

i n v e n s y s

NUCLEAR QUALIFIED PRODUCTS

Non -Proprietary copy per 10CFR2.390
- Areas of proprietary information have been redacted.
- Designation letter corresponds to Triconex proprietary
policy categories (Ref. transmittal number TCXNRC-
09-01, Affidavit, Section 4.)

LICENSING TOPICAL REPORT

7286-545-2-NP

Revision 0

INVENSYS CYBER SECURITY PROGRAM PLAN

(Non-Proprietary Version)

Issue Date: August 31, 2009

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	2 of 44

TABLE OF CONTENTS

1. INVENSYS CYBER SECURITY	3
1.1 EXECUTIVE SUMMARY	3
1.2 BACKGROUND AND OVERVIEW	3
1.3 OBJECTIVE	6
1.4 SCOPE.....	6
1.5 PROGRAM DESCRIPTION.....	7
1.6 INVENSYS APPROACH.....	8
1.6.1 <i>Invensys Licensing Position</i>	8
1.6.2 <i>Invensys Summary for RG 1.152, Rev 2, for Engineering Development Projects</i>	8
1.6.3 <i>Invensys Summary for RG 1.152, Rev 2, for System Application Projects</i>	12
1.7 ACRONYMS, ABBREVIATIONS, AND DEFINITIONS.....	17
2. REGULATORY REQUIREMENTS, GUIDELINES, AND INDUSTRY STANDARDS AND SUPPORTING DOCUMENTS.....	18
2.1 SUPPORTING DOCUMENTS.....	18
2.2 CODES AND STANDARDS	18
2.2.1 <i>Regulatory Guide and Interim Staff Guidance</i>	18
2.2.2 <i>NUREG</i>	18
2.2.3 <i>Branch Technical Positions</i>	18
2.2.4 <i>Nuclear Energy Institute (NEI)</i>	19
2.2.5 <i>Code of Federal Regulations (CFR)</i>	19
2.2.6 <i>Institute of Electrical and Electronics Engineers (IEEE)</i>	19
2.3 SUPPLEMENTAL DOCUMENTS.....	19
2.4 CORRESPONDENCE	19
3. INVENSYS CYBER SECURITY PROGRAM MANAGEMENT	21
3.1 ROLES AND RESPONSIBILITIES	21
3.2 POLICIES AND PROCEDURES	22
3.3 INVENSYS CYBER SECURITY DEFENSIVE MODEL.....	23
3.4 TRAINING AND AWARENESS.....	25
3.4.1 <i>User Awareness Training</i>	25
3.4.2 <i>Specialized Cyber Security Training</i>	26
3.5 CONTINGENCY AND INCIDENT RECOVERY	26
3.6 PERIODIC THREAT ASSESSMENT	26
3.7 PERIODIC PROGRAM ASSESSMENT	26

LIST OF FIGURES

Figure 3-1 Defensive Model for Nuclear Delivery Projects,	25
---	----

APPENDICES

APPENDIX A - DEFINITIONS.....	28
APPENDIX B - CYBER SECURITY PLAN CONFORMANCE REVIEW	40
APPENDIX C - ACRONYMS AND ABBREVIATIONS	43

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 3 of 44

1. INVENSYS CYBER SECURITY

1.1 Executive Summary

The increasing use of computers for various functions at nuclear facilities brings forth new technical challenges that must be addressed in a rigorous and balanced manner. Digital computers in nuclear power plants are used in safety-related and non-safety systems, where non-availability or malfunction could affect nuclear safety and continuity of power. These computers are also used in the control of access to sensitive areas, where their malfunction could adversely impact access control. Computers are also used to store important and sensitive data, where malfunction could lead to the loss or unavailability of data. As the complexity of these computer systems increases comprehensive methods to assure computer system dependability need to be employed.

Invensys will implement a Cyber Security Program to support an appropriate level of protection against cyber security risks throughout the complete life cycle of the digital computer systems.

This program plan should be used in conjunction with the policy and guidance provided by United States NRC Regulatory Guide 1.152 [2.2.1(1)], which includes guidance criteria for cyber security of computers in safety systems used in nuclear power plants, as well as DI&C-ISG-01, Cyber Security [2.2.1(2)].

