ATTACHMENT 2

Letter from Mark L. Marchi (WPSC)

To

Document Control Desk (NRC)

Dated

June 7, 1999

Reactor Protection and Engineered Safety Features Upgrade

Project Description – Non-Proprietary Class 3

Kewaunee Nuclear Power Plant
RPS Upgrade Project
Description

June 1999

Introduction

This report is being submitted to the US Nuclear Regulatory Commission (USNRC) in support of the Kewaunee Nuclear Power Plant (KNPP) Reactor Protection System (RPS) Upgrade Project. The project is intended to replace the Reactor Protection System (RPS) and Engineered Safety Features (ESF) process protection and relay cabinets with a state-of-the-art digital system utilizing the Westinghouse safety system based upon the Ovation platform. The scope of the upgrade project includes eight racks of Foxboro H-Line process protection electronics and fourteen racks of relay logic. These racks consist of four process protection channels, two trains of reactor trip signals, two trains of engineered safety feature signals, and test features.

The digital system upgrade will provide for a one-on-one functional replacement while providing a much simpler hardware platform to maintain, operate, and test. The upgrade will provide for enhanced reliability, testability, fault detection, fault identification, improved information flow, and expandability.

The RPS and ESF digital upgrade will be manufactured and tested to applicable regulatory requirements and industry standards. The KNPP RPS and ESF existing systems are designed to meet the intent of IEEE Std. 279-1968. The RPS/ESF upgrade project will be manufactured and installed in compliance with IEEE Std. 603-1991. Field devices, which provide the input signals to these cabinets, will not be replaced as part of this upgrade. The upgrade system will continue to interface with the control room consoles and panels, plant computer, and annunciator system. Field sensor wiring into the process cabinets and output wiring from the RPS/ESF cabinets are not anticipated to be modified as part of this upgrade. Areas such as random single failure immunity, testing strategy, software design, configuration and testing, electromagnetic compatibility, Diversity & Defense-in-Depth, and environmental and seismic qualification will be addressed during this upgrade project.

This report addresses the following areas associated with the Kewaunee RPS Upgrade Project:

Section I: Protection System Architecture

This section presents an overview of the KNPP replacement architecture. The architecture facilitates the existing four process channels, two trains of reactor trip and ESF logic, and associated testing features.

Section II: Protection System Testing Approach

This section presents an overview of the KNPP protection system testing approach. The following features are discussed: periodic semi-automatic test for process protection racks, periodic semi-automatic test for reactor trip logic, periodic semi-automatic test for ESF actuation logic , and continuous self diagnostic testing.

Section III: Diversity & Defense-in-Depth Analysis

This section presents a summary of the Diversity & Defense-in-Depth analysis that was performed to identify if any diverse means are required to mitigate anticipated operational occurrences and design basis events following a postulated software common mode failure in order to meet specified acceptance criteria.

As the RPS Upgrade Project design progresses, additional submittals will be made to describe the Software Life Cycle Plan, the Independent Verification & Validation Plan, the Equipment Qualification Plan, and a Failure Modes and Effects Analysis.

Section 1

Protection System Architecture

for the Kewaunee Nuclear Power Plant
Reactor Protection System
Upgrade Project

June, 1999

Table of Contents

Acronyms and Abbreviations

AUX	Auxiliary
CMF	Common Mode Failure
CRC	Cyclic Redundancy Checksum
D&D-in-D	Diversity and Defense-in-Depth
DAS	Diverse Actuation System
DHC	Data Highway Controller
DLC	Datalink Controller
DTB	Dynamic Trip Bus
E/O	Electrical/Optical
ESF	Engineered Safety Features
ESFALS	ESF Actuation Logic Subsystem
FOT	Fiber Optic Transceiver
FW	Feedwater
HMI	Human-Machine Interface
I	Isolator
I/O	Input/Output
KNPP	Kewaunee Nuclear Power Plant
NR	Narrow Range
PROC	Processor
RTL	Reactor Trip Logic
SG	Steam Generator
USAR	Updated Safety Analysis Report
UV	Undervoltage

Protection System Architecture

1.0 Introduction

An overview of the Kewaunee Nuclear Power Plant (KNPP) RPS Upgrade Project architecture is shown in Figure I-1. The architecture is based upon a [ ]^{a,c,f} that it will replace. Maintaining the process protection and voting logic configuration simplifies the task of retrofitting protection systems in operating plants such as KNPP. It also supports the capability to upgrade other portions of safety systems in the future.

a,c,f

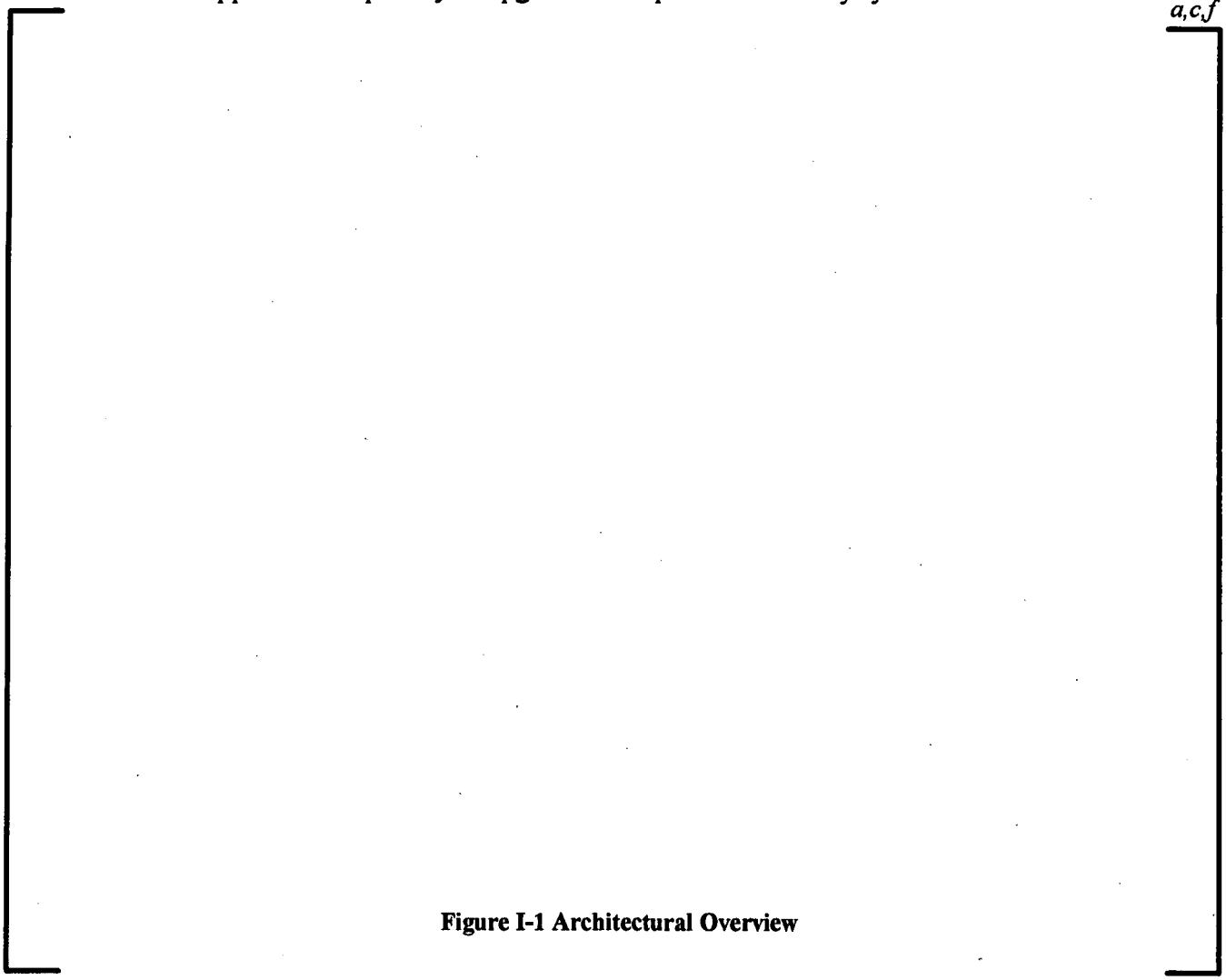


Figure I-1 Architectural Overview

The architecture is shown in more detail in I-11. Each major block of the architecture has been decomposed into microprocessor-based controllers. The internal architecture of a typical controller is shown in Figure I-2. The controller consists of a microcomputer chassis containing [ ]^{a,c,f}. The first is a [

]^{a,c,f}.

Figure I-11 identifies the various functions performed by the blocks along the left edge. In the following sections, the major levels will be described in more detail.

a,c,f

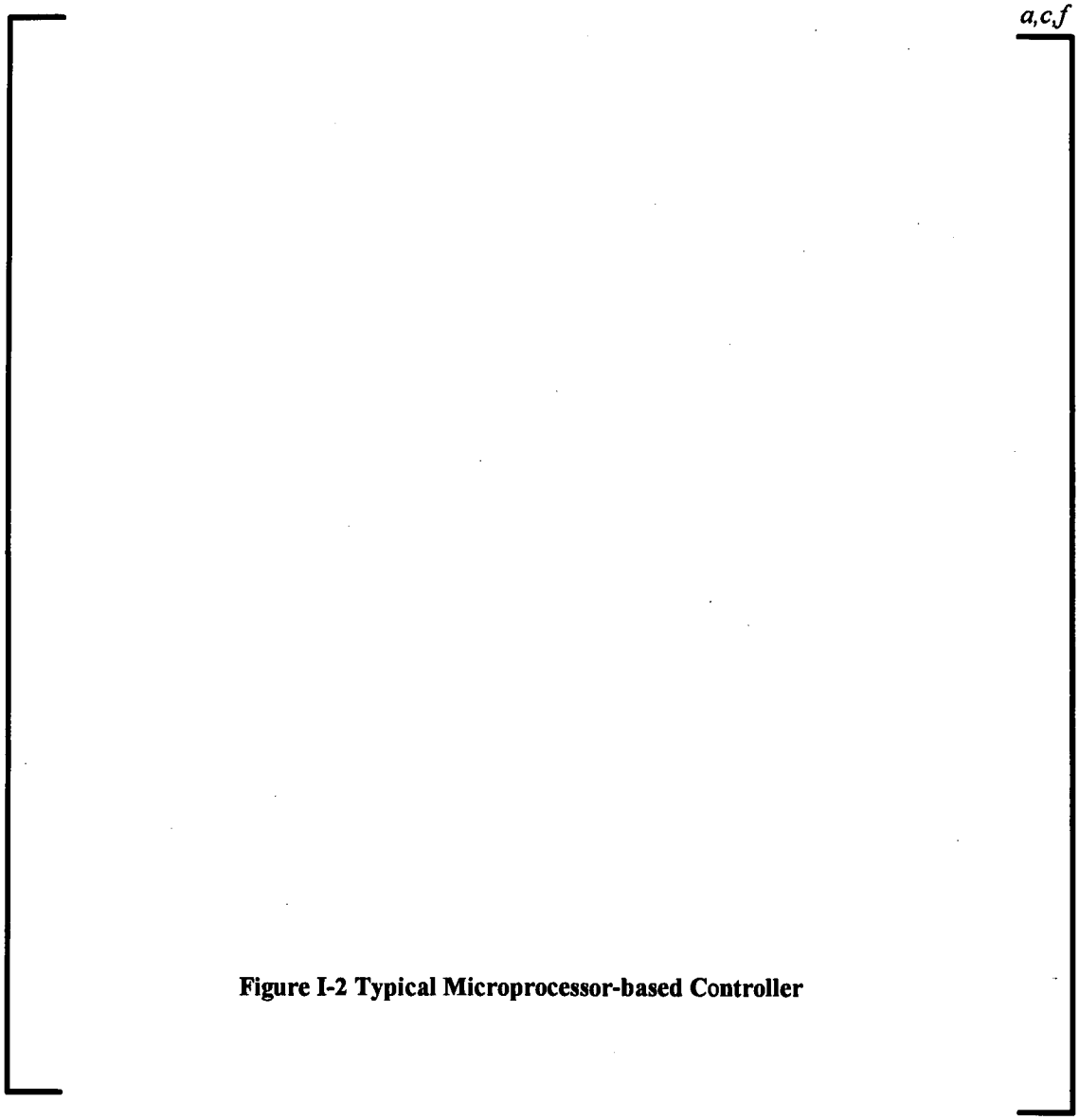


Figure I-2 Typical Microprocessor-based Controller

1.1 Process Protection

The Process Protection Block contains four independent process protection channels which are currently implemented on Foxboro equipment. Internally (as shown in Figure I-3), each protection channel includes [

]^{a,c,f}. Details can be found in the Diversity & Defense-in-Depth (D&D-in-D) analysis presented in Section III. [

]^{a,c,f}. Each controller receives all of the analog inputs required for its protection functions, [

]^{a,c,f}. Selected process calculations are available as analog outputs which are isolated and sent to the control board, the control system, and other plant systems. The bistable states represent [

]^{a,c,f}.

