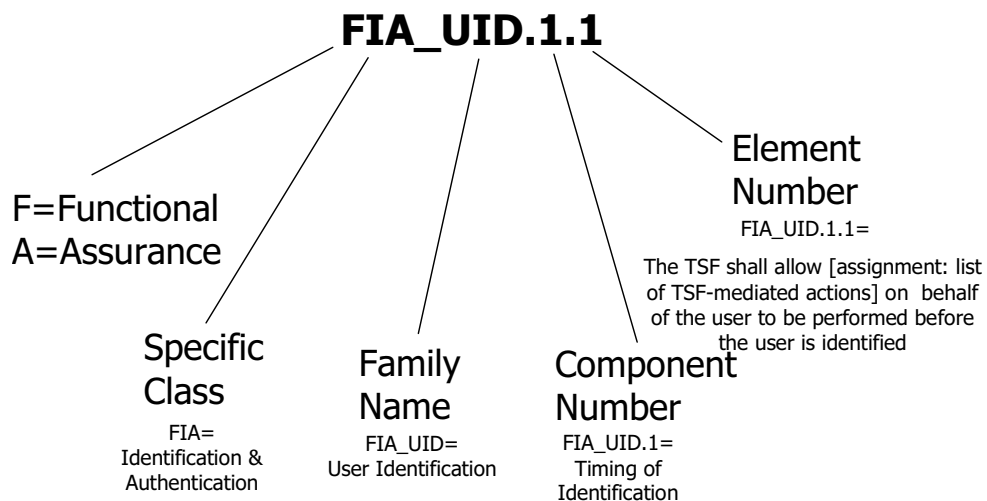


Figure 3. Common Criteria Nomenclature for the specification of requirements.

The Common Criteria documents state that new requirements may be defined by users as necessary. The U.S. National Institute of Standards and Technology (NIST) document *System Protection Profile – Industrial Control Systems*<sup>4</sup> in fact defines two new functional classes, Configuration Management (FCM) and Event Definition (FEM), and excludes the Common Criteria functional classes of Communications (FCO) and Privacy (FPR).

Common Criteria is published by both the NIST and the ISO. The current version of the Common Criteria standard is Version 2.2, and it consists of three primary documents. These documents<sup>5</sup> encompass the following topics:

1. Part 1: Introduction and general model (NIST: CCIMB-2004-01-001, ISO: ISO/IEC 15408-1)
2. Part 2: Security functional requirements (NIST: CCIMB-2004-01-002, ISO: ISO/IEC 15408-2)
3. Part 3: Security assurance requirements (NIST: CCIMB-2004-01-003, ISO: ISO/IEC 15408-3).

Common Criteria Part 2 is effectively a catalog of functional security requirements that may be specified for a system or component. Part 3 is a catalog of security assurance requirements. The Common Criteria establishes specific information assurance goals and requires product testing by a laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program. Products are tested against functional security requirements based on predefined Evaluations Assurance Levels defined in Part 3 of the standard. Common Criteria certification is required for hardware and software devices used by the federal government on national security systems.

The Common Criteria continues to evolve. Common Criteria Version 2.2, as well as earlier versions, focused on the delineation of standards for security related components and did not include system-level requirements critical to the implementation of secure systems. Decisive Analytics has recently published *An Enhanced ISO/IEC 15408 Standard for System Security Specification and Evaluation*<sup>6</sup> that provides both functional and assurance requirements specifically intended to address system security issues and solutions.

---

4. National Institute of Standards, *System Protection Profile – Industrial Control Systems*, Decisive Analytics, Version 1.0, April 14, 2004.

5. <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2>

6. Decisive Analytics, *An Enhanced ISO/IEC 15408 Standard for Systems Security Specification and Evaluation*, Version 1.0, May 12, 2004.

## 2. SECTOR STANDARDS REVIEWED

The Standards Awareness Team searched relevant documents to identify and evaluate the requirements and constraints for companies in critical infrastructure sectors that imply a control system cyber dependency.

### 2.1 Chemical Sector

A total of 45 documents (standards, best practices, regulatory, and industry-related process control and cyber-security guidelines) pertaining to the chemical process industry were identified in sub-task I of this project. Only Chemical Industry Data Exchange (CIDX) cyber-security standard “*Guidance for Addressing Cybersecurity in the Chemical Sector*, version 2.0,” was selected for comparison to the Framework.

The CIDX cyber-security standard was selected for analysis because most of the standards, industry best practices, and regulatory requirements identified were very general in nature and, therefore, did not provide details with respect to the overall Framework cyber-security requirements pertinent to the application of controls in the operation of the process and chemical industries. Performing a comparison on each of these standards would have been time-consuming and not cost-effective for this analysis.

The CIDX cyber-security standard differs from other standards in design philosophies, operational considerations, corporate risk profile, and policies. The CIDX cyber-security standard provides best practices and guidance to include in corporate policies, procedures, and practices. Elements of cyber-security protection actions and information that increases awareness are presented in simple language that can be easily understood and adopted by chemical industry members.

### 2.2 Energy - Natural Gas Sector

Sub-task 1 of this project identified 86 standards, best practices, regulatory, and related industry process control and cyber security standards pertaining to the natural gas industry. Only American Gas Association (AGA) *Report Number 12 (AGA 12)*, *Cryptographic Protection of SCADA Communications*, was selected for comparison to the Framework. Specifically, *Draft 5 of Part 1: “Background, Policies and Test Plan,”* was reviewed because it focuses specifically on cyber security of control systems and reviewing it was deemed the most cost-effective use of available resources. *Part 2: “Retrofit link encryption for asynchronous serial communications,” Part 3: “Protection of networked systems,” Part 4: “Protection embedded in SCADA components,”* and *Addendums: “Key Management,” “Protection of Data at Rest,”* and *“Security Policies”* are forthcoming and were not available for review. *FIPS PUB 140-2, “Security Requirements for Cryptographic Modules,”* was also examined because it is referenced by AGA 12, Part 1, and lends significant support to the document.

The stated purpose of the AGA 12 series is to recommend a comprehensive system designed specifically to protect Supervisory Control and Data Acquisition (SCADA)

system communications. As such, it addresses an important vulnerability of most current SCADA systems—plaintext transmission of control system data over unprotected channels between control centers and remote sites. These systems are key components that provide monitoring and control functions associated with much of the critical infrastructure in the United States, including natural gas transmission and distribution systems.

### **2.3 Energy - Petroleum & Oil Sector**

The requirement under Task II was to review one of the cyber security standards identified in Task I and determine its compliance with respect to each discrete requirement set forth in the Framework. Of the 30 security standards related to petroleum operations identified in Task I of this project, American Petroleum Institute (API) Standard 1164 (API 1164), *Pipeline SCADA Security*, was selected for comparison to the Framework. Most of the standards identified were not comprehensive with respect to the overall Framework requirements. Performing a comparison on each of these standards would have been time-consuming and not cost-effective for this analysis.

API 1164 focuses on defining the responsibilities of authorities and also on prescribing the conditions for system access. It lists the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks, and provides a comprehensive list of practices intended to harden the core architecture. The standard appears to focus on preventing system compromise, in which case control of losses may be less of a concern. The Framework takes such intrusions into consideration, and significant portions of its requirements are aimed at minimizing losses.

### **2.4 Transportation-Rail Sector**

A total of 22 standards, guidelines, laws, and best practices for the transportation sector were reviewed. Most of these documents addressed control system cyber security in only minimal terms. The transportation standard selected for review was *Transportation Specification – Standards for Development and Use of Processor-Based Signal and Train Control Systems* because it seemed to be the standard that had the most complete coverage of control system cyber security, although this coverage was still quite limited. This standard was issued by the Federal Railroad Administration (FRA) as a performance standard for the development and use of processor-based signal and train control systems. It also covers systems that interact with highway-rail grade-crossing warning systems and establishes requirements for notifying FRA prior to installation and for training and recordkeeping.

The transportation sector consists of several sub-sectors: aviation; passenger rail and railroads; highways, trucking, and busing; pipelines; maritime; and mass transit systems. Each of these sub-sectors was considered in selecting a standard for review. Some of the sub-sectors do not rely on cyber control systems, while with others the control system is confidential in nature. There is a limited amount of cyber control used within the rail industry.

The *Transportation Specification – Standards for Development and Use of Processor-Based Signal and Train Control Systems* standard was issued to promote the safe operation of trains on railroads using processor-based signal and train control equipment. This standard addresses the use of processor-based control systems and the concerns related to their use. This standard was chosen for the following reasons:

- After reviewing several transportation-related standards, it was determined that this one dealt with control system security more completely than the others.
- Although this standard deals with areas other than control systems, it does address processor-based control systems and, hence, does cover some common control concerns.

Control systems used for trains are much different from those used for manufacturing plants, chemical refineries, or the electrical distribution systems. The objective of this standard is for processor-based signal and train control systems to meet or exceed the safety level of the traditional signal systems they replace. As a result, new systems must be compared by relative performance, and not against a fixed set of requirements. Therefore, the standard is a performance-based standard that is neutral with regard to the technology that implements it. Because this is a performance-based standard, it is not easily compared to the requirements in the Framework, which tends to be prescriptive in nature.

The differences in the standards are due to the differences in the way the systems provide control. Although the railroad system is a processor-based control system, it is still primarily a hands-on control system. The system is mostly hard-wired, with the operator always having immediate override capabilities. For these reasons, many of the security classes, such as “Security Alarms” and “Cryptographic Support,” have little application on a railroad control system.

## **2.5 Cross Sector**

Two cross-sector technical reports were reviewed for the comparison study. These reports, published by ISA (Instrumentation, Systems, and Automation Society) are ISA-TR99.00.01-2004 (TR99-01), *Security Technologies for Manufacturing and Control Systems*, and ISA-TR99.00.02-2004 (TR99-02), *Integrating Electronic Security into the Manufacturing and Control System (M&CS) Environment*. These reports, which are precursors to standards for the cyber security of manufacturing and control systems (M&CS), are informative in nature, describing areas that should be considered when setting up an M&CS cyber security system.

Manufacturing and control systems are found in many organizations within the nation’s critical infrastructure. The two reports reviewed provide common ground in analyzing and securing the cyber component of M&CS, independent of the type of organization or the sector with which it is aligned.



These reports were issued to promote the safe and secure operation of M&CS by identifying best practices, as determined by representatives of organizations within a wide variety of sectors. These two reports were chosen for the following reasons:

- They are sector cross-cutting reports dealing primarily with the cyber security of manufacturing and control systems.
- They are supported by representatives of organizations from many of the critical infrastructures.
- They delineate baseline cyber security requirements dealing with manufacturing and control systems.

Strictly speaking, these are not standards but technical reports. However, they still provide much the same information, with less detail, as the follow-on standards will provide. As cross-sector documents, they are more generic in nature than many other standards. Their primary focus is on manufacturing and control systems, so they do not address some special areas of concern. These are high-level documents that identify high-level concerns and present possible solutions, while not addressing specific lower-level requirements. They are also informative, or performance based in nature, which makes it more difficult to compare them to prescriptive, low-level, requirement-based standards.

## **2.6 Energy - Electric Power Sector**

A total of 84 cyber security standards, guidelines, and industry best practices were identified in the electric/energy sector. Most of these were very general in nature or only covered a portion of the material contained in the Framework. The North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) series (Draft 3) was selected for this effort because:

1. It is the most complete and thorough standard.
2. Industry is currently working on the standard.
3. It covers some areas that are not in the first version of the Framework, providing for a more complete comparison study.

NERC is a voluntary organization whose mission is to ensure that the bulk electric system in North America is reliable, adequate, and secure. The component of NERC responsible for the CIP standard is the Critical Infrastructure Protection Committee.

The sections contained in the NERC CIP series are:

- CIP-002-1 Critical Cyber Assets
- CIP-003-1 Security Management Controls
- CIP-004-1 Personnel & Training
- CIP-005-1 Electronic Security
- CIP-006-1 Physical Security

- CIP-007-1 Systems Security Management
- CIP-008-1 Incident Reporting and Response Planning
- CIP-009-1 Recovery Plans.

Within each CIP section, requirements are labeled with an R followed by a number, and measurements are labeled with an M followed by a number. In Section 3 of this report, the section identifier and requirement or measurement is listed. For example, CIP-008-1 R1 means requirement 1 from section CIP-008-1.

The NERC CIP series aligns nicely with the viewpoint that cyber security is addressed through the application of three categories of controls: management, operational, and technical. Management controls include items such as risk assessment, personnel screening, etc. Operational controls include items such as backup procedures, configuration management procedures, backup power, etc. Technical controls include the specific hardware and software used to counter cyber threats. Examples of technical controls are firewalls, intrusion detection systems, anti-virus software, etc. In applying these tools, an organization should first understand their security problem — that is, what needs to be protected, what it needs to be protected from, and why it needs to be protected. This analysis should be built using some form of risk management and analysis methodology. The Framework focuses on technical controls that have been identified through analysis of security requirements for a generic industrial control system. The NERC CIP series, on the other hand, addresses all three categories of security controls.

## **2.7 Telecommunications Sector**

A total of 31 industry and federal government cyber security-related telecommunications standards and requirements were reviewed. Many of these standards relate to very specific and limited telecommunications services. Because it was impossible to review all cyber security-related telecommunications standards, the review effort attempted to focus on those telecommunications standards that were not service specific.

ANSI standard T1.276-2003, Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane, was selected for comparison to the Framework requirements. T1.276 was chosen because:

- It is an ANSI accredited standard.
- The T1 committee that developed this standard is an industry group sponsored by the Alliance for Telecommunications Industry Solutions (ATIS).
- The standard delineates a set of baseline security requirements for the telecommunications management plane. The management plane includes the operation, administration, maintenance, and provisioning (OAM&P) systems for network elements and various supporting systems.

ATIS is a U.S.-based organization funded by the telecommunication industry. ATIS develops technical and operations standards for communications and related

information technology industries, worldwide. The original version of T1.276 was developed by the Security Requirements Working Group (SRWG) established in 2002 by the President's National Security Telecommunications Advisory Committee. SRWG was tasked with developing standards that could help ensure the security of telecommunication network management functions. At the conclusion of their effort, the SRWG recommended to the President that the underlying principles delineated by the working group be applied to the computing elements of other critical infrastructures.

T1.276 specifies requirements as mandatory (M) or as security objectives (O). The delineated requirements are intended to address the following principles of OAM&P security:

- Secure management traffic with strong encryption and authentication.
- Authenticate and attribute all management actions.
- Manage security resources and configurations with integrity.
- Maintain logs for all of the above.
- Support least privilege.
- Support security alarms.

T1.276 defines six "categories" of security requirements. These are:

- Cryptographic Algorithms and Keys
- Authentication
- Administration
- Network Element/Management System Use and Operation
- Communications
- Network Element/Management System Development and Delivery.

## **2.8 Water Sector**

The water sector standard reviewed for this application was taken from the American Water Works Association's (AWWA) *Security Guidance for Water Utilities*. This document was developed to address a number of unpredictable acts that could hinder the operations of water utilities. Section 5, *Cyber Security Management, Operations, and Design Considerations*, is focused specifically on acts that affect the cyber security of a utility. This document was chosen because:

- It was produced under a cooperative agreement with the Environmental Protection Agency (EPA) to improve infrastructure security.
- It has been reviewed by members of the Water Infrastructure Security Enhancements (WISE) Standards Committee.
- It was reviewed by various AWWA divisions to ensure the ideas will work for a wide range of utility configurations and sizes.

This document focuses on process control systems in general. None of its statements provide any hint that process control systems (PCS) in the water sector have any special requirements for proper operation.

The AWWA is an international, nonprofit organization whose focus is the supply, treatment, and distribution of the nation's drinking water. This standard was created to specifically address related concerns. Both the Water Environment Federation and the American Society of Civil Engineers have also taken part in this effort, creating standards corresponding to the wastewater systems and contamination detection and monitoring systems, accordingly.

### 3. COMPARISON RESULTS

In each sub-section, comparison results are reported by Framework class and family of cyber security requirements. Each sub-section summarizes the results for a Framework class using a table, such as the following:

	Cryptographic Support	
	Cryptographic Key Management	Cryptographic Operation
Chemical	○	○
Natural Gas	●	●
Petroleum & Oil	○	○
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	●	○
Cross-Sector ISA TR99-02	●	○
Electrical Power	○	○
Telecommunications	●	●
Water	○	○

○ = Gap   ● = Partial Match   ● = Match

In this table, ○ indicates that the standard reviewed does not adequately address the requirements of the Framework family identified in the column heading, ○ indicates that the standard reviewed only partly addresses the requirements of the Framework family, and ● indicates that the standard reviewed mostly or completely addresses the requirements of the Framework family.

There are several ways to read these tables. First, reading by row it is possible to get a sense of the maturity and scope of the security standard reviewed for each sector. Where all entries in a row are ● except one or two, there are likely to be marginal improvements that can be made in that standard to address remaining cyber security concerns. Second, reading by column it is possible to identify cyber security concerns standards organizations may need to address where, for example, all or most of the column entries are ○. Also reading by column, one sector may find an existing standard adopted by another sector that addresses some family of requirements related to the family that it has yet to address.

There are some caveats to keep in mind when reviewing these tables. First, the tables report only the state of control systems security standards in relation to the Framework, and they do not report the state of control systems security practice. Even if a table row is marked ○, indicating that a sector has not adequately addressed a class of Framework cyber security requirements, companies in that sector may, in practice, fully satisfy the requirements. Also, it may be that including company proprietary practices and operational requirements would change a ○ to a ●. Finally, the standards compared against the Framework cyber security requirements have, in most cases, been thoroughly reviewed and adopted, whereas the Framework is still in development.

The comparison results below should not be taken as a judgment for or against any existing standard, but only as an honest attempt to understand the relation of each standard reviewed to the Framework.

Refer to Appendix A: “Synopsis of Comparison Results,” for a complete graphical representation of the study’s findings.

### **3.1 Common Acronyms**

Each class and family of Framework cyber security requirements is identified both by written word and by a three letter acronym, for example, Security Audit (FAU) and Audit Data Generation (GEN). Specific cyber security requirements are identified by class, family, and number as in FAU\_GEN.1. Also, the following common acronyms are used throughout the comparison results:

- STOE or TOE– System Target of Evaluation or Target of Evaluation (TOE)
- TSF – Technical Security Functions or Trusted Security Functions
- TSC – TSF Scope of Control.

### 3.2 Class: Security Audit (FAU)

	Security Audit					
	Security Alarms	Audit Data Generation	Potential Violation Analysis	Audit Review	Selective Audit	Potential Audit Trail Storage
Chemical	○	○	○	○	○	○
Natural Gas	○	○	○	○	○	○
Petroleum & Oil	○	●	○	●	○	○
Transportation – Rail	○	○	○	○	○	○
Cross-Sector ISA TR99-01	●	○	○	○	○	○
Cross-Sector ISA TR99-02	●	○	○	○	○	○
Electrical Power	●	●	●	●	○	○
Telecommunications	○	○	○	○	○	○
Water	○	○	○	○	○	○

○ = Gap

○ = Partial Match

● = Match

#### 3.2.1 Family Definitions

- Security Alarms (ARP) - This family defines the responses to be taken for detected events indicative of a potential security violation.
- Audit Data Generation (GEN) - This family defines requirements for recording the occurrence of security relevant events that take place under TSF control, including identifying the user that caused the event.
- Potential Violation Analysis (SAA) - This family defines requirements for automated means that analyze system activity and audit data looking for possible or real security violations and also includes profile-based anomaly detection and attack heuristics.
- Audit Review (SAR) - This family defines the requirements for audit tools that should be available to authorized users to assist in the review of audit data and also includes restricted and selectable audit reviews.
- Selective Audit (SEL) - This family defines requirements to select the events (include or exclude) to be audited during STOE operation.
- Protected Audit Trail Storage (STG) - This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. It also includes guarantees of audit data availability and actions for and prevention of audit data loss.

#### 3.2.2 Chemical Sector: CIDX Cyber-security Standards Version 2.0

##### 3.2.2.1 Security Alarms, Audit Data Generation, Audit Review, Selective Audit, and Potential Audit Trail Storage ○

The CIDX cyber-security standard provides general guidelines for vigilance against security breaches. It provides the user with guidance for reporting, deterring, protection,

developing security policies, etc., to protect the system from future intrusion. The document also defines and describes this process in general terms and emphasizes incident planning and response action. The plan recommends steps to take in keeping track of incidents, investigations, recording, tracking, and learning from each incident to develop action plans for securing the known security breaches. The CIDX standard, under Auditing Process, discusses audit tools for tracking software patches, etc., but does not recommend tools for control system devices subject to system failure from automated scanning.

### **3.2.2.2 Potential Violation Analysis** ○

Under the Framework requirement (FAU\_SAA.1.1), the TSF shall be able to apply a set of rules for monitoring the audited events and, based on these rules, indicate a potential violation of the TSP. The CIDX cyber-security standard does not provide details on how to monitor events. Guidance is very general in nature and, therefore, may not adequately satisfy the Potential Violation Analysis class (SAA) requirements. In addition, under potential violation rules, the standard does not provide or define a profile-based anomaly mechanism, nor does it provide an automated response to security violations. This is a gap from the Framework requirements.

### **3.2.3 Energy - Natural Gas Sector: AGA Report Number 12**

#### **3.2.3.1 Security Alarms, Audit Data Generation, and Selective Audit** ○

AGA 12, Part 1, requires collection and reporting of usage and forensic data to provide an audit trail of critical actions and events. However, it does not specify the level of detail contained in the Framework. For example, AGA 12, Part 1, requires that information needed to legally prosecute cyber attackers be recorded. It can be inferred that this includes such things as the date and time an event occurred, although this is not explicitly stated. Therefore, the intent of AGA 12, Part 1, is deemed to correspond in large part with the Framework.

#### **3.2.3.2 Audit Review** ○

Although the interpretability of data is not specifically addressed, this is implied by the AGA 12, Part 1, requirement that the data be “made available.” The Framework audit review requirements are partially met because availability should also include requirements for accessible data for useful purposes and presentation in understandable terms. Explicit read access to audit data does not appear to be required, and selectable audit review is not addressed.

#### **3.2.3.3 Potential Violation Analysis and Protected Audit Trail Storage** ○

As stated previously, AGA 12, Part 1, was deemed to comply with the intent of the Framework, although most of the required detail is missing. Since authorized access and availability for audit purposes is specified, it can be inferred that unauthorized modification or deletion would be prohibited. The detail needed to address the



discrepancies in this area may be included in forthcoming parts of the AGA 12 document.