This plan document provides an avenue to evaluate existing programs, model desired defensive strategies, assess critical digital assets, and identify appropriate risk reduction measures. The goal of this document is to accomplish a continuing program that maintains the desired level of cyber protection for Invensys products and systems. This document does not specify a specific set of mitigation measures. In contrast, the program presented in this document is process-oriented. It is designed to support the need for different security levels of protection for various facility functions. The operation of a nuclear-related facility offers unique challenges that separate it from other industrial complexes as well as from a nominal information technology (IT) computer security program. This program will provide a basis for licensees to incorporate Invensys delivered products into their cyber security program under 10CFR73.54.

1.2 Background and Overview

Security is a computer system property that to be effective must be addressed during the development of digital safety systems, in order to either preclude cyber attacks or preserve the safety functions during a cyber attack.

Invensys is a supplier of safety-related systems to nuclear licensees. Invensys has created nuclear safety design and quality processes (e.g., software quality assurance programs) that comply with applicable NRC regulations. As a supplier to nuclear licensees, Invensys must

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 4 of 44

provide products that satisfy customer (i.e., licensee) requirements, which, in turn, must comply with NRC regulations and guidance. As such, the Invensys Cyber Security Program has two facets. First, the program will protect Invensys infrastructure to maintain integrity of Invensys' nuclear design and quality processes. Therefore, the design environment will be protected against compromise from internal and external threats. Second, the program will ensure delivered products comply with NRC cyber security requirements to support licensee compliance for the same requirements when Invensys-delivered systems are installed and operated at licensee facilities.

a, b, f

General Design Criterion (GDC) 21, "Protection System Reliability and Testability", of Appendix A, "General Design Criteria for Nuclear Power Plants", to Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities", of the Code of Federal Regulations (10 CFR Part 50), states in part that "the protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed." Criterion III, "Design Control", of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants", to 10 CFR Part 50, requires, among other things, that quality standards must be specified and design control measures must be provided for verifying or checking the adequacy of design. Thus, it is necessary to secure the development environment and to ensure that adequate security features are built into the design of computer-based systems to minimize the risk of failure to maintain cyber security for such systems.

Conformance with the requirements of IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. However, IEEE Std 7-4.3.2-2003 does not provide guidance regarding security measures for computer-based system equipment and software systems. Consequently, the NRC developed Regulatory Positions that provide specific guidance concerning computer-based (cyber) safety system security.

The Nuclear Energy Institute (NEI) issued NEI 04-04, Rev 1, "Cyber Security Program for Power Reactors", November 18, 2005, regarding cyber security guidance for safety-related digital instrumentation and control systems. NRC Staff Guidance DI&C-ISG-01, Rev 0,

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 5 of 44

December 2007, Task Working Group (TWG) on Cyber Security, stated there were no major inconsistencies between RG 1.152, Rev 2 and NEI 04-04, Rev 1. It also indicated that the TWG analysis indicates that guidance in Regulatory Positions 2.1-2.9 of RG 1.152, Rev 2, complements the NEI programmatic guidance in NEI 04-04, Rev 1. NEI also issued draft NEI 04-04, Rev. 2, “Cyber Security Program for Power Reactors”, August 2007. However, ISG-01 indicated that NRC’s review of NEI 04-04, Rev. 2 had not been completed and that ISG-01 did not constitute formal acceptance of NEI 04-04, Rev 2.

Regulatory Guide (RG) 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”, Rev. 2, January 2006, provides cyber security criteria for development and implementation of protection measures for digital instrumentation and controls used in safety system applications. It also addresses aspects of the implementation of cyber security that were not adequately covered in IEEE Std 7-4.3.2-2003. RG 1.152 Rev 2, describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) deems acceptable for complying with the Commission’s regulations for promoting high functional reliability, design quality, and cyber-security for the use of digital computers in safety systems of nuclear power plants. In this context, the term “computer” is a system that includes computer hardware, software, firmware, and interfaces.

