Project Title: ***UFTR DIGITAL CONTROL SYSTEM UPGRADE***

UFTR-QA1-103, Diversity and Defense-in-Depth (D3) Analysis

Prepared by,

Prof. Alireza Haghighat

..... (Signature)

Date: 7/7/10

Reviewed by,

Dr. Gabriel Ghita

..... (Signature)

Date: 7/7/10

Approved by,

Prof. Glenn Sjoden

..... (Signature)

Date: 7/7/2010

THE DISTRIBUTION LIST:

No.	*Name*	*Affiliation*	*Signature*	*Date*
1.				
2.				
3.				
4.				
5.				
6.				

THE LIST OF THE REVISED PAGES OF THE DOCUMENT

Revision no.	Reviewed by	Approved by	The Modified Pages	Date

TABLE OF CONTENTS

1. Purpose

The purpose of this analysis is to determine whether the proposed UFTR protection system upgrade exhibits adequate diversity and defense-in-depth (D3) to address all reasonable vulnerabilities to system failure. The proposed TELEPERM XS (TXS) system upgrade consists of both hardware and software that monitors and automatically initiates protective action for the UFTR. This document is consistent with guidelines provided by NUREG/CR 6303, /6/, and in accordance with acceptance criteria established by BTP 7-19, /4/.

2. References

2.1 UFTR Documents

/1/ UFTR-QA1-14, "Safety System Design Basis," 2009

/2/ UFTR "Safety Analysis Report (SAR)".

/3/ UFTR Supplementary Safety Analysis Report (SSAR) 2009.

2.2 Regulation

/4/ BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Controls Systems," March 2007

/5/ IEEE Std. 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 1998

/6/ NUREG/CR 6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994

/7/ NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems"

2.3 AREVA NP Inc Documents

/8/ "TXS Manual: System Overview," 2006.

3. Definitions, Acronyms, and Abbreviations

3.1 Definitions

Common Cause Failure: Multiple failures attributable to a common cause.

Defense-in-Depth: The practice of having multiple, redundant, and independent layers of safety systems to reduce the risk that a single failure of a component or system will cause the catastrophic failure of the reactor.

Design Basis Event: Postulated events used in the design to establish the acceptable performance requirements for the structures, systems, and related components.

Diversity: In fault tolerance, realization of the same function by different means. For example, use of different signals, processors, storage media, programming languages, algorithms, or development teams.

Invalid: A signal is invalid if it experiences any type of failure or is not within the range defined by the design basis.

Nuclear Instrumentation (NI): The portion of a train that directly senses and responds to changes in neutron and/or gamma ray levels in the reactor core and converts the measured interaction into an electric, optic, or pneumatic signal.

Operating Bypass: The inhibition of the capability to accomplish a safety function that could otherwise occur in response to a particular set of generating conditions

Protective Action: The initiation of a signal within the sense and command features or the operation of equipment within the execute features for the purpose of accomplishing a safety function.

Redundant Equipment or System: A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function, regardless of the state of operation or failure of the other.

Safety Function: One of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event.

Sensor: The portion of a train, other than nuclear instrumentation, that responds to changes in a plant variable or condition and converts the measured process variable into an electric, optic, or pneumatic signal.

Sensing Equipment: This expression includes both nuclear instrumentation (NI) and sensors.

Train: An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A train loses its identity where single protective action signals are combined.

3.2 Acronyms

AC	Alternating Current
AQP	Acquisition and Processing
BDT	Blade-Drop Trip
BTP	Branch Technical Position
CCF	Common Cause Failure
D3	Diversity and Defense-in-Depth
DAR	Design Analysis Report
DC	Direct Current
ESFAS	Engineered Safety Features Actuation System
FT	Full Trip
GW	Gateway
HEU	Highly Enriched Uranium
HMI	Human Machine Interface
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
LEU	Low Enriched Uranium
LOCA	Loss of Coolant Accident
MCR	Main Control Room
MIS	Monitoring and Indicator System
MRS	Manual Reactor Scram
MSI	Monitoring Service Interface
NI	Nuclear Instrumentation
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
NUREG	Nuclear Regulatory Commission Regulation
PAM	Post Accident Monitoring
PI	Process Instrumentation
QDS	Qualified Display System
RTS	Reactor Trip System
SAR	Safety Analysis Report
SU	Service Unit
SWCCF	Software Common Cause Failure
TXP	TELEPERM XP
TXS	TELEPERM XS
UFTR	University of Florida Training Reactor