### **3.2.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.2.4.1 Security Alarms ○**

Virtually all existing control systems incorporate audible and/or visible alarms as a basic security detail. Surprisingly, there is no mention of such alarms in API 1164. One exception found is a door remaining open for an excessive period. This standard does provide some detail on event monitoring, mostly related to information flow and data retention for future audit. This is a gap in the API standard, denoting non-compliance.

#### **3.2.4.2 Audit Data Generation and Audit Review ●**

The provisions of API Standard Number 1164 closely match the requirements for auditing. The standard provides for the generation of audit records for all user activity, maintenance of the records for a specified (by the operator) time, review only by authorized personnel, implementation of intrusion detection capabilities, and also assignment of responsibility for oversight. The API Standard is in compliance with the audit generation requirements.

#### **3.2.4.3 Potential Violation Analysis ○**

API 1164 addresses most of the requirements covered in this family. However, its provisions are not designed to identify potential violations through the use of profiling techniques, such as analysis of user historical patterns. Thus, the standard has a compliance level of approximately 67% in meeting these requirements.

#### **3.2.4.4 Selective Audit and Protected Audit Trail Storage ○**

These two sub-class requirements are partially satisfied in API 1164. The standard provides no provision for varying audit requirements based on a discerned difference in user attributes, such as the size, speed, and complexity of different user systems. The standard prohibits the modification of data collected from the Industrial Control System (ICS) for audit purposes, but does not require the system to detect these modifications. Nor does it require the system to maintain audit records. Instead these are made a responsibility of the staff and supervision, but without stipulating how this is to be accomplished.

### **3.2.5 Transportation-Rail Sector**

#### **3.2.5.1 Security Audit – FAU ○**

None of the requirements listed under the Security Audit class (FAU) in the Framework are addressed in the transportation standard. This may be due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.2.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.2.6.1 Security Alarms ●**

Security alarms (FAU-ARP) are addressed in Sections 8.3 and 8.3.1 of the standard covering intrusion detection systems and alarms.

#### **3.2.6.2 Audit Data Generation ○**

Audit data generation (FAU-GEN) is partly covered by TR99-01 in Sections 6.1.4 and 6.1.6, which address event logging.

#### **3.2.6.3 Potential Violation Analysis ○**

Potential violation analysis (FAU-SAA) is addressed to a minimal extent in Sections 8.1, 8.3, and 8.3.2, which address reviewing event for intrusion detection. Section 9.1.6 addresses providing a full security audit trail, and 8.2 indicates that a detection system must be comprehensive enough to cover all the possible ways a file can enter a system. Sections 8.3 and 8.3.1 discuss immediate alarms to security personnel. Additional areas covered by TR99-01 that are not addressed in the Framework but fall under this general topic include audit planning and log maintenance in Section 8.1, and virus detection systems in Sections 8.2.3, 8.2.4, and 8.2.6.

#### **3.2.6.4 Audit Review ○**

Audit review (FAU-SAR) audit log organization is addressed in Section 8.1 of TR99-01. In addition, Section 8.1.3 addresses scripting and management of log auditing tools.

#### **3.2.6.5 Selective Audit ○**

Selective audit (FAU-SEL) is not addressed in TR99-01.

#### **3.2.6.6 Protected Audit Trail Storage ○**

Protective audit trail storage (FAU-STG) audit file protection is covered in Section 10.1.2 of TR99-01. Section 9.1.6 discusses file checking for signs of tampering, and Sections 8.1 and 9.1.6 cover recording critical events in the audit logs. Additionally, Section 10.2.6 addresses protecting sensitive documents, a topic not addressed in the Framework.

### **3.2.7 Cross Sector - ISA-TR99.00.02-2004**

#### **3.2.7.1 Security Alarms ●**

Security alarms (FAU-ARP) are addressed in Sections 18.11, 18.12.1, and 18.12.3 of the standard covering intrusion detection and alarms.

### **3.2.7.2 Audit Data Generation ○**

Audit data generation (FAU-GEN) is partly covered by TR99-02 in Sections 6.6.6 and 18.10, which address event logging and the examination and monitoring of system logs.

### **3.2.7.3 Potential Violation Analysis ○**

Potential violation analysis (FAU-SAA) is addressed in Section 18.10, which covers examination and monitoring of system logs, and Sections 18.11, 18.12.1, and 18.12.2, which address intrusion detection notification and documentation of events or incidents. Sections 10.2.4 and 18.11 address intrusion detection.

### **3.2.7.4 Protected Audit Trail Storage ○**

Protective audit trail storage (FAU-STG) is covered in Sections 6.6.8.4 and 6.7.4 of TR99-02. They discuss development of policies for communication and operations management and backing up vital data. Additionally, Sections 18.4, 18.5, and 18.6 address the audit planning, expression of audit results, and sending performance metrics to appropriate stakeholders—topics not addressed in the Framework.

### **3.2.7.5 Selective Audit and Audit Review ○**

None of the remaining families listed under the Security Audit class (FAU) in the Framework are addressed in TR99-02. This is probably due to the differences in area of emphasis between the two documents.

## **3.2.8 Energy - Electric Power Sector: NERC CIP**

### **3.2.8.1 Security Alarms, Audit Data Generation, Potential Violation Analysis, and Audit Review ●**

Security Alarms requirements are addressed primarily in CIP-008-1 R3. Under R3, an entity must define incident response actions and communication plans. The response and communication plans can be written to include alarms in audible or visual form, satisfying FAU\_ARP.

Audit data generation requirements, FAU\_GEN, are addressed primarily in CIP-007-1 R7. Under R7, an entity must ensure it is possible to create an audit trail from logs of security-related events affecting critical cyber assets. Logs in R7 refer to system logs, logs generated from monitoring systems, such as an Intrusion Detection System (IDS), and/or physical access logs for areas where automated logs are not available.

Numerous potential violation analysis requirements, FAU\_SAA, are addressed, primarily in CIP-003-1, CIP-007-1, and CIP-008-1. Requirements for detecting, assessing, reporting, and gathering signatures for specific events, as well as defining

roles for assuming responsibility, are all defined in the associated requirements and measures.

Audit review requirements, FAU\_SAR, are addressed in numerous NERC CIP sections, including CIP-003-1 R5, CIP-007-1 R3, and CIP-008-1 R3. Access to audit information is controlled by roles with the CIP standard. In addition, CIP-008-1 identifies the types of audit data to be captured. Assessment is mentioned, but the CIP is not specific regarding filtering methods.

### **3.2.8.2 Selective Audit** ○

Requirements in the NERC CIP address generating, analyses, and storage of audit data, but there is no provision in the NERC CIP for selective audit capabilities. This capability is neither allowed nor prohibited by the requirements and measurements in the CIP.

### **3.2.8.3 Protected Audit Trail Storage** ○

CIP-008-1 and CIP-003-1 indicate a partial match with requirements contained in FAU\_STG. There is no requirement in the CIP for redundant storage of audit files, but retaining audit files for a specified time and protecting audit files from change are addressed.

## **3.2.9 Telecommunications Sector: ANSI T1.276**

### **3.2.9.1 Audit Data Generation** ○

T1.276 specifies two requirements that closely match two audit data generation requirements. T1-276 requirements M-35 and M-37 closely match FAU\_GEN.1.1 and FAU\_GEN.1.2, respectively. In addition, T1.276 states an audit data generation requirement and an objective that are not included in the Framework requirements. Objective O-2 specifies that the system should provide the capability to configure the critical security administration actions that are to be included in the security log. Requirement M-36 specifies that the system shall be capable of remote logging over a trusted path.

### **3.2.9.2 Security Alarms, Potential Violation Analysis, Audit Review, Selective Audit, and Protected Audit Trail Storage** ○

T1.276 does not include requirements that are a close match to the remaining Security audit family requirements.

## **3.2.10 Water Sector: AWWA**

### **3.2.10.1 Security Alarms, Audit Review, and Selective Audit** ○

The AWWA standard has very light requirements for auditing process control systems. It requires that Human Machine Interface (HMI) processes log files that are associated

with user logon credentials with actions and changes made to HMI (creating a non-refutable audit trail of operator actions). It also states that the log files shall be reviewed for inappropriate activity, but does not specify a timeframe for this process. The standard fails to recommend that specific actions, such as system shutdown, be included in the logs or that the logs contain proper date and time stamps. The standard does state to install an intrusion detection system (IDS) at the Internet gateway and regularly audit IDS logs for evidence of unauthorized entry. Since many IDS systems use a rule set to perform their analysis, this statement could align with some of the requirements in FAU\_SAS.

### **3.2.10.2 Audit Data Generation, Potential Violation Analysis, and Protected Audit Trial Storage** ●

The AWWA standard states that appropriate tapes should be stored offsite to ensure disaster recovery, but it does not state that the audit trail is part of these backups. This makes it difficult to determine whether there is any coverage of family FAU\_STG.

### 3.3 Class: Configuration Management (FCM )

Configuration Management		Security Alarms
Chemical		○
Natural Gas		◐
Petroleum & Oil		●
Transportation – Rail		○
Cross-Sector ISA TR99-01		◐
Cross-Sector ISA TR99-02		◐
Electrical Power		●
Telecommunications		◐
Water		○

○ = Gap                      ◐ = Partial Match                      ● = Match

#### 3.3.1 Family Definitions

- Identification Information (IDI) - This family defines the requirements for Configuration Management (CM) as they apply to the PCS for as-built documentation, vendor manuals, drawings, set points, limits, etc. It also includes requirements for change control, design, testing, implementation, and review and approval processes.

#### 3.3.2 Chemical Sector: CIDX Cyber-security Standard

##### 3.3.2.1 Identification Information ◐

The CIDX cyber-security standard provides guidance for a Cyber-security Management System (CSMS) that includes the following:

- Information systems - including all operating systems, data bases, applications of the company, including joint ventures, and other third party business activities
- Manufacturing and control systems - including all PCS, SCADA, Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), configuration workstations, and plant or lab information systems for both real-time and historical data
- Networks, local area networks (LANs), wide area networks (WANs) - including hardware, applications, firewalls, intrusion detection systems
- Integration points with value chain partners
- User responsibilities - including policies to address authentication and audit, and Information protection, including access requirements and individual accountability.

The information is in general terms and explains user identification, management and authentication techniques, etc., and, therefore, can meet the Framework controls security requirement, though not in the exact terminology identified under the criteria.

### **3.3.3 Energy - Natural Gas Sector: AGA Report Number 12**

#### **3.3.3.1 Identification Information** ○

Minimum requirements for a configuration management system are specified in the AGA 12. Some of the details included in the Framework, such as management of action lists and user identities, are not addressed.

### **3.3.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.3.4.1 Identification Information** ●

API 1164 provides extensive and explicit configuration management requirements that appear to exceed the requirements of the Framework. It is very specific with respect to authorization, documentation, testing, etc. The standard satisfies the Identification Information requirements very well.

### **3.3.5 Transportation-Rail Sector**

#### **3.3.5.1 Identification Information – FCM** ○

CM Identification information (FCM-IDI) partly covers four of the requirements listed in Configuration Management Identification Information (FCM-IDI) of the Protection of System Configuration class. Section 236.18 of the transportation standard addresses a management control plan aimed at ensuring that the proper hardware and software are in use. In addition, Section 236.18 discusses the use of a Software Management Control Plan.

### **3.3.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.3.6.1 Identification Information** ○

CM Identification information (FCM-IDI) is partly covered by Section 10.1.4 of TR99-01, which addresses mapping of security areas under access control. In addition, TR99-01 covers the need to extensively document and maintain scripts in Section 8.1.3.

### **3.3.7 Cross Sector – ISA-TR99.00.02-2004**

#### **3.3.7.1 Identification Information** ○

CM identification information (FCM-IDI) is covered in TR99-02 by the following sections:

- Section 6.4.4 — Addresses the assessment and classification of vital information based on consequences of loss, damage, or failure

- Section 6.7 — Addresses that the change management plan should identify components within the security boundary
- Section 8.2.2 — Addresses the development of a network diagram of the system
- Section 6.7.4 — Addresses maintaining documentation of system security aspects
- Section 18.3 — Addresses establishing a change management program
- Sections 6.7.4 and 17 — Addresses reviewing proposed changes, performing system validation testing after changes, and communicating changes to the proper stakeholders
- Sections 6.6.3 and 6.6.8.2.2 — Addresses defining user roles and responsibilities and the development of policies for user responsibilities
- Sections 6.6.2 and 6.7.4 — Covers the need to define the hardware and software within the security perimeter and to assess and test the vulnerability of the security boundary
- Sections 6.5, 6.6.6, and 6.7 — Address the need for change management control
- Sections 6.5, 6.7.4, 12.1, and 17 — Address testing
- Section 6.6.6 — Address training.

### **3.3.8 Energy - Electric Power Sector: NERC CIP**

#### **3.3.8.1 Identification Information ●**

Between CIP-002-1, CIP-003-1, and CIP-007-1, all of the requirements in FCM\_IDI are addressed, with the exception of FCM\_IDI.1.5 and the database requirement contained in FCM\_IDI.1.2. The provisions in the CIP adequately address a configuration management process, the identification of critical assets, defining secure settings, and system/sub-system documentation.

### **3.3.9 Telecommunications Sector: ANSI T1.276**

#### **3.3.9.1 Identification information ○**

Three T1.276 requirements and one objective relate to configuration management, however, these requirements/objectives differ from those specified in the Framework. M-66 requires the system to be able to electronically determine current hardware and software revision levels and validate appropriate configurations. M-64 requires all new software to have cryptographic authentication and integrity protection mechanisms. O-3 states that all receiving software should be capable of interpreting the cryptographic authentication and integrity protection mechanisms. M-65 requires that all software updates be transmitted over a trusted path.

### **3.3.10 Water Sector: AWWA**

#### **3.3.10.1 Identification Information ○**

The AWWA standard states that the utility should install third-party software or upgrade current HMI versions to enable change propagation capability that monitors revisions to



programming, including changes to both date/time and login credentials. This software can also “undeploy” programming changes and revert to a previous version. This statement provides partial coverage of the FCM\_IDI family. There is no mention of a broad configuration management system or method for organizing documents relating to system configuration.

### 3.4 Class: Cryptographic Support (FCS)

	Cryptographic Support	
	Cryptographic Key Management	Cryptographic Operation
Chemical	○	○
Natural Gas	●	●
Petroleum & Oil	○	○
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	●	○
Cross-Sector ISA TR99-02	●	○
Electrical Power	○	○
Telecommunications	●	●
Water	○	○

○ = Gap      ○ = Partial Match      ● = Match

#### 3.4.1 Family Definitions

- Cryptographic Key Management (CKM) - This family includes the requirements to manage cryptographic keys through their lifecycle, including the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access, and cryptographic key destruction.
- Cryptographic Operation (COP) - This family includes requirements for cryptographic operation to function correctly, including specifying the algorithms and key sizes for the STOE.

#### 3.4.2 Chemical Sector: CIDX Cyber-security Standard

##### 3.4.2.1 *Cryptographic Key Management and Cryptographic Operation* ○

The CIDX cyber-security standard recommends using available encryption technology, key generation, and management practices, but does not clearly include the details, as required in the Framework. The standard cites two standards for system administration, which include the use of cryptographic technology prescribed under ISO/IEC- 17799: ISA-TR99.00.02-2004 and NIST PCSRF ICS-SPP. From the analysis, it can be concluded that if the user follows the other standards for cryptographic support, the CIDX cyber-security standard will meet some of the Framework security requirements.

#### 3.4.3 Energy - Natural Gas Sector: AGA Report Number 12

##### 3.4.3.1 *Cryptographic Key Management and Cryptographic Operation* ●

AGA 12, Part 1, proposes the use of encryption to secure SCADA data communications, and it addresses many of the details specified in the Framework, including a secure key management system and cryptographic algorithms approved by NIST. It also requires that cryptographic modules be FIPS 140-2 compliant and

recommends certification. Any remaining disparities may be addressed in the comprehensive key management specification to be published in AGA 12, Part 1, Addendum 1.

### **3.4.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.4.4.1 *Cryptographic Key Management and Cryptographic Operation* ○**

API 1164 recommends encryption in certain cases, and mandates it in others. However, it lacks the detail necessary for a comprehensive security design. At a minimum, a reference to some existing encryption standard, including key management, should have been included. Possible references include Federal Information Processing Standards (FIPS) publications for Data Encryption Standard (DES) or Advanced Encryption Standard (AES). The standard has a gap in meeting the requirements of this class.

### **3.4.5 Transportation-Rail Sector**

#### **3.4.5.1 *Cryptographic Key Management and Cryptographic Operation* ○**

None of the requirements listed under the Cryptographic Support class (FCS) in the Framework are addressed in the transportation standard. No references to cryptographic-based security measures were found. This is probably due to the lack of need for encryption of the control data, as well as the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.4.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.4.6.1 *Cryptographic Key Management* ●**

Cryptographic key management (FCS-CKM) is extensively covered in Sections 7.1.6, "Cryptographic Key Establishment," 7.1.2 and 7.1.6, "Key Deployment," and 7.2, "Secret and Public Key." Sections 10.1.6 and 10.2.6 address management policy. In addition, TR99-01 addresses hardware and software based on cryptography.

#### **3.4.6.2 *Cryptographic Operation* ○**

Cryptographic operation (FCS-COP), as described in the Framework, is not addressed in TR99-01. It does cover several other requirements that are not addressed in the Framework dealing with cryptographic operation, including key changes (Section 7.1.3), protection of encryption hardware (Section 7.1.6), protection against replay and forging (Section 7.1.6), use of a good quality random number generator (Section 7.1.6), protection of the private key (Section 7.2), and thorough testing of the cryptographic system (Section 7.4.6).

### **3.4.7 Cross Sector - ISA-TR99.00.02-2004**

#### **3.4.7.1 *Cryptographic Key Management and Cryptographic Operation*** ○

None of the requirements listed under the Cryptographic Support class (FCS) in the Framework document are addressed in the TR99-02. This is probably due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used. TR99-02 does address providing encryption where appropriate (Section 10.2.3).

### **3.4.8 Energy - Electric Power Sector: NERC CIP**

#### **3.4.8.1 *Cryptographic Key Management and Cryptographic Operation*** ○

The provisions of the NERC CIP standard do not contain any requirements to match the FCS family. In fact, the word cryptography is not even in the standard. Confidentiality is not the primary focus area in the electric sector; instead, the focus is on availability and integrity.

### **3.4.9 Telecommunications Sector: ANSI T1.276**

#### **3.4.9.1 *Cryptographic Key Management and Cryptographic Operation*** ●

T1.276 requirements relating to cryptographic key management are very similar to the requirements delineated in the Framework; however, the requirements delineated in T1.276 are more specific. T1.276 provides specific requirements for key strength (M-6), in addition to specific standards for secure key generation and management (M-7). Keys must be distributed out of band or by secure cryptographic processes, as specified in (M-8).

T1.276 requirements for cryptographic operation are also very similar to the requirements delineated in the Framework, and the T1.276 requirements are more specific. T1.276 specifies encryption standards to be implemented (M-1). Specific algorithms are also required for symmetric (M-4) and asymmetric (M-5) data integrity applications.

### **3.4.10 Water Sector: AWWA**

#### **3.4.10.1 *Cryptographic Key Management and Cryptographic Operation*** ○

The AWWA standard does not include information about the methodologies to generate, use, or destroy cryptographic keys; it does not appear to cover this class.

### 3.5 Class: User Data Protection (FDP)

	User Data Protection				
	Subset Access Control	Security Attribute Based Access Control	Data Authentication with Identity of Generator	Export of User Data Without Security Attributes	Subset Information Flow Channel
Chemical	●	●	○	○	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	●	●	○	○	○
Telecommunications	○	○	○	○	○
Water	○	○	○	○	○

	Simple Security Attributes	Data Exchange Integrity
Chemical	○	●
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	○	○
Telecommunications	○	○
Water	○	○

○ = Gap                      ○ = Partial Match                      ● = Match

#### 3.5.1 Family Definitions

- Subset Access Control (ACC) - This family identifies the access control security function policies and defines the scope of control of the policies that form the identified access control portion of the TSP.
- Security Attribute Based Access Control (ACF) - This family addresses security attribute usage and describes the rules for the specific functions, scope of control, and characteristics of access control policies.
- Data Authentication with Identity of Guarantor (DAU) - This family describes the requirements to provide a guarantee of the validity of information transfers in the STOE.
- Export of User Data without Security Attributes (ETC) - This family defines functions for exporting user data from the STOE such that its security attributes

and protection either can be explicitly preserved or can be ignored once it has been exported.

- Subset Information Flow Control (IFC) - This family identifies the information flow control security function policies, which define the scope of control for the identified information flow control portion of the TSP.
- Simple Security Attributes (IFF) - This family describes the rules for specific functions that can implement the information flow control security function policies.
- Data Exchange Integrity (UIT) - This family defines the requirements for providing integrity for user data in transit between the TSF and another trusted IT source/destination and recovering from detectable errors.

### **3.5.2 Chemical Sector: CIDX Cyber-security Standard**

#### **3.5.2.1 Subset Access Control, Security Attributes Based Access Control, and Data Exchange Integrity ●**

The CIDX cyber-security standard provides strong guidance for access control and data exchange integrity and, therefore, meets the access control and data exchange integrity requirements of the Framework.

The standard provides best practices and guidelines for an administrative process for the creation of all user accounts. It recommends that the accounts be role-based and grant the user only those privileges and access to resources that are necessary to perform the particular job function. The account administration process includes principles to separate the duties of the approvers and implementers of account configuration.

The standard also specifies that rules should be established to confirm that user access to systems and data is controlled. The standard states that rules generally should be applied to roles or groups of users who should only have access to systems and data that are required to meet defined business requirements. For data exchange integrity, the standard strongly recommends that all communications of private information over the Internet are encrypted with Secure Socket Layer (SSL) or (if non-web) with encryption of equivalent or better integrity.

Data Authentication with Identity of Guarantor, Export of User Data without Security Attributes, Subset Information Flow Control, and Simple Security Attributes ●

The CIDX cyber-security standard guidelines are not specific in defining data authentication, but instead point to reference standards to define the requirements. References are made to the following standards:

- Guidance for Cyber-security Vulnerability Assessment Methodology Process, Version 1.0
- ISO/IEC 17799, Information Technology – Code of Practice for Information Security Management, First Edition, Section 9, “Access Control,” 2000

- U.S. Chemical Sector Cyber-security Strategy
- ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004
- ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems, 2004, Section-5, “Authentication and Authorization Technologies.”

Based on the reference standards, it can be concluded that the standard meets the intent of the FDP\_DAU requirements.

