DIVERSITY AND DEFENSE-IN-DEPTH ANALYSIS FOR I&C SYSTEMS OF RESEARCH REACTORS: A CASE STUDY ON TWO RESEARCH REACTORS

Seung Ki Shin*, Yong Suk Suh, and Sang Mun Seo
Division of Research Reactor System Design
Korea Atomic Energy Research Institute
111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea
skshin@kaeri.re.kr; yssuh@kaeri.re.kr; smsuh@kaeri.re.kr

ABSTRACT

This paper provides the analysis results of the diversity and defense-in-depth (D3) applied to two research reactors designed by the Korea Atomic Energy Research Institute. The D3 assessments for instrumentation and control (I&C) systems of two research reactors are performed according to the guidelines documented in NUREG/CR-6303. The I&C systems are classified into four echelons of defense: control echelon, reactor trip echelon, engineered safety feature (ESF) actuation echelon, and monitoring and indication echelon. The diversity between the echelons of defense is assessed to determine that a single software common cause failure (CCF) does not impair the functions of multiple echelons of defense. In addition, the effects of a software CCF of the reactor protection system on the design basis events of the research reactors are analyzed by assuming that the automated reactor trip and ESF actuation functions of the reactor protection system are inoperable due to the software CCF. From the D3 analyses for the research reactors, it is verified that (1) adequate diversity has been provided, (2) adequate defense-in-depth has been provided, and (3) the displays and manual controls for critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection system.

Key Words: Diversity and defense-in-depth, Research reactor, Instrumentation and control system, Common cause failure, Reactor protection system

1 INTRODUCTION

Digital instrumentation and control (I&C) systems can be vulnerable to a common cause failure (CCF) caused by software errors or software developed logic, which could defeat the redundancy achieved by the hardware architecture [1]. The principle of diversity and defense-in-depth (D3) is applied to the design of I&C systems to reduce the potential for the CCFs. The United States Nuclear Regulatory Commission (USNRC) published the branch technical position (BTP) 7-19 of NUREG-0800 [1] to provide guidance for a D3 assessment of digital I&C systems and confirm the vulnerabilities to CCF. The foundation of BTP 7-19 is the "NRC position on D3" from the SRM on SECY-93-087 [2], Item 18, II.Q. The BTP 7-19 requires that the following be verified through a D3 assessment.

- Adequate diversity has been provided.
- Adequate defense-in-depth has been provided.
- Displays and manual controls for critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems.

* Correspondence to: Seung Ki Shin

NUREG/CR-6303 [3] provides detailed D3 analysis methods for digital I&C systems to discover design vulnerabilities to CCFs. It describes fourteen specific guidelines for a D3 analysis. According to the guidelines, I&C systems are categorized into four echelons of defense: control, reactor trip, engineered safety features (ESF) actuation, and a monitoring and indicator system. It should be verified that sufficient diversity among the echelons of defense exists so that any design basis events (DBE) in conjunction with a software CCF of reactor protection system can be mitigated by the echelon of defense that is not impaired by the postulated CCF.

When the reactor protection system cannot perform automated protective functions due to a potential software CCF, the required protective functions should be accomplished through diverse means, either an automated system or manual operator actions performed from the main control room (MCR). The automated system is generally preferred for the diverse means. To use manual operator actions as a diverse means to perform protective functions, the manual operator actions should be credited using a suitable human factors engineering (HFE) analysis. NUREG-0800, Appendix 18-A [4], defines a methodology for evaluating manual operator actions as a diverse means of coping with DBEs concurrent with a software CCF of the reactor protection system. To credit manual operator actions, it should be shown that the time available to perform the required manual actions is greater than the time required for the operator to perform the manual actions.

As the software components of reactor protection systems have been increased in research reactors, the potential for a software CCF has become an important issue in the safety of research reactors, and D3 assessments are required for the I&C design. This paper provides the analysis results of D3 for two research reactors designed by the Korea Atomic Energy Research Institute (KAERI). The two research reactors are called “RR-1” and “RR-2” in this paper. RR-1 is a 5 MW open-pool type research reactor and is currently under commissioning. RR-2 is a 15 MW open-pool type research reactor and is currently in the licensing process for a construction permit.

The remainder of this paper is structured as follows. In the second section, the RR-1 I&C architecture is introduced briefly, and the D3 analysis for the RR-1 I&C systems is performed. In the third section, the major differences of the RR-2 I&C architecture from the RR-1 are briefly described and D3 analysis for the RR-2 I&C systems is performed. The fourth section encompasses the summary and conclusion of this paper.

2 D3 ANALYSIS FOR I&C SYSTEMS OF RR-1

The I&C systems of the RR-1 are composed mainly of the Reactor Protection System (RPS), Post-Accident Monitoring System (PAMS), Reactor Regulating System (RRS), Alternate Protection System (APS), Information Processing System (IPS), and Process Instrumentation and Control System (PICS). Most I&C systems have been implemented using digital technology. The RPS and PAMS are categorized as the safety class to mitigate the effects of DBEs, while the other systems are as the non-safety class. The overview of the RR-1 I&C architecture is shown in Fig.1.