The controllers each read their associated [

]^{a,c,f}. The communication uses fiber optic data links.

a,c,f

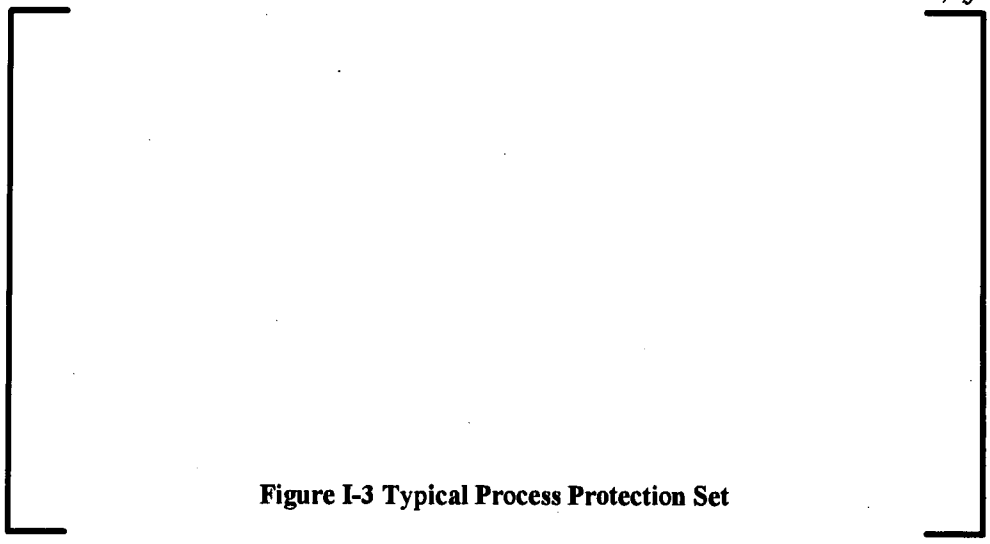


Figure I-3 Typical Process Protection Set

The Process Protection Block does not directly [

]^{a,c,f}.

Within the Process Protection Block, protection against a random single failure preventing a trip (or actuation) or causing a spurious trip (or actuation) is provided by the [ ]^{a,c,f}.

1.2 [ ]^{a,c,f}

[

]^{a,c,f}.

Within the [

]^{a,c,f}.

1.3 Voting Logic

The Voting Logic Block contains [

]^{a,c,f}.

a,c,f

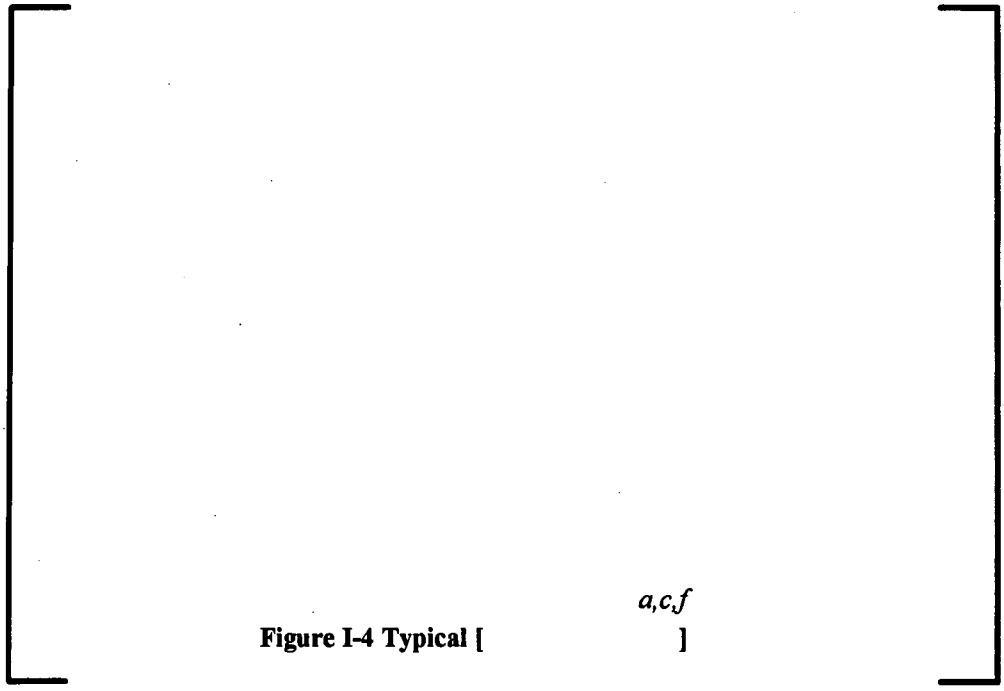


Figure I-4 Typical [a,c,f **]**

The voting logic controllers receive the outputs of the [

]a,c,f. If data is not available from one of the process protection channels, all of its bistables are assumed to be unbypassed and in the partial trip or partial actuation state. The controllers then perform the [

]a,c,f.

Within each [

]a,c,f section of this document. Similarly, within each [

]a,c,f.

a,c,f

[

]

Figure I-5 Typical [*a,c,f* **]**

The primary output of the [

]^{a,c,f}. The controllers drive the existing non-Class 1E control board indicators, recorders, annunciators, and plant computer signals. Each [

]^{a,c,f}.
(Normal procedure is to manually trip the reactor if a function trip indication is received without an automatic reactor trip.) The circuits are shown functionally in Figure I-6. The appropriate inter-train and Class 1E/non-Class 1E isolation will be provided. The [ ]^{a,c,f} drives existing non-Class 1E circuits in a similar manner.

Within the Voting Logic Block, protection against a random single failure preventing a reactor trip or ESF actuation is provided by the [

]^{a,c,f}.

a,c,f

[

]

Figure I-6 Typical Status Indication

1.4 [ ]^{a,c,f}

Within each train, the reactor trip request outputs from the [

]^{a,c,f} technology implemented in the Sizewell B and Temelin designs.

The [ ]^{a,c,f} directly powers the undervoltage (UV) trip circuit for the associated train's trip breaker and for the opposite train's bypass breaker. An external relay is provided for the shunt trip circuit.

Within the [

]^{a,c,f}.

a,c,f

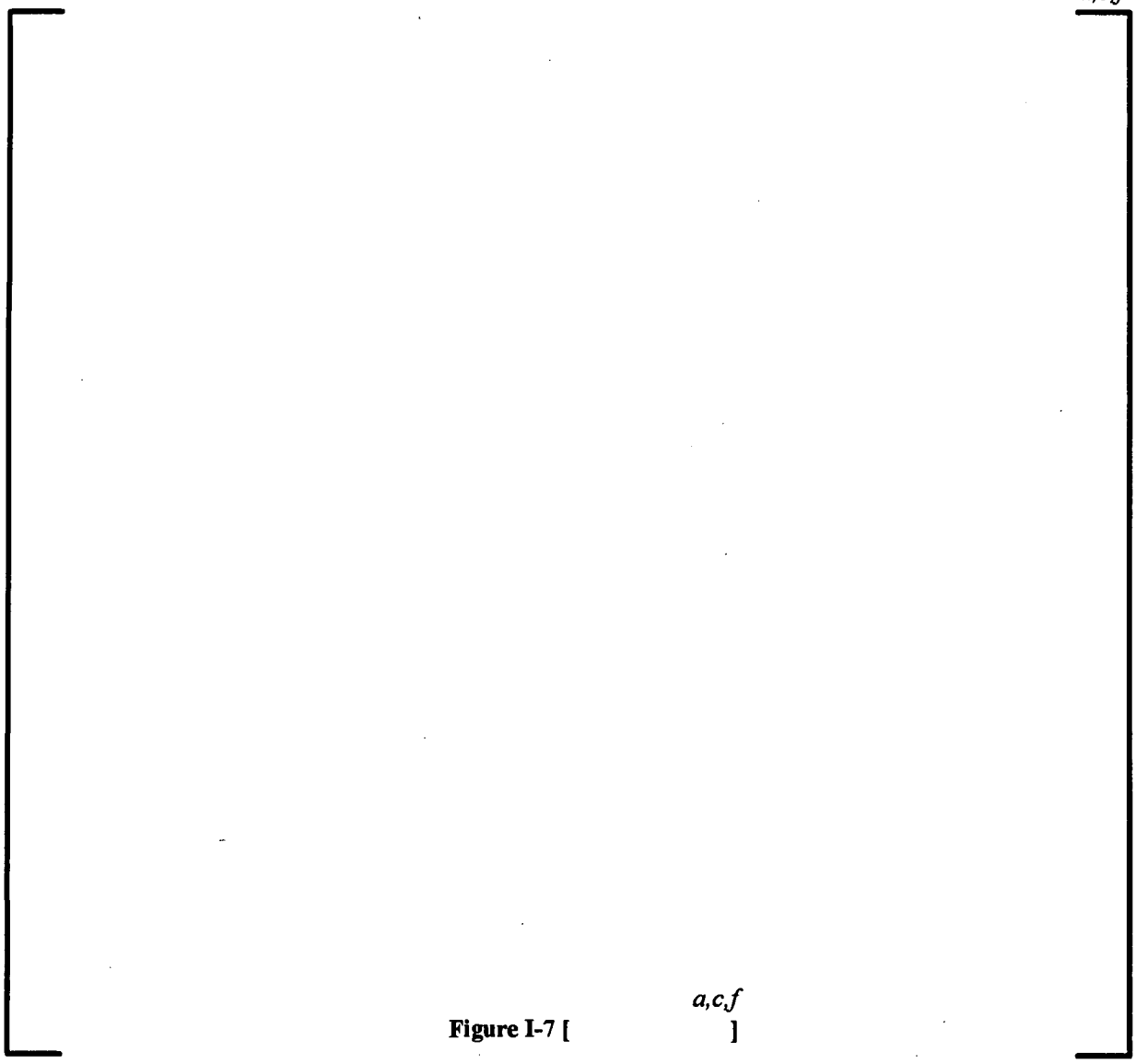


Figure I-7 [a,c,f **]**

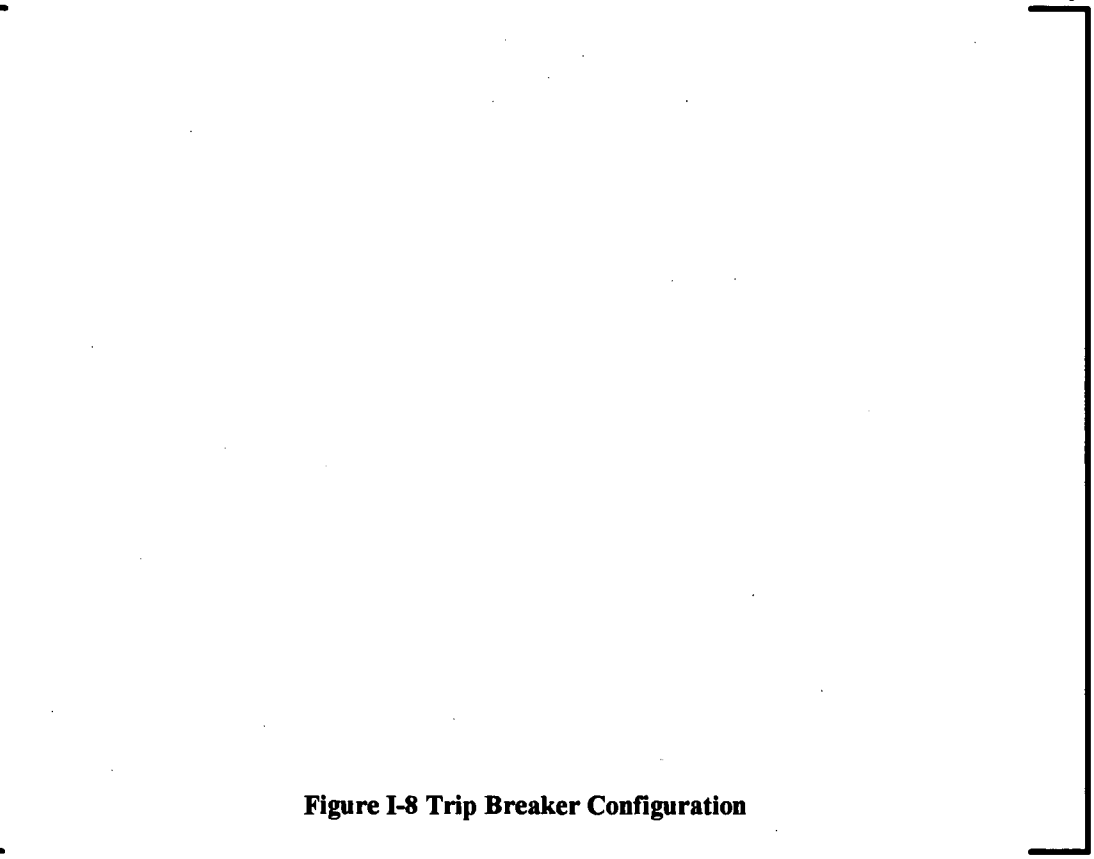
1.5 Trip Breaker Circuits

KNPP has only two trip breakers, one per train, wired in a one-out-of-two configuration. Each of the two trip breakers is in parallel with a Bypass Breaker which is used during testing. Each of the two trip breakers is controlled by the Reactor Trip Logic Subsystem in the corresponding logic train. Each bypass breaker is controlled by the Reactor Trip Logic Subsystem in the opposite train (so that failure of a single breaker cannot prevent a required trip which may occur during a test). The breaker configuration is shown in Figure I-8.