Branch Technical Position 7-14, Rev 5, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” March 2007, also contains relevant information. This document provides NRC staff review guidelines for evaluating software lifecycle processes associated with safety-related digital systems. It also addresses characteristics that should be present within an acceptable software management plan, e.g., that licensees should provide a description of the methods employed to prevent corruption of the software by viruses, Trojan horses, or other malicious intrusions. This is addressed in appropriate Invensys software control and testing procedures, as well as quality procedures.

As indicated above, RG 1.152 Rev 2 describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) deems acceptable for complying with the Commission’s regulations for promoting high functional reliability, design quality, and cyber-security for the use of digital computers in safety systems of nuclear power plants. Therefore, the Invensys Cyber Security Program will focus on the technical and programmatic guidance on cyber security provided in RG 1.152, Rev 2.

RG 1.152 uses the waterfall lifecycle phases as a framework for describing specific digital safety system security guidance and states that the digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle.

The framework waterfall lifecycle consists of the following phases:

- Concepts
- Requirements
- Design
- Implementation

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	6 of 44

- Test
- Installation, Checkout, and Acceptance Testing
- Operation
- Maintenance
- Retirement

Accordingly, this Program Plan will be structured to reflect cyber security in relationship to this lifecycle framework.

1.3 Objective

This Program Plan is intended to be a top-tier basis and high-level implementation guide for the Invensys Cyber Security Program, per RG 1.152. The primary goals of the program are to:

-

a, b, f

1.4 Scope

This Program Plan defines the requirements for the development and management of an effective Invensys Cyber Security Program. The program scope addresses the policies, procedures, and tools to manage the cyber security risk of Invensys-delivered nuclear safety-related systems. It is intended that the program will address security of the design as well as the implementation environment within Invensys infrastructure.

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	7 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	8 of 44

a, b, f

1.6 Invensys Approach

This section describes Invensys overall approach relative to the implementation of the Invensys Cyber Security Program.

1.6.1 Invensys Licensing Position

Invensys will follow the guidance in NRC Regulatory Guide 1.152, Rev. 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, January 2006, when implementing the Invensys Cyber Security Program. The table in Appendix B provides details on specific commitments to Regulatory Guide 1.152, Rev. 2.

a, b, f

1.6.2 Invensys Summary for RG 1.152, Rev 2, for Engineering Development Projects

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	9 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	10 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	11 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	12 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	13 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	14 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	15 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	16 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	17 of 44

a, b, f

1.7 Acronyms, Abbreviations, and Definitions

Acronyms and abbreviations are defined in Appendix C. Definitions for terms used in this Plan are provided in Appendix A, Glossary of Terms.

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 18 of 44

2. REGULATORY REQUIREMENTS, GUIDELINES, AND INDUSTRY STANDARDS AND SUPPORTING DOCUMENTS

This section includes applicable supporting and supplemental documents; requirements, guides, codes and standards; and correspondence. Supporting documents provide inputs and relevant information to this Plan, and along with Supplemental documents, are used in conjunction with this Plan,

2.1 Supporting Documents

The following supporting documents are used as controlling documents in the production of this Plan:

Document Title

1. Engineering Department Manual (EDM) Rev 37, June 29, 2009
2. Project Procedures Manual (PPM) Rev 21, June 29, 2009
3. Quality Procedures Manual (QPM) Rev 60, August 10, 2009

2.2 Codes and Standards

The following codes and standards are applicable to the activities specified within this Plan.

2.2.1 Regulatory Guide and Interim Staff Guidance

1. Regulatory Guide (RG) 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," January 2006.
2. Interim Staff Guidance, Revision 0, Digital Instrumentation and Controls, DI&C-ISG-01, "Task Working Group #1: Cyber Security", December, 2007.
3. Interim Staff Guidance, Revision 1, Digital Instrumentation and Controls, DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc)," March 2009.

2.2.2 NUREG

1. NUREG/CR-6847, PNNL-14766, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants"

2.2.3 Branch Technical Positions

1. Branch Technical Position HICB 7-14 Rev. 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, March 2007.

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 19 of 44

2.2.4 Nuclear Energy Institute (NEI)

1. NEI 04-04, Revision 1, “Cyber Security Program for Power Reactors”, November 18, 2005.
2. NEI 04-04, Revision 2, “Cyber Security Program for Power Reactors”, August 2007.