The standard provides practical guidance in the export of user data, with or without security attributes. It provides references to practices described in both the BS 7799-2:2002, Section 4.3, and ISO/IEC 17799, Section 5.2. BS 7799-2:2002, Section 4.3 describes processes associated with data classification, information safeguarding, and document management associated with an information security management system (ISMS). Although the standard defines rules for document management and security protocols, it does not describe specific details of communication links and security, per Framework requirements. Based on the reference standards cited, it can be inferred that the standard meets the intent of the FDP\_ETC requirements.

The provisions under the subset “Information Flow Control and Simple Security Attributes” of the standard does not clearly state details that match the Framework requirement in this class; therefore, this area has been identified as a gap in the comparison analysis. The standard does recommend classifying information according to sensitivity and criticality. It recommends employing a simple classification scheme, including designations for public, company use, restricted, and confidential types for data access and authorization. Special consideration is given to data protected by data privacy regulations. It recommends that the company workforce, or subsets of the workforce, be assigned access to these document classifications, according to their need (which relates to their job description). Based on the interpretation, the standard loosely satisfies the FDP\_IFC and FDP\_IFF requirements. Therefore, overall, the standard partially meets the Framework requirements under this class.

### **3.5.3 Energy - Natural Gas Sector: AGA Report Number 12**

#### **3.5.3.1 Subset Access Control, Security Attribute Based Access Control, Data Authentication with Identity of Guarantor, Subset Information Flow Control, Simple Security Attributes, and Data Exchange Integrity ○**

Access control to user data is currently limited to the recommendation that communication access to data repositories should be protected from cyber attack. As such, the standard partially meets the sub-class requirements.

#### **3.5.3.2 Export of User Data without Security Attributes ○**

This class may be addressed in one or both of the following planned AGA 12, Part 1, addendums “Protection of Data at Rest,” and “Security Policies.” This class was deemed a gap, pending these forthcoming specifications.

### **3.5.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.5.4.1 *Subset Access Control, Security Attribute Based Access Control, Data Authentication with Identity of Guarantor, Export of User Data Without Security Attributes, Subset Information Flow Control, Simple Security Attributes, and Data Exchange Integrity* ●**

There are seven families within this class. Appendix A of API 1164 describes specific authentication requirements for a subject (user, administrator, etc.) to gain access to the system, and for a subject to gain access to data residing on the system. The rules are explicitly extended to include both access via communications media and access by third parties. There is a requirement for protecting data that is exported or imported. Every family requirement of the User Data Protection Class is addressed by one or more sections of Appendix A.

### **3.5.5 Transportation-Rail Sector**

#### **3.5.5.1 *Security Attribute Based Access Control* ○**

Security attribute based access control (FDP-ACF) is addressed in Section 236.907 (a)(15) which discusses unauthorized access.

#### **3.5.5.2 *Subset Access Control, Data Authentication with Identity of Guarantor, Export of User Data Without Security Attributes, Subset Information Flow Control, Simple Security Attributes, and Data Exchange Integrity* ○**

None of the remaining families listed under the User Data Protection class (FDP) in the Framework are addressed in the transportation standard. This is probably due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.5.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.5.6.1 *Subset Access Control* ○**

Subset access control (FDP-ACC) is discussed in Section 8.3.3 of TR99-01, which addresses security access policy.

#### **3.5.6.2 *Security Attribute Based Access Control* ●**

Security attribute based access control (FDP-ACF) is addressed in some detail in Sections 5.1, "Role-based Authorization Tools," and 9.1.6, "Mandatory Access Control." Sections 5, 8.33, and 9.1.6 cover establishing the rule sets governing access between the users and the components. Section 5.1 alludes to explicit authorization and denial of access, but does not address this in detail. In addition, TR99-01 covers requirements for blocking all communication, with the exception of specifically enabled communication, enforced destination authorization (Section 6.1.4), firewall configuration (Section 6.1.6), operator capability to easily configure and monitor the intrusion



detection system (Section 8.3.3), configuration of the intrusion detection system (Section 8.3.6), and review of rule sets providing protection in light of ever-changing security threats (Section 6.1.6).

### **3.5.6.3 Subset Information Flow Control** ○

Subset information flow control (FDP-IFC) is addressed in Sections 5 and 9.1.6, which discuss authorization and authentication, in general terms, and providing a control administrator. In addition, TR99-01 covers establishing specific permissions for each user, frequent updating of access permissions, and basing roles on location, projects, etc., (Section 5.1.1). Also, it covers associating users with roles and roles with permissions (Section 5.1.2), minimizing the amount of external traffic to and from the control system, and having information flow only out of the control room (Section 5.1.6).

### **3.5.6.4 Data Authentication with Identity of Guarantor, Export of User Data without Security Attributes, Simple Security Attributes, and Data Exchange Integrity** ○

None of the remaining families listed under the User Data Protection class (FDP) in the Framework document are addressed in the TR99-01. This is probably due to the differences in area of emphasis between the two documents.

## **3.5.7 Cross Sector - ISA-TR99.00.02-2004**

### **3.5.7.1 Subset Access Control** ○

Subset access control (FDP-ACC) is discussed in Sections 6, 6.1, and 6.6.6 of TR99-02, which address defining and executing a comprehensive program of all aspects of security, the commitment of senior management to security, and the development of policies on appropriate security clearance levels.

### **3.5.7.2 Security Attribute Based Access Control** ○

Security attribute based access control (FDP-ACF) is addressed in Sections 6.7.4 and 10.2.3, which cover identification, control, and limiting access to sources of hardware, software, etc., and use of proper access controls.

### **3.5.7.3 Data Authentication with Identity of Guarantor** ○

- Data authentication (FDP-DAU) requirements found in the Framework are not addressed by TR99-02; however, it does address the following:
- Developing policies for network access control (Section 6.6.8.2.3)
- Developing policies for operating system access control (Section 6.6.8.2.4)
- Developing policies for application access control (Section 6.6.8.2.5)
- Developing policies for monitoring system access and use (Section 6.6.8.2.6)
- Monitoring user access (Section 6.7.4)
- Identifying or developing policies of modem access (Section 6.6.6)

- Identifying or developing policies on remote access (Section 6.6.8.2.7)
- Developing policies for the review of user access rights and privilege management (Section 6.6.8.2.1).

### **3.5.7.4 Export of User Data without Security Attributes** ●

Export of user data without security attributes (FDP-ETC) is addressed by Section 6.5, which discusses the importance of practical precautions to eliminate malicious in-bound information.

### **3.5.7.5 Subset Information Flow Control, Simple Security Attributes, and Data Exchange Integrity** ○

None of the remaining families listed under the User Data Protection class (FDP) in the Framework are addressed in TR99-02. This is probably due to the differences in area of emphasis between the two documents.

## **3.5.8 Energy - Electric Power Sector: NERC CIP**

### **3.5.8.1 Subset Access Control and Security Attribute Based Access Control** ●

Subset access control, FDP\_ACC, requirements are met by CIP-006-1 M3, CIP-003-1 R1, and CIP-008-1 R1. The CIP series has been called an effort in documentation, and the policies and procedures outlined in FDP\_ACC.2.2 are adequately met. A combination of both electronic and physical access controls are used to meet FDP\_ACC.2.1. There is a partial match for FDP\_ACC.1.1 in CIP-008-1 R1.

Security attribute based access controls, FDP\_ACF, are primarily met by CIP-003-1 and CIP-007-1. The provisions in these CIP sections call for limiting access based upon a user's role, defining what assets a role may access, obtaining management approval for asset access, and denying access to an asset that is not needed.

### **3.5.8.2 Data Authentication with Identity of Guarantor, Export of User Data without Security Attributes, Simple Security Attributes, and Data Exchange Integrity** ○

The provisions of the NERC CIP standard generally match the requirements of the data authentication with identity of guarantor. For example, CIP-006-1 addresses this from a physical access perspective. However, the requirement to validate non-physical alarms is not included. The incident response procedures outlined in CIP-008-1 R3 are a good match for FDP\_DAU.2.2.

FDP\_ETC.1.1 is satisfied by CIP-007-1 R10 and M9. Monitoring information flow is implied by monitoring normal system operation. FDP\_ETC.1.2, regarding exporting data without associated security attributes, is not addressed in the CIP.

### **3.5.8.3 Subset Information Flow Control** ○

Subset information flow control, FDP\_IFF, is not addressed by the NERC CIP standard. The provisions of the NERC CIP do not include requirements regarding information flow, flow extensions, etc., for user data.

### **3.5.9 Telecommunications Sector: ANSI T1.276**

#### **3.5.9.1 Subset Access Control, Security Attribute Based Access Control, Data Authentication with Identity of Guarantor, Subset Information Flow Control, Simple Security Attributes, and Data Exchange Integrity** ○

Although T1.276 provides extensive guidance regarding data integrity, encryption algorithms, and user access controls, these requirements were judged to better match Framework requirements other than those delineated in these User data protection families.

#### **3.5.9.2 Export of User Data without Security Attributes** ●

None of the T1.276 requirements were judged to best match requirements in this family. However, a partial match was assigned to this family because closely related T1.276 requirements that were assigned to other Framework requirements families do provide extensive guidance regarding data integrity, encryption algorithms, and user access controls.

### **3.5.10 Water Sector: AWWA**

#### **3.5.10.1 Subset Access Control, Data Authentication with Identity of Guarantor, Export of User Data without Security Attributes, Subset Information Flow Control, Simple Security Attributes, and Data Exchange Integrity** ○

The AWWA standard does not address these families.

#### **3.5.10.2 Security Attribute Based Access Control** ●

The AWWA standard suggests that routers be configured to restrict traffic to a small number of destinations, as regulated by an Access Control List (ACL), which is a partial match in the FDP\_ACF category. It also states that the configuration of HMI logon privileges should correspond with the respective responsibility level, which seems to match the FDP\_ACF family.

### 3.6 Class: Event Definition (FEM)

Event Definition	Security Alarms
Chemical	●
Natural Gas	○
Petroleum & Oil	●
Transportation – Rail	○
Cross-Sector ISA TR99-01	○
Cross-Sector ISA TR99-02	○
Electrical Power	●
Telecommunications	○
Water	○

○ = Gap                      ● = Partial Match                      ● = Match

#### 3.6.1 Family Definitions

- Event Definition and Identification (EDI) - This family identifies the PCS events to be defined and monitored, alarmed, and identified, and it identifies how they interact and how events are audited.

#### 3.6.2 Chemical Sector: CIDX Cyber-security Standard

##### 3.6.2.1 Event Definition and Identification ○

The CIDX cyber-security standard provides practices to detect, report, document, and investigate incidents, weaknesses, and unrecognized risks. It recommends establishing an incident reporting and investigation program that addresses recording incidents, remaining alert to incidents experienced by other organizations, and lessons learned for incidents.

This guiding element provides input to the elements of preventive and corrective actions in order to successfully manage recovery from incidents, but does not specify responses with enough detail to determine if it satisfies the Framework requirements. Within this class, the standard loosely satisfies the intent of the requirement. But in other cases, the attributes do not match exactly to the Framework cyber-security requirements, so these are highlighted as showing a gap in the standard. Therefore, the standard has a partial match with FEM class requirements.

#### 3.6.3 Energy - Natural Gas Sector: AGA Report Number 12

##### 3.6.3.1 Event Definition and Identification ○

AGA 12, Part 1, specifies that an IDS shall include an alarm output that may be used if a security event is detected. However, critical actions and events are not enumerated

or defined. Also AGA 12, Part 1, specifies that a system operator may be alerted in the event of a security alarm, but this does not appear to be mandatory. This class is largely unaddressed by the standard and, therefore, the standard does not meet the requirements.

### **3.6.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.6.4.1 Event Definition and Identification** ○

Many of the provisions of the Framework deal with the expected response to a security-related event. There are specific steps mandated when intrusions or other attacks occur. API 1164 requires event monitoring and logging. It does not specify actions to be taken when a security-relevant event failure occurs. Rather, it focuses on prevention of the event. Therefore, the standard only partially meets the requirements.

### **3.6.5 Transportation-Rail Sector**

#### **3.6.5.1 Event Definition and Identification** ○

None of the requirements listed under the Identification and Authentication class (FIA) in the Framework are addressed in the transportation standard. No reference to event definition or identification was found. This is probably due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.6.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.6.6.1 Event Definition and Identification** ○

None of the requirements listed under the Event Definition and Identification class (FIA) in the Framework are addressed in TR99-01. This is probably due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.6.7 Energy - Electric Power Sector: NERC CIP**

#### **3.6.7.1 Event Definition and Identification** ●

NERC CIP-005-1 specifies monitoring electronic access controls, detecting intrusions, and detecting attempted intrusions. The latter two can be considered events, as specified in FEM\_EDI.1.1. The incident response procedures outlined in CIP-008-1 address alarms, severity, how the alarm is made, etc. FEM\_EDI.1.2 specifies the ability to alarm on a parameter setting change (while this level of detail is not included in the CIP, it is implied).

### **3.6.8 Telecommunications Sector: ANSI T1.276**

#### **3.6.8.1 Event Definition and Identification** ○

T1.276 delineates two requirements (M-55 and M-56) that relate to automated event monitoring; however, these requirements differ significantly from those provided in the Framework. Requirement (M-55) requires the generation of an alert for accounts that have been dormant for a user-defined period of time. Requirement (M-56) requires disabling accounts, other than administrator accounts, that have been dormant for a user-defined period of time.

### **3.6.9 Water Sector: AWWA**

#### **3.6.9.1 Event Definition and Identification** ○

The AWWA standard requires that PLC be programmed with a set point of ranges to prevent potentially harmful out-of range adjustments from occurring. It also states that antivirus software should be installed and configured for daily virus pattern updates on all servers and workstations. The AWWA standard also recommends that the utility install an IDS at the internet gateway and regularly audit IDS logs for evidence of unauthorized entry. Although the AWWA standard documents the need to monitor events, it lacks any recommendations for alarms based on the monitoring activity.

### 3.7 Class: Identification and Authentication (FIA)

	Identification and Authentication				
	Authentication Failure Handling	User Attribute Definition	Verification of Passwords	Timing of Authentication	Timing of Identification
Chemical	●	○	○	●	●
Natural Gas	○	○	●	●	●
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	●	○	○
Cross-Sector ISA TR99-02	○	○	●	○	○
Electrical Power	●	○	●	●	○
Telecommunications	●	○	●	●	●
Water	○	○	○	○	○

○ = Gap                      ● = Partial Match                      ● = Match

#### 3.7.1 Family Definitions

- Authentication Failure Handling (AFL) - This family contains requirements for defining values for the number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures.
- User Attribute Definition (ATD) - This family defines the requirements for associating user security attributes with users, as needed to support the STOE security policy.
- Verification of Passwords (SOS) - This family defines requirements for mechanisms that enforce defined quality metrics for password verification.
- Timing of Authentication (UAU) - This family defines the types of user authentication mechanisms supported by the TSF and includes the required attributes on which the user authentication mechanisms must be based.
- Timing of Identification (UID) - This family defines the conditions under which users shall be required to identify themselves before performing any other actions mediated by the TSF.

#### 3.7.2 Chemical Sector: CIDX Cyber-security Standard

##### 3.7.2.1 Authentication Failure Handling ●

The CIDX cyber-security standard provides details and practices to handle authentication failure by prescribing guidelines that require the system to disable a user’s account after five failed login attempts. The user is instructed to authenticate after 15 minutes of inactivity. This fully meets the Framework requirements.

### **3.7.2.2 User Attribute Definition and Verification of Password** ○

The standard discusses use of physical token authentication that employs both a physical device that must be in the possession of the remote user and knowledge of a personal identification number (PIN). Examples are Smartcard authentication; Biometric authentication; and Location-based authentication. The standard stresses authentication rules in general to safeguard the control system from any security breach. However, the standard does not provide any specific details on setting up user attributes defined in the Framework requirements. In addition, there is no mention of rules for developing and verifying passwords. Based on the definition of the criteria, there is a gap in the standard in meeting the FIA\_ATD and FIA\_SOS family requirements.

### **3.7.2.3 Timing of Authentication and Timing of Identification** ○

The standard partially satisfies the requirements of the timing of authentication and timing of identification requirements, as identified by the Framework. For example, it recommends that a standard administrative process be followed for the creation of all user accounts. In addition, the accounts should be role-based and grant the user only those privileges and access to resources that are needed to perform the particular job function. The account administration process includes principles of separation of duties, with separate approvers and implementers of account configuration. The CIDX cyber-security standard requires that the management process include periodic reviews of user accounts to make sure the roles, access needs, or users are still correct, and to remove inactive and unneeded accounts.

The CIDX cyber-security standard does not provide any details or discussion on any non-forgable authentication mechanism. It does not require the control system to be able to detect and prevent the use of authentication data that has been forged or copied, as stated under the FAU\_UAU requirements. This is a gap in the standard because it does not satisfy the overall intent of the FIA timing of authentication in CS requirements.

Due to the general nature of the recommendation in the standard for authorization and identification procedures, there is not a clear match to the timing of identification FAU\_UID requirements. Therefore, this is a gap in satisfying the Framework requirements. In summary, this family is only a partial match to the overall Framework requirements.

## **3.7.3 Energy - Natural Gas Sector: AGA Report Number 12**

### **3.7.3.1 Authentication Failure Handling and User Attribute Definition** ○

The Framework anticipates proactive recognition of possible security failures by tracking (mapping) the attributes of previous security events. There is no mention of such activity in AGA 12, Part 1. AGA 12, Part 1, also provides no defensive actions to prevent such failures. In addition, the user attribute requirement is not very well defined



in the document. Use of identity-based and role-based access control were found to be unclear and many items, including individual user credential management, authentication failure thresholds, actions to be taken upon exceeding such thresholds, and individual user security attribute list maintenance, are not addressed. Therefore, the standard has a gap in fulfilling the family requirements.

### **3.7.3.2 *Timing of Authentication*** ○

AGA 12, Part 1, requires unique identification of operators performing configuration management (CM) or requesting services. However, actions allowed prior to authentication, such as forged authentication information and single-use authentication mechanisms, are not addressed. Therefore, the standard has a partial match with the requirements of this family.

### **3.7.3.3 *Timing of Identification and Verification of Passwords*** ○

AGA 12, Part 1, does specify that components shall uniquely identify operators performing CM or requesting services. Also, compliance with FIPS 140-2 requires that feedback of authentication data to an operator be obscured during authentication. The standard provides some information on the generation and verification of passwords. Thus, the standard partially matches the requirements of these families.

## **3.7.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

### **3.7.4.1 *Authentication Failure Handling and Timing of Authentication*** ○

API 1164 complies with most of the requirements for user attribute verification and password verification. It is extremely detailed in its requirements for passwords and the verification procedures. It does not require detection of fraudulent entry attempts, only prevention. It also does not require detection of forged authentications. Due to these limitations, the standard only partially meets these requirements.

### **3.7.4.2 *User Attribute Definition, Verification of Passwords, and Timing of Identification*** ●

API 1164 complies with the requirements for user attribute verification and password verification. It is extremely detailed in its requirements for passwords and the verification procedures. Thus, the standard fully meets the requirements.

## **3.7.5 Transportation-Rail Sector**

### **3.7.5.1 *Authentication Failure Handling, User Attribute Definition, Verification of Passwords, Timing of Authentication, and Timing of Identification*** ○

None of the requirements listed under the Identification and Authentication class (FIA) in the Framework are addressed in the transportation standard. No reference to authentication or identification was found. This is probably due to the differences in

emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.7.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.7.6.1 Verification of Passwords ●**

Verification of passwords (FIA-SOS) is discussed in Section 5.2 of TR99-01, which addresses passwords but uses a different approach than is used in the Framework. Section 5.2.6 indicates that passwords should have appropriate length and entropy. Section 5.2.2 addresses passwords and user authorization. In addition, Sections 5.23, 5.26, and 9.16 discuss password protection, use, care, and use with other forms of authentication. Sections 5.3, 5.4, and 5.6 discuss other forms of authentication, including physical token, smart card, and biometric. These areas are not covered in the Framework.

#### **3.7.6.2 Timing of Identification ○**

Although timing of authentication (FIA-UAU) is addressed in Section 5.2.3 of TR99-01, which covers weakness in third-party eavesdropping, it was not covered in sufficient detail to be considered as partial coverage. In addition, TR99-01 covers the enforcement of secure authentication in gaining access in Section 6.1.4.

#### **3.7.6.3 Authentication Failure Handling, User Attribute Definition, and Timing of Authentication ○**

None of the remaining families listed under the Identification and Authorization class (FIA) in the Framework are addressed in TR99-01. This is probably due to the differences in area of emphasis between the two documents.

### **3.7.7 Cross Sector - ISA-TR99.00.02-2004**

#### **3.7.7.1 Authentication Failure Handling ○**

Authentication failure handling (FIA-ALF) requirements found in the Framework are not addressed by TR99-02; however, it does state that a program must identify or develop policies on authentication (Section 6.6.6).

#### **3.7.7.2 Timing of Authentication ○**

Timing of authentication (FIA-UAU) requirements found in the Framework is not addressed by TR99-02; however, it does state that policies for user password management should be developed (Section 6.6.8.2.1) and that a program team must identify or develop policies on passwords and authentication (Section 6.6.6).

### **3.7.7.3 Timing of Identification** ○

Timing of identification (FIA-UID) is addressed in Section 6.7.4, although not in sufficient detail, which requires the identification, control, and limitation of access to sources of hardware, software, spare parts, patches, and service packs used for system development, testing, and installation.

### **3.7.7.4 User Attribute Definition and Verification of Passwords** ○

None of the remaining families listed under the Identification and Authorization class (FIA) in the Framework are addressed in TR99-02. This is probably due to the differences in area of emphasis between the two documents.

## **3.7.8 Energy - Electric Power Sector: NERC CIP**

### **3.7.8.1 Authentication Failure Handling and Verification of Passwords** ●

CIP-005-1 R5 is a good match for FIA\_AFL.1.1. The provisions in the CIP call for the ability to detect unauthorized access attempts for critical infrastructure assets. This provision, coupled with CIP-008-1, provides for the ability to monitor and alarm when failed authentication attempts occur.

CIP-005-1 R4 specifies that the responsible entity shall implement strong procedural or technical measures to ensure authenticity of the accessing party. In addition, CIP-007-1 R3 specifies a minimum password complexity and specifies that passwords be changed on a periodic basis. Together these satisfy FIA\_SOS.