Within the Trip Breaker Circuits, protection against a random single failure preventing a reactor trip is provided by the serial/parallel breaker configuration.

a,c,f

[



]

Figure I-8 Trip Breaker Configuration

1.6 SafetyNet Information Buses

Each of the microprocessor-based controllers in the [

]^{a,c,f} is to provide information to other systems for plant operation, maintenance, and testing. The information passes through a [

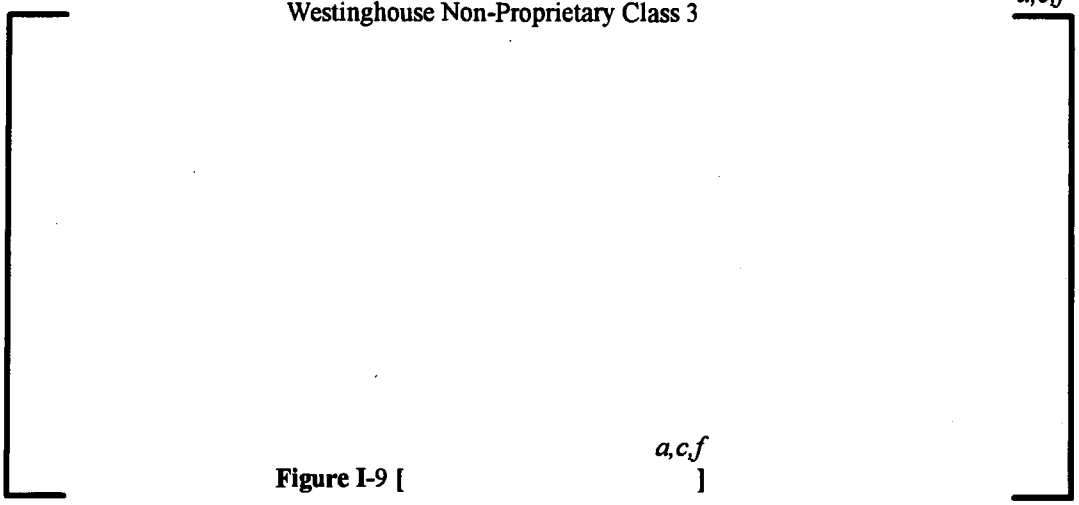
]^{a,c,f}. The architecture provides the capability to add a safety grade display system. The safety grade display system will feature a redundant configuration with each half connected to [

]^{a,c,f}.

a,c,f

[

]



a,c,f

Figure I-9 [ ]

Within the [

]a,c,f. Communication isolation is provided by the following design features:

a. [

]a,c,f

b. [

]a,c,f

c. [

]a,c,f

d. [ ]a,c,f;

Within the [

]a,c,f.

a. [ ]a,c,f;
b. [ ]a,c,f;
c. [ ]a,c,f;
d. [ ]a,c,f;
e. [ ]a,c,f;
f. [ ]a,c,f;
g. [ ]a,c,f;
h. [ ]a,c,f;
i. [ ]a,c,f.

1.7 Diverse Actuation System

The KNPP RPS Upgrade Project architecture also includes a Diverse Actuation System (DAS) as discussed in Section III of this report . This system is defined by the D&D-in-D analysis presented in Section III of this report. The DAS is a [

]^{a,c,f}. The primary functions of the DAS, as shown in Figure I-10, are as follows:

a. The DAS only implements the following [ ]^{a,c,f}:
   1. [ ]^{a,c,f};
   2. [ ]^{a,c,f};
   3. [
   4.]^{a,c,f}
b. [ ]^{a,c,f};
c. [ ]^{a,c,f};
d. Several diverse [ ]^{a,c,f} are provided in the control room to enable the operator to assess the status of DAS and also monitor plant status to determine if manual action is necessary

The D&D-in-D analysis verified that the above listed diverse functions are sufficient to mitigate the consequences of any anticipated operational occurrence and design basis event analyzed in the KNPP USAR Chapter 14.

a,c,f

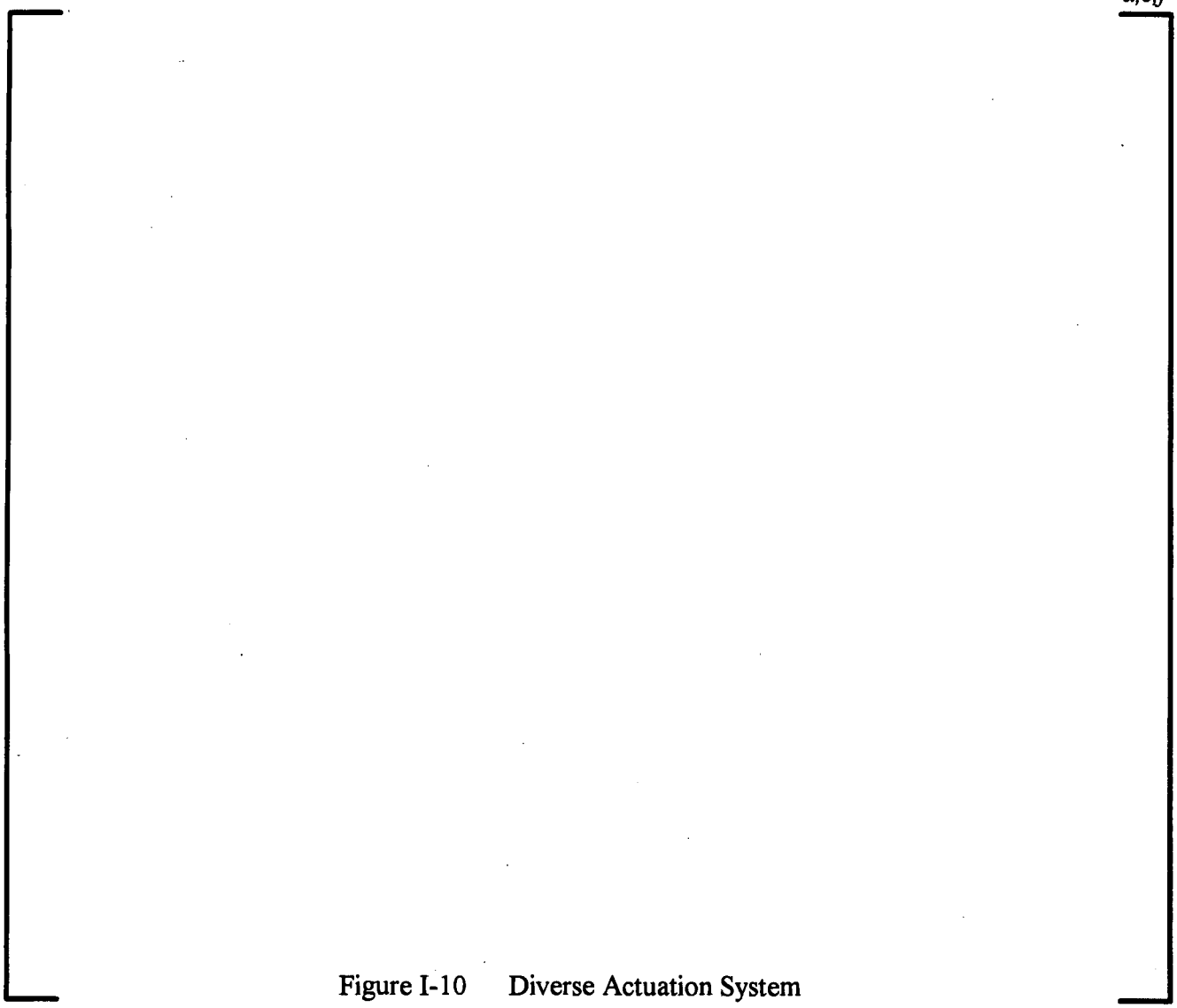


Figure I-10 Diverse Actuation System

a,c,f

Figure 1-11 Detailed Architecture

Section II

Protection System Test Approach

for the Kewaunee Nuclear Power Plant
Reactor Protection System
Upgrade Project

June 1999

Table of Contents

Acronyms and Abbreviations

Cal	Calibration
Chks	Checks
Comp	Comparator
Cont	Continuous
CRC	Cyclical Redundancy Checksum
DTB	Dynamic Trip Bus
ESF	Engineered Safety Features
E/O	Electrical/Optical
HIS	Human System Interface
Inp	Input
I/C	Instrumentation and Control
I/O	Input/Output
KNPP	Kewaunee Nuclear Power Plant
MSMIE	Multiprocessor Shared Memory Information Exchange
O/E	Optical/Electrical
PST	Periodic Semi-automatic Test
RPS	Reactor Protection System
RTM	Real Time Monitor
TSP	Test Sequence Processor
V&V	Verification and Validation

Protection System Test Approach

1.0 Introduction

The KNPP RPS Upgrade Project uses a combination of [

]^{a,c,f}, to provide a complete test of the system.

Figure II-1 graphically shows (only reactor trip system) the process protection racks (vertically) and the voting logic (horizontally). The [ ]^{a,c,f} is shown with bold lines. Representative [ ]^{a,c,f}. Finally, the [sensor test coverage]^{a,c,f} is shown with a dashed line.

The remainder of this document primarily focuses on [ ]^{a,c,f}.

1.1 Periodic Semi-automatic Test Features

The periodic semi-automatic test (PST) demonstrates that the protection system is operational and able to perform its intended function. The PST primarily focuses on the safety related functions, but also supports the test of related non-safety signals generated by the system.

To the extent practicable, all the system is testable during operation of the nuclear power generating station. (The entire system is testable when the station is shut down.) The test can be performed with the channels under test placed in [

]^{a,c,f}. Indication is provided in the control room if a channel of the safety system is bypassed. [ ]^{a,c,f} are applied and removed automatically. The tester monitors system status via the [

]^{a,c,f}. The processing of bypass requests is implemented as part of the [

]^{a,c,f}.

The test interface is part of the [

]^{a,c,f}. There is no loss of independence between redundant channels.

The tester has the capability to vary the [

]^{a,c,f}.

The tester uses a [

]^{a,c,f}.

The tester supports the procedural requirement to [

]^{a,c,f}.