The RPS consists of three redundant channels and performs a reactor trip and ESF actuation functions. It generates a trip signal to insert control absorber rods and second shutdown rods into the core when a trip parameter exceeds the trip setpoint. In addition, the RPS actuates ESFs, such as opening siphon break valves (SBVs) to maintain the reactor pool level and closing confinement isolation dampers (CIDs) to prevent the release of radioactive material to the outside. The bistable logic is digitalized using the programmable logic controller (PLC) and the coincidence, initiation, and actuation logics are implemented based on analog circuits. The reactor trip and ESF can be actuated by operators in the MCR using hardwired manual switches, and a manual initiation is not affected by software failures.

The PAMS consists of two redundant channels and provides important information for operators to assess the reactor conditions to determine whether the safety functions are being performed and

maintained so that the operators can perform their role in ensuring reactor safety during and following a DBE. The functions of PAMS are implemented using the PLC. The important safety parameters are continuously displayed at the PAMS cabinets installed in the MCR, and displayed data are stored in the high-capacity memory through a storage device. The PAMS transmits all safety signals to the IPS through unidirectional data communication, and those signals are displayed continuously on the operational workstation in the MCR.

The RRS regulates the reactor power using control absorber rods so as not to exceed the operational allowance limit. It performs the functions for a reactor startup/shutdown, changing the power levels, and maintaining operation at a pre-specified power level. The RRS has a setback mode which moves all control rods downward simultaneously with the maximum speed until all control rods reach their bottom positions when any predefined conditions that indicate an abnormal reactor status are met. The RRS is physically and electrically isolated from the RPS.

The APS performs a diverse reactor trip function to mitigate the effects of an anticipated transient without scram (ATWS). It initiates a reactor trip when the RPS fails to trip the reactor. The APS consists of two channels, and the reactor trip function is performed using two-out-of-two coincidence logic. The bistable logic is digitalized and the initiation and actuation logics are implemented using analog circuits. The PLC used for the bistable logic of the APS is diverse from the RPS.

The IPS is a computer-based system that performs primary monitoring, information recording, alarm functions, and non-safety network management. It periodically collects and records the reactor variables from other I&C systems through a data communication network, and provides reactor information, alarms to operators in the MCR through operator workstations (OWSs) and large display panels (LDPs) to assist the safe reactor operation.

The PICS is a computer-based data processing and man-machine interface system that provides an operational means for monitoring and controlling the reactor. It receives signals from the selected sensors in the process systems and sends control commands to the various facility areas. The PICS transmits these signals to the IPS through a data communication network.

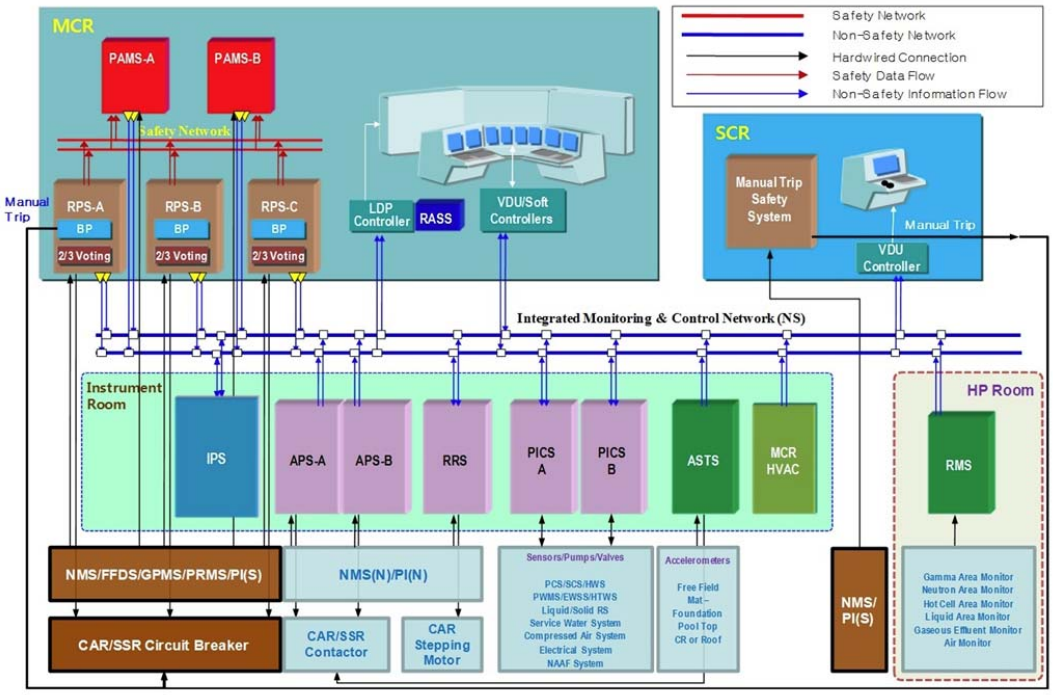

Figure 1. I&C architecture of RR-1.

2.1 Echelons of Defense

The echelons of defense structure of the RR-1 I&C systems are shown in Table I.

