HITACHI

GE Hitachi Nuclear Energy

NEDO-33295
Revision 1
Class I
DRF 0000-0074-4841
July 2009

Licensing Topical Report

# ESBWR – CYBER SECURITY PROGRAM PLAN

*Copyright 2007, 2009 GE-Hitachi Nuclear Energy Americas LLC*

*All Rights Reserved*

## INFORMATION NOTICE

This document NEDO-33295, Rev. 01, contains no proprietary information.

## IMPORTANT NOTICE REGARDING THE CONTENTS OF THIS REPORT

### Please Read Carefully

The information contained in this document is furnished as a reference to the NRC Staff for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of GE Hitachi Nuclear Energy (GEH) with respect to information in this document are contained in contracts between GEH and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

# Table of Contents

1. Introduction ..... 1
1.1 Overview ..... 1
1.2 Purpose and Scope ..... 1
1.3 (Deleted) ..... 2
1.4 (Deleted) ..... 2
1.5 (Deleted) ..... 2
1.6 (Deleted) ..... 2
1.7 GEH ESBWR Licensing Position ..... 2
1.7.1 (Deleted) ..... 2
1.7.2 (Deleted) ..... 2
1.8 Acronyms, Abbreviations, and Definitions ..... 2
2. Regulatory Requirements, Guidelines, and Industry Standards ..... 3
2.1 Supporting Documents ..... 3
2.2 Codes and Standards ..... 3
2.2.1 Regulatory Guide and Interim Staff Guidance ..... 3
2.2.2 NUREG ..... 3
2.2.3 Branch Technical Positions ..... 3
2.2.4 Nuclear Energy Institute (NEI) ..... 3
2.2.5 Code of Federal Regulations (CFR) ..... 3
2.2.6 Institute of Electrical and Electronics Engineers (IEEE) ..... 4
2.3 Supplemental Documents ..... 4
2.4 (Deleted) ..... 4
3. Program Management ..... 5
3.1 Roles and Responsibilities ..... 5
3.2 Policies and Procedures ..... 6
3.3 ESBWR Cyber Security Defensive Model ..... 7
3.4 Training and Awareness ..... 8
3.4.1 User Awareness Training ..... 9
3.4.2 Specialized Cyber Security Training ..... 9
3.5 Contingency and Disaster Recovery Plans ..... 9
3.6 Periodic Threat and Vulnerability Review ..... 9
3.7 Cyber Security Assessment (CySA) Report ..... 9
4. Planning Phase ..... 11
4.1 Identification of Critical Digital Assets ..... 11
4.1.1 Grouping of Digital Devices ..... 11
4.1.2 Communication Pathways ..... 11
4.2 Identification of Security Capabilities ..... 13
4.3 Development of List of Vulnerabilities ..... 13
4.4 Technologies for Cyber Security ..... 13
5. Requirements Phase ..... 16
5.1 Development of Requirements for System Architecture ..... 16
5.2 Development of Requirements for Network Architecture ..... 16
5.3 (Deleted) ..... 17
5.4 System Configurations ..... 17
5.5 Interfaces ..... 17
5.6 Software ..... 17
5.7 Verification and Validation ..... 18
6. Design Phase ..... 19

6.1 Design of Physical and Logical Access ..... 19
6.2 Data Communication with Other Networks ..... 20
6.2.1 Interfaces ..... 20
6.2.2 Securing the Cyber Security Defensive Model Security Levels ..... 20
7. Implementation Phase ..... 21
7.1 Code Design ..... 21
7.2 Identification and Evaluation of Proprietary Systems ..... 21
7.3 Cyber Security Program Plan Coordination with SMPM and SQAPM ..... 22
8. Test Phase ..... 23
9. Installation Phase ..... 24
10. Operations and Maintenance Phase ..... 25
10.1 Change Management ..... 25
10.2 Patch Management ..... 25
10.3 Contingency and Disaster Recovery Plans ..... 26
10.4 Periodic Threat and Vulnerability Review ..... 26
10.5 Maintenance Procedures ..... 26
11. Retirement Phase ..... 27
12. Quality Assurance ..... 28
13. Incident Response and Recovery Plan ..... 29
APPENDIX A: Definitions ..... 30
APPENDIX B: Cyber Security Program Plan Conformance Review ..... 40
APPENDIX C: Acronyms and Abbreviations ..... 44
APPENDIX D: ESBWR Distributed Control and Information System DCIS Functional Network Diagram ..... 47

# List of Tables

**No tables.**

# List of Figures

Figure 3.3-1. Cyber Security Defensive Model Level Diagram ..... 7
Figure 4-1a. ESBWR Cyber Security Process Overview ..... 14
Figure 4-1b. ESBWR Cyber Security Process Overview ..... 15

