US-APWR Cyber Security Program

Non Proprietary Version

August 2008

Revision History

Revision		Page	Description
0	August 2008	All	Original issued

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

The application of computer system for various functions at nuclear power plants including digital instrumentation and control systems increases the potential for threats from cyber intrusions. Thus cyber security shall ensure high assurance of protection against cyber attacks. This document describes the cyber security program for the US-APWR, which ensures the plant's critical systems are protected against cyber threats.

The US-APWR Cyber Security Program protects the plant against cyber threats in accordance with the applicable codes and standards of the U.S. NRC and industry. The program and the defensive strategy described in this document, are based on the industrial guidance, NEI 04-04. The program applies a graded approach, with varying levels of security based on the significance of the system function. This program document identifies the requirements for each level of cyber security, how separation between levels of cyber security is incorporated, and the approach taken to mitigate risk for each level of cyber security. The US-APWR Cyber Security Program encompasses plant equipment as well as programmatic aspects such as administration, procedures and personnel training.

The US-APWR Cyber Security Program focuses on protecting all critical systems from cyber threats during the operations and maintenance phase of their digital systems/equipment life cycle. In addition, for the plant's digital safety system the program encompasses the complete digital systems/equipment life cycle process including planning, design concepts, software development, and verification and validation. The portion of the cyber security program applicable to the US-APWR digital safety system is based on regulatory guidance, RG 1.152 and BTP 7-14. For digital non-safety systems, the US-APWR Cyber Security Program invokes NEI 04-04 for the development phases of the digital systems/equipment life cycle. These practices provide high assurance that non-safety systems are delivered to the plant without internal cyber threats.

This document describes the key defensive strategies of the US-APWR Cyber Security Program. However, cyber threats are continuously evolving as persons with malicious intent find new ways to breach security barriers. To address this concern, the program also includes programmatic requirements for ongoing periodic audit and assessment of the effectiveness of the program, including ongoing assessment of cyber threats. Ongoing enhancements to the plant's cyber security defenses are expected.

Table of Contents

List of Tables

N/A

List of Figures

List of Acronyms

ACL	access control list
BOP	balance of plant
CCSE	certified cyber security expert
CDA	critical digital asset
CSIRT	cyber security incident response team
COL	Combined License
COLA	Combined License Application
CSM	cyber security manager
DAS	diverse actuation system
DCD	Design Control Document
DMZ	demilitarized zone
EOF	emergency operations facility
EOP	emergency operating procedure
ERDS	emergency response data system
HSI	human system interface
I&C	instrumentation and control
IDS	intrusion detection system
IP	internet protocol
IRP	incident response plan
ISG	Interim Staff Guidance
IT	information technology
LAN	local area network
MCR	main control room
MHI	Mitsubishi Heavy Industries, Ltd.
MITM	man-in-the-middle
NRC	Nuclear Regulatory Commission
O&M	operation and maintenance
OCA	owner controlled area
PA	protected area
PC	personal computer
PCMS	plant control and monitoring system
PSMS	protection and safety monitoring system
PIF	power interface
RSR	remote shutdown room
SANS	SysAdmin, Audit, Network, Security
SMS	senior management sponsor
TSC	technical support center
UDP	user datagram protocol
UMC	unit management computer
VA	vital area
V&V	verification and validation
VDU	visual display unit
VoIP	voice over internet protocol
VPN	virtual private network
WAN	wide area network
WWW	world wide web

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to describe the cyber security program for the US-APWR. This program is applicable to Mitsubishi Heavy Industries (MHI) and its suppliers/partners, during the development of the US-APWR. It is also applicable to the Combined License (COL) applicant during operation of the nuclear facility. This document is intended to be referenced from Combined License Applications (COLA), which reference the US-APWR certified design.

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

The program focuses on the operation and maintenance (O&M) phase of the digital systems/equipment life cycle for all critical systems. In addition, for digital safety instrumentation and control (I&C) systems the cyber security program imposes specific requirements for the complete digital systems/equipment life cycle, including planning and design concepts, software development, and verification and validation (V&V), in accordance with RG 1.152 and BTP 7-14. For the development of digital non-safety systems, the US-APWR Cyber Security Program invokes NEI 04-04. These practices provide high assurance that non-safety systems are delivered to the plant without internal cyber threats.

This program document is intended to form the basis of specific cyber security management procedures which are implemented by each organization (MHI, suppliers/partners, COL Applicant). The actual implementation of the program at the COL facility, and the result of the final detail design for that facility, would be the subject of the COL Applicant's plant implementing procedures. This document describes the key defensive strategies of the US-APWR Cyber Security Program. However, cyber threats are continuously evolving as persons with malicious intent find new ways to breach security barriers. To address this concern, the program also includes programmatic requirements for ongoing periodic audit and assessment of the effectiveness of the program, including ongoing assessment of cyber threats. Ongoing enhancements to the plant's cyber security defenses are expected. Specific organizational procedures shall be updated, as necessary, to reflect these ongoing programmatic changes.