2.2.5 Code of Federal Regulations (CFR)

1. 10 CFR 2.390, “Public Inspections, Exemptions, Request for Withholding.”
2. 10 CFR Parts 50 and 52, “Domestic Licensing of Production and Utilization Facilities.”
3. 10 CFR Part 73.55, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.”
4. 10 CFR Part 73.54, “Protection of Digital Computer and Communication Systems and Networks.”

2.2.6 Institute of Electrical and Electronics Engineers (IEEE)

1. IEEE Std. 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations.
2. IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” December 19, 2003.

2.3 Supplemental Documents

a, b, f

2.4 Correspondence

1. Letter from Mr. Roy P. Zimmerman (NRC - Director, Office of NSIR) to Mr. Michael T. Coyle (NEI – VP Nuclear Operation, Nuclear Generation Division);

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	20 of 44

Subject: NRC Acceptance of NEI 04-04, "Cyber Security Program for Power Reactors," Revision 1; dated December 23, 2005 (ML053320256).

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	21 of 44

3. INVENSYS CYBER SECURITY PROGRAM MANAGEMENT

This section describes the program management components that will be evaluated to lay the foundations for an effective and continuing cyber security program, as described in section 1.5, including potential roles and responsibilities to carry out the program.

3.1 Roles and Responsibilities

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	22 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	23 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	24 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	25 of 44

a, b, f

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	26 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	27 of 44

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	28 of 44

APPENDIX A - Definitions

This section defines the terms and abbreviations generally used in reference to Cyber Security. A number of these terms and definitions are used within this document. This list is to be used as a reference for the creation of the supporting documents. This is not a conclusive list of terms and may be updated at anytime. It should be considered a subset of current cyber security programs.

Term	Definition
Access	The ability and means to communicate with or otherwise interact with a system in order to use system resources
Access Control	The protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy [1]
Accountability	The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions [1]
Application	A software program that performs specific functions initiated by a user command or a process event and that can be executed without access to system control, monitoring, or administrative privileges [2]
Area	A subset of a site’s physical, geographic, or logical group of assets <i>NOTE: An area may contain manufacturing lines, process cells, and production units. Areas may be connected to each other by a site local area network and may contain systems related to the operations performed in that area.</i>
Asset	Any tangible or intangible object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization
Attack	Assault on a system that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system [1]

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	29 of 44

Term	Definition
Authorization	A right or a permission that is granted to a system entity to access a system resource [1]
Availability	The probability that an asset will be able to fulfill its required function at a given point in time. System availability is related to readiness for usage.
Communication Path	Logical connection between a source and one or more destinations, which could be devices, physical processes, data items, commands, or programmatic interfaces <i>NOTE: The communication path is not limited to wired networks, but includes other means of communication such as memory, procedure calls, and state of physical plant, portable media, and human interactions.</i>
Communication Security	(1) Measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities (2) State that is reached by applying security services, in particular, confidentiality, integrity, and authentication <i>NOTE: This phrase is usually understood to include cryptographic algorithms and key management methods and processes, devices that implement them and the life-cycle management of keying material and devices. However, cryptographic algorithms and key management methods and processes may not be applicable to some control system applications.</i>
Communication System	Arrangement of hardware, software, and propagation media to allow the transfer of messages (ISO/IEC 7498 application layer service data units) from one application to another
Compromise	The unauthorized disclosure, modification, substitution, or use of information (including plaintext cryptographic keys and other critical security parameters) [4]
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices [2]