### **3.7.8.2 Timing of Authentication** ○

CIP-005-1 presents the need to authenticate to critical assets. This matches the first part of the FIA\_UAU requirements. However, the CIP falls short of being a good match because timing requirements are not addressed. In addition, forged authentication data is not directly addressed. Either this is a gap in the standard, or a partial match.

### **3.7.8.3 User Attribute Definition and Timing of Identification** ○

FIA\_ATD.1.1 is not explicitly specified in the NERC CIP document. A method for distributing one-time passwords and the use of secure e-mail is not contained in any CIP provisions.

Timing of identification is a gap in the document; the NERC CIP document does not contain any of the CIP device identification provisions.

### **3.7.9 Telecommunications Sector: ANSI T1.276**

#### **3.7.9.1 Verification of Passwords and Timing of Identification ●**

T1.276 effectively covers all of the requirements delineated for these two families. In addition, the requirements delineated in T1.276 are more specific than those delineated in the Framework. T1.276, for example, delineates 22 requirements relating to password age limits, changing, complexity, reuse, transmission, and storage.

#### **3.7.9.2 Authentication Failure Handling and Timing of Authentication ○**

A number of requirements are delineated in T1.276 that match these two Framework families. T1.276 delineates specific requirements regarding system response to login failures (M-50, M-34). Mechanisms for bypassing the login process are explicitly forbidden (M-51).

#### **3.7.9.3 User Attribute Definition ○**

There are no T1.276 requirements that directly relate to or match requirements within this Framework family.

### **3.7.10 Water Sector: AWWA**

#### **3.7.10.1 Authentication Failure Handling, User Attribute Definition, Timing of Authentication, and Timing of Identification ○**

The AWWA document does not address these families.

#### **3.7.10.2 Verification of Passwords ●**

The AWWA document only partially addresses the need for strong authentication in process control systems. It does have requirements for appropriate password strength rules for user access (i.e., more complex passwords for those with higher access privileges, such as administrators). However, these rules fall short of the FIA\_SOS family requirement for generated passwords. The AWWA standard also addresses the need to change default passwords. One requirement is to confirm that every administrator password for the operating system and HMI have been changed from the default password. Another similar requirement states to reset all operating systems and HMI passwords away from default settings. Both of these requirements seem to fit into the FIA\_SOS family as well.

### 3.8 Class: Security Management (FMT)

	Security Management				
	Management of Security Functions Behavior	Management of Security Attributes	Management of Security Function Data	Access Revocation	Time-limited Authorization
Chemical	○	●	○	●	○
Natural Gas	○	○	●	○	○
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	●	○	○	○
Cross-Sector ISA TR99-01	○	●	○	○	○
Cross-Sector ISA TR99-02	○	●	○	○	○
Electrical Power	●	●	●	○	○
Telecommunications	●	●	○	○	○
Water	○	○	○	○	○

	Specification of Management Functions	Security Roles
Chemical	●	○
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	●	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	●	○
Telecommunications	○	○
Water	○	○

○ = Gap                      ● = Partial Match                      ● = Match

#### 3.8.1 Family Definitions

- Management of Security Functions Behavior (MOF) - This family allows authorized users control over the management of security functions and policies in the TSF.
- Management of Security Attributes (MSA) - This family defines authorized users' control over the management of security attributes.
- Management of Trusted Security Function (TSF) Data (MTD) - This family allows authorized users control over the management of TSF data and policies mapped to data.
- Access Revocation (REV) - This family addresses revocation of security attributes for a variety of entities within a STOE.
- Time-limited Authorization (SAE) - This family addresses the capability to enforce time limits for the validity of security attributes.

- Specification of Management Functions (SMF) – This family specifies the types of security management functions provided by the TSF.
- Security Roles (SMR) - This family addresses the assignment of different security roles to users, including restrictions and policy mapping of security roles.

### **3.8.2 Chemical Sector: CIDX Cyber-security Standard**

#### **3.8.2.1 Management of Security Functions, Management of Security Attributes, Time-limited Authorization, and Security Roles ●**

The CIDX cyber-security standard provides guidance for identification and classification of assets to help in the definition of the companies' risk. It recommends the creation of a checklist to group the assets into categories. It also outlines methods: use of a diagram of an application portfolio, a computer system, or a network to guide asset management for manufacturing and process control. The standard also recommends use of automated tools (e.g., provisioning and identity management) to manage the process of access approval, account creation, suspension, and deletion. The steps recommended by the CIDX cyber-security standard loosely satisfy the intent of the security attributes, limited authorization, and roles, per the Framework requirement. Therefore, they are designated as a partial match to the requirements.

#### **3.8.2.2 Management of TSF Data ○**

The CIDX cyber-security standard recommends that on highly critical systems, it is a good practice to perform all system management or configuration functions at the device (locally), to reduce the potential for a network interruption to cause a problem with the control of the process. The system manager coordinates all changes with the operator for the area so that production is not impacted during a configuration change.

According to the Framework requirement, authentication from the origin command should be verified before any configuration change can be accepted. The CIDX cyber-security standard does not describe details for authenticating configuration change and, therefore, this is a gap in the standard, based on these requirements.

#### **3.8.2.3 Access Revocation and Specification of Management Functions ●**

The standard strongly recommends that access accounts be suspended or removed and access permissions be revoked as soon as they are no longer needed (e.g., job change). The need for access to critical systems is explicitly reconfirmed on a regular basis. All established accounts are reviewed regularly to ensure they are authorized and still in use. If an access account remains unused for an extended period, the need for it is explicitly reconfirmed. In addition, the CIDX cyber-security standard recommends that, based on its risk assessment, the organization develop a disaster recovery plan that addresses hardware and software redundancy, etc., which meets the Framework requirements for fault tolerance and redundant system installation.

Overall, the CIDX cyber-security standard partially meets the requirements for security management functions within this class.

### **3.8.3 Energy - Natural Gas Sector: AGA Report Number 12**

#### **3.8.3.1 Management of Security Functions Behavior, Management of TSF Data, and Security Roles** ○

AGA 12, Part 1, requires significant FIPS 140-2 compliance and, therefore, several areas of concern related to this family are addressed. These include cryptographic officer role support, cryptographic module security policy requirements, role-based access control, authentication initialization mechanisms, discretionary access control mechanisms, and association of users with roles. AGA 12, Part 1, also references ANSI Standards X9.69 and X9.73 regarding role-based access control, but neither document was available for review in this analysis.

#### **3.8.3.2 Management of Security Attributes, Access Revocation, Time-limited Authorization, and Specification of Management Functions** ○

Due in large part to the overview nature of AGA 12, Part 1, security management is not addressed in the degree of detail set forth in this family. For example, not all FMT\_MOF administrative functions are addressed, a comprehensive list of security management functions is not provided, roles allowed to modify security attribute values are not specified, and dynamic policy mapping is not addressed. It is anticipated that forthcoming parts of the AGA 12 document, implementation of the standard and recommendations, will address many of these deficiencies and gaps.

### **3.8.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.8.4.1 Management of Security Functions Behavior, Access Revocation, Time-limited Authorization, Specification of Management Functions, and Security Roles**



API 1164 has very detailed requirements for granting or revoking access. These include considering inactive time, user attributes, authorization level, etc. The standard provisions comply with each of these five families listed, and therefore match very well with the Framework requirements.

#### **3.8.4.2 Management of Security Attributes and Management of TSF Data** ○

These two families deal with the protection of data during configuration change or loss of system integrity. API 1164 meets all the requirements except one. Specifically, it does not address the procedures for mapping security attributes to the associated security policies. Thus, the standard partially meets the requirements.

### **3.8.5 Transportation-Rail Sector**

#### **3.8.5.1 Management of Security Functions Behavior** ○

Management of security functions behavior (FMT-MOF) is discussed in Section 236.907(a)(15), which addresses unauthorized access.

#### **3.8.5.2 Management of Security Attributes** ○

Management of security attributes (FMT-MSA) is addressed in Section 236.907(a)(15), which addresses the enforcement of access.

#### **3.8.5.3 Specification of Management Functions** ○

Specification of management functions (FMT-SMF) is discussed in Sections 236.907(a)(6) and 236.907(a)(8), which covers hazards assessment and mitigation.

#### **3.8.5.4 Management of TSF Data, Access Revocation, and Time-limited Authorization, Security Roles** ○

None of the remaining families listed under the Security Management class (FMT) in the Framework are addressed in the transportation standard. This is probably due to the differences in area of emphasis between the two documents.

### **3.8.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.8.6.1 Management of Security Functions Behavior** ○

Management of security functions behavior (FMT-MOF) is discussed in Sections 5 and 6.1 of TR99-01 which address authentication and authorization technologies and dedicated firewalls.

#### **3.8.6.2 Management of Security Attributes** ○

Management of security attributes (FMT-MSA) is addressed in Sections 5 and 6.1 of TR99-01, which address authentication and authorization technologies and dedicated firewalls.

#### **3.8.6.3 Management of TSF Data, Access Revocation, Time-limited Authorization, and Specification of Management Functions, Security Roles** ○

None of the remaining families listed under the Security Management class (FMT) in the Framework are addressed in the TR99-01. This is probably due to the differences in area of emphasis between the two documents.



### **3.8.7 Cross Sector - ISA-TR99.00.02-2004**

#### **3.8.7.1 Management of Security Attributes ○**

Management of security attributes (FMT-MSA) is addressed in Section 6.7.4, which requires the identification, control, and limitation of access to sources of hardware, software, spare parts, patches, and service packs used for system development, testing, and installation.

#### **3.8.7.2 Security Roles ○**

Security roles (FMT-SMR) are addressed in Section 6.6.6, which states that the program team must identify or develop policies for accounts.

#### **3.8.7.3 Management of Security Functions Behavior, Management of TSF Data, Access Revocation, Time-limited Authorization, and Specification of Management Functions ○**

None of the remaining families listed under the Security Management class (FMT) in the Framework are addressed in the TR99-02. This is probably due to the differences in area of emphasis between the two documents.

### **3.8.8 Energy - Electric Power Sector: NERC CIP**

#### **3.8.8.1 Management of Security Functions Behavior and Management of Security Attributes ●**

The FMT\_MOF requirements are primarily addressed by CIP-003-1, CIP-005-1, and CIP-007-1. For example, CIP-003-1 R3 defines the roles and responsibilities of critical asset owners, custodians, and users. This addresses the requirement of FMT\_MOF.1.1 to restrict the ability of authorized personnel to disable/enable. CIP-003-1 R2 addresses the need to categorize and protect information. CIP-005-1 satisfies the requirement to authenticate users for control system resources.

FMT\_MSA requirements are also a good match with the NERC CIP standard. CIP-003-1 satisfies FMT\_MSA.1.1 by requiring authentication and the use of role-based access. The role-based access method also addresses FMT\_MSA.3.1 by providing the user role with the most limited level of access. While user access being the default access level is not specifically mentioned, it is implied.

#### **3.8.8.2 Management of Trusted Security Function Data, Access Revocation, Specification of Management Functions, and Security Roles ○**

Of the three requirements in the FMT\_MTD family, the CIP series only addresses one. CIP-003-1 R3 outlines the use of user roles to restrict the ability to modify critical assets. Device to device authorized communication, domains, and data within the domain are not addressed.

Regarding access revocation, the CIP addresses revoking electronic access (user accounts), but does not include revocation for physical access. CIP-003-1 R5 addresses account suspension, but is less stringent regarding timeframe.

Specification of management functions, FMT\_SMF, is also a partial match. CIP-009-1 R1 addresses the creation of recovery plans and the exercise thereof. The requirement to protect the confidentiality of sensitive assets is not addressed by the CIP.

Security roles requirements are partially satisfied by the provisions in CIP-007-1. The CIP meets this requirement by associating users with roles to ensure operational security. However, the roles defined in the CIP are user, custodian, and owner; the Framework is more granular, identifying roles such as process control engineer and security engineer. The CIP does define a process for approving changes to the functionality of critical assets. Instead of a security engineer, management is acceptable for approving changes.

### **3.8.8.3 Time-limited Authorization** ○

The requirements in FMT\_SAE for restricting the capability to specify an expiration date for any security feature and authorizing security functions after an expiration time are not directly addressed in the CIP.

## **3.8.9 Telecommunications Sector: ANSI T1.276**

### **3.8.9.1 Management of Security Functions Behavior** ●

T1.276 provides excellent coverage of this FMT family. In addition, some of the T1.276 requirements could reasonably be assigned to more than one Family in this Class because of wording differences between the Framework and T1.276 requirements.

As with other Classes and Families in the Framework, T1.276 requirements related to this family are more specific than the requirements delineated in the Framework. M-42 requires the use of access controls and partitions to appropriately restrict user actions and access. Requirements M-57 through M-58 specify who has the authority to re-enable a login and remove a lockout. M-59 and M-60 delineate requirements relating to configuring systems to automatically log-out after a period of inactivity. M-62 requires strong authentication and cryptographic protection for any physical or logical interface that carries management traffic. M-18 and M-43 require, respectively, that each user ID have a unique settable password and that each user have a unique user ID. M-47 requires the display to the user of the time and date of the last successful authentication. M-61 specifies that the user role shall remain unchanged during the execution and exit from any NE/MS application.

### **3.8.9.2 Management of Security Attributes and Security Roles** ●

T1.276 delineates a number of requirements that relate to the management of security attributes and security roles; however, T1.276 provides greater detail than delineated in the Framework. T1.276 details Critical Administrator Actions (M-26) and the System

Security Administrator role (M-27 through M-30). Requirements M-61, M-24, M-25, and M-46 delineate a number of requirements relating to user roles. M-39 and M-40 are a close match to FPT\_SMR.4.1, requiring that security management actions be properly authenticated and executed via trusted channels.

### **3.8.9.3 Management of TSF Data, Access Revocation, Time-limited Authorization, and Specification of Management Functions** ○

T1.276 does not cover the remaining families within this class.

## **3.8.10 Water Sector: AWWA**

### **3.8.10.1 Management of Security Functions Behavior, Management of Security Attributes, Management of TSF Data, Time-limited Authorization, Specification of Management Functions, and Security Roles** ○

The AWWA standard does not address these families.

### **3.8.10.2 Access Revocation** ○

The AWWA standard makes little mention of security management-related requirements. One requirement requests the immediate removal of a user account from the HMI if the account becomes inactive due to voluntary and, especially, involuntary termination. This statement corresponds to family FMT\_REV.

### 3.9 Class: Trusted Security Functions (FPT)

Protection of Trusted Security Functions

	Failure with Preservation of Secure State	Availability with a Defined Availability Metric	Confidentiality during Transmission	Detection of Modification	Passive Detection of Physical Attack
Chemical	○	○	○	○	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	○	○	○	○	●
Telecommunications	○	○	○	○	○
Water	○	○	○	○	○

	Automated Recovery	Replay Detection	Domain Separation	Strength of Boundary Access Control	Simple Trusted Acknowledgement
Chemical	○	○	○	○	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	○	●	○	●	○
Telecommunications	○	○	○	○	○
Water	○	○	○	○	○

	Reliable Time Stamps	Data Consistency	Internal Consistence
Chemical	○	○	○
Natural Gas	○	○	○
Petroleum & Oil	●	●	●
Transportation – Rail	○	○	○
Cross-Sector ISA TR99-01	○	○	○
Cross-Sector ISA TR99-02	○	○	○
Electrical Power	○	○	○
Telecommunications	●	○	○
Water	○	○	○

○ = Gap                      ○ = Partial Match                      ● = Match

### 3.9.1 Family Definitions

- Failure with Preservation of Secure State (FLS) - The requirements of this family ensure that the STOE will not violate its STOE security policy in the event of identified categories of failures in the TSF.
- Availability within a Defined Availability Metric (ITA) - This family defines the rules for the prevention of loss of availability of TSF data moving between the TSF and a remote, trusted IT source/destination.
- Confidentiality during Transmission (ITC) - This family defines the rules for the protection from unauthorized disclosure of TSF data during transmission between the TSF and a remote, trusted IT source/destination.
- Detection of Modification (ITI) - This family defines the rules for the protection from unauthorized modification of TSF data during transmission between the TSF and a remote, trusted IT source/destination.
- Passive Detection of Physical Attack (PHP) – This family defines the requirements for automated detection of unauthorized physical access to the TSF, including the notification of, resistance to, definition of, and alarm response for unauthorized physical access to the TSF.
- Automated Recovery (RCV) - The requirements of this family ensure that the TSF can determine that the STOE is started up without protection compromise and can recover without protection compromise after discontinuity of operations.
- Replay Detection (RPL) - This family addresses detection of replay for various types of entities and subsequent actions to correct and prevent replay attacks.
- Domain Separation (SEP) - This family ensures that at least one security domain is available for the TSFs own execution and that the TSF is protected from external interference and tampering by untrusted entities.
- Strength of Boundary Access Control (SOB) – This family defines physical access control to critical locations and equipment within the STOE.
- Simple Trusted Acknowledgement (SSP) – This family defines the requirements for acknowledgment of data transmissions, including verification of status of transmitted data and receipts for both internal and external TSF data transfers.
- Reliable Time Stamps (STM) - This family addresses requirements for a reliable time stamp function within a STOE.
- Basic Data Consistency (TDC) - This family defines the requirements for an STOE to exchange TSF data with another trusted IT source/destination.
- Internal Consistency (TRC) - The requirements of this family address the need to ensure the consistency of TSF data when such data is replicated internal to the STOE.

## 3.9.2 Chemical Sector: CIDX Cyber-security Standard

### 3.9.2.1 *Failure with Preservation of Secure State, Availability within a Defined Availability Metric, Confidentiality during Transmission, Detection of Modification, Passive Detection of Physical Attack, Automated Recovery, Strength of Boundary Access Control, Simple Trusted Acknowledgement, and Reliable Time Stamps* ○

The CIDX cyber-security standard prescribes practices to establish a disaster recovery site somewhere outside normal business facilities that is not impacted by natural disasters (e.g., fire, flood, tornado, terrorism). The standard recommends that business owners identify the maximum time their systems may be unavailable before the application is transferred by computer operations to the disaster recovery site. In addition, the standard provides recommendations for controls over information transmitted and stored to ensure confidentiality, authenticity, integrity, and non-repudiation. Under the communications, the standard recommends interface methods to verify that the requesting device is the correct device to perform the task. Critical interfaces check the Internet protocol (IP) address, multi-port adaptor card (MAC) address, and use a secret code or an encryption key to verify that the request is coming from the expected device. The standard does not describe time stamp of record requirements, but it is assumed that the log maintains both time and date for all access.

Access to control rooms is managed by appropriate combinations of entrance control technologies and administrative authentication practices. Therefore, it is concluded that the CIDX cyber-security standard has a partial match with the Framework requirements for this family.

Based on analysis of all the sub-classes, it was found that the standard discusses all the protection steps at a very high level, but does not provide specifics steps at the component/system level to fully satisfy the Framework requirements under this class. Therefore, the CIDX cyber-security standard only partially satisfies the specifics of these requirement families.

### 3.9.2.2 *Replay Detection, Domain Separation, Basic Data Consistency, and Internal Consistency* ○

The CIDX cyber-security standard does not discuss replay detection, domain separation, and basic data consistency. However, the standard does reference ISO and ISA standards. The standard refers to secure communication practices (encryption recommended in the standard), which could be interpreted to mean that consideration for domain separation may be included.

The standard does not provide details or procedures for data consistency and event traces. Under the incident and response section, the standard discusses documenting the details of the incident, the lessons learned, and the course of action to prevent incident reoccurrence. Restoration of the system is discussed in the Contingency planning section of the standard. However, due to several areas not being addressed,

the CIDX cyber-security standard has a gap in satisfying the core requirements of the Framework.

### **3.9.3 Energy - Natural Gas Sector: AGA Report Number 12**

#### **3.9.3.1 *Failure with Preservation of Secure State, Availability within a Defined Availability Metric, Passive Detection of Physical Attack, Automated Recovery, and Replay Detection* ●**

This Family relates to the physical security required to maintain operational integrity for the machines and equipment that make the process control (PC) system viable. The provisions of AGA 12, Part 1, address some of the 13 sub-topics within this Family. For example, tamper-evident packaging is required and strong enclosures may be required with tamper detection and response mechanisms for removable covers and doors. However, detection by IT means is not required. Thus, the standard only partially meets the family sub-class requirements.

#### **3.9.3.2 *Confidentiality during Transmission, Detection of Modification, Domain Separation, Strength of Boundary Access Control, Simple Trusted Acknowledgement, Reliable Time Stamps, Inter- Basic Data Consistency, and Internal Consistency* ○**

AGA 12, Part 1, addresses failure modes, particularly environmentally induced. Specifics such as back-up mechanisms are not addressed. AGA 12, Part 1, requires automatic reestablishment of normal cryptographic system operation after non-fatal faults. However, physical attacks on SCADA communications, fail-safe mode details, reliable time stamps, and data consistency mechanisms are not addressed. Replay attack mitigation is to be addressed in forthcoming documents. Thus, the standard has a gap in meeting these sub-class requirements.

### **3.9.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.9.4.1 *Failure with Preservation of Secure State, Availability within a Defined Availability Metric, Confidentiality during Transmission, Detection of Modification, Passive Detection of Physical Attack, Automated Recovery, Replay Detection, Domain Separation, , Strength of Boundary Access Control, Simple Trusted Acknowledgement, Reliable Time Stamps; Basic Data Consistency, and Internal Consistency* ●**

This Class relates to the physical security required to maintain operational integrity for the machines and equipment that make the PC system viable. The provisions of API 1164 address each of the 13 sub-topics within this Family, and meet the requirements for nearly all of them. Only in the category of *Passive Detection of Physical Attack* is there a gap. API 1164, consistent with its provisions in most other areas, does not provide for automatic resistance to physical tampering, and therefore does not meet the requirements of FPT\_PHP.3.1. However, overall, the standard closely matches these family requirements.

### 3.9.5 Transportation-Rail Sector

#### 3.9.5.1 Automated Recovery ●

Automated recovery (FPT-RCV) is addressed in Section 236.907 (a)(19), which includes a description of backup methods of operation in the Product Safety Plan.