## Changes from Previous Revision

| Item | Section | Details of Change |
|---|---|---|
| 1 | Entire Document | References updated to reflect the renaming of the Software Management Plan (SMP) to the Software Management Program Manual (SMPM). This update is reflected throughout the contents of the CySPP. |
| 2 | Entire Document | References updated to reflect the renaming of the Software Quality Assurance Plan (SQAP) to the Software Quality Assurance Program Manual (SQAPM). This update is reflected throughout the contents of the CySPP. |
| 3 | Entire Document | Per RAI 7.1-137, used "Cyber Security Program Plan" consistently throughout LTR. |
| 4 | Entire Document | Updated all references to use consistent naming throughout the document and to include the names of sections that are referenced. The first instance of references will spell out the full name of the reference, and shortened names are used thereafter. |
| 5 | Entire Document | Corrected grammar and spelling, fixed formatting and capitalization, improved readability, enhanced clarity, and fixed consistency issues throughout the document. |
| 6 | Entire Document | Replaced wording that used "commits to", "must", and "will" with the word "shall" as appropriate. |
| 7 | Entire Document | The word "all" has been removed or replaced throughout the document. The intent of the usage has not been removed, but "all" is an abstract term that cannot be applied to quantifiable metrics. |
| 8 | Entire Document | Acronyms have been fixed so that they are defined only at first use. |
| 9 | Entire Document | Mentions of "emergency preparedness" have been changed to "emergency preparedness and response" based on feedback provided by the NRC. |
| 10 | Entire Document | Per RAI 7.1-83 and NRC request, changed the words "GEH Policy and Procedures" to "ESBWR cyber security policies and procedures" to indicate that the GEH Policy and Procedures are not a separate document. |
| 11 | Section 1 | The introduction section has been adjusted to include the feedback provided by the NRC, to be consistent with the SMPM, and to follow the flow of the CySPP in a clear and concise manner. |
| 12 | Section 1.2 | Per RAI 7.1-137, clarified GEH's responsibility by bounding it within GEH scope of supply. |
| 13 | Section 1.2 | [[ ]] |
| 14 | Section 1.3 – 1.6, 1.7.1, 1.7.2 | Sections deleted as part of restructuring to incorporate the feedback provided by the NRC and to create a clear and concise introduction. |
| 15 | Section 1.7 | [[ ]] |
| 16 | Section 1.7 | [[ ]] |
| 17 | Section 2 | All references have been updated for formatting. |
| 18 | Section 2 | Removed the words "and correspondence" from the first paragraph because the correspondence section has been deleted. |
| 19 | Section 2.1 | Moved reference to ESBWR Man-Machine Interface System and Human Factors Engineering to Section 2.3 "Supplemental Documents." |
| 20 | Subsection 2.2.1(2) | Per RAI 7.1-80, revised DI&C-ISG-04 reference by adding " Section 1" |

| Item | Section | Details of Change |
|---|---|---|
| 21 | Subsection 2.2.2 | Deleted references to NUREG-0800 that are no longer used. |
| 22 | Subsection 2.2.3(1) | Updated reference to BTP HICB 14 by clarifying that it is part of NUREG-0800, Chapter 7. |
| 23 | Subsection 2.2.5 | Removed "Parts" from the 10 CFR references. |
| 24 | Subsection 2.2.5(4) | Added reference to 10 CFR 73.54. |
| 25 | Subsection 2.2.6(1) | Added reference to the correction sheet for IEEE-603-1991 |
| 26 | Section 2.3 | Per RAI 7.1-95, added reference to ESBWR Safeguards Assessment Report NEDE-33391. |
| 27 | Section 2.3 | Clarified that updates to supplemental documents do not require a CySPP revision. |
| 28 | Section 2.4 | Deleted the correspondence section because the only reference is no longer used and has been deleted. |
| 29 | Section 3 | Clarified that risk is managed for the ESBWR product. |
| 30 | Section 3 | Removed the last sentence of the first paragraph because it not within GEH's scope and relates only to the licensee. |
| 31 | Section 3.1 | [[ ]] |
| 32 | Section 3.1 | [[ ]] |
| 33 | Section 3.1 | [[ ]] |
| 34 | Section 3.1 | [[ ]] |
| 35 | Section 3.1 | [[ ]] |
| 36 | Section 3.1 | [[ ]] |
| 37 | Section 3.1 | [[ ]] |
| 38 | Section 3.1 | [[ ]] |
| 39 | Section 3.1 | [[ ]] |
| 40 | Section 3.1 | [[ ]] |
| 41 | Section 3.2 | Moved information from the deleted philosophy section of the introduction to the beginning of Section 3.2 to discuss security and the need for policy and procedures. |
| 42 | Section 3.2 | The second to last sentence of the first paragraph has been removed. It discusses a policy for managing cyber security at a nuclear power plant, which is outside the GEH scope of supply. |
| 43 | Section 3.2 | The last sentence of the first paragraph has been changed to cover both policies and procedures. Additionally, the policies and procedures are kept throughout the life of the CySP, not the CySPP. |

| Item | Section | Details of Change |
|---|---|---|
| 44 | Section 3.2 | [[ ]] |
| 45 | Section 3.2 | [[ ]] |
| 46 | Section 3.2 | [[ ]] |
| 47 | Section 3.2 | [[ ]] |
| 48 | Section 3.2 | [[ ]] |
| 49 | Section 3.2 | [[ ]] |
| 50 | Section 3.2 | [[ ]] |
| 51 | Section 3.2 | [[ ]] |
| 52 | Section 3.2 | [[ ]] |
| 53 | Section 3.2 | [[ ]] |
| 54 | Section 3.2 | [[ ]] |
| 55 | Section 3.2 | [[ ]] |
| 56 | Section 3.2 | [[ ]] |
| 57 | Section 3.3 | [[ ]] |
| 58 | Section 3.3 | [[ ]] |
| 59 | Section 3.3 | [[ ]] |