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 30 of 44

Term	Definition
Continuity of Power	Those systems having a direct immediate impact on continuity of operation, the ability to generate electric power. They are systems that may cause an immediate reactor trip or systems that are required by regulations for personal safety and other commitments that would force a decision to shut down the plant. [6]
Control Equipment	A class that include distributed control systems, programmable logic controllers, associated operator interface consoles, and field sensing and control devices used to manage and control the process <i>NOTE: The term also includes field bus networks where control logic and algorithms are executed on intelligent electronic devices that coordinate actions with each other.</i>
Control Network	Those networks that are typically connected to equipment that controls physical processes and that is time critical (See “ <i>safety network</i> ”) <i>NOTE: The control network can be subdivided into zones, and there can be multiple separate control networks within one company or site.</i>
Countermeasure	An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken [1]
Critical Digital Asset	A digital device or system that plays a role in the operation or maintenance of a critical system that can impact the proper functioning of that critical system. A CDA may be a component or a subsystem of a critical system; the CDA may be itself a critical system; or the CDA may have a direct or indirect connection to a critical system. Direct connections include both wired and wireless communications pathways. Indirect connections include pathways by which data or software is manually carried from one digital device to another and transferred using disks or other modes of data transfer. [6]
Critical System	Any system that is important to safety or defined as within scope of this procedure. [6]

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	31 of 44

Term	Definition
Defense-In-Depth	<p>The integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program.</p> <p><i>NOTE: Defense in depth implies layers of security and detection, even on single systems, and provides the following features:</i></p> <p><i>attackers are faced with breaking through or bypassing each layer without being detected</i></p> <p><i>a flaw in one layer can be protected by capabilities in other layers</i></p> <p><i>system security becomes a set of layers within the overall network security</i></p>
Demilitarized Zone	<p>A perimeter network segment that is logically between internal and external networks [2]</p> <p><i>NOTE: The purpose of a demilitarized zone is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks.</i></p> <p><i>NOTE: In the context of industrial automation and control systems, the term "internal network" is typically applied to the network or segment that is the primary focus of protection. For example, a control network could be considered "internal" when connected to an "external" business network.</i></p>
Denial of Service	<p>The prevention or interruption of authorized access to a system resource or the delaying of system operations and functions [1]</p>
Distributed Control System	<p>A type of control system in which the system elements are dispersed but operated in a coupled manner, generally with coupling time constants much shorter than those found in SCADA systems</p> <p><i>NOTE: Distributed control systems are commonly associated with continuous processes such as electric power generation; oil and gas refining; chemical, pharmaceutical and paper manufacture, as well as discrete processes such as automobile and other goods manufacture, packaging, and warehousing.</i></p>

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 32 of 44

Term	Definition
Emergency Response Digital Assets	<p>Emergency response digital assets are limited to those digital assets that are vital to successful implementation of the Emergency Plan. Operation of these assets is controlled by emergency plan procedures. Commercial digital assets such as EOF HVAC controls, EOF building security systems, the commercial phone system, copiers, and fax machines are not under a configuration control program and are not identified. These commercial components are not critical to successful implementation of the Emergency Plan.</p> <p><i>NOTE: The scope of Emergency Plan digital assets is limited to those unique aspects of the Emergency Plan. The sensors that provide data used in calculating offsite release, the sensors that provide data to the ERDS for transmittal of data to the NRC, and the plant monitoring system are evaluated as part of safety related, "important to safety," and continuity of power assets. All sensors used to determine Emergency Action Levels (EAL) are within the scope of the cyber security plan.</i></p>
Failure Mode and Effects Analysis	<p>A tabular method of providing traceability from the modes by which a system may fail and the effect of that failure on the ability of the system to perform its function, or the ability of a collection of systems to recover from the failure.</p>
Field I/O Network	<p>The communications link (wired or wireless) that connects sensors and actuators to the control equipment</p>
Firewall	<p>An inter-network connection device that restricts data communication traffic between two connected networks [1]</p> <p><i>NOTE: A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting what ports are open.</i></p>

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:
				33 of 44

Term	Definition
Gateway	<p>A relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other [1]</p> <p><i>NOTE: Also described as an intermediate system that is the translation interface between two computer networks.</i></p>
Geographic Site	<p>A subset of an enterprise’s physical, geographic, or logical group of assets. It may contain areas, manufacturing lines, process cells, process units, control centers, and vehicles and may be connected to other sites by a wide area network.</p>
Important to Safety	<p>Those systems or components that support a safety system, or are designated as “Important to Safety” by the site procedures. [6]</p> <p><i>NOTE: There are a number of definitions of the term "important to safety" in various industry documents. It was determined that maintenance rule risk significant structures, systems, and components (SSC) meet the intent of NEI 04-04. Defining the term in this manner allows the use of work done to support implementation of the maintenance rule (i.e., classification and review by the maintenance rule expert panel). This methodology assures that "important to safety" digital assets used for accident monitoring instrumentation, fire protection, safe shutdown, and ATWS are included in the cyber security program.</i></p>