#### 3.9.5.2 *Failure with Preservation of Secure State, Availability within a Defined Availability Metric, Confidentiality during Transmission, Detection of Modification, Passive Detection of Physical Attack, Replay Detection, TSF Domain Separation, Strength of Boundary Access Control, Simple Trusted Acknowledgement, Reliable Time Stamps, Basic Data Consistency, and Internal Consistency* ○

None of the remaining families listed under the Trusted Security Functions class (FPT) in the Framework are addressed in the transportation standard. This may be due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### 3.9.6 Cross Sector - ISA-TR99.00.01-2004

#### 3.9.6.1 Passive Detection of Physical Attack ●

Passive detection of physical attack (FPT-PHP) is discussed in some detail in Section 10.1.3 of TR99-01, which addresses daily inspections and audits of highly sensitive equipment to ensure adequacy of physical security controls. In addition, TR99-01 covers the protection of personnel (Section 10.1.2), vulnerability assessment (10.1.3), physical security plan, hardening of communication lines, physical security controls (Section 10.1.4), definition of security perimeters, manned reception areas, monitoring of physical access, periodic investigations, location of sensitive equipment, isolation of delivery and loading areas from critical areas, inventory of critical assets, and implementation of clear-desk policy (Section 10.1.6).

#### 3.9.6.2 Strength of Boundary Access Control ○

Physical security (FPT-SOB) is addressed, although not in sufficient detail, in Sections 10.1.2, 10.1.4, and 10.16.6 of TR99-01, which cover prevention of unauthorized introduction or removal of materials, physical security perimeters, and physical barriers.

#### 3.9.6.3 *Failure with Preservation of Secure State, Availability within a Defined Availability Metric, Confidentiality during Transmission, Detection of Modification, Automated Recovery, Replay Detection, Domain Separation, Simple Trusted Acknowledgement; Reliable Time Stamps; Basic Data Consistency, and Internal Consistency* ○

None of the remaining families listed under the Trusted Security Functions class (FPT) in the Framework are addressed in the TR99-01. This is probably due to the differences in area of emphasis between the two documents.



### **3.9.7 Cross Sector - ISA-TR99.00.02-2004**

#### **3.9.7.1 Failure with Preservation of Secure State** ○

Failure with preservation of secure state (FPT-FLS) requirements found in the Framework are not addressed by TR99-02; however, it does address identifying countermeasures for those vulnerabilities that are most immediate (Section 10), separating the business LAN from the Manufacturing and Control Network (Section 10.1.1), establishing a secure default state instead of an “open” default state, and establishing connections only when needed (Section 10.2.3). It also states that contingency plans should include procedures for restoring the system from known good backups (Section 18.13), establishing corrective action procedures (Section 18.8), and maintaining system recovery sources for rebuilding the existing system and previous versions (Section 6.7.4).

#### **3.9.7.2 Confidentiality during Transmission** ○

Inter-TSF confidentiality during transition (FPT-ITC) requirements found in the Framework are not addressed by TR99-02. However, it does address the development of policies for communications and operations management (Section 6.6.8.4).

#### **3.9.7.3 Automated Recovery** ○

Automated recovery (FPT-RCV) is addressed, although not in sufficient detail, in Sections 6.7.4 and 18.9, which discuss backing up vital data and operating parameters, and they specify addressing the detailed recovery process to restore both the operational and security aspects of the system in the disaster recovery plan. In addition, TR99-02 discusses that written records should be kept of all policies and procedures, as well as the results of their application, and that backups or archives should be maintained so that system failures or compromise will not destroy records (Section 6.6).

#### **3.9.7.4 Strength of Boundary Access Control** ○

Physical security (FPT-SOB) is addressed, although not in sufficient detail, in Section 6.6.8.3, which states that the control and field network segments should be strictly physically secured and that the security perimeter for the Manufacturing and Control System should be defined, specifying the components that make up the security boundary for the system. In addition, TR99-02 addresses the development of policies for security areas, equipment security, and general controls (Section 6.6.8.3).

### **3.9.7.5 Availability within a Defined Availability Metric, Detection of Modification, Passive Detection of Physical Attack, Replay Detection, Domain Separation, Simple Trusted Acknowledgement, Reliable Time Stamps, Basic Data Consistency, and Internal Consistency ○**

None of the remaining families listed under the Trusted Security Functions class (FPT) in the Framework are addressed in the TR99-02. This is probably due to the differences in area of emphasis between the two documents.

## **3.9.8 Energy - Electric Power Sector: NERC CIP**

### **3.9.8.1 Passive Detection of Physical Attack, Replay Detection, and Strength of Boundary Access Control ●**

Passive detection of physical attack and strength of boundary access control are addressed by the provisions in CIP-006-1. This section details physical security requirements, including monitoring physical security (R4) and the strength/depth of physical protection (R1). The provisions in CIP-006-1 exceed those in the Framework. The requirement to detect communication replay is addressed in CIP-007-1 R7, which identifies the need to monitor system events that are related to cyber security (i.e., message replay).

### **3.9.8.2 Failure with Preservation of Secure State ○**

CIP-008-1 covers incident response and recovery requirements. The wording from R1 is: “*The Responsible Entity shall develop and maintain an accurate and adequate Cyber Security Incident response plan.*” There is room to enforce preservation of secure state within this statement, but the CIP still falls short of requiring state preservation.

### **3.9.8.3 Availability within a Defined Availability Metric, Confidentiality during Transmission, Detection of Modification, Automated Recovery, Domain Separation, Simple Trusted Acknowledgement, Reliable Time Stamp, Basic Data Consistency, and Internal Consistency ○**

The provisions in the CIP do not address FPT\_ITA.1.1, which calls for an alternate communication path to a remote, trusted device. In the electric sector, a redundant communication link may be in place to address the need for continuous availability. However, this is not a requirement in the CIP.

Confidentiality during transmission is not contained in the CIP. The protocols used by industry are typically clear text. The industry focus is availability, not confidentiality, leading to the gap in the standard.

Detecting modification of data to remote, trusted devices with clear-text, unauthenticated protocols is a hurdle the electric industry must overcome. The understanding is present in industry that integrity of communication is critical, and this

supports the focus on availability. The CIP does not contain provisions to address FPT\_ITI.

CIP-009-1 provides the requirements for recovery from critical infrastructure failure. The provisions in the CIP fail to meet FPT\_RCV.3, FPT\_RCV.4, and FPT\_RCV.5.

The requirements specified in Domain Separation, Simple Trusted Acknowledgement, Reliable Time Stamps, Basic Data Consistency, and Internal Consistency are not addressed by any of the requirements or measurements specified in the CIP.

### **3.9.9 Telecommunications Sector: ANSI T1.276**

#### **3.9.9.1 *Failure with Preservation of Secure State, Availability within a Defined Availability Metric, Confidentiality during Transmission, Detection of Modification, Passive Detection of Physical Attack, Automated Recovery, Replay Detection, Domain Separation, Strength of Boundary Access Control, Simple Trusted Acknowledgement, Basic Data Consistency, and Internal Consistency*** ○

The Framework delineates an extensive set of requirements relating to these families. In contrast, T1.276 does not cover this set of Framework requirement families. T1.276 is intended to provide a set of management network security requirements for a wide variety of communication technologies. As such, the detailed requirements specified in this class may be outside of the scope intended for T1.276.

#### **3.9.9.2 *Reliable Time Stamps*** ●

The only requirement delineated in T1.276 that relates to this class is M-38, which requires reliable time stamps.

### **3.9.10 Water Sector: AWWA**

#### **3.9.10.1 *Failure with Preservation of Secure State, Availability within a Defined Availability Metric, Automated Recovery, Domain Separation, and Strength of Boundary Access Control*** ●

Only a subset of the requirements in the Trusted Security Functions class is emphasized in this standard. The AWWA standard requires that the SCADA systems should have “fail-over” redundancy, which implies there is always a secure state that corresponds to family FPT\_FLS.

The standard also requires that the utility should provide a backup method from the remote systems similar to family FPT\_ITAs requirements in case of a communications failure. Another requirement is to backup SCADA servers and programming workstations to tape every night, with the appropriate tapes being stored offsite. However, nightly backups are not as stringent as the 1% maximum loss acceptable by the FPT\_RCV family. This family also requires backups for system configurations. The AWWA standard requires routine backup of all SCADA programs for PLC, distributed

control units, remote terminal units (RTUs), SCADA servers, and similar programmable devices.

Family FPT\_SOB is primarily focused on the physical security of the PCS. The AWWA contains a number of requirements addressing this area as listed below.

- Install and use a lock with an intruder switch on control panels.
- Implement restricted access (and policies) to the SCADA control room. Consider biometric devices for areas requiring the highest levels of security.
- Provide a climate-controlled, locked enclosure for SCADA servers and networking components.
- Install safeguards against theft or unauthorized use for laptops used for onsite programming of remote PLCs or RTUs.
- Restrict access to the control room (and network/server room) with an entry system that stores information about who has entered and departed.
- Use protective, lockable casing for exposed outdoor RTUs.
- Use lockable PLC cabinets.
- Secure SCADA servers in locked, climate-controlled areas.
- Provide “hardened,” lockable enclosures for all remote control system units.

***3.9.10.2 Confidentiality during Transmission, Detection of Modification, Passive Detection of Physical Attack, Replay Detection, Simple Trusted Acknowledgement, Reliable Time Stamps, Basic Data Consistency, and Internal Consistency*** ○

The AWWA requirements do not address these families.

### 3.10 Class: Resource Utilization (FRU)

	Resource Utilization	
	Degraded Fault Tolerance	Limited Priority of Service
Chemical	○	○
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	●	○
Telecommunications	○	○
Water	●	○

○ = Gap                      ○ = Partial Match                      ● = Match

#### 3.10.1 Family Definitions

- Degraded Fault Tolerance (FLT) - The requirements of this family ensure that the STOE will operate correctly even in the event of failures.
- Limited Priority of Service (PRS) - The requirements of this family allow the TSF to control the use of resources within the TSF scope of control by users and subjects such that high priority activities within the TSF scope of control will always be accomplished without undue interference or delay caused by low priority activities.

#### 3.10.2 Chemical Sector: CIDX Cyber-security Standard

##### 3.10.2.1 Degraded Fault Tolerance and Limited Priority of Service ○

The CIDX cyber-security standard partially meets the Framework requirement under this class. For example, the standard recommends that the cyber-security team determine the amount of time/resources required for system restoration, location of back up files, hardware, frequency of backup, and need for hot spares, etc., to ensure critical systems can be restored in the event of a disaster situation. The conclusion based on the language and terminology under this class is that the standard partially meets the intent of the fault-tolerance backup system provisions of the FRU\_PRS that require the companies to ensure that the STOE will maintain correct operation even in the event of failures.

#### 3.10.3 Energy - Natural Gas Sector: AGA Report Number 12

##### 3.10.3.1 Degraded Fault Tolerance and Limited Priority of Service ○

This class deals with the challenge of maintaining operations when confronted with degraded service levels or partial failures. AGA 12, Part 1, does not deal with these

contingencies. This is probably due to the fact that transmission and distribution systems and the SCADA systems that monitor and control them are designed to be fault tolerant and already include priority-of-service mechanisms. AGA 12, Part 1, is primarily concerned with securing ongoing data communications on SCADA channels. Good SCADA design involves eliminating single points of failure. Therefore, in many cases when a primary communication channel fails, a separate alternate channel independently secured by AGA 12 mechanisms will automatically provide operations continuity. For failed channels, AGA 12 is irrelevant.

However, it should be noted that AGA 12 mechanisms must be designed to deal with common causes of channel failures and must not impede restoration efforts and reestablishing communication. For example, cryptographic mechanisms must deal efficiently with communication noise issues that frequently degrade channel performance. If they do not, the mechanisms themselves can easily become the cause of channel failure. Such fundamental design flaws should quickly be identified in field tests and would be corrected long before being deployed in a production environment.

### **3.10.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.10.4.1 *Degraded Fault Tolerance and Limited Priority of Service* ●**

This class deals with the challenge of maintaining operations when confronted with degraded service levels or partial failures. API 1164 deals with these contingencies by establishing backup requirements that are commensurate with the criticality of the operation. It also establishes priorities for the various operations, in accordance with their criticality, and for the subjects that will have access to the system in order to perform these operations. These procedures are mandated to be part of the system, but may not be automated. The standard fully meets the Framework requirements.

### **3.10.5 Transportation-Rail Sector**

#### **3.10.5.1 *Degraded Fault Tolerance and Limited Priority of Service* ○**

None of the requirements listed under the Resource Utilization class (FRU) in the Framework are addressed in the transportation standard. No reference was found to either fault tolerance or priority of service. This is probably due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.10.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.10.6.1 *Degraded Fault Tolerance and Limited Priority of Service* ○**

None of the families listed under the Resource Utilization class (FRU) in the Framework are addressed in the TR99-01. This is probably due to the differences in area of emphasis between the two documents.

### **3.10.6.2 Cross Sector - ISA-TR99.00.02-2004**

### **3.10.6.3 Degraded Fault Tolerance and Limited Priority of Service ○**

None of the families listed under the Resource Utilization class (FRU) in the Framework are addressed in the TR99-02. This is probably due to the differences in area of emphasis between the two documents.

### **3.10.7 Energy - Electric Power Sector: NERC CIP**

#### **3.10.7.1 Degraded Fault Tolerance ●**

The provisions in CIP-009-1 address the requirements for recovery from events or conditions that would necessitate the activation of the recovery plan. The term “event” can be interpreted to be a power outage - making this a good match to the Framework requirement.

#### **3.10.7.2 Limited Priority of Service ○**

Besides identifying when the recovery plan needs to be activated, CIP-009-1 addresses who must be involved. However, it does not contain a requirement for restoring devices in a pre-determined, priority order.

### **3.10.8 Telecommunications Sector: ANSI T1.276**

#### **3.10.8.1 Degraded Fault Tolerance and Limited Priority of Service ○**

No requirements are delineated in T1.276 that are a close or partial match to the Framework requirements delineated in the Resource Utilization (FRU) class. FRU is concerned with ensuring the availability of resources. M-48 is the only resource utilization requirement specified in T1.276. However, this relates to the improper use of resources by system users, not ensuring the availability of resources. M-48 specifies that systems display an improper usage warning banner before any logical access is allowed. The Framework does not delineate a similar requirement, so this is a possible gap in the Framework, itself.

### **3.10.9 Water Sector: AWWA**

#### **3.10.9.1 Degraded Fault Tolerance ●**

The AWWA standard recognizes the need to avoid power failures, so it states that a UPS be provided for critical SCADA devices, servers, networking components, and vital workstations. It also states to consider whether or not to use diesel powered generators for critical components. This partially fulfills the FRU\_FLT family.

### **3.10.9.2 Limited Priority of Service** ○

Unfortunately, the standard does not require a methodology to assign priorities to the devices in order to determine which are the most critical, which is required to meet the FTU\_PRS family.



### 3.11 Class: Target [STOE] Access (FTA)

	Target Access	
	Session Locking	Session Establishment
Chemical	●	●
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	○	○
Telecommunications	●	●
Water	○	○

○ = Gap                      ● = Partial Match                      ● = Match

#### 3.11.1 Family Definitions

- Session Locking (SSL) - This family defines requirements for the TSF to provide the capability for locking and unlocking of interactive sessions (e.g., keyboard locking).
- Session Establishment (TSE) - This family defines requirements to deny a user permission to establish a session with the STOE based on the attributes of the user.

#### 3.11.2 Chemical Sector: CIDX Cyber-security Standard

##### 3.11.2.1 Session Locking and Session Establishment ○

The CIDX cyber-security standard recommends that a user be required to re-authenticate after 15 minutes of inactivity for a given session. After five failed login attempts, the system disables the user’s account for 30 minutes. This helps deter brute force attacks. This practice meets the family requirements of FTA\_SSL under the Framework.

The standard discourages use of screen savers for session locking. The reason provided is that screen savers have the potential to interfere with the operator by blocking the view to the process and delaying response to an emergency situation. Per Framework requirements under FTA\_TSE this represents a gap in the CIDX cyber-security standard. In conclusion, the CIDX cyber-security standard partially meets the Framework requirements within TOE Access class.

#### 3.11.3 Energy - Natural Gas Sector: AGA Report Number 12

##### 3.11.3.1 Session Locking and Session Establishment ○

TSF-initiated session management is not addressed in AGA 12, Part 1.

### **3.11.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.11.4.1 Session Locking and Session Establishment ●**

This Class deals with the requirements for establishing an interactive session and with the rules for terminating such a session, once begun. API Standard 1164 requires that only users meeting specific authorization criteria can begin a session. It also directs that a time period of 30 minutes be set as the limit of inactivity before which a session is automatically terminated. This applies to both system- or user-initiated sessions. In practice, the system administrator can determine an alternative time standard. The standard matches the requirements of this class very well.

### **3.11.5 Transportation-Rail Sector**

#### **3.11.5.1 Session Locking and Session Establishment ○**

None of the requirements listed under the Target [STOE] Access class (FTA) in the Framework are addressed in the transportation standard. No reference to was found to either session locking or session establishment. This is probably due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.11.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.11.6.1 Session Locking and Session Establishment ○**

None of the families listed under the Target [STOE] Access class (FTA) in the Framework are addressed in the TR99-01. This is probably due to the differences in area of emphasis between the two documents.

#### **3.11.6.2 Cross Sector - ISA-TR99.00.02-2004**

#### **3.11.6.3 Session Locking and Session Establishment ○**

None of the families listed under the Target [STOE] Access class (FTA) in the Framework are addressed in the TR99-02. This is probably due to the differences in area of emphasis between the two documents.

### **3.11.7 Energy - Electric Power Sector: NERC CIP**

#### **3.11.7.1 Session Locking ○**

The operational needs of the electric industry are in conflict with the session locking requirement, and this is reflected in the CIP. The time-critical nature of the electric industry requires that a control center workstation be available at all times. To this end, locking screen savers and separate passwords for operators are not typically used.

### **3.11.7.2 Session Establishment** ○

The operational needs of the electric industry are in conflict with the time requirements specified for session establishment. The CIP was written with the operational needs in mind and reflects this by excluding this requirement.

### **3.11.8 Telecommunications Sector: ANSI T1.276**

#### **3.11.8.1 Session Locking and Session Establishment** ●

T1.276 requirement M-33 closely matches the Framework requirement FTA\_SSL.3.1. However M-33 provides more specific guidance by requiring the system inactivity timer to be configurable by the security administrator and the default value to be 60 minutes. T1.276 requirement M-45 is a partial match to FTA\_TSE.1.1 in that it delineates specific conditions that will result in a denial of session establishment. The conditions delineated in M-45 differ from those listed in FTA\_TSE.1.1. FTA\_TSE.1.1 states that the PCS shall deny session establishment based on factors such as day-of-the-week and time-of-day. M-45 specifies that simultaneous sessions by one user shall be limited to prevent a single user from consuming all available resources.

### **3.11.9 Water Sector: AWWA**

#### **3.11.9.1 Session Locking** ●

The AWWA standard states the need for an inactivity timeout logout (or proximity sensor) to protect the control system if no one is present in the control room — which partially fulfills the FTA\_SSL family.

#### **3.11.9.2 Session Establishment** ○

The AWWA standard does not address this family (TSE).

### 3.12 Class: Trusted Path/Channels (FTP)

#### Trusted Path and Channel

	Trusted Path and Channel		
	Trusted Channel	Mutually Trusted Acknowledgement	Trusted Path
Chemical	○	○	○
Natural Gas	○	○	○
Petroleum & Oil	●	●	●
Transportation – Rail	○	○	○
Cross-Sector ISA TR99-01	○	○	●
Cross-Sector ISA TR99-02	○	○	●
Electrical Power	○	○	○
Telecommunications	○	○	○
Water	○	○	○

○ = Gap      ○ = Partial Match      ● = Match

#### 3.12.1 Family Definitions

- Trusted Channel (ITC) - This family defines requirements for the creation of a trusted channel between the TSF and other trusted IT source/destinations for the performance of security critical operations.
- Mutually Trusted Acknowledgment (SSP) - This family defines requirements for mutual acknowledgment of the data exchange between two trusted entities.
- Trusted Path (TRP) - This family defines the requirements to establish and maintain trusted communications from/to users of the TSF.

#### 3.12.2 Chemical Sector: CIDX Cyber-security Standard

##### 3.12.2.1 *Trusted Channel, Mutually Trusted Acknowledgement, and Trusted Path*



The CIDX cyber-security standard does not fully explain the mechanics of implementing a trusted channel between the TSF and other trusted IT products for the performance of security-critical operations. The standard recommends that controls over information transmitted and stored should be developed to ensure confidentiality, authenticity, integrity, and non-repudiation. Overall, the analysis of the CIDX cyber-security standard found that it partially meets the intent of the secure communications FTP class requirements.

### **3.12.3 Energy - Natural Gas Sector: AGA Report Number 12**

#### **3.12.3.1 *Trusted Channel*** ●

AGA 12, Part 1, addresses this family topic generally by requiring a clearly defined trusted path for loading keys and separate data and security parameter ports. However, communication initiation, assured identification of end points, and other characteristics are not addressed. Therefore, there is only a partial match to this Framework family.

#### **3.12.3.2 *Mutually Trusted Acknowledgement and Trusted Path*** ○

Communication initiation, transmitted data status, and details regarding establishing and maintaining trusted communications will probably be addressed in a forthcoming AGA Standard document. Until then, a gap in this standard exists.

### **3.12.4 Energy - Petroleum & Oil Sector: API Standard Number 1164**

#### **3.12.4.1 *Trusted Channel, Mutually Trusted Acknowledgement, and Trusted Path***



API 1164 provides guidelines for data validity and security. It also requires that the security procedures be transparent to the operation of the system. These are the same qualities this Class requires. The standard matches these requirements very well.

### **3.12.5 Transportation-Rail Sector**

#### **3.12.5.1 *Trusted Channel, Mutually Trusted Acknowledgement, and Trusted Path***



None of the requirements listed under the Trusted Path/Channels class (FTP) in the Framework are addressed in the transportation standard. No reference was found to trusted path or trusted channels. This is probably due to the differences in emphasis between the two documents and the difference in the way in which the control systems are used.

### **3.12.6 Cross Sector - ISA-TR99.00.01-2004**

#### **3.12.6.1 *Trusted Channel*** ●

Inter-TSF trusted channel (FTP-ITC) is discussed in Section 9.1.5 of TR99-01, although not in full. It addresses the safe movement of data from the keyboard/mouse to applications and from applications to a region of the screen.

#### **3.12.6.2 *Trusted Path*** ●

Trusted path (FTP-TRP) is discussed in Section 9.1.5 of TR99-01, which addresses the safe movement of data from the keyboard/mouse to applications and from applications to a region of the screen.

### **3.12.6.3 Mutually Trusted Acknowledgement** ○

None of the families listed under mutual trusted acknowledgement class (SSP) in the Framework are covered in TR99.01

### **3.12.7 Cross Sector - ISA-TR99.00.02-2004**

#### **3.12.7.1 Trusted Channel, Mutually Trusted Acknowledgement, and Trusted Path**

○

None of the families listed under the trusted path/channels class (FTP) in the Framework are addressed in the TR99-02. This is probably due to the differences in area of emphasis between the two documents.