| Item | Section | Details of Change |
|---|---|---|
| 60 | Section 3.3 | [[ ]] |
| 61 | Section 3.3 | [[ ]] |
| 62 | Section 3.3 | [[ ]] |
| 63 | Section 3.3 | [[ ]] |
| 64 | Section 3.3 | [[ ]] |
| 65 | Section 3.3 | [[ ]] |
| 66 | Section 3.3 | [[ ]] |
| 67 | Section 3.4 | [[ ]] |
| 68 | Section 3.4 | [[ ]] |
| 69 | Section 3.4 | [[ ]] |
| 70 | Subsection 3.4.1 | [[ ]] |
| 71 | Subsection 3.4.1 | [[ ]] |
| 72 | Subsection 3.4.1 | [[ ]] |
| 73 | Subsection 3.4.1 | [[ ]] |
| 74 | Section 3.5 | [[ ]] |
| 75 | Section 3.6 | [[ ]] |
| 76 | Section 3.6 | [[ ]] |
| 77 | Section 3.6 | [[ ]] |

| Item | Section | Details of Change |
|---|---|---|
| 78 | Section 3.7 (new) | [[ ]] |
| 79 | Section 4 | [[ ]] |
| 80 | Section 4 | [[ ]] |
| 81 | Section 4.1 | [[ ]] |
| 82 | Section 4.1 | [[ ]] |
| 83 | Section 4.1 | [[ ]] |
| 84 | Section 4.1 | [[ ]] |
| 85 | Subsection 4.1.1 | [[ ]] |
| 86 | Subsection 4.1.1 | [[ ]] |
| 87 | Subsection 4.1.2 | [[ ]] |
| 88 | Subsection 4.1.2 | [[ ]] |
| 89 | Subsection 4.1.2 | [[ ]] |
| 90 | Subsection 4.1.2 | [[ ]] |
| 91 | Subsection 4.1.2 | [[ ]] |
| 92 | Subsection 4.1.2 | [[ ]] |
| 93 | Subsection 4.1.2 | [[ ]] |
| 94 | Section 4.2 | [[ ]] |
| 95 | Section 4.2 | [[ ]] |
| 96 | Section 4.3 | [[ ]] |

| Item | Section | Details of Change |
|---|---|---|
| 97 | Section 4.3 | [[ ]] |
| 98 | Section 4.3 | [[ ]] |
| 99 | Section 4.3 | [[ ]] |
| 100 | Section 4.4 | [[ ]] |
| 101 | Section 4.4 | [[ ]] |
| 102 | Section 4.4 | [[ ]] |
| 103 | Section 4.4 | [[ ]] |
| 104 | Section 4.4 | [[ ]] |
| 105 | Section 4.4 | [[ ]] |
| 106 | Section 4.4 | [[ ]] |
| 107 | Section 5 | Rewrote the first paragraph for clarity only. |
| 108 | Section 5 | [[ ]] |
| 109 | Section 5 | [[ ]] |
| 110 | Section 5.1 | [[ ]] |
| 111 | Section 5.1 | [[ ]] |
| 112 | Section 5.1 | [[ ]] |
| 113 | Section 5.2 | [[ ]] |
| 114 | Section 5.2 | [[ ]] |
| 115 | Section 5.2 | [[ ]] |
| 116 | Section 5.3 | [[ ]] |
| 117 | Section 5.4 | [[ ]] |
| 118 | Section 5.5 | [[ ]] |
| 119 | Section 5.5 | [[ ]] |
| 120 | Section 5.5 | [[ ]] |

| Item | Section | Details of Change |
|---|---|---|
| 121 | Section 5.6 | [[ ]] |
| 122 | Section 5.6 | [[ ]] |
| 123 | Section 5.6 | [[ ]] |
| 124 | Section 5.7 | Added the word "also" in the statement "Security is also a software characteristic" to emphasize that security is not exclusively software. |
| 125 | Section 5.7 | In the first paragraph, clarified that verification and validation is performed on the design documentation and outputs. |
| 126 | Section 5.7 | [[ ]] |
| 127 | Section 5.7 | [[ ]] |
| 128 | Section 5.7 | [[ ]] |
| 129 | Section 6 | [[ ]] |
| 130 | Section 6 | [[ ]] |
| 131 | Section 6 | [[ ]] |
| 132 | Section 6 | [[ ]] |
| 133 | Section 6.1 | [[ ]] |
| 134 | Subsection 6.2.1 | Deleted the word "external" from the first sentence because the command and control may be external or internal to a CDA. |
| 135 | Subsection 6.2.1 | [[ ]] |
| 136 | Subsection 6.2.1 | [[ ]] |
| 137 | Subsection 6.2.1 | [[ ]] |
| 138 | Subsection 6.2.2 | [[ ]] |
| 139 | Subsection 6.2.2 | [[ ]] |
| 140 | Section 7 | [[ ]] |
| 141 | Section 7 | [[ ]] |