4. Background

The UFTR was built in 1959 and was one of the first nuclear reactors on a university campus. Originally designed for highly enriched uranium (HEU) fuel, the UFTR was converted to a low enriched uranium (LEU) fuel system in 2006. The UFTR is currently completing relicensing to update the Safety Analysis Report (SAR) for the new fuel enrichment. The current licensed protection system for the UFTR has not changed since its original design. The existing analog system has become outdated with the onset of digital controls for commercial plants. The proposed digital protection system upgrade is designed to make the UFTR more relevant to current trends towards digital protection/control in commercial reactors for training purposes.

5. New or Unusual Design Features

The UFTR is a self-limiting research and training reactor which requires no additional engineered safeguards beyond those designed into the reactor core or incorporated into the main cooling, protection, control and radiation monitoring systems. As a result of low power and high thermal conductivity of metallic fuel, there is no need for protective cooling. Further, the UFTR core design has negative coefficient of reactivity for both primary coolant void and temperature. Analysis of UFTR design in the UFTR Safety Analysis Report (SAR), /2/, and the UFTR Supplementary Safety Analysis Report (SSAR), /3/, show that there is no credible accident that would result in radiological exposures to the public, facility staff and the environment, and therefore, there is no need for the ESFAS. As a result, the four echelons of defense listed in NUREG/CR-6303, /6/, become three for the UFTR:

- Control System
- Reactor Trip System (RTS)
- Monitoring and Indicator System (MIS)

Echelons of defense are specific applications of the principle of defense-in-depth, which exist to provide multiple barriers to radiation release for a reactor. The following analysis will define the proposed system architecture and analyze the diversity that exists between system components to improve the defense-in-depth for the UFTR.

6. Scope

6.1 What is in Scope

This analysis considers all system components that provide for the aforementioned three echelons of defense. All of these components are discussed in Section 12 of this document. In accordance with BTP 7-19, /4/, since the UFTR license does require any redundancy, there is no concern for the common-cause failure (CCF).

6.2 What is not in Scope

The information provided by UFTR-QA1-14, /1/, shall not be repeated in this document. This includes analysis of design basis events, since the current UFTR SAR, /2/, shows that no diverse mitigation is required for these events and no additional best-estimate analysis is required for this analysis. Single failure of components is not considered in this document because the current SAR, /2/, Chapter 7, does not require it.

7. Description of Analysis Methods

The method used in this analysis shall be consistent with the method given in NUREG/CR-6303, /6/. The system architecture shall be defined by system blocks, which shall be justified by criteria given in the aforementioned document. The resulting diversity and defense-in-depth (D3) between system blocks will be analyzed.

8. Authorities and Guidelines

The analysis performed in this document shall be consistent with the guidelines provided in Section 3 of NUREG/CR-6303, /6/. Additional standards and guidelines are provided by the UFTR-QA1-14, /1/.

9. Types of Failures

Since the plant design basis can accommodate a complete failure of the protection system, it bounds any Software Common Cause Failure (SWCCF) (NUREG/CR-6303/15/). As such, no additional analysis of the SWCCF is necessary.

10. Sources of Design Information

The following list cites the sources for design information used to perform this analysis.

- UFTR-QA1-14, /1/
- UFTR SAR, /2/
- UFTR SSAR, /3/
- TXS Manual: System Overview, /8/

11. Assumptions

11.1 Worst-Case Assumptions

Failure Consequences

Failures are assumed to occur in the most limiting fashion possible consistent with hardware or software construction. For instance, a module which de-energizes to trip is assumed to fail so that it continues to block trip.

Latency of Failures

Failures are assumed to be latent and undetectable until stressed by event or accident, at which time the failure becomes manifest.