It should be noted that the PST does not include [

]^{a,c,f}.

a,c,f

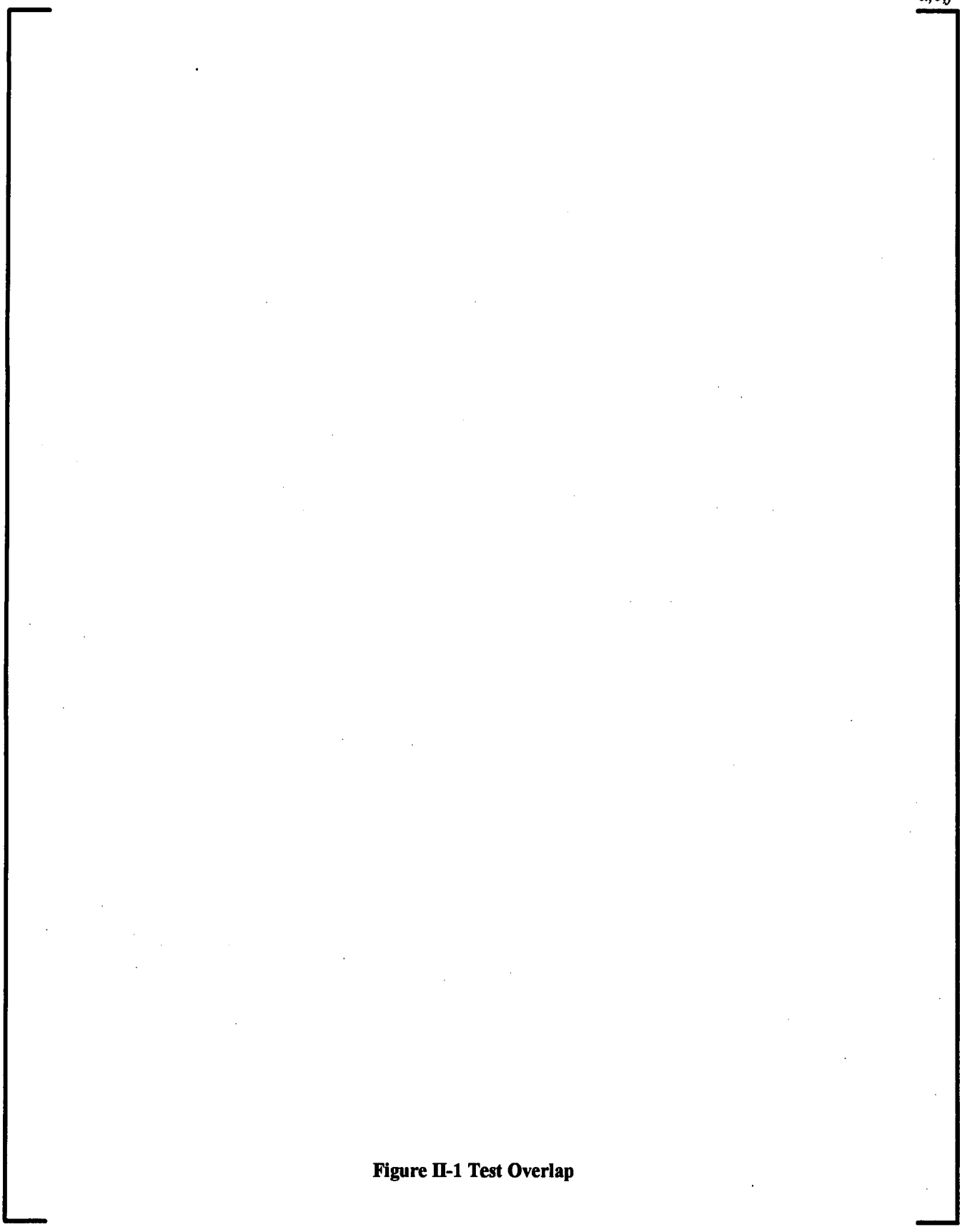


Figure II-1 Test Overlap

1.2 [ ]^{a,c,f}

The periodic semi-automatic test (PST) requires [

]^{a,c,f}.

a. [

]^{a,c,f};

b. [

]^{a,c,f};

c. [

]^{a,c,f};

d. [

]^{a,c,f};

e. [ ]^{a,c,f};

f. [ ]^{a,c,f}.

The test signal generation equipment and the signal monitoring equipment must be periodically calibrated to traceable standards.

1.3 Periodic Semi-Automatic Test (PST) of the [ ]^{a,c,f}

The [

]^{a,c,f}.

The PST requires physical connection to each controller with the [

]^{a,c,f}.

Once connected to the [

]^{a,c,f}.

A key switch on the controller must be used to enable the test interface by selecting [

]^{a,c,f} and all channels associated with the

controller under test are placed in the selected state. Enabling the test interface will actuate an indication in the control room. Additionally, if "Test in Partial Bypass" is selected, the bypass condition will be indicated in the control room. When the key switch is in the "Normal" position, power is removed from the test injection interface, thus preventing test signal injection.

a. [ ]^{a,c,f}

All hardware [ ]^{a,c,f} will be stimulated by the test equipment. The stimulation occurs as [

]^{a,c,f}. While the input is being stimulated, the test equipment monitors the resulting input values as seen by the software running in the subsystem under test. The values are monitored via the [

]^{a,c,f} specified in the plant licensing basis.

Optionally, the manual [

]^{a,c,f}

b. [ ]^{a,c,f}

The tester interacts with the system under test[

]^{a,c,f}.

c. [ ]^{a,c,f}

Hardware outputs (typically data links) required by the safety function are monitored by the test equipment. The outputs are manipulated by [

]^{a,c,f} is calculated and compared to the required value.

d. Manual Test

The tester allows test personal to stimulate the hardware inputs and monitor the outputs to perform specialized tests or trouble shooting.

e. System Restoration

When all tests for the controller under test are complete, the tester will inject the input vector sequences necessary to restore any latches or other retentive memories. The input stimulation portion of the test equipment is then automatically disengaged, and the subsystem is monitored to determine if it was returned to the normal state. Finally, the keyswitch is returned to the normal position.

1.4 Periodic Semi-Automatic Test of the [ ]^{a,c,f}

The [

]^{a,c,f} at a time.

The PST requires physical connection to [

]^{a,c,f}.

While [

]^{a,c,f}. The test of each controller overlaps with this manual test.

A key switch on the controller must be used to [

]^{a,c,f}, thus preventing test signal injection.

a. Input Test

All digital or contact inputs into the [ ]^{a,c,f} will be stimulated by the test equipment. The stimulation occurs as early as practicable in the input circuitry. Only the [originating equipment (e.g., NIS signals) and limited passive components (e.g., relays, resistors) are excluded. These elements are tested during the test of the originating equipment and verification of the overlap at that time. While the input is being stimulated, the test equipment monitors the resulting input values as seen by the software running in the subsystem under test. The values are monitored via the SafetyNet Information Bus]^{a,c,f}.

The [

]^{a,c,f} of the process protection controllers.

b. [ ]^{a,c,f}

The tester interacts with the system under test [

]^{a,c,f}.

c. Output Test

Hardware outputs required by the protection function are monitored by the test equipment. The outputs are manipulated by [

]^{a,c,f}

During the output test, the status of the controller's [

]^{a,c,f}

Note that indicator, status light, and annunciator outputs, although active during the PST, are [

]^{a,c,f}.

d. Manual Test

The tester allows I&C personal to use the test interface to perform specialized tests or trouble shooting.

e. System Restoration

When all tests for the controller are complete, the tester will inject the input vector sequences necessary to restore any latches or other retentive memories. The input stimulation portion of the test equipment is then automatically disengaged, and the subsystem is monitored to determine if it was returned to the normal state. Finally, the keyswitch is returned to the normal position.

1.5 Periodic Semi-Automatic Test of the [ ]^{a,c,f}

The [

]^{a,c,f} at a time.

The PST requires physical connection to each controller with the [

]^{a,c,f}.

Once connected to the [

]^{a,c,f}.

A key switch on the controller must be used to enable the test interface. Enabling the test interface will actuate an indication in the control room. When the key switch is in the "Normal" position, power is removed from the test injection interface, thus preventing test signal injection.

a. Input Test

All hardware inputs (typically digital or contact inputs) required by the protection function will be stimulated by the test equipment. The stimulation occurs as [

]^{a,c,f}.

[

]^{a,c,f}.

b. Software Transfer Function, Timing, and Filtering Algorithm Test

The tester interacts with the system under test [

]^{a,c,f}.

c. Output Test

Hardware outputs (typically contact outputs) required by the protection function are manipulated by [

]^{a,c,f}

The contact output modules directly drive the [

]^{a,c,f}.

In the case of [

]^{a,c,f}. The truth table for the threshold circuits is shown in Table II-I.

[*a,c,f*]

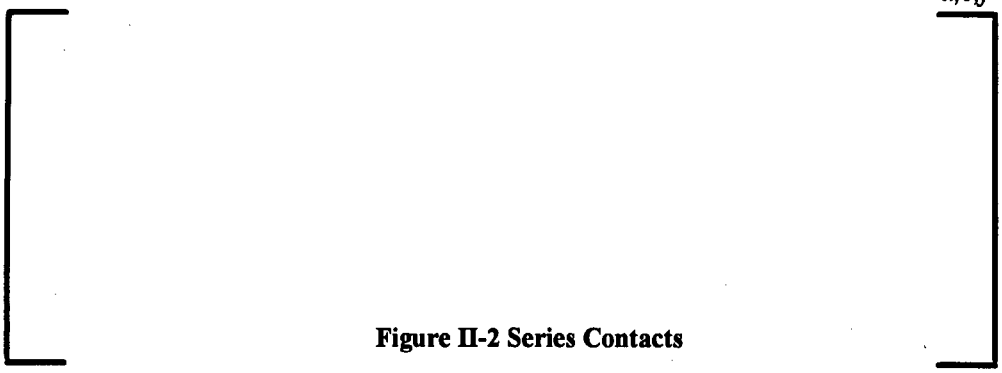


Figure II-2 Series Contacts

[*a,c,f*]

Table II-I Truth Table of Threshold Circuits for Series Contacts

In the case of [

]^{a,c,f}.

a,c,f

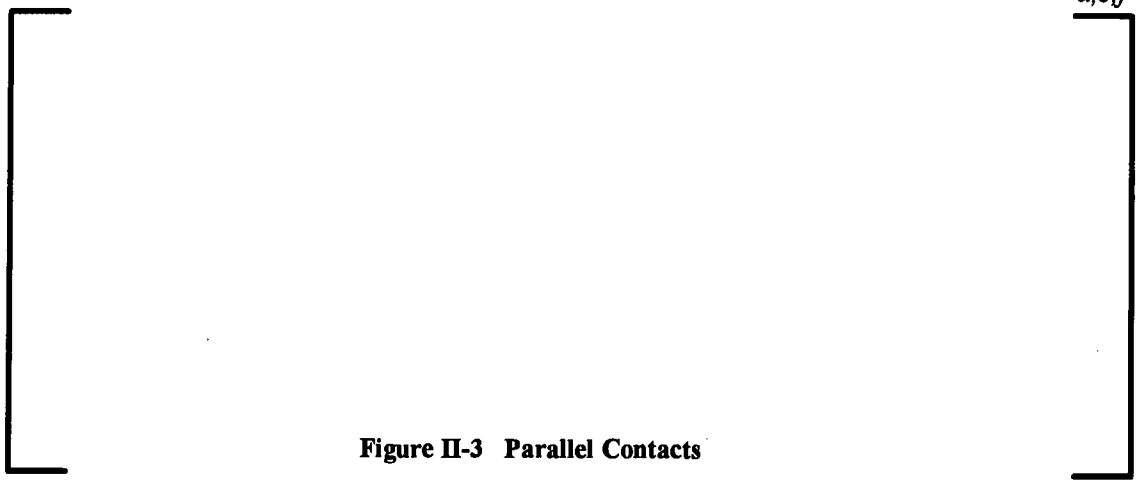


Figure II-3 Parallel Contacts

In the event that the plant state does not result in V_s being available at the contacts (i.e., the external circuit has another set of open series contacts), administrative procedures will be required to direct I&C personnel to manually confirm contact position.

Note that indicator, status light, and annunciator outputs, although active during the PST, are [

]^{a,c,f}.

d. Manual Test

The tester allows I&C personal to use the test interface to perform specialized tests or trouble shooting.

e. System Restoration

When all tests for the controller under test are complete, the tester will inject the input vector sequences necessary to restore any latches or other retentive memories. The input stimulation portion of the test equipment is then automatically disengaged, and the subsystem is monitored to determine if it was returned to the normal state. Finally, the keyswitch is returned to the normal position.