| Item | Section | Details of Change |
|---|---|---|
| 142 | Section 7 | [[ ]] |
| 143 | Section 7 | [[ ]] |
| 144 | Section 7.1 | [[ ]] |
| 145 | Section 7.1 | [[ ]] |
| 146 | Section 7.2 | [[ ]] |
| 147 | Section 7.3 | [[ ]] |
| 148 | Section 7.3 | [[ ]] |
| 149 | Section 7.3 | [[ ]] |
| 150 | Section 8 | Multiple corrections throughout the section to enhance readability, update the references, and fix grammatical errors. |
| 151 | Section 8 | [[ ]] |
| 152 | Section 8 | [[ ]] |
| 153 | Section 8 | [[ ]] |
| 154 | Section 8 | [[ ]] |
| 155 | Section 8 | [[ ]] |
| 156 | Section 9 | Per RAI 7.1-84, change the title of Section 9 to "INSTALLATION PHASE" to be consistent with the SMPM. |
| 157 | Section 9 | [[ ]] |
| 158 | Section 9 | [[ ]] |
| 159 | Section 9 | [[ ]] |
| 160 | Section 10 | [[ ]] |

| Item | Section | Details of Change |
|---|---|---|
| 161 | Section 10.1 | [[ ]] |
| 162 | Section 10.1 | [[ ]] |
| 163 | Section 10.1 | [[ ]] |
| 164 | Section 10.2 | [[ ]] |
| 165 | Section 10.3 | [[ ]] |
| 166 | Section 10.3 | [[ ]] |
| 167 | Section 10.3 | [[ ]] |
| 168 | Section 10.4 | [[ ]] |
| 169 | Section 10.4 | [[ ]] |
| 170 | Section 10.4 | [[ ]] |
| 171 | Section 10.5 | In the first paragraph, replaced the word "it" with "the component or system" for clarity. |
| 172 | Section 10.5 | [[ ]] |
| 173 | Section 10.5 | [[ ]] |
| 174 | Section 11 | [[ ]] |
| 175 | Section 11 | [[ ]] |
| 176 | Section 12 | [[ ]] |
| 177 | Section 12 | [[ ]] |
| 178 | Section 13 | [[ ]] |
| 179 | Section 13 | [[ ]] |
| 180 | Appendix A | [[ ]] |
| 181 | Appendix A | [[ ]] |

| Item | Section | Details of Change |
|---|---|---|
| 182 | Appendix A | [[ ]] |
| 183 | Appendix A | [[ ]] |
| 184 | Appendix A | [[ ]] |
| 185 | Appendix A | Definition of Gateway: Removed the note that provides an alternative definition for gateway that is not used in the CySPP LTR. |
| 186 | Appendix A | Definition of Remote Access: Per RAI 7.1-80-S01, clarified in the NEDE-33295P, as: "Remote access is the ability to access a computer, node, or network resource located within an identified defensive level from a computer or node that is physically located in a less secure defensive level." |
| 187 | Appendix A | Definition of Remote Access: Additionally to RAI 7.1-80-S01, removed "Remote access is" from the beginning of the sentence because it is already implied that this is the definition for remote access. Also added an example to the end of the definition for clarity. |
| 188 | Appendix A | Definition of Security Policy: Updated to clarify that security policies apply to sensitive and critical system resources. |
| 189 | Appendix B | Title: Per RAI 7.1-137, clarified the scope to be the Cyber Security Program Plan. |
| 190 | Appendix B | [[ ]] |
| 191 | Appendix B | [[ ]] |
| 192 | Appendix B | [[ ]] |
| 193 | Appendix B | [[ ]] |
| 194 | Appendix B | [[ ]] |
| 195 | Appendix B | [[ ]] |
| 196 | Appendix B | [[ ]] |
| 197 | Appendix B | [[ ]] |
| 198 | Appendix C | Added definitions for the acronym **CySA**, **CySPP**, **CyST** and **DI&C**. The definition for CySPP was added per RAI 7.1-137 to represent the ESBWR Cyber Security Program Plan. |
| 199 | Appendix C | The acronym meanings for **DCIS, ESBWR, GEH, N-DCIS, NRC, PDS,** and **Q-DCIS** were corrected. |
| 200 | Appendix D (new) | [[ ]] |

# 1. INTRODUCTION

## 1.1 Overview

The Cyber Security Program Plan (CySPP) defines the requirements for the development and management of an effective cyber security program for GE Hitachi Nuclear Energy (GEH) and its ESBWR product. This document is a top-tier design basis and high-level implementation guide for the ESBWR Cyber Security Program, per Regulatory Guide (RG) 1.152 [2.2.1(1)].

## 1.2 Purpose and Scope

The purpose of this document is to provide guidance for developing the ESBWR Cyber Security Program (CySP) for critical digital assets (CDAs) within the GEH scope of supply.

[[

]]



{{{Security-Related Information – Withheld Under 10 CFR 2.390}}}

### 1.3 (Deleted)

### 1.4 (Deleted)

### 1.5 (Deleted)

### 1.6 (Deleted)

### 1.7 GEH ESBWR Licensing Position

[[

]]

#### 1.7.1 (Deleted)

#### 1.7.2 (Deleted)

### 1.8 Acronyms, Abbreviations, and Definitions

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

# 2. REGULATORY REQUIREMENTS, GUIDELINES, AND INDUSTRY STANDARDS

This section includes applicable supporting and supplemental documents; requirements, guides, and codes and standards. Supporting documents provide the input requirements to this plan. Supplemental documents are used in conjunction with this plan.