### **3.12.8 Energy - Electric Power Sector: NERC CIP**

#### **3.12.8.1 Trusted Channel, Mutually Trusted Acknowledgement, and Trusted Path**

○

The trusted path/channels Framework class primarily addresses the issue of ensuring secure remote access. There are no CIP requirements that address these issues. In fact, certain requirements, such as CIP-005-1 R1.3, with the exception of endpoints, exclude the communication link from the scope of the requirement.

### **3.12.9 Telecommunications Sector: ANSI T1.276**

#### **3.12.9.1 Trusted Channel, Mutually Trusted Acknowledgement, and Trusted Path**

○

The trusted path/channels Framework class primarily addresses the issue of ensuring secure remote access. Although there are many T1.276 requirements that relate to establishing secure channels, none relate specifically to security considerations for remote access.

### **3.12.10 Water Sector: AWWA**

#### **3.12.10.1 Trusted Channel** ●

This class is partially covered in the AWWA standard. There are many statements from this standard that seem to fit into the FTP\_ITC family, including the following:

- Utilities should eliminate unauthorized wireless networking.
- Non-SCADA modems connected to business networks should be coordinated with the enterprise IT department to verify security.
- When telephone lines are used to connect to RTUs from the field, encrypting commands should be considered.
- Encrypt radio traffic between RTUs (or PLCs) to master unit with scrambler/descrambler devices.

- Provide signal supervision and tamper alarms to detect loss of signal and tampering attempts.

### **3.12.10.2 Trusted Path** ○

There are also a number of requirements relating to the family FTP\_TRP, most of which describe how to secure the computer network. One requirement states to identify and disconnect all connections between the business and control networks that have no security controls. These requirements are listed below:

- Virtual Air-Gap - Allows one-way data traffic from a control network server to a business network server by means of an optical isolator.
- Dual-homed Server - Directs SCADA process data into a database server via one network card on the control side; allows access to the database only from the other network card on the business network.
- Router - Restricts traffic to a small number of destinations as regulated by an Access Control List (ACL). A firewall is appropriate here as well, especially if control of the Internet gateway is not under the utility IT purview.
- Firewall - Of particular value in the case where utility IT has no control over the enterprise Internet gateway.
- Consider using a virtual private network (VPN) solution to prevent unauthorized access into the enterprise network.

### **3.12.10.3 Mutually Trusted Acknowledgement** ○

The AWWA standard does not address this family (SSP).

### 3.13 Identification of new Framework Cyber-Security Classes/Families

The INL Cyber Security Framework was distributed internally for review at Revision 0.9 and only included security functional requirements (technical requirements related to control system components). Section 4.5 of the Framework document (Rev. 0.9) identifies the future incorporation of additional requirements.

The Framework Tool introduced with Framework Rev. 1.0, released in September 2005, incorporates 100+ policy and procedure functional requirements. The Framework will continue to evolve with the addition of cyber security assurance and functional requirements as well as policy and procedure requirements.

Unclassified Families				
	Software Management Control Plan	Product Safety Plan	Operations & Maintenance Manual	Records Retention
Chemical	●	◐	○	●
Natural Gas	○	○	○	○
Petroleum & Oil	●	◐	○	●
Transportation – Rail	●	●	●	●
Cross-Sector ISA TR99	○	○	○	○
Electrical Power				
Telecommunications	●	○	●	○
Water				
	Verification & Validation	Risk Assessment	Hazards Analysis	Human Factors Analysis
Chemical	●	●	●	◐
Natural Gas	●	●	◐	○
Petroleum & Oil	○	●	○	◐
Transportation – Rail	●	●	●	●
Cross-Sector ISA TR99	○	○	○	○
Electrical Power				
Telecommunications	●	○	○	○
Water				
	Failure Analysis	Testing	Training & Security Awareness	Compliance
Chemical	◐	●	●	●
Natural Gas	◐	●	◐	○
Petroleum & Oil	◐	●	◐	●
Transportation – Rail	●		●	○
Cross-Sector ISA TR99	○		●	●
Electrical Power			●	●
Telecommunications	○		●	
Water		●	○	
○ = Gap                      ◐ = Partial Match                      ● = Match				



## ***Family Definitions***

- Software management control plan – This family defines requirements for managing the software components that are associated with all PCs used in the control systems.
- Product safety plan – This family defines requirements for protecting systems that provide data that is made available to third parties.
- Operations & maintenance manual – This family defines requirements for keeping and maintaining standing security plans for cyber control systems for operators and maintenance personnel.
- Records retention - This family defines requirements for retaining records of critical control system data as well as data access, authentication, security configuration information, etc., that may be useful for auditing, forensics, etc.
- Verification & validation – This family defines more detailed requirements that the Framework for data verification and validation processes such as data validation and user authentication.
- Risk assessment – This family defines requirements to assess the relative risks and consequences associated with the critical portions of the control systems.
- Hazards analysis – This family defines requirements for analyzing hazards involved with operating and maintaining control systems including hazards that may occur with cyber attacks.
- Human factors analysis – This family defines requirements for analyzing human factors involved in both identifying malicious threats and defending them.
- Failure analysis – This family defines requirements for the process of analyzing system failures that occur and likelihood/consequences associated with failures.
- Testing – This family defines the requirements for validating the competence of personnel who administrate, operate, etc. control systems.
- Training & security awareness – This family defines requirements for equipping administrators, operators, etc. with basic security information to be aware of security issues and be able to react and respond to security issues according to security plans and policies.
- Compliance – This family defines metrics for compliance for the classes and families of requirements delineated in the Framework in such a way which administrators and operators, etc. can measure how secure products and components in control system are relative to the Framework.

## ***Telecommunications Sector: ANSI T1.276***

The Classes and Families delineated in the Framework provide good coverage for the requirements delineated in T1.276. T1.276 requirements that could not be matched with equivalent or similar Framework requirements could generally be associated with a specific Framework class. Only one T1.276 requirement could not be matched with a specific class. T1.276 requirement M-48 requires that systems display an improper

usage warning banner. This requirement, to some extent, is a personnel education tool and, as such, is identified in this section with “Training”.

In addition to the requirements specified in the main body of T1.276, Annex B of the standard delineates security procedures that are, as stated in the standard, “tutorial in nature.” The procedures included in this annex touch upon a number of the classes/families discussed in this section and excluded from the Framework document. Classes/families that are excluded from both the main body of T1.276, T1.276 Annex B, and the framework include:

- Product Safety Plan
- Operations and Maintenance Manual
- Records Retention
- Human Factors Analysis
- Failure Analysis
- Authority/Responsibility
- Cyber security Management System (Partial match in Framework Requirements)
- Security Policy (Partial match in Framework Requirements)
- Personnel Safety
- Compliance

The extent to which T1.276 addresses the remaining classes/families that have been identified as excluded from the Framework is addressed below.

***Software Management Control Plan (Not addressed in Framework Requirements, partial match in T1.276 Annex B)***

Although T1.276 does not specifically require a software management control plan, the standard does delineate a number of requirements relating to the verification of software configurations and authentication of the source of software. As such, the requirements could be interpreted as requiring a software plan for effective implementation. Section B.5 of Annex B delineates specific software lifecycle considerations and procedures for ensuring secure software installations and configurations.

***Verification and Validation (Partial match in Framework Requirements and T1.276)***

T1.276 provides extensive guidance regarding data integrity, encryption algorithms, and user access controls. Although T1.276 provides a number of requirements relating to cryptographic algorithms and user access controls, the standard does not provide specific guidance regarding the verification and validation of data.

***Risk Assessment (Not addressed in Framework Requirements & Good match in T1.276 Annex B)***

Risk assessment is not discussed in the main body of the T1.276 standard. The importance and application of risk assessments is discussed a number of times in

Annex B. Section B.4.3 discusses the importance of assessing the risk of natural disasters, serious accidents, and power interruptions at critical sites. Section B.5.3.3, entitled *Risk Assessment*, discusses the risk management process as being fundamental to information security and the importance of performing a risk analysis for each new product or service.

***Hazards Analysis (Not addressed in Framework Requirements & match in T1.276 Annex B)***

Annex B Section B.4.3 of T1.276 discusses the importance of understanding site hazards and establishing plans for the response to hazardous material incidents.

***Testing (Not addressed in Framework Requirements & match in T1.276 Annex B)***

Annex B Section B.5.3.12 of T1.276 states that testing should be conducted to provide assurance that components and security features have been robustly implemented and correctly configured.

***Training and Security Awareness (Not addressed in Framework Requirements, match in T1.276 Annex B)***

Only one T1.276 requirement, M-48, could not be matched with a specific Framework class. M-48 requires that systems display an improper usage warning banner. This requirement, to some extent, is a personnel education tool and, as such, could be associated with training and security awareness.

Annex B Section B.5.3.2 of T1.276, entitled *Security Awareness and Training*, explicitly discusses the importance of maintaining personnel awareness of security policies and procedures and the importance of protecting information assets. This section asserts that personnel are often the weakest security link and that training can dramatically strengthen this link.

***Sector specific classes/family***

- ***Organizational Security (Not addressed in Framework CS, partial match in T1.276 Annex B)***

T1.276 does not address organizational chain of command issues however Annex B does include an extensive section, Section B.4 *Physical Security Considerations* that addresses a number of physical security issues including building security, guards, locks, and badging.

- ***Contingency/Emergency Planning (Not addressed in Framework Requirements, match in T1.276 Annex B)***

T1.276 Annex B Section B.4.2.2, entitled *Emergency Facilities*, discusses the importance of assessing the adequacy of emergency facilities such as fire and environmental protection systems necessary for the continued operation of critical systems. This section states that emergency facilities are important in the aftermath of a security breach. Section B.4.3 discusses the importance of emergency planning within the context of natural disasters.

### ***Natural Gas Sector: AGA Report No. 12***

#### ***Software Management Control Plan (Not addressed in Framework CS Requirements & AGA Report No. 12)***

The Framework Document is deficient in defining requirements for managing the software components that are the heart of all PC systems. This should be interpreted to include both the functional software suites controlling the system, and the data captured for immediate or future purposes. As *Software Management* logically includes *Software Security* and *Software Maintenance*, an appropriate location for such CSRs might be in conjunction with the small section referencing Configuration Management. Software Management is also a part of Configuration Management.

AGA 12, Part 1 essentially recommends implementation of a crypto system to protect SCADA communications. As such, it recognizes that this necessarily entails a collective of keys, algorithms, hardware, software and security policies that must be employed to apply cryptographic services to this problem. However, it should be noted that AGA 12, Part 1 does not recommend performing cryptography in a purely software environment because it exposes cryptographic tools and algorithms as well as keys to potential threats such as malicious code or intentional malicious actions by users.

Software development practices are addressed in FIPS 140-2, Appendix B, but as information and not normative practices. Also, AGA 12, Part 1 does not specifically reference this part of the FIPS document or itself address software management control.

#### ***Product Safety Plan (Not addressed in Framework CS Requirements & AGA Report No. 12)***

Essentially all natural gas-related physical operations, including storage facilities and pipelines, maintain and abide by a written Product Safety Plan. Portions of these plans require the gathering and retention of data through the PC system. This data may well need to be made available to a more public user group than the bulk of the PC-gathered data. The Framework Document does not provide any guidance in how to maintain security while making data available to a select group of third parties.

AGA 12, Part 1 recommends that cryptographic modules and authentication modules installed in field sites be designed for an indoor substation environment as defined in IEEE STD™ 1613. Beyond that it does not directly address product safety.

***Operations and Maintenance Manual (Not addressed in Framework CS Requirements & AGA Report No. 12)***

The Framework Document does not require the Control System operator to keep any type of manual setting forth the operating structure under which the CS functions. In practice, firms operating a process control system virtually always maintain an Operations Manual and a Maintenance Operations Manual (albeit the names may vary, and they may be combined). It is here that all the security plans pertaining to CS operations should be gathered. The Framework Document should stipulate certain documents pertaining to cyber security and to the CS plan that should be a part of this manual(s).

AGA 12, Part 1 does not address Operations and Maintenance Manuals.

***Records Retention (Partial match in Framework CS Requirements & Gap in AGA Report No. 12)***

Every operating company has a comprehensive records retention policy. The Framework Document should set forth requirements for retention of cyber data that reflect the best practices currently available in industry. The requirements include a data protection class that discusses data access, authentication and security controls, but they do not provide for comprehensive collection of other company records vital to the operation of the facility.

AGA 12, Part 1 does not contain normative records retention specifications. It makes a reference to audit log retention as being appropriately defined in an auditing document.

***Verification and Validation (Partial match in Framework CS Requirements – Good match in AGA Report No. 12)***

The Framework Document, under “User Data Protection and Trusted Security Class”, discusses minimal requirements for verifying and validating data gathered for the control system pertaining to data authentication and password verification. The standard overall does not provide detailed data verification and validation requirements.

AGA 12, Part 1 recommended practices are specifically designed to provide data communications that are known to be unaltered by potential attackers and that can be authenticated as having originated from valid authorized users.

***Risk Assessment (Not addressed in Framework CS Requirements – Good match in AGA Report No. 12)***

The Framework Document makes no mention of Risk Assessment.

AGA 12, Part 1, Appendix F, makes extensive normative recommendations regarding risk assessment and analysis.

***Hazards Analysis (Not addressed in Framework CS Requirements – Gap in AGA Report No. 12)***

The Framework Document makes no mention of Hazards Analysis.

There is no mention of Hazards Analysis in AGA 12, Part 1.

***Human Factors Analysis (Not addressed in Framework CS Requirements & AGA Report No. 12)***

The Framework Document makes no mention of Human Factors Analysis.

There is no mention of Human Factors Analysis in AGA 12, Part 1.

***Failure Analysis (Not addressed in Framework CS Requirements – Partial match in AGA Report No. 12)***

Many provisions of the Framework Document pertain to dealing with failures, and documenting the recognition that failures will occur. It should go a step further and stipulate a procedure for failure analysis. This will conceivably aid the operator by identifying failure paths, and thereby improve security.

AGA 12, Part 1 recommends that an InfoSec team make use of failure mode analysis, but does not specify procedures for doing so.

***Testing (Not addressed in Framework CS Requirements – Good match in AGA Report No. 12)***

Testing, in this context, is meant to refer to verifying Operator qualifications. The Framework Document recognizes numerous types of performance testing that apply directly to the system components. None of these provisions are meant to measure the knowledge and competence of the Operator.

AGA 12, Part 1, Annex H sets forth detailed normative recommendations for a cryptographic system test plan including test and evaluation objectives, evaluation criteria, functional and performance requirements, operability and interoperability testing, test reports and ownership of test results.

***Training and Security Awareness (Not addressed in Framework CS Requirements – Partial match in AGA Report No. 12)***

While the Framework Document focuses heavily on the security attributes of the ICS, it makes no reference to equipping the Operator to recognize and react to potential security threats. Most industry standards acknowledge the existence of insider security threats, whether intentional or not. The Framework document should as well.

AGA 12, Part 1 recognizes the importance of personnel training in maintaining a secure system, and addresses it in Annex F: *Cyber security practice fundamentals*. Formal documents are recommended including the following:

- A malicious code protection document defining the procedures for how and what software may be loaded on to systems and networks, requirements for scanning tools, updates to scanning tools, employee training and awareness, violation enforcement, and recovery procedures.
- A personal cyber security document defines the policy and procedures for personnel hiring and termination, including background checks, security clearances, signed agreements, account management, and training and education.
- An education training and awareness document defines the policy and procedures for initial and periodic review of security policies, standard operating procedures, and security trends and vulnerabilities.

***Organizational Security (Not addressed in Framework CS & Partial Gap in AGA Report No. 12)***

Organizational security, in this context, refers to both the physical security of the control system and the operational hierarchy (chain of command), from the senior manager down to the control center staff and field personnel. The Framework Document does not address either of these concepts, though a stable environment (both physical and hierarchical) is necessary for dependable operation.

AGA 12, Part 1 does not provide normative requirements for physical security, but recognizes that cryptography is only effective if it is deployed as part of a comprehensive set of cyber security policies, and when it is combined with adequate attention to physical security. It does recommend that cyber security goals and standards address both departmental operating requirements and corporate business practice requirements and that the security goals and standards be extended to include all business partners, contractors, and vendors to ensure consistent treatment of information, transactions, and company resources.

***Compliance (Not addressed in Framework CS Requirements - Good match in AGA Report No. 12)***

The Framework Document specifies enforcement of a number of the various sub-categories within the different families of the matrix of classes. It fails to stipulate any compliance requirements for any of these; these details are left to the system operator to define. The Framework Document should provide more detail as to the level of required compliance, what constitutes compliance, and what are reasonable consequences for non-compliance. AGA 12, Part 1 establishes specific compliance requirements within the document and provides references to FIPS 140-2. It sets forth extensive normative material that is mandatory for the product or system to claim

compliance with AGA 12. Curiously however, it states that it is mandatory that products or systems claiming compliance with AGA12 comply with all normative parts *or explicitly state and characterize areas of non-compliance.*

### ***Sector specific classes/family***

- ***Authority/Responsibility (Not addressed in Framework CS Requirements – Partial match in AGA Report No. 12)***

The Framework Document addresses authority and responsibility only minimally, and then only in the context of the user with respect to proper use of the system. It ignores the area of overall authority and responsibility for the design, maintenance, operation, and security of the control system.

AGA 12, Part 1 requires role-based authentication, defines a User Role, Crypto Officer Role and a Maintenance Role and requires that these be provided in the context of cryptographic modules. It also recommends the creation of an InfoSec team with clearly defined roles, responsibilities and authorities for information owners, organizations and users.

- ***Contingency/Emergency Planning (Not addressed in Framework CS Requirements – Partial match in AGA Report No. 12)***

The Framework Document makes a reference to recovery from system failure, which involves a type of contingency planning. However, it doesn't detail any requirements for including contingencies for operational security in the system design. It doesn't require the system operator to analyze potential security issues and use the analysis to develop alternative operating scenarios designed to maintain security and service.

AGA 12, Part 1 addresses the need for a contingency plan which identifies single points of failure, backup and restoration plans and procedures, and man-made or natural events that may disrupt an organizations ability to conduct business. However, it does not provide a detailed plan.

- ***Cyber security Management System (Partial match in Framework CS Requirements – Good match in AGA Report No. 12)***

The Framework CS requirements for Configuration Management represent a portion of what is required for a cyber security management system. It should also require specific proactive security efforts, such as routine scanning for vulnerabilities and self-assessments of organizational and individual performance.

AGA 12, Part 1 recognizes the importance of proactive security efforts and addresses it in Annex F: *Cyber security practice fundamentals.*

It makes numerous recommendations including formation of an InfoSec team, self-assessments and reassessments and development and maintenance of numerous formal cyber security documents.



- ***Personnel Safety (Not addressed in Framework CS Requirements & in AGA Report No. 12)***

The Framework Document does not address personnel safety considerations.

AGA 12, Part 1 does not address the subject of personnel safety.

- ***Security Policy (Partial match in Framework CS Requirements & in AGA Report No. 12)***

The Framework Document makes multiple references to security violations, which implies recognition of an existing security policy. Nowhere does it set forth any requirements or guidelines for what should be included in a security policy for a process control system.

AGA 12, Part 1 specifically recommends that all cyber security goals and standards be clearly described in cyber security policies. As a minimum, these policies are to describe all cyber security requirements for choosing, installing, maintaining, and decommissioning software, hardware and information associated with the cyber portion of the company's control system, including field operation's systems and networks. Each security policy should dictate the responsibilities, practices, and procedures of every employee, contractor, business partner, and third party that has access to, or performs some type of service affecting a company's cyber controls.

A forthcoming addendum to AGA 12, Part 1 will contain a number of sample cyber security policies developed for gas, water, wastewater, electric and pipeline SCADA systems. Most of these security policies will be included as *Informative*, meaning they are provided for reference. Some of these policies may be *Normative*, meaning to claim compliance with AGA 12, Part 1 requires the end user and manufacturers to implement and adhere to the cyber security policies as written. End users are encouraged to take ownership of the *informative* policies by reviewing them, modifying them to match their corporate needs and culture, and implementing them.

#### ***Oil Sector: API Standard No. 1164***

##### ***Software Management Control Plan (Not addressed in Framework CS Requirements – Good match in API Standard No. 1164)***

The Framework Document is deficient in defining requirements for managing the software components that are the heart of all PC systems. This should be interpreted to include both the functional software suites controlling the system, and the data captured for immediate or future purposes. As *Software Management* logically includes *Software Security* and *Software Maintenance*, an appropriate location for such CSRs might be placed in conjunction with the small section referencing Configuration Management. Software Management is also a part of Configuration Management.

API Standard No. 1164 includes extensive provisions for managing software, for in-house developed and for commercial software applications. It requires inclusion of

security standards in all such software, with the level of security commensurate with the criticality and sensitivity of the application. Standards for criticality and sensitivity are also established, in another section of API Standard No. 1164.

***Product Safety Plan (Not addressed in Framework CS Requirements – Partial match in API Standard No. 1164)***

Essentially all petroleum-related physical operations, including refineries, storage facilities, and pipelines, maintain and abide by a written Product Safety Plan. Portions of these plans require the gathering and retention of data through the PC system. This data may well need to be made available to a more public user group than the bulk of the PC-gathered data. The Framework Document does not provide any guidance in how to maintain security while making data available to a select group of third parties.

API Standard No. 1164 does not directly address product safety. It does extensively address proper handling of data agreements between owners and contractors, and how contractors that access company information are contractually bound to uphold the Company's information security policies.

***Operations and Maintenance Manual (Not addressed in Framework CS Requirements and in API Standard No. 1164)***

The Framework Document does not require the Control System operator to keep any type of manual setting forth the operating structure under which the CS functions. In practice, firms operating a process control system virtually always maintain an Operations Manual and a Maintenance Operations Manual, albeit the names may vary, and they may be combined. It is here that all the security plans pertaining to CS operations should be gathered. The Framework Document should stipulate certain documents pertaining to cyber security and to the CS plan that should be a part of this manual (or these manuals). API Standard No. 1164 does not address Operations and Maintenance Manuals.

***Records Retention (Partial match in Framework CS Requirements – Good match in API Standard No. 1164)***

Every operating company has a comprehensive records retention policy. The Framework Document should set forth requirements for retention of cyber data that reflect the best practices currently available in industry. The requirements include a data protection class that discusses data access, authentication and security controls, but it does not provide for comprehensive collection of other company records vital to the operation of the facility.