Section III

Diversity & Defense-in-Depth Analysis

for the
Kewaunee Nuclear Power Plant
Reactor Protection System
Upgrade Project

June 1999

Table of Contents

Acronyms and Abbreviations

AC	Alternating Current
AMSAC	ATWS Mitigating System Actuation Circuitry
AOO	Anticipated Operational Occurrence
ATWS	Anticipated Transient Without Scram
CFR	Code of Federal Regulations
CMF	Common Mode Failure
DBE	Design Basis Event
D&D-in-D	Diversity & Defense-in-Depth
DNBR	Departure from Nucleate Boiling
ESF	Engineered Safety Features
I&C	Instrumentation and Control
I/O	Input/Output
IV&V	Independent Verification and Validation
KNPP	Kewaunee Nuclear Power Plant
LOCA	Loss of Coolant Accident
M-G	Motor Generator
NIS	Nuclear Instrumentation System
NRC	Nuclear Regulatory Commission
NRS	Narrow Range Span
PLC	Programmable Logic Controller
RCCA	Rod Control Cluster Assembly
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RMS	Radiation Monitoring System
RPS	Reactor Protection System
RT	Reactor Trip
RTD	Resistance Temperature Device
RWST	Refueling Water Storage Tank
RXCP	Reactor Coolant Pump
SI	Safety Injection
SG	Steam Generator
USAR	Updated Safety Analysis Report

Definitions

Redundant Component or System

A component or system that independently duplicates the function of another component or system

Diverse component or system

A component or system that duplicates the function of another component or system by employing different physical construction or different principles of operation

Echelons of Defense

Specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip system, the ESF system and the monitoring and indicator system (including manual controls).

Diversity & Defense-in-Deptb Analysis

1.0 Introduction

As analog equipment that is being used to implement the protection functions within operating plants approach the end of its design life, many plants are evaluating the feasibility of replacing the analog equipment with digital-based systems. Analog system failure modes and consequences have been historically defined. Licensing precedent has established that failures in analog systems are considered single random failures. However, the installation of digital-based I&C replacement systems raises an additional concern of software failures and increases the vulnerability of the protection systems to common mode failures due to software errors. As stated in Reference 5,

> "Common mode failures (CMFs) are causally related failures of redundant or separate equipment, for example, (1) CMF of identical subsystems across redundant channels, defeating the purpose of redundancy, or (2) CMF of different subsystems or echelons of defense, defeating the use of diversity. CMF embraces all causal relations, including severe environments, design errors, calibration and maintenance errors, and consequential failures".

The NRC has stated in Reference 8,

> "that software design errors are a credible source of common-mode failures. Software cannot be proven to be error-free, and therefore is considered susceptible to common-mode failures because identical copies of the software are present in redundant channels of safety-related systems".

To address the increased potential for common mode errors due to the implementation of protection systems on digital-based systems, the NRC has taken the position in Reference 8 that applicants assess the Diversity & Defense-in-Depth (D&D-in-D) of the proposed digital-based I&C system to demonstrate that vulnerabilities to CMFs have been adequately addressed.

This report provides a summary of the results of the D&D-in-D analysis that was conducted on the proposed Kewaunee Reactor Protection System Upgrade Project.

2.0 Types of I&C System Diversity

Diversity is a principle in instrumentation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a postulated event. Types of diversity have been segregated into six different areas (Reference 5): functional diversity; signal diversity; design diversity; equipment diversity; software diversity; and human diversity.

Several design aspects of the architecture were chosen to maximize the degree of diversity of the system. The various design features of the I&C architecture illustrated in Figure III-1, as they relate to diversity, will be discussed.

a. Functional Diversity

The reactor trip and ESF protective functions have been [ ]^{a,c,f} to the extent practicable. [ ]^{a,c,f}. This strategy results in a design that maximizes functional diversity.

The following [ ]^{a,c,f} has been identified. These two [ ]^{a,c,f} for nearly all the AOOs and DBEs analyzed in the USAR.

[ ]^{a,c,f}

[ ]^{a,c,f}
[ ]^{a,c,f}
[ ]^{a,c,f}
[ ]^{a,c,f}
[ ]^{a,c,f}
[ ]^{a,c,f}
[ ]^{a,c,f}
[ ]^{a,c,f}

b. Signal Diversity

Review of the [ ]^{a,c,f} protective functions illustrates that many diverse process variables are input to the protection system. The list below segregates the variables into groups associated with various plant systems.

System	Variables Monitored
Reactor Coolant System	RCS temperature Pressurizer pressure

	Pressurizer level RCS flow
Secondary Loop	Steamline pressure Steam generator level Feedwater flow Steamline flow
Reactor Containment	Containment pressure Containment radiation (via RMS)
Neutron Flux	Neutron flux magnitude Neutron flux axial distribution Neutron flux rate of change
Electrical Parameters	RXCP bus voltage RXCP bus frequency

The type of sensor, process measurement technique, associated analog or contact input card, and software processing modules used are significantly different for pressure, temperature, electrical and neutron flux measurements.

An example of a design feature within the protection system that illustrates the use of signal diversity is as follows: the Permissive P-7 is generated from Permissive P-10 and Permissive P-13. Permissive P-10 is derived from a neutron flux measurement and Permissive P-13 is derived from a turbine flrst stage pressure measurement. These two measurements provide a diverse means of measuring reactor power.

In addition, requirements are provided to the I&C system designers concerning specifIc input signals that must not be [

]^{a,c,f} associated with a channel.

For example, the following pressure and delta pressure process variable inputs must not be [ ]^{a,c,f}

[ ]^{a,c,f}
[ ]^{a,c,f}
[ ]^{a,c,f}

Another example concerning process flow measurements, the following variables must not]^{a,c,f}

[ ]^{a,c,f}
[ ]^{a,c,f}

These process variable input signals are required to be [ ]^{a,c,f} since they provide protection for different flssion product barriers.

c. Equipment Diversity

1. Signiflcantly different types of equipment are utilized for measuring the various types of process and system variables. Examples of equipment diversity are provided in the measurement of pressure, temperature, bus voltage and frequency, neutron flux, and radiation variables.
2. The NIS system, which is implemented on a diverse platform, is not being replaced as part of the KNPP RPS upgrade project
3. The RXCP bus voltage and breaker position signals are not being replaced as part of the KNPP RPS upgrade project
4. The plant control system hardware is not being replaced as part of the I&C upgrade project which is currently implemented on analog equipment.
5. KNPP has installed an AMSAC system using an Allen Bradley Programmable Logic Controller (PLC) to implement the requirements of 10 CFR Part 50.62 (Reference 2).
6. No modifications are being made to the control room control consoles associated with the I&C upgrade project, i.e., the same analog controls and indicators will continue to be used by the operators.

d. Design Diversity

Several aspects of the design process minimize the probability of software CMFs occurring in the digital-based system. Included among these features are the following:

1. Following a rigid implementation of a quality assurance and quality control plan that meets 10 CFR Part 50 Appendix B, "Quality Assurance Criteria for Nuclear Power Plants".
2. Independent verification and validation (IV&V) - Several intermediate products of the design are independently verified that each module meets the requirements specifled in the module software speciflcations.

Also, as discussed under equipment diversity, parts of each of the four echelons of defense are not included in the RPS I&C replacement project.

The original plant equipment, which is being maintained, was designed by diverse design organizations. The equipment not being replaced includes the NIS system, plant control systems, ATWS mitigation system, and control room control consoles.

e. Software Diversity

There exists several levels of defense against software CMFs:

First Level of Defense

The primary defense against software CMFs is to generate and install software that exhibits high integrity which ensures the system performs its required protective functions. The NRC stated in Reference 6,

> "the two principle factors for defense against common-mode/common-cause failures are quality and diversity. Maintaining high quality will increase the reliability of both individual components and complete systems. Diversity in assigned functions (for both equipment and human activities), equipment, hardware, and software can reduce the probability that a common-mode failure will propagate".

There is no single process that can guarantee the production of high integrity software. Important aspects of the KNPP upgrade project software life-cycle plan that contribute to high integrity software include the following:

1. Software architecture and implementation that supports a value-added IV&V process. For example, [

   ]^{a,c,f} lead to highly deterministic processor operation. This design concept results in a [

   ]^{a,c,f}. Adoption of these features facilitates verifying the software will operate correctly during all postulated AOOs and DBEs in the plant licensing basis.
2. Generating application software that is as simple as possible. The goal is to have a [

   ]^{a,c,f}. This increases the probability that the protection function requirements will be correctly translated. This approach improves the [

]^{a,c,f}.

3. Use of a [ ]^{a,c,f} that support a wide range of application functions that may be required. These [ ]^{a,c,f}. These [ ]^{a,c,f} are decomposed into a number of functions that will work together, but whose internal designs are as independent as practical. As much of the software complexity as possible should be implemented in the [ ]^{a,c,f}.
4. The [ ]^{a,c,f}, and do not have to be recreated and verified for each instance of use.
5. The software associated with the protection channels have a different [ ]^{a,c,f}. This is illustrated by the sensors terminated in the various process protection racks as shown in Table III-1.

Second Level of Defense

A second level of defense against software CMFs is the use of fail-safe system design principles and defensive software design principles. Hardware modules are designed to revert to the safe state if the hardware fails. The use of simple [ ]^{a,c,f} simple and reliable. Extensive diagnostic checks are made to detect the presence of incorrect operation and to place the system in default safe states when errors are detected. Each software module performs [ ]^{a,c,f} over which the module has been verified to operate correctly. Software design and coding standards constrain the use of design and implementation techniques that are known to be error prone.

Third Level of Defense

The third line of defense against software CMFs is D&D-in-D. D&D-in-D is defined as "a concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment" in Reference 5. Several features of the design incorporate diversity in software including the following:

1. Different software exists in process protection [ ]^{a,c,f} due to different input sensors and different protection functions
2. Different software in the protection system and DAS.

f. Human Diversity

As mentioned above, the NIS instrumentation, the ATWS mitigation system, the plant control systems and the control board indicators have been designed by different design organizations over a period of many years. As a result, different maintenance and calibration procedures are associated with each of these subsystems.

For the I&C replacement system, the personnel in the hardware and software design groups are different from the personnel that will conduct the hardware and software IV&V tests.

3.0 Evaluation of Echelons of Defense

An evaluation was conducted to identify the diversity that exists between the echelons of defense for the KNPP RPS upgrade project. The results of the evaluation, as provided in Table III-2, can be summarized as follows:

a. [ ]^{a,c,f};

b. [ ]^{a,c,f};

c. [ ]^{a,c,f}.

4.0 Plant Licensing Basis Following Postulated Anticipated Operational Occurrences and Design Basis Events

An evaluation was conducted to determine the primary and back-up protection functions that are assumed for mitigation of each of the anticipated operational occurrences and design basis events that are analyzed in the KNPP USAR Chapter 14. Table III-3 provides a tabular listing for each anticipated operational occurrence (AOO) and design basis event (DBE) discussed in Chapter 14 of the KNPP USAR. Through a comparison of the primary and back-up protections functions for each AOO and DBE provided in Table III-3 and the protection functions identifled in Groups 1 and 2 (section 2.a), the primary [ ]^{a,c,f}.

5.0 Diversity and Defense-in-Depth Analysis Guidelines

Prior to performing the D&D-in-D evaluation, acceptance criteria were established upon which to determine if the diversity principles that are evident with the proposed I&C replacement system are adequate. Based upon the guidance presented in Reference 5, the following acceptance criteria are adopted:

a. For each anticipated operational occurrence analyzed in the plant licensing basis as presented in the KNPP USAR occurring in conjunction with each postulated CMF, the plant response calculated using best-estimate assumptions (realistic assumptions) should not exceed a small fraction (10%) of the 10 CFR Part 100 dose limit or violation of the integrity of the primary coolant pressure boundary.
b. For each limiting fault in the plant licensing basis as presented in the KNPP USAR occurring in conjunction with each postulated CMF, the plant response calculated using best-estimate (realistic assumptions) should not exceed the 10 CFR Part 100 dose limits, violate the integrity of the primary reactor coolant pressure boundary, or violate the integrity of the containment pressure boundary.

Based upon the above assumptions, the following software CMFs were considered when performing the evaluation (refer to Figure III-1 for block designation):

a. [ ]^{a,c,f,};

b. [ ]^{a,c,f,};

c. [ ]^{a,c,f,};

d. [ ]^{a,c,f,};

e. [ ]^{a,c,f,};

f. [ ]^{a,c,f,};

g. [ ]^{a,c,f}.

6.0 Diversity & Defense-in-Depth Evaluation Results

An evaluation was conducted to determine which diverse actuation functions, if any, are required to demonstrate sufficient diversity exists in the plant I&C system design for each AOO and DBE, in conjunction with a postulated software CMF, analyzed in the plant USAR chapter I4. The results of the evaluation are provided

in Table III-4. A brief discussion for each anticipated operational occurrence and design basis event presented in the KNPP USAR is provided in the attached Appendix A.

Automatic Diverse Protection Functions

As illustrated in Table III-4, there are [ ]^{a,c,f}.

a. [ ]^{a,c,f};
b. [ ]^{a,c,f};
c. [ ]^{a,c,f}.

A brief description of the required diverse actuation systems is provided in Table III-5.