## 2.1 Supporting Documents

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

(1) ESBWR Design Control Document (DCD), Chapter 7, Instrumentation and Control (I&C) Systems, 26A6642AW

(2) (Deleted)

## 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) RG 1.152-2006, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

(2) Digital Instrumentation and Controls Interim Staff Guidance Task Working Group #4 (DI&C-ISG-04), Highly-Integrated Control Rooms-Communications Issues (HICRc), Revision 0, September 2007, Section 1

### 2.2.2 NUREG

(1) NUREG/CR-6847, PNNL-14766, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants, October 2004

(2) (Deleted)

(3) (Deleted)

(4) (Deleted)

### 2.2.3 Branch Technical Positions

(1) NUREG-0800, Standard Review Plan, Chapter 7, BTP HICB-14, R4, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

### 2.2.4 Nuclear Energy Institute (NEI)

(1) NEI 04-04, Cyber Security Program for Power Reactors, Revision 1, November 18, 2005

### 2.2.5 Code of Federal Regulations (CFR)

(1) 10 CFR 2.390, Public Inspections, Exemptions, Request for Withholding

(2) 10 CFR 50, Domestic Licensing of Production and Utilization Facilities

(3) 10 CFR 73.55, Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage

(4) 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks

### 2.2.6 Institute of Electrical and Electronics Engineers (IEEE)

(1) IEEE 603-1991 including correction sheet dated January 30, 1995, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

(2) IEEE 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

## 2.3 Supplemental Documents

Supplemental documents are subject to revision to remain current with GEH internal procedures, and do not require the CySPP to be updated when they are revised. The following supplemental documents are used in conjunction with this document:

(1) ESBWR Software Quality Assurance Program Manual, NEDE-33245P

(2) ESBWR Software Management Program Manual, NEDE-33226P

(3) ESBWR Safeguards Assessment Report, NEDE-33391P

(4) ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan, NEDE-33217P

## 2.4 (Deleted)

(1) (Deleted)

# 3. PROGRAM MANAGEMENT

This section describes the management components needed to lay the foundations for an effective cyber security program, including the specific roles and responsibilities assigned to carry out the program. Cyber security program management ensures that necessary cyber security issues are addressed programmatically within the ESBWR cyber security policies and procedures to achieve a reasonable level of risk for the ESBWR product.

## 3.1 Roles and Responsibilities

[[

]]

## 3.2 Policies and Procedures

Security is both a form of protection (e.g. a safeguard such as a firewall) and a software characteristic; it is an important consideration during the development of software products. Policies and procedures are applied to prevent contamination of the software products with viruses, trojan horses, or other nefarious intrusions throughout the software life cycle of the software product. Effective and manageable cyber security programs are built upon policies and procedures. These policies and procedures will be created and kept with the policies and procedures developed throughout the life of the CySP.

[[

]]

## 3.3 ESBWR Cyber Security Defensive Model

The Cyber Security Defensive Model is used to evaluate and support the ESBWR's overall cyber security defensive strategy.

[[

]]

[[ ]]

**Figure 3.3-1. Cyber Security Defensive Model Level Diagram**

[[

]]

### 3.4 Training and Awareness

[[

]]

### 3.4.1 User Awareness Training

[[

]]

### 3.4.2 Specialized Cyber Security Training

[[

]]

## 3.5 Contingency and Disaster Recovery Plans

[[

]]

## 3.6 Periodic Threat and Vulnerability Review

[[

]]

## 3.7 Cyber Security Assessment (CySA) Report

[[

]]

# 4. PLANNING PHASE

Figure 4-1a and Figure 4-1b, "ESBWR Cyber Security Process Overview," shows how cyber security is integrated into the software development lifecycle process. The software development process is described in the SQAPM [2.3(1)] and SMPM [2.3(2)]. Cyber security-related tasks that supplement the SQAPM [2.3(1)] and SMPM [2.3(2)] are described within Sections 4, 5, 6, 7, 8, 9, 10, and 11. Input and output documents are representative of the type of document to be used or produced; the actual document types and names may vary according to the requirements of the SQAPM [2.3(1)] and SMPM [2.3(2)]. The process flow has been simplified to show the overall relationship between process steps. Complex informational flow patterns, which may exist between process steps, are not shown because these details are developed later as part of project-specific cyber security programs.

## 4.1 Identification of Critical Digital Assets

[[

]]

### 4.1.1 Grouping of Digital Devices

[[

]]

### 4.1.2 Communication Pathways

[[

]]

## 4.2 Identification of Security Capabilities

[[

]]

## 4.3 Development of List of Vulnerabilities

[[

]]

## 4.4 Technologies for Cyber Security

[[

]]

[[ ]]

**Figure 4-1a. ESBWR Cyber Security Process Overview**

[[ ]]

**Figure 4-1b. ESBWR Cyber Security Process Overview**

# 5. REQUIREMENTS PHASE

The cyber security requirements for each of the CDAs identified in the planning phase need to be developed as part of the overall system requirements, following RG 1.152, Section 2.2, Requirements Phase [2.2.1(1)]. This strategy will also help in determining the approach for incorporating protective measures into these systems in adherence to the GEH ESBWR Cyber Security Defensive Model.

[[

]]

The following sections describe the various areas of requirements development.

## 5.1 Development of Requirements for System Architecture

[[

]]

## 5.2 Development of Requirements for Network Architecture

[[

]]

## 5.3 (Deleted)

## 5.4 System Configurations

Systems will require configuration while being designed, installed, maintained, or in production. The configuration of any CDA can affect the security of that particular device.

[[

]]

## 5.5 Interfaces

The access to any system is the interface that is connected to external resources. Each interface on a system will need to have its functional requirements reviewed.