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	34 of 44

Term	Definition
Industrial Automation and Control System	<p>A collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process</p> <p><i>Note: These systems include, but are not limited to:</i></p> <ul style="list-style-type: none"> ○ <i>industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), networked electronic sensing and control, and monitoring and diagnostic systems (In this context, process control systems include basic process control system and safety-instrumented system [SIS] functions, whether they are physically separate or integrated.)</i> ○ <i>associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems</i> ○ <i>associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes</i>
Insider	<p>A “trusted” person, employee, contractor, or supplier who has information that is not generally known to the public (See “outsider”)</p>
Integrity	<p>The quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data [2]</p> <p><i>NOTE: In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.</i></p>

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:
				35 of 44

Term	Definition
Interception	Capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes
Interface	A logical entry or exit point that provides access to the module for logical information flows
Intrusion	Unauthorized act of compromising a system (See “ <i>attack</i> ”)
Intrusion Detection	A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner
IP Address	Inter-network address of a computer that is assigned for use by the Internet Protocol and other protocols [1]
Local Area Network	A communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 kilometers) [5]
Malicious Code	<p>Programs or code written for the purpose of gathering information about systems or users, destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel</p> <p><i>NOTE: Malicious code attacks can take the form of viruses, worms, Trojan Horses, or other automated exploits.</i></p> <p><i>NOTE: Malicious code is also often referred to as “malware.”</i></p>
Operational Control Systems	Digital systems that are used for normal operations and control plant processes, but are not relied upon to perform safety functions following anticipated operational occurrences or accidents. This category includes systems that have a direct impact on generation. Systems are limited to plant primary and secondary generation equipment up to and including the main generator switchyard relay/breaker. [6]

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 36 of 44

Term	Definition
Outsider	A person or group not “trusted” with inside access, who may or may not be known to the targeted organization (See “insider”) <i>NOTE: Outsiders may or may not have been insiders at one time</i>
Penetration	Successful unauthorized access to a protected system resource [1]
Reliability	A conditional probability that a system will correctly perform (a required function) over a specified interval (t ₀ , t), given that the system was performing correctly at time t ₀ . System reliability relates to continuity of service.
Remote Access	Communication with assets that are outside the perimeter of the security zone being addressed
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [1]
Risk Assessment	Process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures (e.g., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure
Risk Management	Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment [2]
Risk Mitigation Controls	A combination of countermeasures and business continuity plans
Router	A gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router passes Internet Protocol (IP) packets. [1]

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:
				37 of 44

Term	Definition
Security	<ul style="list-style-type: none"> • measures taken to protect a system • condition of a system that results from the establishment and maintenance of measures to protect the system • condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss [1] • capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems [4]
Security Components	Assets such as firewalls, authentication modules, or encryption software used to improve the security performance of an industrial automation and control system (See “countermeasure”)
Security Digital Assets	Security digital assets are limited to those digital assets that are vital to successful implementation of the Security Plan. Operation of these assets is controlled by site procedures. Commercial digital assets such as commercial phone systems, commercial building HVAC controls, video cameras not required for the security plan, badge printing computers, fingerprint machine, copiers, and fax machines are not under a configuration control program and are not identified. These commercial components are not critical to successful implementation of the Security Plan.
Security Incident	<p>An adverse event in a system or network or the threat of the occurrence of such an event [5]</p> <p><i>NOTE: The term “near miss” is sometimes used to describe an event that could have been an incident under slightly different circumstances.</i></p>
Security Intrusion	Security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so [1]