As indicated in Figure III-1, the automatic diverse actuation functions are implemented on a diverse hardware and software platform [ ]^{a,c,f} that provides actuation signals to the final actuated device. In the case of reactor trip, the trip signal removes the generator output voltage to the M-G voltage regulator that supplies voltage to the exciter fleld resulting in loss of the M-G set output voltage. For the auxiliary feedwater pumps, the actuation signal from the diverse actuation circuitry closes a contact in parallel with a contact that is closed by the actuation signal from the RPS.

Manual Diverse Controls

The operator must also have the capability to manually initiate several protection components following any AOO or DBS in conjunction with a postulated software CMF:

a. [ ]^{a,c,f}
b. [ ]^{a,c,f}
c. [ ]^{a,c,f}
d. [ ]^{a,c,f}
e. [ ]^{a,c,f}
f. [ ]^{a,c,f}
g. [ ]^{a,c,f}
h. [ ]^{a,c,f}
i. [ ]^{a,c,f}
j. [ ]^{a,c,f}

k. [ ]^{a,c,f}

Also illustrated in Figure III-1, the signals from the control room control consoles [^{a,c,f} with the flnal actuated device. The relationship between the [ ]^{a,c,f} and the AOO or DBE in which the operator must utilize the control is illustrated in Table III-6.

Diverse Monitoring

Process and system variables must be displayed on the control room control consoles to enable the operator to [ ]^{a,c,f}. The relationships between the [ ]^{a,c,f} are provided in Table III-7.

The diverse indications must not be susceptible to a postulated software CMF in the RPS. As illustrated in Figure III-1, the outputs from the sensors which have associated [ ]^{a,c,f}. This ensures that a postulated software CMF in the RPS process cabinet controllers would not degrade the [ ]^{a,c,f}.

7.0 Summary

The installation of digital-based I&C replacement systems introduces an additional postulated failure mode mechanism and increases the vulnerability of protection systems across redundant channels due to software CMFs. The NRC staff is concerned that the use of digital-based systems in protection systems could result in safety significant common-mode failures. The staff "considers common-mode software errors to be a special case of single failure and, therefore, protection against such errors is to be part of the design basis". The NRC has stated that "the two principle factors for defense against common-mode/common-cause failures are quality and diversity. Maintaining high quality will increase the reliability of both individual components and complete systems. Diversity in assigned functions ... can reduce the probability that a common-mode failure will propagate".

There are several different types of diversity, each of which offers protection against common-mode failures. Types of diversity include functional diversity, signal diversity, equipment diversity, design diversity, software diversity and human diversity. There are many aspects of the system design process that minimize the exposure to postulated CMFs. These include the following:

a. Implementing primary and back-up protection functions on different processors
b. Measurement of diverse process variable inputs
c. Implementing the "echelon of defense" on different platforms
d. Utilizing different design organizations for design of the "echelons of defense"
e. Establishing a simple design and software life cycle process
f. Providing continuous self-diagnostic features
g. Requiring IV&V of each step in the process

Based upon the D&D-in-D analysis that was performed, the following conclusions are reached:

a. [

]^{a,c,f} as summarized in Table III-5. The existing AMSAC at KNPP generates the following automatic actuation signals:

1. Reactor trip and turbine trip on three out of four steam generator low-low level signals below the set point
2. Auxiliary feedwater pumps actuation on three out of four steam generator low-low level signals below the set point

The only [ ]^{a,c,f} is the following:

1. [

]^{a,c,f}.

The combination of these [

]^{a,c,f}.

b. The operator must have the capability to [

]^{a,c,f} to mitigate various AOOs and DBEs. The signals from dedicated controls on the control room control console interface directly with the flnal actuated device. The components that must be [

]^{a,c,f} are summarized in Table III-6.

c. Process and system variables must be displayed in the control room to enable the operator to monitor the [

]^{a,c,f} that must be available following a postulated software CMF are listed in Table III-7. The outputs from the [

]^{a,c,f}.

8.0 References

1. NUREG-0493, A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System, March 1979
2. 10 CFR Part 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants
3. SECY-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, Section II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems, April 2, 1993
4. Diablo Canyon Safety Evaluation Report on Eagle 21 Reactor Protection System Modification, October 7, 1993
5. NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, December 1994
6. NUREG-1512, Final Safety Evaluation Report Related to Final Certification of the AP600 Standard Design
7. NUREG-1503, Final Safety Evaluation Report Related to the Certification of the US ABWR Design
8. Branch Technical Position HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

Sensor/Cabinet Termination Arrangement
Table III-1

Cabinet 1R1 (108)	Cabinet 1W1 (114)	Cabinet 1B1 (112)	Cabinet 1Y1 (106)	Protection Function
TE-401A	TE-402A	TE-403A	TE-404A	RCS Hot Leg Temperature
TE-405A	TE-406A	TE-407A	TE-408A	Spare Hot Leg RTD
TE-401B	TE-402B	TE-403B	TE-404B	RCS Cold Leg Temperature
TE-405B	TE-406B	TE-407B	TE-408B	Spare Cold Leg RTD
NE-41 Q_u	NE-42 Q_u	NE-43 Q_u	NE-44 Q_u	Upper Detector Flux
NE-41 Q_l	NE-42 Q_l	NE-43 Q_l	NE-44 Q_l	Lower Detector Flux
PT-429	PT-430	PT-431	PT-449	Pressurizer Pressure
LT-426	LT-427	LT-428		Pressurizer Level
	PT-485	PT-486		Turbine Impulse Pressure
Cabinet 1R2 (109)	Cabinet 1W2 (115)	Cabinet 1B2 (113)	Cabinet 1Y2 (107)	Protection Function
PT-464	FT-465			Steam Flow Loop A
		FT-474	FT-475	Steam Flow Loop B
PT-468	FT-469	PT-482		Steamline Pressure Loop A
PT-483		PT-478	PT-479	Steamline Pressure Loop B
FT-466	FT-467			Feed Flow Loop A
		FT-476	FT-477	Feed Flow Loop B
LT-461		LT-462	LT-463	SG Level Loop A
LT-472	LT-473		LT-471	SG Level Loop B
PT-411	FT-412	FT-413		RCS Flow Loop A
FT-414		FT-415	PT-416	RCS Flow Loop B
PT-945	PT-946		FT-947	Containment Pressure
	PT-949	PT-948	FT-950	Containment Pressure

Diversity Between Echelons of Defense
Table III-2

Feature	Control	Reactor Trip		ESF		Indication and Monitoring
		Process Protection	Voting Logic	Process Protection	Voting Logic	
Sensors	• [ ]^{a,c,f} • Sensors ouly used for control independent of other systems • Sensors shared with RPS and ESF dependent upon RPS and ESF systems	Senses different types of process variables - pressure - temperature - water level - flow - bus voltage - breaker position - neutron flux	• RXCP bus voltage and breaker position input directly to voting logic • NIS signals input directly to voting logic	• Different sensors used between reaetor trip, ESF and control	Not Applicable	• [ ]]^{a,c,f} • Sensors (direct) inputs independent of other systems • Display devices utilize diverse platform

Diversity Between Echelons of Defense
Table III-2

Feature	Control	Reactor Trip		ESF		Indication and Monitoring
		Process Protection	Voting Logic	Process Protection	Voting Logic	
Hardware	Implemented on analog platform	• Implemented on safety platform • NIS implemented on diverse platform	Implemented on safety platform	Same as RPS	Same as RPS	• Signals displayed in control room on "analog" meters • Manual component control independent of RPS and ESF
Software	Not Applicable, analog platform	• [ ]^{a,c,f} • [ ]^{a,c,f} • NIS implemented on diverse platform	• [ ]^{a,c,f} • [ ]^{a,c,f}	• Same as RPS	• Same as RPS	• Sensor (direct) inputs independent of other systems • [ ]^{a,c,f} • [ ]^{a,c,f}

Plant Licensing Basis Analysis Results
Tahle III-3

Anticipated Operatioual Occurrenee or Design Basis Event	USAR Referenee Section	Primary Mitigation Protection Function	Back-up Mitigation Protection Function
Uncontrolled RCCA Withdrawal froin a Subcritical Condition	14.1.1	Power range high flux (low set point) RT	Source range high flux RT Intermediate range high flux RT Power range high flux (high set point) RT Pressurizer high pressure RT
Uncontrolled RCCA Withdrawal at Power	14.1.2	Power range high flux (high set point) RT Overtemperature ΔT RT	Overpower ΔT RT Pressurizer high pressure RT Pressurizer high water level RT
RCCA Misalignment	14.1.3	Power range negative flux rate RT	Manual
CVCS Malfunction (Boron Dilution)	14.1.4	Overtemperature ΔT RT	Power range high flux (high set point) RT Overpower ΔT RT Source range high flux RT Intermediate range high flux RT
Startup of an Inactive Reaetor Coolant Pump	14.1.5	None required	Power range high flux (high set point) RT
Excessive Heat Reinoval due to Feedwater Systeiu Malfunctions	14.1.6	Power range high flux (low set point) RT	Overtemperature ΔT RT Overpower ΔT RT Steam generator high level TT Steam generator high level FWI
Excessive Load Increase	14.1.7	None required	Power range high flux (high set point) RT Overtemperature ΔT RT Overpower ΔT RT Pressurizer low pressure RT
Loss of Reactor Coolant Flow	14.1.8	RCS low flow RT RXCP breaker open RT	RXCP undervoltage RT Overtemperature ΔT RT Pressurizer high pressure RT

Plant Licensing Basis Analysis Results
Table III-3

Anticipated Operatioual Occurrence or Design Basis Event	USAR Reference Section	Primary Mitigation Protectiou Function	Back-up Mitigation Protection Function
Loss of External Electrical Load	14.1.9	Pressurizer high pressure RT	Overtemperature ΔT RT Overpower ΔT RT Pressurizer high water level RT
Loss of Normal Feedwater	14.1.10	Steam generator low-low water level RT Auxiliary feedwater pnmp actuation	Steam generator low feedwater flow RT Pressurizer high pressure RT Pressurizer High water level RT Loss of voltage auxiliary feedwater pnmps actuation
Anticipated Transients Without Scram	14.1.11	Refer to diverse mitigating functious in Table 4.2	Refer to diverse mitigating functions in Table 4.2
Loss of AC Power to Plant Auxiliaries	14.1.12	RXCP bus undervoltage RT Loss of voltage auxiliary feedwater pnmps actuation	Steam generator low-low water level RT
Fuel handling Accidents	14.2.1	Admimistrative control	Administrative control
Accidental Release-Recycle of Waste Liquid	14.2.2	Admimistrative control	Administrative control
Accideutal Release-Waste Gas	14.2.3	Admimistrative control	Administrative control
Steam Generator Tube Rupture	14.2.4	Pressurizer low pressure RT Pressurizer low pressure SI	Overtemperature ΔT RT Steam generator high level turbine trip Auxiliary feedwater pump actuation on SI signal
Steamline Break	14.2.5	Pressurizer low pressure SI Steamline low pressure SI Containment hi pressure SI and SLI SI & steamline hi-hi flow SLI SI & steamline hi flow & low-low T_{avg} SLI	Overpower ΔT RT Overtemperature ΔT RT Power range high flux RT
Rupture of a Control Rod Drive Mechanism Housing (RCCA Ejection)	14.2.6	Power range high flux (high set point) RT Power range high flux (low set point) RT	Source range high flux RT Intermediate range high flux RT Overteinperature ΔT RT Overpower ΔT RT

Plant Licensing Basis Analysis Resnlts Table III-3			
Anticipated Operatioual Occurrence or Design Basis Event	USAR Reference Section	Primary Mitigation Protection Function	Back-up Mitigation Protection Function
Turbine Missile Damage to Spent Fuel Pool	14.2.7	None required	None required
Loss of Reactor Coolant froin Small Ruptured Pipes or froin Cracks in Large Pipes which Actuates Emcrgency Core Cooling Systeiii	14.3.1	Pressurizer low pressure RT Pressurizer low pressure SI	Containment hi pressure SI Containment hi-hi pressure spray actuation
Major Reactor Coolant Systeiii Pipe Ruptures (Loss of Coolant Accident)	14.3.2	Pressurizer low pressure SI	Containment hi pressure SI Containment hi-hi pressure spray actuation
Core and Internals Integrity Analysis	14.3.3	Refer to USAR sectious 14.3.1 and 14.3.2.	NA
Containment Integrity Evaluation	14.3.4	Refer to USAR sections 14.3.1 and 14.3.2.	NA
Off-Site Dose Calculations	14.3.5	Refer to USAR sections 14.3.1 and 14.3.2.	NA
Delcted in USAR	14.3.6	NA	NA
Effects of Leakage from Residual Heat Removal Systeiii	14.3.7	None required	None required
Charcoal Filter Ignition Hazard Due to Iodine Absorption	14.3.8	None required	None required
Generation and Disposition of Hydrogen	14.3.9	None required	None required
Steam Generator Tube Sleeving	14.3.10	Not an AOO or DBE	Not an AOO or DBE
Steam Generator Tube Fatigue Analysis	14.3.11	Not an AOO or DBE	Not an AOO or DBE
Steam Generator Plug PIPs	14.3.12	Not an AOO or DBE	Not an AOO or DBE
Voltage Bused Repair Criteria for Steam Generator Tubes	14.3.13	Not an AOO or DBE	Not an AOO or DBE
F* and Elevated F* Alternative Repair Criteria for Steam Generator Tubes	14.3.14	Not an AOO or DBE	Not an AOO or DBE
Steam Generator Tube Removal	14.3.15	Not an AOO or DBE	Not an AOO or DBE