[[

]]

## 5.6 Software

The use of commercial-off-the-shelf (COTS) software and previously developed software (PDS) will be a very common solution for vendors, partners, and GEH.

[[

]]

## 5.7 Verification and Validation

Security is also a software characteristic, and therefore it is an important consideration during the development of software products. The verification and validation of the design documentation and outputs will follow the SQAPM, Section 5, Software Verification and Validation Plan [2.3(1)] for safety-related and other designated software.

[[

]]

# 6. DESIGN PHASE

This section describes the creation of the system based on the requirements. The design phase incorporates the objectives of the ESBWR as a whole and on the individual system security level. The requirements will be translated into specific design criteria.

[[

]]

## 6.1 Design of Physical and Logical Access

The analysis has been completed and the list of critical digital assets has been made in the planning and requirements phases.

[[

]]

## 6.2 Data Communication with Other Networks

### 6.2.1 Interfaces

The interface of each critical digital asset is the entry point for command and control of that system.

[[

]]

### 6.2.2 Securing the Cyber Security Defensive Model Security Levels

Each security level of the Cyber Security Defensive Model requires its own methods of securing the information and systems that reside on that security level.

[[

]]

# 7. IMPLEMENTATION PHASE

This section is focused on implementation of the secure design for creation of secure hardware and software.

[[

]]

## 7.1 Code Design

Planning, Requirements and Design phases have led to this step.

[[

]]

## 7.2 Identification and Evaluation of Proprietary Systems

As noted in RG 1.152, Subsection 2.4.2, Development Activities [2.2.1(1)], COTS systems may be proprietary and generally unavailable for review.

[[

]]

## 7.3 Cyber Security Program Plan Coordination with SMPM and SQAPM

[[

]]

# 8. TEST PHASE

Testing shall be conducted in the SQAPM [2.3(1)] and SMPM [2.3(2)] to verify and validate that the cyber security requirements are correctly and completely designed and implemented in the CDAs.

[[

]]

# 9. INSTALLATION PHASE

[[

]]

# 10. OPERATIONS AND MAINTENANCE PHASE

The operations and maintenance phase is the responsibility of both GEH, under this Plan and within the GEH scope of supply, and the licensee, under the licensee specific cyber security plan.

[[

]]

## 10.1 Change Management

Change management processes follow GEH procedural and licensing commitments, as applicable, for maintaining both licensing basis and configuration control as described in the SQAPM [2.3(1)] and SMPM [2.3(2)].

[[

]]

## 10.2 Patch Management

Patch management processes support life cycle management by providing a systematic approach for maintaining system's current software revision security levels and firmware from the vendor, as required.

[[

]]

## 10.3 Contingency and Disaster Recovery Plans

[[

]]

## 10.4 Periodic Threat and Vulnerability Review

[[

]]

## 10.5 Maintenance Procedures

During the system life cycle, when component or system maintenance or surveillance testing is performed, the component or system must be restored to full security condition during the return to service process.

[[

]]

# 11. RETIREMENT PHASE

The purpose of the Retirement Phase is to remove the existing software product from the operating environment. An effective continuing program, within GEH scope of supply, shall consider the retirement phase and procedures shall be in place to address proper retirement of CDAs and disposal of media and resident software in a controlled manner.

[[

]]

# 12. QUALITY ASSURANCE

[[

]]

# 13. INCIDENT RESPONSE AND RECOVERY PLAN

[[

]]

# 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 an inclusive list of terms and may be updated at anytime. The list 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 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.<br>*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.* |
| 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] |
| 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. |

| Term | Definition |
|---|---|
| [[ | ]] |
| [[ | ]] |
| 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] |
| 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<br>*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.* |
| Control Network | Those networks that are typically connected to equipment that controls physical processes and that is time critical. (See "*safety network*")<br>*NOTE: The control network can be subdivided into zones, and there can be multiple separate control networks within one company or site.* |

| Term | Definition |
|---|---|
| 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] |
| | |
| | |
| Defense-In-Depth | A security architecture based on the idea that any one point of protection may, and probably will, be defeated.<br>*NOTE: Defense in depth implies layers of security and detection, even on single systems, and provides the following features:*<br>• *attackers are faced with breaking through or bypassing each layer without being detected*<br>• *a flaw in one layer can be protected by capabilities in other layers*<br>• *system security becomes a set of layers within the overall network security* |
| Demilitarized Zone | A perimeter network segment that is logically between internal and external networks. [2]<br>*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.*<br>*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.* |
| Denial of Service | The prevention or interruption of authorized access to a system resource or the delaying of system operations and functions. [1] |



{{{Security-Related Information – Withheld Under 10 CFR 2.390}}}

| Term | Definition |
|---|---|
| Distributed Control System | 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.<br>*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.* |
| Emergency Preparedness Digital Assets | Emergency preparedness 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. |
| ESBWR I&C Network | The ESBWR DCIS is subdivided into the safety-related DCIS (Q-DCIS) and the nonsafety-related DCIS (N-DCIS). A functional network diagram of the ESBWR DCIS appears in Appendix D, which is a functional representation of the current design. The final DCIS design may alter equipment locations and actual hardware components depending on the chosen DCIS vendors. Q-DCIS and N-DCIS architectures, their relationships, and their acceptance criteria are further described in the ESBWR Design Control Document (DCD), Chapter 7, Section 7.1, "Introduction" [2.1(1)]. |
| Failure Mode and Effects Analysis | 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. |
| Field I/O Network | The communications link (wired or wireless) that connects sensors and actuators to the control equipment. |
| Firewall | An inter-network connection device that restricts data communication traffic between two connected networks. [1]<br>*NOTE: A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance)which 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.* |

| Term | Definition |
|---|---|
| Gateway | 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] |
| Geographic Site | 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. |
| | |
| Industrial Automation and Control System | A collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.<br>*NOTE: These systems include, but are not limited to:*<br>• *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.)*<br>• *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*<br>• *Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes* |