1.2 Scope

The cyber security program described in this document is intended to protect all critical digital assets (CDAs) of the US-APWR. The CDAs encompass all critical systems.

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

2.0 CODES AND STANDARDS

This section identifies the applicable codes and standards which establish the basis for the US-APWR Cyber Security Program:

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

(2) “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”, Regulatory Guide 1.152, Revision 2, January 2006.

(3) ”Guidance of Software Reviews for Digital Computer-based Instrumentation and Control Systems”, BTP 7-14, NUREG-0800, March 2007.

(4) “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants”, NUREG/CR-6847, October 2004.

(5) “Nuclear Power Plant Access Authorization Program”, NEI-03-01.

(6) “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”, IEEE Std 603-1991.

(7) “IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations”, IEEE Std 7-4.3.2-2003.

(8) “Cyber Security”, Interim Staff Guidance, Revision 0, DI&C-ISG-01, Task Working Group #1, December 2007.

(9) “Highly-Integrated Control Rooms - Communications Issues (HICRc)”, Interim Staff Guidance, Revision 0, DI&C-ISG-04, Task Working Group #4, September 2007.

3.0 CYBER SECURITY PROGRAM

The Cyber Security Program is designed to protect CDAs. The Cyber Security Program addresses the following major elements needed for an effective ongoing program.

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.1 Roles and Responsibilities

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

The key roles and responsibilities are as follows:

3.1.1 Senior Management Sponsor

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.1.2 Cyber Security Manager

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.1.3 CDA Managers

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.1.4 Certified Cyber Security Expert

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.2 Policies and Procedures

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

In addition, for safety and non-safety digital I&C systems additional cyber security precautions are maintained during system design.

Cyber security is addressed in the following plans, which govern the development phase of the digital systems/equipment life cycle for safety systems:

- Program management
- Quality assurance
- Safety assessment
- Development
- Verification and validation
- Testing

Further discussion of the digital systems/equipment life cycle for non-safety and safety I&C systems is provided in Section 5.

3.3 Training and Awareness

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.4 Defensive Strategy

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

A detailed description of the defensive strategy and defensive model is described in Section 4. This defensive model pertains to the operational phase and is therefore applicable only to the COL Applicant and its suppliers responsible for operating or maintaining CDAs.

3.5 Configuration Management

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

For digital safety I&C systems, additional configuration management controls are in place throughout the digital safety system life cycle and are controlled by MHI and its suppliers/partners. These additional configuration management controls for digital safety I&C systems are discussed in Section 5.

For non-safety systems, good configuration management practices are applied during the design phase, as discussed in Section 5.

3.6 Asset Retirement

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.7 Incident Response and Recovery

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

3.7.1 Information Technology Systems

Security Related Information – Withhold Under 10CFR 2.390

(SRI)

3.7.2 Plant Systems

Security Related Information – Withhold Under 10CFR 2.390

(SRI)

3.8 Periodic Audit and Assessment

Cyber threats are expected to evolve as persons with malicious intent find new ways to breach cyber security barriers. To counter this, risk assessment and management is ongoing to ensure:

Security Related Information – Withhold Under 10CFR 2.390

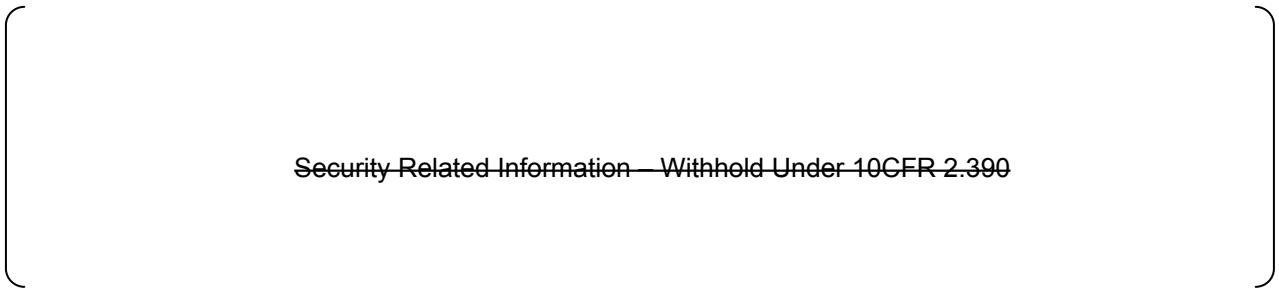
(SRI)

(SRI)

Figure 3.8-1 Assessment and Risk Management Process Flow Diagram

3.8.1 Identification of CDAs

CDAs are identified by the following criteria:



(SRI)

3.8.2 CDA Assessment Attributes

CDAs are assessed for the following attributes:

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

4.0 CYBER SECURITY DEFENSIVE STRATEGY

Security Related Information – Withhold Under 10CFR 2.390

(SRI)

4.1 Defensive Model

Security Related Information – Withhold Under 10CFR 2.390

(SRI)

Security Related and Proprietary Information – Withhold Under 10CFR 2.390

(SRI/PROP)

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

An overview of the plant network architecture which encompasses the systems within each level described above, is shown in Figure 4.1-2. More detail about the I&C system (i.e., PSMS and PCMS) network architecture is described and shown in Chapter 7 of the Design Control Document (DCD) for the US-APWR [Reference 1].