Anticipated Operational Occnrrences and Design Basis Events Diverse Mitigation Functions
Table III-4

Anticipated Operatioual Occurrence or Design Basis Event	USAR Reference Section	Diverse Mitigation Function	Worst Assumed Software CMF as Defined in Section 4.0
Uncontrolled RCCA Withdrawal from a Subcritical Condition	14.1.1	[ ]^{a,c,f}	[ ]^{a,c,f}
Uncontrolled RCCA Withdrawal at Power	14.1.2	[ ]^{a,c,f}	[ ]^{a,c,f} [ ]^{a,c,f}
RCCA Misalignment	14.1.3	[ ]^{a,c,f}	NA
CVCS Malfunction	14.1.4	[ ]^{a,c,f} [ ]^{a,c,f}	[ ]^{a,c,f}
Startup of an Inactive Reaetor Coolant Pump	14.1.5	[ ]^{a,c,f}	NA
Excessive Heat Removal due to Feedwater System Malfunctions	14.1.6	[ ]^{a,c,f}	[ ]^{a,c,f} [ ]^{a,c,f}
Excessive Load Increase	14.1.7	[ ]^{a,c,f}	NA
Loss of Reaetor Coolant Flow	14.I.8	[ ]^{a,c,f}	[ ]^{a,c,f} [ ]^{a,c,f}
Loss of External Electrical Load	14.1.9	[ ]^{a,c,f}	[ ]^{a,c,f}
Loss of Normal Feedwater	I4.1.10	[ ]^{a,c,f} [ ]^{a,c,f}	[ ]^{a,c,f}
Anticipated Transieuts Without Scram	14.1.11	[ ]^{a,c,f} [ ]^{a,c,f} [ ]^{a,c,f}	NA
Loss of AC Power to Plant Auxiliaries	14.1.12	[ ]^{a,c,f} [	[ ]^{a,c,f}

Anticipated Operational Occnrrences and Design Basis Events Diverse Mitigation Functions
Table III-4

Anticipated Operatioual Occurrence or Design Basis Event	USAR Reference Section	Diverse Mitigation Function	Worst Assumed Software CMF as Defined in Section 4.0
		[ ]a,c,f	
Fuel handling Accidents	14.2.1	[ ]a,c,f	NA
Accidental Release-Recycle of Waste Liquid	14.2.2	[ ]a,c,f	NA
Accidental Release-Waste Gas	14.2.3	[ ]a,c,f	NA
Steam Generator Tube Rupture	14.2.4	[ ]a,c,f [ ]a,c,f [ ]a,c,f	[ ]a,c,f
Steamline Break	14.2.5	[ ]a,c,f [ ]a,c,f [ ]a,c,f [ ]a,c,f [ ]a,c,f [ ]a,c,f [ ]a,c,f	[ ]a,c,f
Rupture of a Control Rod Drive Mcchanism Housing (RCCA Ejection)	14.2.6	[ ]a,c,f	[ ]a,c,f
Turbine Missile Damage to Spent Fuel Pool	14.2.7	[ ]a,c,f	NA
Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes which Actuates Emergency Core Cooling	14.3.1	[ ]a,c,f [ ]a,c,f	[ ]a,c,f

Anticipated Operational Occurrences and Design Basis Events Diverse Mitigation Fnnctions
Table III-4

Anticipated Operatioual Occurrence or Design Basis Event	USAR Refereuce Section	Diverse Mitigation Function	Worst Assumed Software CMF as Defined in Section 4.0
System		[ ]^{a,c,f} [ ]^{a,c,f}	
Major Reactor Coolant Systeın Pipe Ruptures (Loss of Coolant Accident)	14.3.2	[ ]^{a,c,f} [ ]^{a,c,f} [ ]^{a,c,f} [ ]^{a,c,f} [ ]^{a,c,f}	[ ]^{a,c,f}
Core and Internals Integrity Analysis	14.3.3	Refer to USAR sections 14.3.1 and 14.3.2.	NA
Containment Integrity Evaluation	14.3.4	Refer to USAR sections 14.3.1 and 14.3.2.	NA
Off-Site Dose Calculations	14.3.5	Refer to USAR sections 14.3.1 and 14.3.2.	NA
Deleted in USAR	14.3.6	NA	NA
Effects of Leakage from Residual Heat Removal Systeın	14.3.7	[ ]^{a,c,f}	NA
Charcoal Filter Ignition Hazard Due to Iodine Absorption	14.3.8	[ ]^{a,c,f}	NA
Generation and Disposition of Hydrogen	14.3.9	[ ]^{a,c,f}	NA
Steam Generator Tube Sleeving	14.3.10	Not an AOO or DBE	NA
Steam Generator Tube Fatigne Analysis	14.3.11	Not an AOO or DBE	NA
Steam Generator Plug PIPs	14.3.12	Not an AOO or DBE	NA

Anticipated Operational Occurrences and Design Basis Events Diverse Mitigation Functions Table III-4			
Anticipated Operational Occurrence or Design Basis Event	USAR Reference Section	Diverse Mitigation Function	Worst Assumed Software CMF as Defined in Section 4.0
Voltage Based Repair Criteria for Steam Generator Tubes	14.3.13	Not an AOO or DBE	NA
F* and Elevated F* Alternative Repair Criteria for Steam Generator Tubes	14.3.14	Not an AOO or DBE	NA
Steam Generator Tube Removal	14.3.15	Not an AOO or DBE	NA

** These automatic diverse actuated functions are required to meet NUREG/CR-6303 and 10 CFR 50.62 regulations.

a,c,f

Diverse Antomatic Actuation Function Description
Table III-5

a,c,f

Diverse Manual Control Capability
Table III-6

a,c,f

Diverse Variable Display Reqnirements
Table III-7

a,c,f

Diverse Variable Display Requirements
Table III-7

a,c,f

[

]

Diverse Variable Display Requirements
Table III-7

Appendix A

Summary of

Anticipated Operational Occurrences

and

Design Basis Event

Transient Analysis Evaluation

A.1 Introduction

The purpose of Appendix A is to provide a brief summary of the evaluation that was conducted to determine that adequate diverse mitigating functions exist following a postulated software CMF in the Reactor protection System. A brief discussion is provided for each anticipated operational occurrence (AOO) and design basis event (DBE) that are discussed in the KNPP USAR (using the categorization).

A.2 KNPP Chapter 14 AOOs and DBEs

A.2.1 Core and Coolant Boundary Protection Analysis

A.2.1.1 Uncontrolled RCCA Withdrawal from a Subcritical Condition (USAR 14.1.1)

The primary mitigation function for this event is power range neutron flux (low set point) reactor trip. Backup protection is provided by source range high flux, intermediate range high flux and power range high flux (high set point) reactor trip signals. [

]^{a,c,f} provides the diverse protection and the plant response meets the applicable acceptance criteria.

A.2.1.2 Uncontrolled RCCA Withdrawal at Power (USAR 14.1.2)

The primary mitigating function for this event is either the power range high neutron flux (high set point) or the overtemperature ΔT reactor trip signals, dependent upon the rate of reactivity insertion. The back-up mitigating functions include overpower ΔT, pressurizer high pressure, and pressurizer high water level reactor trip functions. [

]^{a,c,f} provides the diverse protection and the plant response meets the applicable acceptance criteria. For slow reactivity insertion rates, the indication of the initiation of the event is provided to the [

]^{a,c,f}.

A.2.1.3 RCCA Misalignment (USAR 14.1.3)

Most events analyzed within this group do not actuate a reactor trip for accident mitigation. Some of the dropped rod events may result in a reactor trip on power range negative flux rate. Manual reactor trip is considered the back-up protection function. Indications of dropped RCCAs or a statically misaligned RCCA are provided by rod deviation alarms, rod position indications and asymmetric power distribution as measured by the excore detectors and core exit thermocouples. [

]^{a,c,f} the diverse protection and the plant response meets the applicable acceptance criteria.

A.2.1.4 CVCS Malfunction (Uncontrolled Boron Dilution) (USAR 14.1.4)

The primary mitigating functions for this event varies as a function of plant operating mode. For the boron dilution event during refueling, the primary mitigating function is manual operator action. The time to reach criticality due to an uncontrolled boron dilution event is in excess of 30 minutes. Indications available to the operator include the[
]^{a,c,f} which is not susceptible to a software CMF.

For the boron dilution event during startup, the primary mitigating function is manual operator action. The minimum time required to reduce the RCS boron concentration to a point where the reactor could return critical is greater than 15 minutes. Indications of a boron dilution event include
[
]^{a,c,f} which is not susceptible to a software CMF.

For this event during power conditions with the rods in manual, the primary mitigating function is power range high neutron flux. For this event during power conditions with the rods in the automatic mode, the primary mitigating function is overtemperature ΔT reactor trip. The back-up mitigating function during startup includes power range high neutron flux, overpower ΔT, source range high flux and intermediate range high flux reactor trip signals. [

]^{a,c,f} provides the diverse protection during power conditions. The diverse mitigating function during the refueling and startup modes is [ ]^{a,c,f}. Under all operating modes with the assumed diverse mitigating functions, the plant response meets the applicable acceptance criteria.

A.2.1.5 Startup of an Inactive Reactor Coolant Pump (USAR 14.1.5)

The protection system prohibits the plant from operating with one loop out of service above approximately 10 percent of full power. As a result of this operating restriction, the plant response for this event does not require any primary mitigating function. The applicable acceptance criteria is met [ ]^{a,c,f}. (Administratively, when the reactor trip breakers are closed, both reactor coolant pumps must be in operation.)

A.2.1.6 Excessive Heat Removal Due to Feedwater System Malfunctions (USAR 14.1.6)

The primary mitigating function for the feedwater malfunction event from no-load conditions is the power range high neutron flux (low set point) reactor trip. The back-up mitigating function for this event is overtemperature ΔT, and overpower ΔT.

For this event from power conditions, no primary or back-up mitigating function is required for this event from power conditions. The plant attains a slightly higher steady state power condition but the minimum DNBR limit is not violated without an assumed reactor trip. Equipment protection is afforded to the turbine from the steam generator high water level turbine trip and main feedwater isolation.

[

]^{a,c,f}.

A.2.1.7 Excessive Load Increase (USAR 14.1.7)

No primary mitigating function is required for this event. The back-up mitigating functions include power range high neutron flux, overtemperature ΔT, overpower ΔT, and pressurizer low pressure reactor trip functions. For all cases analyzed, [ ]^{a,c,f} is required for the plant response to meet the applicable acceptance criteria.

A.2.1.8 Loss of Reactor Coolant Flow (USAR 14.1.8)

The primary mitigating function for a loss of reactor coolant flow (constant bus frequency) is the RCS low flow reactor trip and RXCP breaker open

position. Back-up mitigating function include RXCP bus undervoltage, overtemperature ΔT, and high pressurizer pressure reactor trip. [

]^{a,c,f}.

A.2.1.9 Loss of External Electrical Load (14.1.9)

The primary mitigating function for a loss of load is pressurizer high pressure reactor trip. Back-up mitigation functions include overtemperature ΔT, overpower ΔT and pressurizer high water level. [

]^{a,c,f}.

A.2.1.10 Loss of Normal Feedwater (USAR 14.1.10)

The primary mitigation function for loss of normal feedwater is steam generator low-low water level reactor trip and auxiliary feedwater pump actuation. Back-up mitigation functions include low feedwater flow coincident with low level, pressurizer high pressure, and pressurizer high water level reactor trip. Back-up functions for actuating the auxiliary feedwater pumps is loss of bus voltage. [

]^{a,c,f} provide adequate protection such that the plant response meets the applicable acceptance criteria.