{{{Security-Related Information – Withheld Under 10 CFR 2.390}}}

| Term | Definition |
|---|---|
| Insider | A "trusted" person, employee, contractor, or supplier who has information that is not generally known to the public. (See *"outsider"*) |
| Integrity | 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]<br>*NOTE: In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.* |
| 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 *"attack")* |
| 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 | 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.<br>*NOTE: Malicious code attacks can take the form of viruses, worms, trojan horses, or other automated exploits.*<br>*NOTE: Malicious code is also often referred to as "malware."* |

| 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*")<br>*NOTE: Outsiders may or may not have been insiders at one time.* |
| 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 | The ability to access a computer, node, or network resource located within an identified defensive level from a computer or node that is physically located in a less secure defensive level (e.g., accessing the plant site LAN from home via a non-company computer.) |
| 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 possible 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. |



{{{Security-Related Information – Withheld Under 10 CFR 2.390}}}

| Term | Definition |
|---|---|
| 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] |
| Security | • measures taken to protect a system<br>• condition of a system that results from the establishment and maintenance of measures to protect the system<br>• condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss [1]<br>• 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 Incident | An adverse event in a system or network or the threat of the occurrence of such an event. [5]<br>*NOTE: The term "near miss" is sometimes used to describe an event that could have been an incident under slightly different circumstances.* |
| 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] |
| 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] |

| Term | Definition |
|---|---|
| [[ | ]] |
| Security Policy | A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources. [1] |
| Security Procedures | Definitions of exactly how practices are implemented and executed.<br>*NOTE: Security procedures are implemented through personnel training and actions using currently available and installed technology.* |
| Security Program | A program that combines 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 possibility 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] |
| Wide Area Network | A communications network designed to connect computers over a large distance, such as across the country or world. [3] |

| Term | Definition |
|---|---|
| Legend: | |
| [1] | RFC 2828, Internet Security Glossary, May 2000, <http://www.faqs.org/rfcs/rfc2828.html> |
| [2] | CNSS Instruction No. 4009, National Information Assurance Glossary, May 2003, <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf> |
| [3] | Federal Information Processing Standards (FIPS) PUB 140-2, (2001) "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES," Section 2, Glossary of Terms and Acronyms, U.S. National Institute of Standards and Technology. |
| [4] | Federal Information Processing Standards Publication, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, December 2002 |
| [5] | SANS Glossary of Terms used in Security and Intrusion Detection, May 2003, <http://www.sans.org/resources/glossary.php> |
| [6] | NEI 04-04 [2.2.4(1)] |

# APPENDIX B: CYBER SECURITY PROGRAM PLAN CONFORMANCE REVIEW

[[

]]

| Conformance Code | Description |
|---|---|
| [[ ]] | |
| [[ ]] | |
| [[ ]] | |
| [[ | ]] |

| Appendix B - Cyber Security Program Plan Conformance Review | | | | | | |
|---|---|---|---|---|---|---|
| **Item** | **Reg Guide** | **IEEE and Industry Std.** | **Cyber Security Program Plan Conformance** | **Deviation** | **Conformance Code** | **Justification** |
| [[ | | ]] | | | | |
| [[ | | | | | | ]] |

| Appendix B - Cyber Security Program Plan Conformance Review | | | | | | |
|---|---|---|---|---|---|---|
| **Item** | **Reg Guide** | **IEEE and Industry Std.** | **Cyber Security Program Plan Conformance** | **Deviation** | **Conformance Code** | **Justification** |
| [[ ]] | | | | | | |
| [[ | | | | | | ]] |
| [[ | | | | | | ]] |
| [[ | | | | | | ]] |
| [[ ]] | | | | | | |
| [[ | | | | | | ]] |