11.2 Assumptions Based on System Structure

Proper Functioning of Equipment

Equipment that has been specially designed to have a specific purpose for protection of electrical equipment, such as isolation or one-way communication, shall be assumed to function correctly.

12. Description of the Design

The proposed protection system is comprised of three blocks. Appendices A-C of this document provides the justification for physical and logical failure containment in each block. System blocks are shown in Figure 12-1 below, where arrows depict intended functional interface.

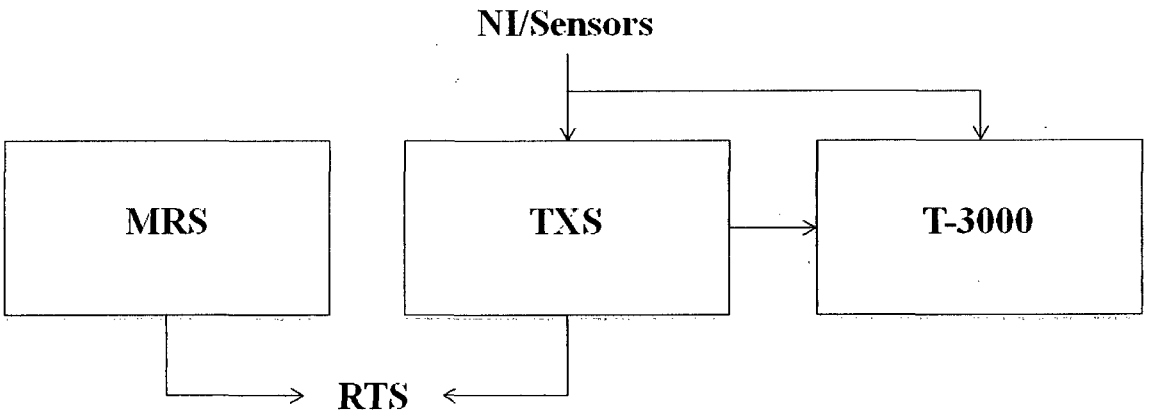

Figure 12- 1. The proposed UFTR Protection System

The above system includes the TXS as the primary protection system, providing Monitoring and Indicator System (MIS) and Reactor Trip System (RTS), the T-3000 system (with a diverse hardware and software) providing reactor control and a diverse MIS, and a hardwired Manual Reactor Scram (MRS) providing a diverse RTS as compared to TXS. Further, because of the unidirectional communication between the TXS and T-3000, and no communication between the TXS and MRS, the failure of the MRS or T3000 blocks will not impact the operation of the TXS. In summary, as shown in Table 12-1, the above proposed system effectively addresses the functions of the RPS.

Table 12- 1: System blocks and their span across the three echelons of defense

Protection System Block	Echelon Defense		
	Control System	RTS	MIS
MRS		✓	
TXS		✓	✓
T-3000	✓		✓

The above Table clearly indicates that the two functions of the protection system, i.e., RTS and MIS, are achieved via two diverse systems. This means that if the TXS fails, especially if its processors freeze, the T-3000 system provides the necessary indication for the operator to engage the MRS.

It is important to note that all the signals within a train are input to both TXS and T-3000. This allows T-3000 to display monitoring information independent of the TXS block, which is crucial during TXS failure. In this situation, operator can identify the status of TXS by monitoring the T-3000 displays, and therefore invoke the MRS. It is also worth noting that the TXS includes a Gateway (GW) for unidirectional communication with the T-3000 as shown in Figure 12-1. A more detailed description of architecture within each block is provided in Appendices A to C of UFTR-QA-14, /1/.

13. Findings

13.1 Diversity Between Blocks

13.1.1 TXS vs. T-3000

Both TXS and T-3000 are computer-based systems. The TXS operating system software is accepted as equivalent to US nuclear standards by the NRC in the safety evaluation report for the TXS Topical Report, /8/.