Security Related and Proprietary Information – Withhold Under 10CFR 2.390

(SRI/PROP)

Figure 4.1-1 Cyber Security Defensive Model

Security Related and Proprietary Information – Withhold Under 10CFR 2.390

(SRI/PROP)

Figure 4.1-2 Plant Network Architecture with Level of Defense

4.2 Defensive Strategy in Each Layer

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

4.2.1 Trust Level 5

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

4.2.2 Trust Level 4

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

Security Related Information – Withhold Under 10CFR 2.390

(SRI)

Security Related Information – Withhold Under 10CFR 2.390

(SRI)

4.2.3 Trust Level 3

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

Security Related and Proprietary Information – Withhold Under 10CFR 2.390

(SRI/PROP)

4.2.4 Trust Level 2

Security Related and Proprietary Information – Withhold Under 10CFR 2.390

(SRI/PROP)

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

4.2.5 Trust Level 1

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

4.2.6 Trust Level 0

Trust Level 0 is the internet. This level includes numerous PC and servers all over the world. The internet represents worldwide open connectivity that can be considered hostile with many active sources for viruses, worms, hackers, etc. Direct connection with this area from any CDAs in Trust Level 3, 4 or 5 is strictly prohibited.

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

4.2.7 Defensive Strategy Features Common to Level 1 and 2

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

4.3 Physical Security Considerations

The physical security of CDAs is an important component in the overall cyber security strategy. The physical control areas at the plant are referred to as VA, PA, and OCA and are represented in the figure below.

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

Figure 4.3-1 General Physical Security Areas

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

~~Security Related Information – Withhold Under 10CFR 2.390~~

(SRI)

4.4 Insider Threat Mitigation

4.4.1 Generic Approach to Insider Threat

The US-APWR implements the elements of the insider mitigation program, utilizing the provisions in NEI 03-01, “Nuclear Power Plant Access Authorization Program.” Cyber connectivity to safety functions of safety related CDAs is controlled to the same degree as the physical system.

4.4.2 Additional Countermeasures to Mitigate Insider Threat

Additional countermeasures to mitigate insider threat are as follows.

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

4.4.3 Personnel Specific Requirements

All organizations (COL Applicant, vendors, contractors, business partners, teaming partners, etc.) with personnel that operate or maintain CDAs should have an auditable personnel trust program that includes the following elements:

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

4.5 External Threat Mitigation

External threat is looked at from an immediate impact on safety (nuclear and personnel) and continued reliable power generation. External threats are applicable to CDAs that are:

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

5.0 SECURITY POLICY FOR THE DEVELOPMENT PHASE

The Cyber Security Program defensive strategy described in Section 4, above, is applicable to all CDAs during the O&M phase of their digital systems/equipment life cycle. This section describes the additional cyber security defensive strategies applied during the development of CDAs.

5.1 Safety Systems

In accordance with RG 1.152, additional cyber security measures are in place for all life cycle phases of the PSMS to protect the US-APWR digital safety I&C systems from cyber threats. The cyber security aspects of the digital systems/equipment life cycle for the PSMS basic software are described in Section 6.1.6 of Topical Report MUAP-07005. The cyber security aspects of the digital systems/equipment life cycle for the PSMS application software is generally described in Section 6.4.3 of Topical Report MUAP-07004, “Safety I&C System Description and Design Process” [Reference 3]. Additional details of the application software cyber security aspects are described in each section of Technical Report MUAP-07017, “Software Program Manual” [Reference 4].

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

5.2 Non-safety Systems

Cyber security is managed during the development of non-safety systems to provide high assurance that non-safety CDAs are delivered to the plant without internal cyber threats. The

US-APWR Cyber Security Program invokes NEI 04-04 for the development phases of the digital systems/equipment life cycle. These are:

~~Security Related and Proprietary Information – Withhold Under 10CFR 2.390~~

(SRI/PROP)

6.0 REFERENCES

References are enumerated in this section, except for codes and standard described in Section 2.

[1] “Design Control Document for the US-APWR”, Revision 1, Mitsubishi Heavy Industries. Ltd., August 2008.

[2] “Safety System Digital Platform - MELTAC -“, MUAP-07005-P (Proprietary) and MUAP-07005-NP (Non-proprietary), Revision 2, Mitsubishi Heavy Industries. Ltd., August 2008.

[3] “Safety I&C System Description and Design Process”, MUAP-07004-P (Proprietary) and MUAP-07004-NP (Non-proprietary), Revision 1, Mitsubishi Heavy Industries. Ltd., July 2007

[4] “Software Program Manual”, MUAP-07017, Revision 0, Mitsubishi Heavy Industries. Ltd., December 2007.