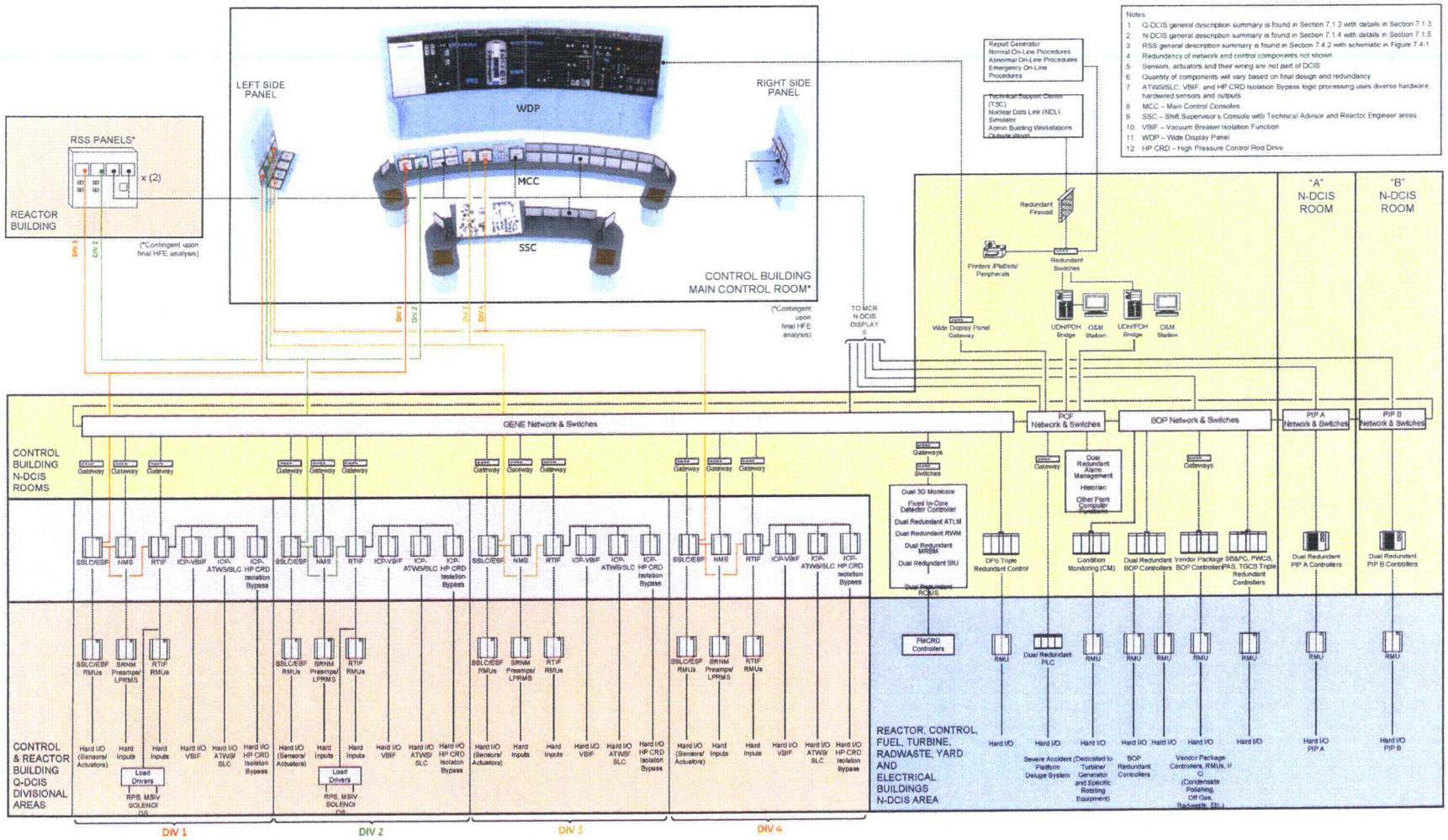
| Appendix B - Cyber Security Program Plan Conformance Review | | | | | | |
|---|---|---|---|---|---|---|
| **Item** | **Reg Guide** | **IEEE and Industry Std.** | **Cyber Security Program Plan Conformance** | **Deviation** | **Conformance Code** | **Justification** |
| [[ | | | | | | ]] |
| [[ | | | | | | ]] |
| [[ | | | | | | |
| | | | | | | ]] |

# 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 |
| CRC | Cyclic Redundancy Check |
| CySA | Cyber Security Assessment |
| CySP | Cyber Security Program |
| CySPP | Cyber Security Program Plan |
| CyST | Cyber Security Team |
| DCD | Design Control Document |
| DCIS | Distributed Control and Information System |
| DI&C | Digital Instrumentation and Controls |
| DMZ | Demilitarized Zone |
| EOF | Emergency Operations Facility |
| ERDS | Emergency Response Data System |
| ESBWR | Economic Simplified Boiling Water Reactor |
| 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 |
| GEH | GE Hitachi Nuclear Energy |
| HFE | Human Factors Engineering |

| Acronym | Meaning |
|---|---|
| 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 |
| IT | Information Technology |
| LAN | Local area Network |
| LTR | Licensing Topical Report |
| MMIS | Man Machine Interface System |
| M&TE | Measurement and Test Equipment |
| N-DCIS | Nonsafety-related - Distributed Control and Information System |
| NEI | Nuclear Energy Institute |
| NIDS | Network Intrusion Detection System |
| NMAP | Network Mapper (also Nmap) |
| NMS | Neutron Monitoring System |
| NRC | Nuclear Regulatory Commission |
| NSIR | Nuclear Security and Incident Response |
| PDS | Previously Developed Software |
| QA | Quality Assurance |
| Q-DCIS | Safety-related - Distributed Control and Information System |
| RAM | Random Access Memory |
| RE | Responsible Engineer |
| Reg. | Regulatory |
| RG | Regulatory Guide |

| Acronym | Meaning |
|---|---|
| RPS | Reactor Protection System |
| SANS | SysAdmin, Audit, Network, Security |
| SMPM | Software Management Program Manual |
| SQAPM | Software Quality Assurance Program Manual |
| SRP | Standard Review Plan |
| Std | Standard (used by IEEE) |
| V&V | Verification and Validation |
| WAN | Wide Area Network |

# APPENDIX D: ESBWR DISTRIBUTED CONTROL AND INFORMATION SYSTEM DCIS FUNCTIONAL NETWORK DIAGRAM