The T-3000 uses industrial technology, which is developed based on different standards resulting in the following general dissimilarities from the TXS technology:

- Different network protocols
- Different diagnostics concept
- Different maintenance concept
- Different HW / operating systems for service units
- Different HMI
- Different signal message format and content
- Different connectivity to external systems
- Different IT security concepts

As a result, the following diversity elements (taken from NUREG/CR-6303, /6/) distinguish the two technologies:

- Design (different approaches within a technology and different architectures)
- Equipment (different manufacturers of fundamentally different equipment designs)
- Functional (different underlying mechanisms to accomplish safety function, different purpose, function, control logic, or actuation means of same underlying mechanism, and different response time scale)
- Human (different design organizations/companies, different designers, engineers, and/or programmers, and different implementation/validation teams (testers, installers, or certification personnel))
- Software (different algorithms, logic, and program architecture, different timing or order of execution, different runtime environments, and different functional representations)

The diversity assessment is informed by using the insights and analysis tool from draft NUREG/CR-6303, /6/.

13.1.2 Manual Reactor Scram (MRS)

The MRS can be shown to have inherent diversity and independence from the TXS. The method for diversity utilized by this block is characterized by "Strategy A" found in NUREG/CR-7007, /7/. This draft document defines this strategy, which is described in the following excerpt:

"Strategy A focuses on the use of fundamentally diverse technologies as the basis for diverse systems, redundancies, or subsystems. The Strategy A baseline, at the system or platform level, is illustrated by the example of analog and digital implementations providing design diversity. This choice of technology inherently contributes notable equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities. Intentional application of life-cycle and equipment manufacturer diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted. The use of a microprocessor-based primary protection [safety] system and an analog (Laddic logic) secondary protection [safety] system at the Sizewell NPP represents the principal example of Strategy A drawn from the survey findings."

The design diversity that exists between analog and digital controls is shown to be sufficient for claiming diversity between MRS and the other two blocks.

13.2 Diversity Between Echelons of Defense

Diversity between echelons of defense for the UFTR allows all three echelons to remain functional during the failure of any one system block. The following list shows the effect of failure of each block on the echelons of defense:

- *MRS Block Failure:* All the echelons of defense will remain operational. TXS will initiate RTS. T-3000 and TXS will also remain available for Monitoring and Indication.
- *TXS Block Failure:* All echelons of defense will remain operational. MIS echelon will only contain indication of failed TXS system (via T-3000) and initiation of RTS will occur via MRS. Sensing equipment will be available via T3000 since it receives its own input from the NIs and sensors.
- *T-3000 Block Failure:* All echelons of defense will remain operational.

In summary, the MRS provides a diverse means for initiating the RTS during TXS failure, while T-3000 provides a diverse indicator in case the TXS failure. It is important to note that failure of the RTS echelon due to TXS failure and lack of operator action cannot cause an uncontrolled release of radioactivity. This inherent feature of UFTR is discussed in UFTR SSAR, /3/.

13.3 Conclusion of Findings

The proposed system exhibits adequate D3 to address all reasonable vulnerabilities to system failure. The TXS system will also have improved reliability due to extensive signal diversity and redundancy monitoring and indication systems (i.e., TXS and T-3000). As a final note, the accident analysis provided in the UFTR SAR, 2/, indicates that no failure of equipment or operator action/inaction can result in fuel failure and therefore there is no possibility of uncontrolled release of radioactivity.

Appendices

Appendix A- Manual Reactor Scram (MRS) Block

The MRS consists of two manual trip switches that are not controlled by software or computer-based components. It spans the RTS and monitoring and indications system echelons. This block receives no input from monitoring equipment and provides two manual trip initiation features: Blade Drop Trip (BDT) or full trip (FT). For more discussion on manual trips, refer to UFTR Safety System Design Basis, /1/. The following Tables A-1 and A-2 provide the methods used for containment of physical and logical failures within this block, respectively.

Table A- 1: Methods for physical failure containment in the MRS block

Criteria for Physical Failure Containment	Method of Containment
Physical separation	MRS shall be physically separate from the TXS block
Electrical isolation	This block does not require electrical connections to other blocks.
Power supply separation	Power supply separation of blocks is not necessary since the BDT is "failsafe" during a loss of power event. For more information on trip functions, refer to the UFTR Safety System Design Basis, /1/.
Electrical shielding	Signal cables to and from the MRS will be shielded from interference.