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	38 of 44

Term	Definition
Security Level	Level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit [4]
Security Policy	A set of rules and practices that specify or regulate how a system or organization provides security services to protect its assets [1]
Security Procedures	Definitions of exactly how practices are implemented and executed <i>NOTE: Security procedures are implemented through personnel training and actions using currently available and installed technology.</i>
Security Program	A program that combines all aspects of managing security, ranging from the definition and communication of policies through implementation of best industry practices and ongoing operation and auditing
Sensors and Actuators	The end elements connected to process equipment
Server	A device or application that provides information or services to client applications and devices [1]
System Software	The special software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs and data [3]
Threat	The potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm [1]
User	A person, organization entity, or automated process that accesses a system, whether authorized to do so or not [1]
Vulnerability	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy [1]

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 39 of 44

Term	Definition
Wide Area Network	A communications network designed to connect computers over a large distance, such as across the country or world [3]
<p><u>Legend:</u></p> <p>[</p>	

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	40 of 44

APPENDIX B - Invensys Cyber Security Plan Conformance Review

The Regulatory Guides, IEEE Standards and industry guidance have been reviewed for conformance with this Plan. In general, the IEEE Standards provide more detailed guidance for the implementation activities. When the Reg. Guide or Standards are specifically addressed in the text of a requirement from this Plan, a commitment to the approach is made. Conformance clarification and justification are provided in this Appendix.

Conformance Code	Description
1	This item does not conform. Discussion is provided in the justification section.
2	This item conforms, except for deviations noted. Conformance clarifications are provided in justification section.
3	This item conforms to the planning requirements. No deviations were identified.
4	This item is not within the scope of the software plans.

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	41 of 44

Appendix B – Cyber Security Plan Conformance Review						
Item	Reg Guide	IEEE and Industry Std.	Cyber Security Plan Conformance	Deviation	Conformance Code	Justification
Regulatory Guides						

a, b, f

Invensys Cyber Security Program Plan					
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page:	42 of 44

Appendix B – Cyber Security Plan Conformance Review						
Item	Reg Guide	IEEE and Industry Std.	Cyber Security Plan Conformance	Deviation	Conformance Code	Justification
IEEE Standards						
Industry Standards						

a, b, f

a, b, f

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 43 of 44

APPENDIX C - Acronyms and Abbreviations

The following acronyms and abbreviations are used throughout this Plan.

Acronym	Meaning
BTP	Branch Technical Position
CDA	Critical Digital Asset
CFR	Code of Federal Regulations
CNSS	Committee of National Security Systems
COTS	Commercial-Off-The-Shelf
CySP	Cyber Security Program
DCD	Design Control Document
DCIS	Distributed Control and Information Center
DMZ	Demilitarized Zone
EOF	Emergency Operations Facility
ESF	Engineered Safety Feature
FAT	Factory Acceptance Test
FIPS	Federal Information Processing Standards
FIPS PUB	Federal Information Processing Standards Publication
FMEA	Failure Modes and Effects Analysis
HFE	Human Factors Engineering
HICB	Instrumentation and Control Branch
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISG	Interim Staff Guidance
ISO	International Organization for Standardization

Invensys Cyber Security Program Plan				
Document No.:	7286-545-2-NP	Date:	August 31, 2009	Page: 44 of 44

Acronym	Meaning
IT	Information Technology
LAN	Local area Network
LTR	Licensing Topical Report
MMIS	Man Machine Interface System
N-DCIS	Nonsafety-Related Distributed Control and Information Center
NEI	Nuclear Energy Institute
NIDS	Network Intrusion Detection System
NMAP	Network Mapper (also Nmap)
NMS	Neutron Monitoring System
NRC	United States Nuclear Regulatory Commission
NSIR	Nuclear Security and Incident Response
QA	Quality Assurance
Q-DCIS	Safety-Related Distributed Control and Information Center
RE	Responsible Engineer
Reg.	Regulatory
RG	Regulatory Guide
RPS	Reactor Protection System
SANS	SysAdmin, Audit, Network, Security
SMP	Software Management Plan
SQAP	Software Quality Assurance Plan
SRP	Standard Review Plan
Std	Standard (used by IEEE)
V&V	Verification and Validation
WAN	Wide Area Network