API Standard No. 1164 addresses Information Retention in the multiple contexts of Change Management; Communications and Network Usage Standards; Information Retention Standards; and, System Security Audit and Review Standards.

***Verification and Validation (Partial match in Framework CS Requirements – Gap in API Standard No. 1164)***

The Framework Document, under “User Data Protection and Trusted Security Class”, discusses minimal requirements for verifying and validating data gathered for the control system pertaining to data authentication and password verification. The standard overall does not provide detailed data verification and validation requirements. API Standard No. 1164 does not address Verification and Validation.

***Risk Assessment (Not addressed in Framework CS Requirements – Good match in API Standard No. 1164)***

The Framework Document makes no mention of Risk Assessment. API Standard No. 1164 requires risk assessment considerations in several contexts. It requires risk assessment of all operator-owned facilities with regard to controlling entry and access. It also requires risk assessment to decide the need and complexity of backup facilities. It is also prescribed for determining the criticality of an application. Additionally, its use is directed as a preamble to proposed procedural changes in the control operation.

***Hazards Analysis (Not addressed in Framework CS Requirements and Gap in API Standard No. 1164)***

The Framework Document makes no mention of Hazards Analysis. There is no mention of Hazards Analysis in API Standard No. 1164. This could be construed as a particular case of risk analysis, but it should be explicitly addressed.

***Human Factors Analysis (Not addressed in Framework CS Requirements – Partial match in API Standard No. 1164)***

The Framework Document makes no mention of Human Factors Analysis. There is no mention of Human Factors Analysis in API Standard No. 1164. However, there is a section in Appendix A that deals with Personnel Security that touches on such topics as what security information is issued to personnel, and how they become accountable. Topics such as physical security and termination are also part of this category. The overall coverage of the subject is incomplete.

***Failure Analysis (Not addressed in Framework CS Requirements – Partial match in API Standard No. 1164)***

Many provisions of the Framework Document pertain to dealing with failures, documenting the recognition of reality that failures occur. It should go a step further and stipulate a procedure for failure analysis. This will conceivably aid the operator by identifying failure paths, and thereby improve security. API Standard No. 1164 also recognizes, and prescribes mitigation methods for, failure. It does not prescribe Failure Analysis.

***Testing (Not addressed in Framework CS Requirements – Partial match in API Standard No. 1164)***

Testing, in this context, is meant to refer to verifying Operator qualifications. The Framework Document recognizes numerous types of performance testing that apply directly to the system components. None of these provisions are meant to measure the knowledge and competence of the Operator.

API Standard No. 1164 also advocates extensive testing of component and software performance. As is the case for the Framework Document, API Standard No. 1164 also does not address Operator testing or competence.

***Training and Security Awareness (Not addressed in Framework CS Requirements – Partial Match in API Standard No. 1164)***

While the Framework Document focuses heavily on the security attributes of the ICS, it makes no reference to equipping the Operator to recognize and react to potential security threats. Most industry standards acknowledge the existence of insider security threats, whether intentional or not. The Framework Document should as well.

API Standard No. 1164 recognizes the importance of personnel training in maintaining a secure system, and addresses it at numerous points throughout the Standard. However, it is somewhat deficient in not specifying or requiring a structured security training program for its industry clientele.

***Organizational Security (Not addressed in Framework CS Requirements – Good Match in API Standard No. 1164)***

Organizational security, in this context, refers to both the physical security of the control system and the operational hierarchy (chain of command), from the senior manager down to the control center staff and field personnel. The Framework Document does not address either of these concepts, but a stable environment, both physical and hierarchical, are necessary for dependable operation.

API Standard No. 1164 establishes specific requirements for physical plant security. These requirements are set forth in Appendix A. It also establishes a requirement for defining the authority and responsibility of each of the personnel levels that are involved with the operation, maintenance, and restoration of control system functions.

***Compliance (Partial Match in Framework CS Requirements – Good Match in API Standard No. 1164)***

The Framework Document specifies enforcement of a number of the various sub-categories within the different families of the matrix of classes. It fails to stipulate any compliance requirements for any of these; these details are left to the system operator to define. The Framework Document should provide more detail as to the level of

required compliance, what constitutes compliance, and what are reasonable consequences for non-compliance.

API Standard No. 1164 establishes compliance requirements with respect to all applications, data bases, policies, etc. It assigns responsibility for ordering and ensuring compliance by users. It also establishes penalties for non-compliance. It requires all employees to report instances of out-of-compliance activities. Finally, it recommends periodic third-party audit of compliance.

### ***Sector specific classes/family***

- ***Authority/Responsibility Awareness (Not addressed in Framework CS Requirements – Good Match in API Standard No. 1164)***

The Framework Document addresses authority and responsibility only minimally, and then only in the context of the user with respect to proper use of the system. It ignores the area of overall authority and responsibility for the design, maintenance, operation, and security of the control system.

API Standard No. 1164 is specific in establishing where responsibility lies with respect to operation and security of the system. It also requires that specific cyber security roles, responsibilities and authorities be clearly defined for managers, system administrators, and users.

- ***Contingency/Emergency Planning (Not addressed in Framework CS Requirements – Good Match in API Standard No. 1164)***

The Framework Document makes a reference to recovery from system failure, which involves a type of contingency planning. However, it doesn't detail any requirements for including contingencies for operational security in the system design. It doesn't require the system operator to analyze potential security issues and use the analysis to develop alternative operating scenarios designed to maintain security and service.

API Standard No. 1164 addresses both the need for a predetermined alternative control site, and the need for addressing and resolving predetermined disruption scenarios. Both activities are aimed at preventing or minimizing service disruptions.

- ***Cyber Security Management System (Partial Match in Framework CS Requirements – Good Match in API Standard No. 1164)***

The Framework CS requirements for Configuration Management represent a portion of what is required for a cyber security management system. It should also require specific proactive security efforts, such as routine scanning for vulnerabilities and self-assessments of organizational and individual performance.

API Standard No. 1164 requires that cyber security roles, responsibilities, and authorities be clearly defined. It also requires Clear identification of cyber security requirements. It also requires that performance standards be established and used for regular review. And it requires accountability of managers, administrators, and users.

- ***Personnel Safety (Not addressed in Framework CS Requirements – Partial Match in API Standard No. 1164)***

The Framework Document does not address personnel safety considerations. API 1164 extensively addresses the subject of personnel security, but in the context of preventing damage to the control system that might be caused by users or other company personnel, whether accidentally or intended. It addresses personnel safety only minimally, in a section that deals primarily with the physical security of the control system components.

- ***Security Policy (Not addressed in Framework CS Requirements – Good Match in API Standard No. 1164)***

The Framework Document makes multiple references to security violations, which implies recognition of an existing security policy. Nowhere does it set forth any requirements or guidelines for what should be included in a security policy for a process control system.

API Standard No. 1164 stipulates a requirement for a SCADA security policy. It details how it should be structured (with a multi-layered approach). Several specific security requirements are listed, along with an additional list of recommendations for inclusion.

### ***Chemical Sector: CIDX Cybersecurity Standard***

#### ***Software Management Control Plan (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework Document is deficient in defining requirements for managing the software components that are the heart of all PC systems. This should be interpreted to include both the functional software suites controlling the system, and the data captured for immediate or future purposes. As *Software Management* logically includes *Software Security* and *Software Maintenance*, an appropriate location for such CSRs might be included in conjunction with the small section referencing Configuration Management. Software Management is also a part of Configuration Management.

CIDX Cybersecurity Standard recommends best practices to include security in the design, development and maintenance of all IT and process control components. The security requirements are specified as part of the front-end design activity and are tested as part of the site acceptance test of the system. Security requirements are considered and assessed during all maintenance activities on the system. This includes system and component configuration changes, operating system level revision changes/patches, application revision changes, and general enhancements. The standard provides references to the following industry standards: ISO/IEC 17799, "Information Technology – Code of Practice for Information Security Management", First Edition, 2000; Section 10, "Systems Development and Maintenance", ISA-TR99.00.02-2004; "Integrating Electronic Security into the Manufacturing and Control Systems

Environment", 2004, ISA—The Instrumentation, Systems and Automation Society, Section 6.9; and, the NIST PCSRF ICS-SPP (National Institute of Standards Process Control Security Requirements Forum Industrial Control System Protection Profile) issued.

***Product Safety Plan (Not addressed in Framework CS Requirements – Partial match in CIDX Cybersecurity Standard)***

Essentially all chemical and process industries maintain and abide by a written Product Safety Plan. Portions of these plans require the gathering and retention of data through the PC system. For an example, the companies are required by Federal mandate to maintain an MSDS (Material Safety Data Sheet) for each chemical product used and stored in the facility. This data must be easily available to sector personnel, partners, responders, and the public user group on a need basis. Most of the data is available via PC and is usually made part of the safety policy and operating product safety plan. Although not mentioned in the standard clearly, the MSDS information is usually available at the operating facility. The standard does mention the need for proper handling and use of all data, sharing, and security agreements between the facility owners and contractors.

The Framework Document does not provide any guidance in how to maintain security while making operational data available to personnel, responders and a select group of third parties.

***Operations and Maintenance Manual (Not addressed in Framework CS Requirements & CIDX Cybersecurity Standard)***

The Framework Document does not require the Control System operator to keep any type of manual setting forth the operating structure under which the CS functions. In practice, chemical and process industry members operating a process control system almost always maintain an Operations and a Maintenance Manual (albeit the names may vary, and they may be combined). It is here that all the security plans pertaining to CS operations should be gathered and included. The Framework Document should stipulate certain documents pertaining to cyber security and to the CS plan that should be a part of this manual (or these manuals). The CIDX Cybersecurity does not address Operations and Maintenance Manuals specifically in the standard.

***Records Retention (Partial match in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

Every operating company has a comprehensive records retention policy. The Framework Document should set forth requirements for retention of cyber data that reflect the best practices currently available in industry. The requirements include a data protection class that discusses data access, authentication and security controls, but it does not provide for comprehensive collection of other company records vital to the operation of the facility.

The CIDX Cybersecurity addresses records retention in the information and document section of the standard. The chemical companies are encouraged to use both comprehensive information and document management policy for their Cybersecurity Management System (CSMS). It emphasizes that information associated with the development and execution of a CSMS is important, sensitive, and should be managed. Risk analyses, business impact studies, risk tolerance profiles, etc. contain sensitive company information and need to be protected. Security controls, philosophy, and implementation strategies are other examples. Additionally as business conditions change, it is good practice to update analyses and studies. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.

***Verification and Validation (Partial match in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework Document, under “User Data Protection and Trusted Security Class”, discusses minimal requirements for verifying and validating data gathered for the control system pertaining to data authentication and password verification. The standard overall does not discuss data verification and validation in detail.

The CIDX Cybersecurity Standard provides various practices to test and verify all data including software patches, etc., under sections “Information and Document”, and “System Development and Maintenance”.

***Risk Assessment (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework Document makes no mention of Risk Assessment. The CIDX Cybersecurity, under section “Risk Identification, Classification, and Assessment”, provides great detail concerning best practices used in industry to identify, classify, and prioritize risk assessment activities based on criticality. It recommends positioning a change management system to identify reassessment criteria based on technology, organization or process changes.

***Hazards Analysis (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework Document makes no mention of Hazards Analysis. The CIDX Cybersecurity Standard under section “Risk Identification, Classification, and Assessment”, provides great detail concerning best practices used in industry to identify, classify, and prioritize hazard analysis activities based on criticality. The standard provides steps to develop a comprehensive list of all the critical assets whose failure could impact the business. It also recommends assigning a risk level to each asset in scope per risk tolerance profile established for the organization. Based on the comprehensive list of threats, risk tolerance, and vulnerabilities evaluate the likelihood that businesses or manufacturing is exposed to each.



***Human Factors Analysis (Not addressed in Framework CS Requirements – Partial match in CIDX Cybersecurity Standard)***

The Framework Document makes no mention of Human Factors Analysis. There is no mention of Human Factors Analysis in CIDX Cybersecurity Standard. However, there is a section “Personnel Security” that deals with employing security responsibilities at the recruitment phase, all contracts, and stresses monitoring during an individual’s employment. It recommends that recruits should be screened, especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality or nondisclosure agreement.

***Failure Analysis (Not addressed in Framework CS Requirements – Partial match in CIDX Cybersecurity Standard)***

Many provisions of the Framework Document pertain to dealing with failures, documenting the recognition that failures occur. It should go a step further and stipulate a procedure for failure analysis. This will conceivably aid the operator by identifying failure paths, and thereby improve security.

The CIDX Cybersecurity Standard provides guidelines under the section “Incident Planning and Response” to detect and deter failures and to prepare contingency and disaster recovery plans to mitigate and restore system operations within a reasonable time. It does not prescribe Failure Analysis specifically.

***Testing (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

Testing, in this context, is meant to refer to verifying Operator qualifications. The Framework Document recognizes numerous types of performance testing that apply directly to the system components. The Framework document does not provide rules or matrix to measure the competence of the Operator for Cybersecurity breach.

The CIDX Cybersecurity Standard provide recommendations under the section, “Staff Training and Security Awareness” cyber security training component that includes defined responsibilities and accountability to the cyber security management system (CSMS) team.

***Training and Security Awareness (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document does not have requirements that address cyber security training and awareness. The CIDX Cybersecurity Standard recommends that industry maintain and review employee competencies against skill requirements, and provide training that addresses basic employee work requirements and security awareness. The standard provides best training practices for adoption by the industry.

***Organizational Security (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document proscribes requirements at a control systems level in contrast to the CIDX Cybersecurity Standard. This gap could be easily bridged with the industry standard by incorporating organizational security practices in the final product of the Framework methodology.

The CIDX Cybersecurity Standard, under the section “Organizational Security”, provides companies guidelines to establish organizational security that includes both cyber and physical aspects. Companies should establish an organization, structure, or network with responsibility for overall security, recognizing there are physical as well as cyber components that should be addressed. The standard includes practical guidance of the ISO/IEC 17799, Section 4 and includes appropriate input from ISA-TR99.00.02-2004 to address both traditional information technology (IT) and manufacturing control systems.

***Compliance (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document proscribes audit requirements at a control systems component level in contrast to the CIDX Cybersecurity Standard.

The CIDX Cybersecurity Standard recommends that companies periodically assess their security programs and processes to affirm that required programs and processes are in place and working, and to take corrective action as appropriate. The standard also emphasizes that in appropriate circumstances, assessments should also apply to the programs and processes of other companies with whom the company conducts business, such as chemical suppliers, logistics service providers, joint ventures, or customers.

The standard also recommends that management should validate or audit for compliance, to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, or security requirements. Further, the management should validate or audit for compliance to corporate security policies and practices for secure and safe operation of its assets.

***Sector specific classes/family***

- ***Authority/Responsibility (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document does not have requirements that address authority, responsibility in context of management policies. The CIDX Cybersecurity Standard describes assignment of authority and responsibility under the sections “Cybersecurity Management System” and “Security Policy”. These sections address various aspects of corporate commitment to establishment, communication, and monitoring of cyber

security within the company. They also discuss user responsibility and individual accountability in the protection of information and systems.

- ***Contingency/Emergency Planning (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document does not have requirements that address contingency and emergency planning requirements. The requirements under the “Resources” class, which discuss backup systems and fault tolerance technology available for timely restoration of systems after failure, are the only contingency-related requirements.

The CIDX Cybersecurity Standard, under the section “Business Continuity Plan”, describes development of contingency and emergency plans to respond to the consequences of disasters, security failures and loss of service to a business. It stresses that the plans should be structured such that they allow business processes to be restored in a timely manner.

- ***Cyber security Management System (Partial match in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document under Configuration Management requirements discusses at the component level capability to prevent and detect the loss of integrity of the process control system operational system configuration and capability. It does not discuss at policy levels how companies should manage risks, develop security policies, objectives, targets, etc.

The CIDX Cybersecurity Standard provides emphasis on the Cybersecurity Management System and recommends establishment of a management framework (i.e., organization) to initiate and control the implementation of cybersecurity within the company to include all aspects of business information systems, manufacturing and control systems, integration points with business partners, customers, and suppliers.

- ***Personnel Safety (Not addressed in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document does not provide any requirements with reference to personnel safety. The CIDX Cybersecurity Standard, under the section “Personnel Safety”, recommends that companies address security responsibilities at the recruitment phase, include these responsibilities in all contracts, and monitor performance during an individual’s employment. The standard emphasizes screening of recruits, especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality or nondisclosure agreement.

- ***Security Policy (Partial match in Framework CS Requirements – Good match in CIDX Cybersecurity Standard)***

The Framework document partially provides requirements that address security policy at a component level in terms of authorization, access, authentication, etc. The document does not specifically mention establishment at a corporate level that covers all aspect of operations as prescribed in the CIDX Cybersecurity Standard.

For example, the CIDX Cybersecurity Standard, under the section “Security Policy”, recommends that companies develop overall policies and activities that include security policy issues. The activities should include information systems and manufacturing and control systems, as well as connectivity with business partners, customers, suppliers and other third party entities.

### ***Transportation-Rail Sector***

The transportation sector standard reviewed for this exercise has several requirements that are mainly administrative in nature. These could be broken into families or classes, such as Analysis, Documentation and Planning, Training, and Verification and Validation.

#### ***Analysis***

The transportation standard addresses requirements in the area of Failure Analysis (Section 236.915), Hazards Analysis (Section 236.907), Human Factors Analysis (Section 236.907 and Appendix E), and Risk Assessment (Sections 236.907 and 236.909).

#### ***Training***

Training is a major area addressed in the transportation standard that is not covered by the Framework requirements. The standard requires a training program describing who must be trained, the level of training, and specific goals to be met by the training (Sections 236.907 and 236.921)

#### ***Verification and Validation***

The transportation standard requires the verification and validation of both the original design and any changes (Section 236.905).

#### ***Sector specific classes/family***

- ***Documents and Planning***

The transportation standard requires an Operations and Maintenance Manual (Section 236.919), a Product Safety Plan (Section 236.907), a Software Management Control Plan (Section 236.18), and Records Retention (Section 236.917).

#### ***Electric Power/Energy Sector: NERC CIP***

In support of the items listed in the above table, the NERC CIP contains the following requirements not contained in the framework:

**Software Management Control Plan:** The Responsible Entity shall implement supporting configuration management activities to identify, control and report any changes to hardware and software components of Critical Cyber Assets.

**Records Retention:** Records retention is covered in multiple requirements and measurements.

**Verification and Validation:** A minimum of identity verification (e.g., Social Security Number verification in the U.S.) and five year criminal check is required.

**Risk Assessment:** Risk assessment is tied to personnel within the CIP. This standard requires that personnel having authorized access to Critical Cyber Assets, including contractors and service vendors have a higher level of risk assessment...etc.

**Testing:** The recovery plan(s) shall be exercised at least annually.

**Training:** Section CIP-003-1 deals with Personnel and Training issues.

**Organizational Security:** In multiple areas, the CIP contains verbiage such as: The Responsible Entity shall maintain documents identifying the organizational, technical and procedural controls for...etc.

**Compliance:** Each section of the CIP contains a compliance section that lists compliance issues and helps an organization determine their level of non-compliance.

### ***Sector specific classes/family***

- ***Authority/Responsibility***

The NERC CIP assigns responsibility to the appropriate management or leadership role throughout. An example is: The Responsible Entity shall assign a senior manager with responsibility for leading and managing the entity's implementation and adherence of the NERC CIP-002 through CIP-009 Standards.

- ***Cyber-security Management System***

The NERC CIP refers to these as Security Management Controls.

- ***Personnel Safety***

Personnel safety is not mentioned specifically in the CIP. However, in the following definition of critical assets, the CIP does mention public health and safety.

Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

- ***Security Policy: Responsible Entities shall document and implement a cyber security policy that defines a structure of relationships and decision-making processes that identify and represent management’s commitment and ability to secure its Critical Cyber Assets.***

### ***Water Sector: AWWA***

The AWWA standard recognizes the need for properly trained employees as it makes several statements concerning what needs to be done. It states that training activities can result in a higher level of cyber security in the workplace and that training sessions help to review security procedures and impart to all employees the importance of individual responsibility.

The training topics specifically mentioned are:

- Don’t share passwords with others
- Don’t write passwords down
- Don’t set up wireless networks or wired connections between networks without authorization
- Password-protect home personal computers (PCs) are to be used to connect to the enterprise
- Train network administrators to analyze server and network log files to pinpoint unauthorized activity
- Training operators should be trained to log out of the HMI whenever leaving the control room to prevent unsupervised access to the SCADA system
- Utilities should instruct employees not to divulge user information—especially passwords—over the telephone
- Employees can be made aware of any authorized need for this information and asked to report any attempt to elicit password information without the proper authorization

This standard does not seem to recognize any of the other excluded classes or families.

### ***Cross Sector - ISA-TR99.00.01-2004***

TR99-01 addresses several requirements that are not addressed in the Framework. For clarification these are grouped below by general areas.

#### ***Data Analysis***

Section 8.4.3 addresses the analysis of control network scanner data.

## ***Testing***

Section 8.4 discusses the importance of regularly testing and monitoring the state of security preparation.

## ***Training***

Sections 10.2.1, 10.2.3, and 10.2.6 address training including training for a particular job function, ensuring that each individual is properly trained, that there is a formal training program, periodic review of training, and the development of training programs.

## ***Sector specific classes/family***

- ***Applications***

Section 9.1.5 addresses ensuring that only the application that saved data can open it.

- ***Organization***

Section 10.2.1 discusses the relationship between an employee and the business organization.

- ***Company Policy***

There are several requirements dealing with company policy. These include: Section 10.2.1 addresses establishing policies on employee issues such as computer use, etc., worker's rights and responsibilities, obtaining employee personal information, background checks, employee behavior and business practices, terms and conditions of employment, and disciplinary policies.

- ***System Isolation***

Section 9.2.6 addresses the need to isolate communication networks used in manufacturing and control systems.

- ***System Capabilities***

Sections 6.1.6 and 9.1.5 address system capabilities such as available disk space, firewalls, and protection of memory to assure that it can not be modified.

- ***Unnecessary Services***

Section 9.1.6 discusses the disabling of any unnecessary services.

- ***Tools***

Sections 8.4.4, 8.4.6, and 8.5 discuss the use of vulnerability scanners on manufacturing and control systems and the use of forensics and analysis tools to gather data on the network.

## **Cross Sector - ISA-TR99.00.02-2004**

TR99-02 addresses several requirements that are not addressed in the Framework. For clarification these are grouped below by general areas.