Table A- 2: Methods for logical failure containment in the MRS block

Criteria for Logical Failure Containment	Method of Containment
Software module separation	There is no software within this block.
No interaction through shared memories	There is no memory required for this block.
Unidirectional communication with other systems	There is no communication with other systems
The software continues to work regardless of local area network faults	This block is not connected to any network.
All input data from other systems are qualified before use	Inputs are directly from manual control from operator.

The preceding two tables show how each failure containment criteriion is met for the MRS, which justifies its designation as a block in the analysis.

Appendix B- TELEPERM XS (TXS) Block

The TXS system block consists of the hardware, software, and displays that are described in UFTR-QA1-14, /1/. The TXS computer cabinets and components shall be physically and logically isolated from all other safety and non-safety equipment. The following Tables B-1 and B-2 describe the requirements and methods for physical and logical failure containment within the TXS block, respectively. These criteria are listed in NURGEG/CR 6303, /15/.

Tables B-1 and B-2 show how each failure containment criteriion is met for the TXS system, which justifies its designation as a block in this analysis.

Table B-1: Methods for physical failure containment in TXS block.

Criteria for Physical Failure Containment	Method of Containment
Physical separation	TXS hardware is contained inside metal cabinets that are physically separate from the other two blocks.
Electrical isolation	Electrical isolation between the signal circuit and the interface to the system bus is implemented by means of optocouplers.
Power supply separation	Power supply separation of blocks is not necessary since the Blade Drop Trip (BDT) function is "failsafe" during a loss of power event. For more information on trip functions, refer to the UFTR Safety System Design Basis, /1/.
Electrical shielding	Prevention of electromagnetic interference is achieved by the shielding effect of metallic front plates in each cabinet. Signal cables to and from TXS will also be shielded from interference.

Table B-2: Methods for logical failure containment in TXS block.

Criteria for Logical Failure Containment	Method of Containment
Software module separation	There are no block divisions within the TXS system, thus there is no need to claim separation of software modules within this system.
No interaction through shared memories	TXS system does not share memory with any other computer system.
Unidirectional communication with other systems	MSI provides unidirectional communication with non-safety system through GW.
The software continues to work regardless of local area network faults	MSI provides the means of prevention of inadvertent and/or malicious attempts on the processing of signals and decision making on reactor operations.
All input data from other systems are qualified before use	The only input to TXS is from NIs/sensors, which is processed by the AQP. Failure of sensing instrumentation will not cause failure in TXS.

Appendix C- T-3000 Block Designation

The T-3000 block is not essential for the safe shutdown of the UFTR, thus one-way propagation of failures from the TXS block is implemented through GW. Methods for physical and logical containments of failure within this block are shown in Tables C-1 and C-2 below.

The two tables show how each failure containment criterion is met for the control system, which justifies its designation as a block in this analysis.

Table C-1: Methods for physical failure containment in the T-3000 block

Criteria for Physical Failure Containment	Method of Containment
Physical separation	Non-safety computer system is in a separate metal cabinet, away from the components of the other blocks.
Electrical isolation	Breakers and fuses
Power supply separation	Power supply separation of blocks is not necessary since the BDT is "failsafe" during a loss of power event. For more information on trip functions, refer to the UFTR Safety System Design Basis, /1/.
Electrical shielding	Non-Class 1E circuitry will not require electrical shielding in accordance with IEEE Std. 603 1998/ 5/ because it is not essential for reactor shutdown. T-3000 will be kept at a safe distance from Class-1E circuitry associated with the other blocks.

Table C-2: Methods for logical failure containment in the T-3000 block

Criteria for Logical Failure Containment	Method of Containment
Software module separation	Block designation does not require software module separation.
No interaction through shared memories	T-3000 does not share memory with other computer systems.
Unidirectional communication with other systems	Unidirectional communication from TXS is achieved through GW.
The software continues to work regardless of local area network faults	MSI
All input data from other systems are qualified before use	Inputs are directly from manual control from operator.