A.2.1.11 Anticipated Transients Without Scram (USAR 14.1.11)

The diverse mitigating functions for ATWS transients are steam generator low-low water level reactor trip and turbine trip, and auxiliary feedwater pumps actuation. The AMSAC system provides a diverse signal for reactor trip by interrupting the voltage to the M-G set exciter field. With these existing diverse functions, the plant response meets the applicable acceptance criteria.

A.2.1.12 Loss of AC Power to Plant Auxiliaries (USAR 14.1.12)

The primary mitigating function for the loss of AC power to station auxiliaries is RXCP bus undervoltage reactor trip and loss of voltage auxiliary feedwater pumps actuation. The back-up mitigating function is steam generator low-low water level reactor trip and auxiliary feedwater pumps actuation. [

]^{a,c,f} provide adequate protection such that the plant response meets the applicable acceptance criteria.

A.2.2 Standby Safety Features Analysis

A.2.2.1 Fuel Handling Accidents (USAR 14.2.1)

The consequences of this postulated event is addressed by administrative action. The USAR calculates an activity release associated with the various events. No automatic protection functions are required.

A.2.2.2 Accidental Release-Recycle of Waste Liquid (USAR 14.2.2)

The consequences of this postulated event is addressed by administrative action. No automatic protection functions are required.

A.2.2.3 Accidental Release-Waste Gas (USAR 14.2.3)

The consequences of this postulated event is addressed by administrative action. The USAR calculates an activity release associated with the various events. No automatic protection functions are required.

A.2.2.4 Steam Generator Tube Rupture (USAR 14.2.4)

The primary mitigation functions for the steam generator tube rupture (SGTR) event is pressurizer low pressure reactor trip and pressurizer low pressure safety injection. Back-up mitigating functions include overtemperature ΔT, auxiliary feedwater pumps actuation on a safety

injection signal, and steam generator high water level turbine trip. [

]^{a,c,f}. By following the appropriate emergency operating procedurcs and using these diverse functions, the plant response meets the applicable acceptance criteria.

A.2.2.5 Steamline Break (USAR 14.2.5)

The primary mitigating functions for the steamline break event include pressurizer low pressure, steamline low pressure, and containment hi pressure safety injection actuation, and containment hi pressure, steamline hi-hi flow coincident with a safety injection signal, and steamline hi flow coincident with low-low Tavg and a safety injection signal main steamline isolation actuation. Backup mitigating functions include overtemperature ΔT, overpower ΔT, and power range high neutron fiux reactor trip.

[

]^{a,c,f}. By following the appropriate emergency operating procedures and using the diverse manual functions, the plant response meets the applicable acceptance criteria.

A.2.2.6 Rupture of a Control Rod Drive Mechanism Housing (RCCA Ejection) (USAR 14.2.6)

The primary mitigating function for the rod ejection event is power range high neutron flux (low set point) for low power initiatmg events and power range high neutron flux (high set point) for high power initiated events. The back-up mitigating functions include source range high neutron flux, intermediate range high neutron flux, overtemperature ΔT, and overpower ΔT reactor trip. [

]^{a,c,f} provides adequate protection such that the plant response meets the applicable acceptance criteria.

A.2.2.7 Turbine Missile Damage to Spent Fuel Pool (USAR 14.2.7)

A calculation is performed in the USAR to determine the maximum expected exclusion boundary thyroid dosage. No automatic protection functions are required.

A.2.3 Reactor Coolant System Pipe Ruptures (Loss of Coolant Accident)

A.2.3.1 Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes Which Actuates Emergency Core Cooling System (14.3.1)

The primary mitigating functions for a small break loss of coolant accident (LOCA) are pressurizer low pressure reactor trip and pressurizer low pressure safety injection actuation. The back-up mitigating function for a small break LOCA is containment hi pressure safety injection and containment hi-hi pressure spray actuation.

[

]^{a,c,f}.

[

]^{a,c,f}.

[

]^{a,c,f}.

[

]^{a,c,f}.

Moreover, evaluations indicate that, [

]^{a,c,f}.

Hence, by following the appropriate emergency operating procedures and using the diverse protection functions, the plant response meets the applicable acceptance criteria.

A.2.3.2 Major Reactor Coolant System Pipe Ruptures (Loss of Coolant Accident) (USAR 14.3.2)

The primary mitigating functions for a LBLOCA is pressurizer low pressure safety injection actuation. The back-up mitigating functions include containment hi pressure safety injection and containment hi-hi pressure spray actuation. For a LBLOCA, no credit is taken for negative reactivity due to control rod insertion. With or without reactor trip, core reactivity would automatically decrease due to void formation in the core.

[Since each of the primary and back-up mitigating functions are susceptible to a postulated software CMF, a diverse mitigating function is required. The key diverse mitigation function is the passive accumulator injection of cool borated water. In addition, diverse functions include manual control of the containment spray system, manual isolation of selected containment vent paths, manual RHR pumps actuation and control of associated suction and discharge valves, and manual control of switchover valves from RWST to containment sump]^{a,c,f}.

[

]^{a,c,f}.

Hence, by following the appropriate emergency operating procedures and using the diverse protection functions, the plant response meets the applicable acceptance criteria.

A.2.3.3 Core and Internals Integrity Evaluation (USAR 14.3.3)

Stress calculations of RCS components are provided in the USAR.

A.2.3.4 Containment Integrity Evaluation (USAR 14.3.4)

The containment response to a spectrum of loss of coolant accidents (LOCAs) was calculated. The primary, back-up and diverse protection functions are discussed above in sections A.2.3.1 and A.2.3.2.

A.2.3.5 Off-Site Dose Consequences (USAR 14.3.5)

The USAR provides a calculation of the estimated dose releases resulting from a design basis LBLOCA.

A.2.3.6 Section 14.3.6 deleted in USAR.

A.2.3.7 Effects of Leakage from Residual Heat removal System (USAR 14.3.7)

The USAR provides a calculation of the estimated doses resulting from this event.

A.2.3.8 Charcoal Filter Ignition Hazard Due to Iodine Absorption (USAR 14.3.8)

The USAR provides a calculation of the maximum charcoal temperature due to iodine absorption.

A.2.3.9 Generation and Disposition of Hydrogen (USAR 14.3.9)

The USAR provides a discussion of the generation and disposition of hydrogen in containment..

A.2.3.10 Steam Generator Tube Sleeving (USAR 14.3.10)

The USAR describes the types of sleeves that have been installed to a maximum of 30% tube plugging for accident analyses. This event is not considered an AOO and DBE.

A.2.3.11 Steam Generator Tube Fatigue Analysis (USAR 14.3.11)

The USAR provides analyses that were performed to address Bulletin 88-02. This event is not considered an AOO or DBE.

A.2.3.12 Steam Generator Plug PIPs (USAR 14.3.12)

The USAR discusses the installation of "Plug in a Plug" in existing mechanical tube plugs. This event is not considered an AOO and DBE.

A.2.3.13 Voltage Based Repair Criteria for Steam Generator Tubes (USAR 14.3.13)

The USAR discusses the analyses that were performed to support usage of a voltage-based repair criteria. This event is not considered an AOO and DBE.

A.2.3.14 F* and Elevated F* Alternative Repair Criteria for Steam Generator Tubes (USAR 14.3.14)

The USAR discusses the usage of the F* and elevated F* repair criteria for indications of degradation occurring within the tube sheet crevice area. This event is not considered an AOO and DBE.

A.2.3.15 Steam Generator Tube Removal (USAR 14.3.15)

The USAR discusses the installation of plugs after removal of a portion of a tube for evaluation. This event is not considered an AOO and DBE.

a,c,f

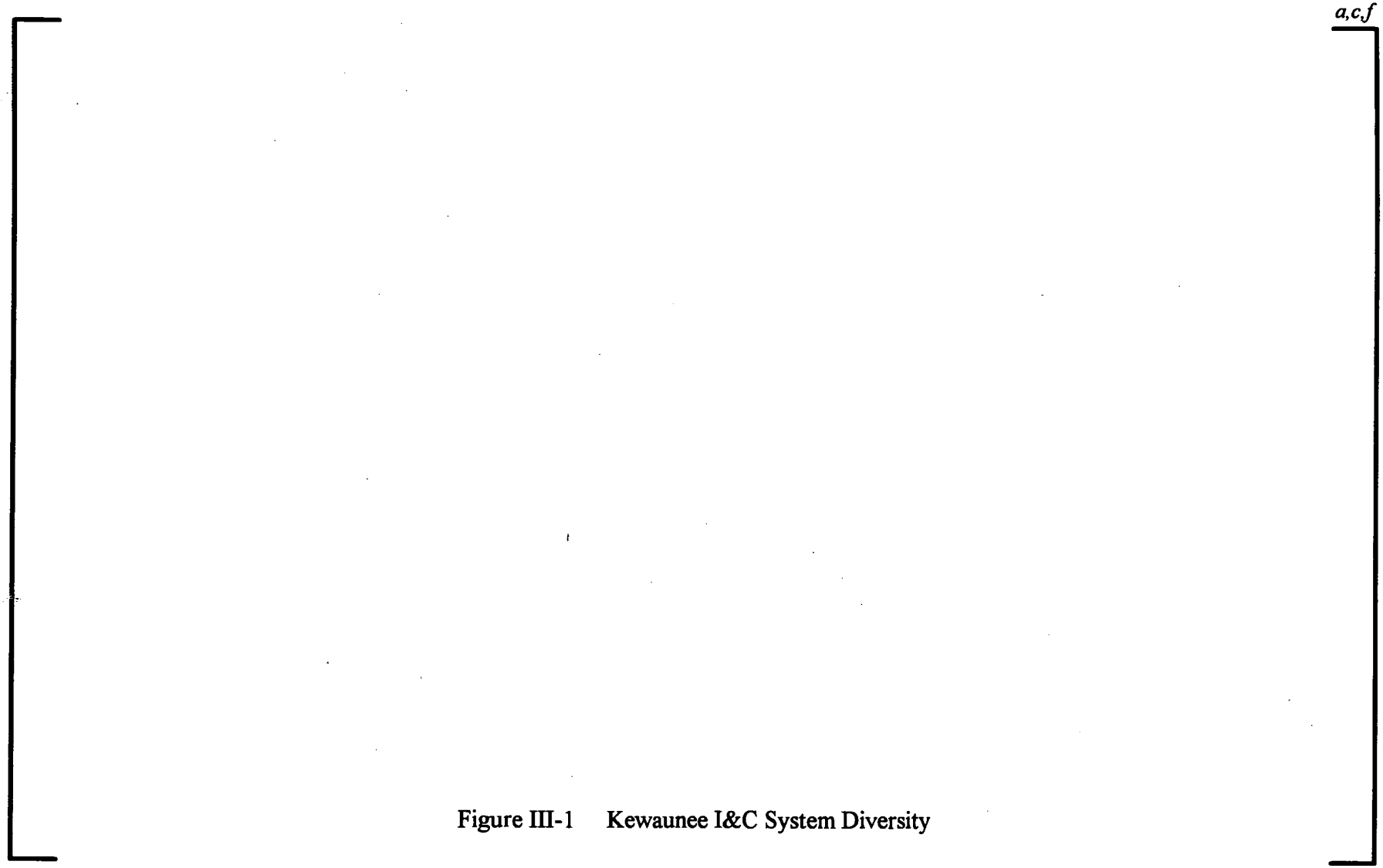


Figure III-1 Kewaunee I&C System Diversity

NRC FORM 199
(9-1999)
NRCMD 3.12

U.S. NUCLEAR REGULATORY COMMISSION

PROPRIETARY INFORMATION

NOTICE

THE ATTACHED DOCUMENT CONTAINS OR IS CLAIMED TO CONTAIN PROPRIETARY INFORMATION AND SHOULD BE HANDLED AS NRC SENSITIVE UNCLASSIFIED INFORMATION. IT SHOULD NOT BE DISCUSSED OR MADE AVAILABLE TO ANY PERSON NOT REQUIRING SUCH INFORMATION IN THE CONDUCT OF OFFICIAL BUSINESS AND SHOULD BE STORED, TRANSFERRED, AND DISPOSED OF BY EACH RECIPIENT IN A MANNER WHICH WILL ASSURE THAT ITS CONTENTS ARE NOT MADE AVAILABLE TO UNAUTHORIZED PERSONS.

COPY NO. _____

DOCKET NO. _____

CONTROL NO. _____

REPORT NO. _____

REC'D W/LTR DTD. _____

PROPRIETARY INFORMATION