### ***Risk***

Section 10.2.4, Complete all vulnerability scans, Section 6.6.5, Every business organization should identify its vital information and assets, classify them based on the consequences of loss or failure, assign appropriate levels of security protection, and assess the vulnerability of its Manufacturing and Control Systems to information loss or compromise, Section 7, Define risk goals based on the company's tolerance level to risk, and operational policies that define how security is to be applied to control systems should be developed, Section 8.4, Conduct a full risk analysis. A risk analysis will help to better understand vulnerabilities and the appropriate mitigation strategy to reduce risk, Section 9, Conduct detailed risk analysis vulnerability assessment of the prioritized assets, Section 6.4.1, Define the potential risks for the Manufacturing and Control System.

### ***Sector specific classes/family***

- ***Availability***

Section 6.5 exhaustive pre-deployment testing to ensure high availability of the system and emergency actions should not be hampered by requiring password authentication and authorization.

- ***Business Case***

Section 6.2, In order to obtain funding, it may be necessary to build a business case.

- ***Compliance***

Section 6.6.6, the program team must identify or develop policies on legal and regulatory compliance

- ***Development***

Section 6.6.9, Good security practices must be followed on offline development tools and systems as well.

- ***Goals***

Section 6.4.2, Establish specific goals to address the risks identified.

- ***Logical rights***

Section 6.6.6, the program team must identify or develop policies on logical rights



- ***Media handling***

Section 6.6.8.4, Management of removable or attachable computer media, Disposal of media, Information handling procedures, Security of system documentation, Exchanges of information and software.

- ***Performance***

Section 6.6.8.5, Ensure that all security features, when taken together, do not adversely affect required time-critical system performance and other functions.

- ***Principles***

Section 6.6.4, the security program should develop or identify principles for process control security that balance the needs of both production and corporate security.

- ***Program Tasks***

Section 6.4, plan the basic tasks that must be accomplished in developing an effective program.

- ***Scope***

Section 6.3, Develop a formal scope that should explain clearly what is to be accomplished and when, Section 6.3.1, Assemble the team of people responsible for developing the various program elements, including guidelines, processes, and procedures.

- ***Software updates***

Section 6.5, Security patches cannot always be implemented on a timely basis because software changes need to be thoroughly tested by the vendor of the manufacturing control application and the end user of the application before being implemented.

- ***System assessment***

Section 8, conduct an assessment of the existing system.

- ***Unused resources***

Section 6.6.6, the program team must identify or develop policies on unused resources.

- ***User registration***

Section 6.6.8.2.1, develop policies for user registration.

- ***Virus protection***

Section 10.2.4, Install and configure virus protection software and make sure it is kept current.

## 4. CONCLUSIONS

It is evident that there is a trend toward security awareness in all industries and the need for control system security measures. The companies are burdened, today, to balance the operational considerations and risks with public safety and return an investment to the stakeholders. The need for security presents operators with significant challenges and change control that can ultimately impact the cost of doing business.

The Framework can provide a means of improving understanding within industry of the potential for system disruption. An improved Framework will need to be even more comprehensive and simpler for the industry to adopt. Chemical industry members are striving hard to make the control systems as safe and secure as they can be. They will continue to develop and improve the standards used by these operators, just as the operators will continue to create and revise their proprietary security plans.

### 4.1 Chemical Sector: CIDX Cyber-security Standard

The gaps in the CIDX cyber-security standard relative to the requirements of the Framework mentioned here are occasioned by a difference in design philosophies, operational considerations, corporate risk profile, and policies, rather than by neglect. The CIDX cyber-security standard provides best practices and guidance related elements of cyber-security protection steps and awareness to include in corporate policies, procedures, and practices.

Based on the analysis of the CIDX cyber-security standard and comparison to the Framework Requirements, the chemical industry could benefit from incorporating in the standard statements that fill the identified requirements gaps, as follows:

- Potential Violation Analysis – The CIDX standard should include automated means of analyzing system activity and auditing data for possible or real security violations. This analysis may work in support of intrusion detection or automatic response to an imminent security violation.
- Identification and Authentication Rules – The CIDX standard can benefit by incorporating guidelines from the Framework for single-use authentication mechanisms that require an authentication mechanism to operate with single-use authentication data. This should include stringent creation-of-password requirements at all user levels.
- Security Management – The CIDX standard can improve procedures that allow authorized users (roles) control over the management of TSF data. Examples of TSF data include audit information, clock, system configuration and other TSF configuration parameters.
- Trusted Security Function – The CIDX standard can benefit by employing rules to detect replay for various types of entities (e.g., messages, service requests, service responses) and subsequent actions to correct from replay actions. The system should also be designed to protect TSF from external interference and

tampering (e.g., by modification of TSF code or data structures) by an un-trusted entity.

## **4.2 Energy - Natural Gas Sector: AGA Report Number 12**

It is likely that many or most of the gaps identified here are due to the fact that AGA 12, Part 1, is a background document addressing general requirements and approaches to protecting SCADA communications. Much of the document is informative not normative.

The informative portions address a very real need within industry by providing at least some of the background information needed to understand current threats to SCADA communications and approaches to mitigate those threats. However, they do not provide requirements suitable for a gap analysis.

The normative portions often do address specific Framework issues and are, therefore, conducive to comparison and analysis. But AGA 12 must ultimately be evaluated as a whole. Part 1 is only the first of several documents, and much of the detail required to implement its recommendations is forthcoming.

Although the effort to produce AGA 12 officially began in 2001, the first of its many parts is still in draft in 2005. This is due to the actual scope of the document, which belies its own statement of focus on page 1 of Part 1:

*“The focus of AGA 12 is to address the single issue of cryptographically protecting SCADA communications traversing unsecured communication links. While AGA 12 focuses only on a single aspect of the total security picture, the report authors fully expect that other groups will address the many other dimensions of the security issues.”*

AGA 12, Part 1, addresses many of those other dimensions at length. Moreover, it is quite possible that the practices recommended to protect SCADA communications against cyber attack are also excessive. Page 1 of Part 1 contains a succinct design statement:

*“The recommended practices are designed to provide confidential SCADA communications that are known to be unaltered by potential attackers and that can be authenticated as having originated from valid authorized users.”*

Widely recognized experts in cyber security and cryptography have pointed out that confidentiality may not be required to protect SCADA communications against cyber attack. While a business case might be made for keeping SCADA communications confidential, this has not been an industry priority, given the long-standing practice of plaintext transmissions.

The current priority is protecting the nation’s critical infrastructure from cyber attack. Removing confidentiality from the AGA 12 design goals and focusing more narrowly on

authentication and integrity would likely simplify the problem and expedite practical solutions.

### **4.3 Energy - Petroleum & Oil Sector: API Standard Number 1164**

It may well be that the gaps in API Standard Number 1164 (relative to the requirements of the Framework) mentioned here are occasioned by a difference in design philosophy, rather than by neglect. API Standard Number 1164 focuses on defining the responsibilities of authority personnel, and also on prescribing the conditions for gaining access to the system. It lists the processes used to identify and analyze the SCADA system vulnerabilities to attacks, and provides a comprehensive list of practices intended to harden the core architecture. In the section on Personnel Security Standards, it addresses numerous procedures aimed at minimizing insider intrusions. For the most part, API Standard Number 1164 does not address the contingencies for preventing or minimizing losses due to security failures. It appears to focus on preventing system compromise, in which case control of losses may be less of a concern. The Framework takes such intrusions into consideration, and significant portions of its requirements are aimed at minimizing losses from intrusions.

Nevertheless, API Standard Number 1164 could be improved by the inclusion of specific requirements pertaining to detecting and countering intrusions. Some of these are:

- Include a section detailing the use of security alarms. This would appear to be basic for such a standard. Certainly, any SCADA system currently in use incorporates them as a routine part of day-to-day operations.
- Discuss the steps to be taken when an intrusion actually occurs. This would provide an operator with a rational defensive procedure.
- Although it is a more complex procedure, the standard should detail which event types to track in order to anticipate potential system attacks. It should also provide guidelines for responding when the potential for an attack has been identified.
- Finally, as API Standard Number 1164 already recommends or requires encryption for certain activities, it should provide some documentation as to the level of encryption required. It could do this by reference to existing outside documents. Examples of such documents include:
  - FIPS PUB 46-3, The Data Encryption Standard (DES)
  - FIPS PUB 197, The Advanced Encryption Standard (AES)
  - AGA Report Number 12, Cryptographic Protection of SCADA Communications.

In summary, API Standard Number 1164 is a very useful tool for all entities within the energy industries that operate SCADA systems. It provides them with a comprehensive

guideline for developing a control system security program that is tailored precisely to their own needs.

It is the output of an industry-supported body that expects to continue revising and upgrading the details of the standard. As new versions are released, it will no doubt become widely accepted as a resource for use when designing or revising corporate security plans.

#### **4.4 Transportation-Rail Sector**

Many of the gaps identified in this report for the transportation sector are due to the differences in the intent of the requirements listed in the Framework and those in the transportation standard. Although the transportation standard is prescriptive in nature, the security needs of a transportation control system are very different from those of a chemical plant or electrical distribution system control system. The transportation standard addresses specific requirements that are specific to railroad control systems.

The control systems for a railroad are mainly manned systems, and the automatic portion is there mainly to provide assistance to the operator, rather than to provide independent control of the system.

The railroad system does not use the internet for transmission of control signals to the same extent as some other sectors and, hence, is not as open to security problems at the present. This situation will probably change as the control systems mature.

Although the transportation sector standard reviewed for this effort is aimed at a very different operation, it could still be improved by considering some of the areas addressed in the Framework requirements. It is not apparent that this standard was prepared with any consideration of the type of actions seen recently in which others are trying to gain access to the control system. Although not all of the requirements would be applicable, many should be reviewed and considered in order to provide a more secure transportation system.

#### **4.5 Cross Sector ISA-TR99.01 and 02-2004**

The gaps identified between the cross-sector standards and the Framework requirements are due to differences in the intent of the two sets of documents. The cross-sector standards are, in fact, technical reports whose intent is to provide guidance, while the Framework requirements are meant to be prescriptive.

In addition, the requirements in the Framework are based on the Common Criteria. The purpose of the Common Criteria is to provide requirements for components. The guidance presented in the cross-sector standard is aimed at systems rather than components, thus, there is an entirely different perspective between the two documents.

Although there are differences in the intent of the two sets of documents, there are areas of commonality that should be carefully reviewed by the respective standards organizations to determine if there are truly gaps in the requirements.

#### **4.6 Energy - Electric Power Sector: NERC CIP**

The following text is taken directly from the NERC CIP Standard:

*NERC Standards CIP-002 through CIP-009 provide a cyber security Framework identifying and assisting with the protection of Critical Cyber Assets to ensure reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.*

Business and operational demands for managing and maintaining a reliable bulk electric system increasingly require cyber assets to support critical reliability functions and processes by which the cyber assets communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets.

This standard requires the identification and enumeration of the critical cyber assets that support reliable operation of the bulk electric system. These critical cyber assets are identified through the application of a risk-based assessment procedure.

The standard is quite strong when detailing what needs to be identified and enumerated. Like most standards it is written at a high level and avoids specific technical implementation details. For example, biometric authentication is mentioned, but a specific solution suggesting finger print readers is not. The standard is written with requirements, measurements, and compliance issues all clearly identified for each section.

#### **4.7 Telecommunications Sector: ANSI T1.276**

Telecommunications represents a broad industry that delivers a wide variety of services. These services require the implementation of a diverse set of communication technologies. As such, it is perhaps unrealistic to expect that an all encompassing security standard can be promulgated for the telecommunications management plane, as a whole.

The main body of T1.276 provides extensive guidance relating to cryptographic algorithms and keys, authentication, and architectural considerations that could be implemented across a wide variety of telecommunication technologies. No requirements are delineated for conducting risk assessments, establishing security policies, or establishing a security management infrastructure. Annex B, however, does provide “guidance” regarding these issues.

Most of the requirements delineated in T1.276 could be matched to some degree to similar Framework requirements. The primary differences between T1.276 and Framework requirements were, typically, that T1.276 requirements were more specific.

The list of T1.276 and the Framework requirements both essentially excluded requirements relating to the various aspects of developing and establishing a formal security management infrastructure. Although T1.276 Annex B discusses a number of issues relating to security management, requirements are not explicitly delineated in the main body of the standard.

#### **4.8 Water Sector: AWWA**

The American Water Works Association's Security Guidance for Water Utilities document was developed to address a number of unpredictable acts that could hinder the operations of water utilities. Section 5, *Cyber Security Management, Operations, and Design Considerations*, is focused specifically on acts that affect the operations and cyber security of a utility's process control systems. While this document has been reviewed by the WISE Standards Committee and various AWWA utilities, none of its language provides any indication that PCS in the water sector require any special or additional requirements outside the already accepted enterprise networks security requirements for proper operations.

## 5. NEXT STEPS

This task has focused on identifying gaps between a limited set of standards relating to several of the critical infrastructure sectors and a framework derived from the Common Criteria. This is only the first step in a process which will require examining additional standards and refining the gap analysis process.

The gaps identified in this report fall into three categories: 1) actual gaps in the standards reviewed; i.e., information that should have been in the standard but was left out through oversight or misunderstanding, 2) information, although pertaining to cyber security, was beyond the identified scope of the standard reviewed, and 3) misunderstanding or mistakes of the reviewer of the standard. Although some of the gaps identified fall into categories 2 or 3, this information may still be of value to the standards bodies in that it may represent areas that need clarification in the standard. In order for this information to be useful, it must be communicated to the various standards bodies, since they are the only ones that can modify the standards. This will require that the standards assessment team communicate these findings to the standards bodies through participation in selected user group meetings and standards committees, and by presenting the information in technical papers or other communication media.

Because of the scope of this work, it is important that there be a group to coordinate the understanding of control system standards between the various critical infrastructure sectors, industries, and government bodies. This group would leverage the understanding gained to increase the effectiveness of the standards comparison efforts.

In addition to assisting the standards bodies in producing better standards, this continued effort will assist the DHS in identifying areas where additional work is needed and in producing strategic recommendations for enhanced cyber security standards development. These results, when used in conjunction with the published Framework requirements, will provide the control system community with the ability to better evaluate the level of security needed and how to achieve that level.

Because of the limited nature of this first effort, the task will need to be expanded to include other standards within the sectors already addressed, as well as sectors not addressed to date. There are a great many standards dealing with cyber security, therefore, it will be necessary to identify those that have the greatest use and potential impact on the industry.



## 6. REFERENCES

### Telecommunications Sector

ANSI standard T1.276-2003 *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*, Alliance for Telecommunications Industry Solutions, 1 July 2003, <http://www.ansi.org/>

### Energy - Natural Gas Sector

AGA Report Number 12, *Cryptographic Protection of SCADA Communications Part 1: "Background, Policies and Test Plan"* (Draft 5), American Gas Association, 14 April, 2005, <http://www.aga.org/>

### Energy – Petroleum & Oil Sector

API Standard Number 1164, First Edition, *Pipeline SCADA Security*, American Petroleum Institute, September 2004, <http://api-ec.api.org/newsplashpage/index.cfm>

### Chemical Sector

*Guidance for Addressing Cybersecurity in the Chemical Sector*, Version 2.0, Chemical Industry Data Exchange, December 2004, <http://www.cidx.org/>

### Transportation-Rail Sector

*Standards for Development and Use of Processor-Based Signal and Train Control Systems; Final Rule*, 49 CFR Parts 209, 234, and 236, Department of Transportation, Federal Railroad Administration, March 7, 2005, <http://www.fra.dot.gov/>

### Energy - Electric Power Sector

NERC CIP Standards, CIP-002-1 through CIP-009-1, *Cyber Security*, Draft 3, North American Electric Reliability Council, 9 May 2005, <http://www.nerc.com>

### Water Sector

American Water Works Association's *Security Guidance for Water Utilities Section 5: Cyber Security Management, Operations, and Design Considerations* [http://www.awwa.org/science/wise/report/AWWA\\_Securities/Section5.htm](http://www.awwa.org/science/wise/report/AWWA_Securities/Section5.htm)

### Cross Sector

ISA-TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems, Instrumentation, Systems, and Automation Society*, March, 2004, <http://www.isa.org/>

ISA-TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control Systems, Instrumentation, Systems, and Automation Society*, April, 2004, <http://www.isa.org/>

## General

National Institute of Standards, *System Protection Profile – Industrial Control Systems*, Decisive Analytics, Version 1.0, April 14, 2004.

<http://csrc.nist.gov/secpubs/rainbow/>

National Institute of Standards, *System Protection Profile – Industrial Control Systems*, Decisive Analytics, Version 1.0, April 14, 2004,

<http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2>

Decisive Analytics, *An Enhanced ISO/IEC 15408 Standard for Systems Security Specification and Evaluation*, Version 1.0, May 12, 2004.

## Appendix A: Synopsis of Comparison Results

### 3.0

	Cryptographic Support	
	Cryptographic Key Management	Cryptographic Operation
Chemical	○	○
Natural Gas	●	●
Petroleum & Oil	○	○
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	●	○
Cross-Sector ISA TR99-02	●	○
Electrical Power	○	○
Telecommunications	●	●
Water	○	○

○ = Gap      ○ = Partial Match      ● = Match

### 3.1

	Security Audit					
	Security Alarms	Audit Data Generation	Potential Violation Analysis	Audit Review	Selective Audit	Potential Audit Trail Storage
Chemical	○	○	○	○	○	○
Natural Gas	○	○	○	○	○	○
Petroleum & Oil	○	●	○	●	○	○
Transportation – Rail	○	○	○	○	○	○
Cross-Sector ISA TR99-01	●	○	○	○	○	○
Cross-Sector ISA TR99-02	●	○	○	○	○	○
Electrical Power	●	●	●	●	○	○
Telecommunications	○	○	○	○	○	○
Water	○	○	○	○	○	○

○ = Gap      ○ = Partial Match      ● = Match

### 3.2

	Configuration Management	Security Alarms
Chemical		○
Natural Gas		○
Petroleum & Oil		●
Transportation – Rail		○
Cross-Sector ISA TR99-01		○
Cross-Sector ISA TR99-02		○
Electrical Power		●
Telecommunications		○
Water		○

○ = Gap      ○ = Partial Match      ● = Match

### 3.3

	Cryptographic Support Cryptographic Key Management	Cryptographic Operation
Chemical	○	○
Natural Gas	●	●
Petroleum & Oil	○	○
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	●	○
Cross-Sector ISA TR99-02	●	○
Electrical Power	○	○
Telecommunications	●	●
Water	○	○

○ = Gap      ○ = Partial Match      ● = Match

### 3.4

	User Data Protection				
	Subset Access Control	Security Attribute Based Access Control	Data Authentication with Identity of Generator	Export of User Data Without Security Attributes	Subset Information Flow Channel
Chemical	●	●	○	○	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	●	●	○	○	○
Telecommunications	○	○	○	○	○
Water	○	○	○	○	○

	Simple Security Attributes	Data Exchange Integrity
Chemical	○	●
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	○	○
Telecommunications	○	○
Water	○	○

○ = Gap

○ = Partial Match

● = Match

### 3.5

#### Event Definition

#### Security Alarms

Chemical	●
Natural Gas	○
Petroleum & Oil	●
Transportation – Rail	○
Cross-Sector ISA TR99-01	○
Cross-Sector ISA TR99-02	○
Electrical Power	●
Telecommunications	○
Water	●

○ = Gap

◐ = Partial Match

● = Match

### 3.6

#### Identification and Authentication

	Authentication Failure Handling	User Attribute Definition	Verification of Passwords	Timing of Authentication	Timing of Identification
Chemical	●	○	○	◐	◐
Natural Gas	○	○	◐	◐	◐
Petroleum & Oil	◐	●	●	◐	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	●	○	○
Cross-Sector ISA TR99-02	○	○	●	○	○
Electrical Power	●	○	●	◐	○
Telecommunications	◐	○	●	◐	●
Water	○	○	◐	○	○

○ = Gap

◐ = Partial Match

● = Match

### 3.7

	Security Management				
	Management of Security Functions Behavior	Management of Security Attributes	Management of Security Function Data	Access Revocation	Time-limited Authorization
Chemical	○	○	○	●	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	○	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	●	●	○	○	○
Telecommunications	●	○	○	○	○
Water	○	○	○	○	○

	Specification of Management Functions	Security Roles
Chemical	●	○
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	○	○
Telecommunications	○	○
Water	○	○

○ = Gap

○ = Partial Match

● = Match

### 3.8

#### Protection of Trusted Security Functions

	Failure with Preservation of Secure State	Availability with a Defined Availability Metric	Confidentiality during Transmission	Detection of Modification	Passive Detection of Physical Attack
Chemical	○	○	○	○	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	○	○	○	○	●
Telecommunications	○	○	○	○	○
Water	○	○	○	○	○

	Automated Recovery	Replay Detection	Domain Separation	Strength of Boundary Access Control	Simple Trusted Acknowledgement
Chemical	○	○	○	○	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	●	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	○	●	○	●	○
Telecommunications	○	○	○	○	○
Water	○	○	○	○	○

	Reliable Time Stamps	Data Consistency	Internal Consistence
Chemical	○	○	○
Natural Gas	○	○	○
Petroleum & Oil	●	●	●
Transportation – Rail	○	○	○
Cross-Sector ISA TR99-01	○	○	○
Cross-Sector ISA TR99-02	○	○	○
Electrical Power	○	○	○
Telecommunications	●	○	○
Water	○	○	○

○ = Gap

○ = Partial Match

● = Match



### 3.9

	Resource Utilization	
	Degraded Fault Tolerance	Limited Priority of Service
Chemical	●	●
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	●	○
Telecommunications	○	○
Water	●	○

○ = Gap      ● = Partial Match      ● = Match

### 3.10

#### Target Access

	Target Access	
	Session Locking	Session Establishment
Chemical	●	●
Natural Gas	○	○
Petroleum & Oil	●	●
Transportation – Rail	○	○
Cross-Sector ISA TR99-01	○	○
Cross-Sector ISA TR99-02	○	○
Electrical Power	○	○
Telecommunications	●	●
Water	○	○

○ = Gap      ● = Partial Match      ● = Match

### 3.11

Trusted Path and Channel

	Trusted Channel	Mutually Trusted Acknowledgement	Trusted Path
Chemical	●	●	●
Natural Gas	●	○	○
Petroleum & Oil	●	●	●
Transportation – Rail	○	○	○
Cross-Sector ISA TR99-01	●	○	●
Cross-Sector ISA TR99-02	●	○	●
Electrical Power	○	○	○
Telecommunications	○	○	○
Water	●	○	●

○ = Gap                      ● = Partial Match                      ● = Match