Table I. Echelons of defense of the RR-1 I&C systems

Echelon	Safety Class	I&C Systems
Control echelon	Non-safety	RRS, PICS, APS
Reactor trip echelon	Safety	RPS, PNMS
ESF actuation echelon	Safety	RPS, PNMS
Monitoring and indication echelon	Safety	PAMS, Manual trip/ESF switches
	Non-safety	IPS (including OWS/LDP), Manual trip switches

The control echelon includes the RRS and PICS that routinely prevents reactor excursions toward unsafe regimes of operation. The APS that trip the reactor against the ATWS is also included in the control echelon.

As the RPS is the safety system to generate a reactor trip signal to reduce reactivity rapidly in response to an uncontrolled excursion and ESF actuation signal to maintain the integrity of the reactor, the RPS is included in both the reactor trip echelon and ESF actuation echelon. The primary cooling system (PCS) neutron monitoring system (PNMS) sends the field signals to the RPS and generates the additional initiation signals for reactor trip and closing CIDs directly without going through the digital controller of the RPS. The direct initiation of the safety functions by the PNMS is designed to mitigate a software failure of the RPS, and the PNMS is thus included in both the reactor trip echelon and ESF actuation echelon.

The monitoring and indication echelon consists of safety equipment such as the PAMS and manual switches for a reactor trip and ESF actuation equipped in the RPS cabinets, and non-safety equipment such as the IPS and manual trip switches equipped in the APS cabinets.

The reactor trip and ESF actuation echelons perform their functions when the control echelon fails, and the monitoring and indication echelon supports the functions of the other echelons. When a CCF of the RPS occurs, the control echelon compensates the reactor trip and ESF actuation echelons in the reversed order.

2.2 Diversity between CCF Groups

The I&C systems classified into each echelon of defense in Table I are classified again into CCF groups as shown in Table II. The systems of each CCF group use identical software, and thus are vulnerable to a software CCF. A software CCF of one group does not impair the functions of other systems classified into another group. In this paper, each CCF group is defined as a block described in NUREG/CR-6303 [3] because internal failures including the effects of software CCFs do not propagate to other groups.

When Group-1 fails, the reactor can be controlled and maintained safely by the RRS, PICS, and APS classified into Group-2. The operators are able to continuously monitor the reactor status through the IPS including OWS/LDP of Group-3, and perform protective actions using manual trip/ESF initiation

switches equipped in the cabinets of the RPS and APS classified into Group-5. The PNMS of Group-4 can generate protective signals independently from the RPS.

Table II. CCF groups of RR-1 I&C systems

CCF Group (Block)	I&C Systems
Group-1	RPS, PAMS
Group-2	RRS, PICS, APS
Group-3	IPS(including OWS/LDP)
Group-4	PNMS
Group-5	Manual trip/ESF switches

NUREG/CR-6303 [3] identifies six aspects of diversity: design diversity, equipment diversity, functional diversity, human diversity, signal diversity, and software diversity. As this paper focuses on the case of the RPS CCF, the diversities between Group-1 and other groups are evaluated. Because the diversities of the Group-4 and Group-5 from Group-1 can be assured intuitively, detailed evaluations for those groups are not required.

In terms of the design diversity, a different architecture (i.e., arrangement and connection of components) is used for each CCF group. For example, the APS consists of two independent channels and analog circuits are structured for 2-out-of-2 voting logic, whereas the RPS consists of three independent channels, and analog circuits are structured for 2-out-of-3 voting logic.

In terms of the equipment diversity, a different CPU architecture from different manufacturers is used for each CCF group. For example, the APS uses the INTEL processor-based PLC, whereas the RPS and PAMS use the Motorola processor-based PLC.

In terms of the functional diversity, a different underlying mechanism, purpose, function, control logic, actuation means, or response time scale is considered for each CCF group. For example, the APS performs a reactor trip based on the energize-to-trip principle, whereas the RPS adopts the de-energize-to-trip principle. In addition, the setpoints of the APS are determined such that the APS does not generate a trip signal prior to the RPS.

In terms of the human diversity, different designers, programmers, and testers are used for each CCF group.

In terms of the signal diversity, the same reactor or process parameters sensed by different redundant sets of similar sensors are used for each CCF group. The RRS, PICS, and APS receive field signals directly from their own sensors, which are not used for any safety functions by Group-1. The IPS receives signals from other systems diverse from Group-1, not directly from its own sensors.

In terms of the software diversity, different algorithms, operating systems, and computer languages are used for each CCF group.

2.3 Diversity among Echelons of Defense

2.3.1 Control/reactor trip echelon interaction

There is no interaction between the control echelon and reactor trip echelon. Signals are electrically and logically isolated between the two echelons. In preparation for the CCF of the RPS, diverse means that are not subject to the CCF are provided such as the APS and manual switches for a reactor trip.

2.3.2 Control/ESF actuation echelon interaction

There is no interaction between the control echelon and ESF actuation echelon. Signals are electrically and logically isolated between the two echelons. In preparation for the CCF of the RPS, diverse means that are not subject to the CCF are provided such as the PNMS and manual switches for ESF actuation.

2.3.3 Reactor trip/ESF actuation echelon interaction

As the RPS performs both functions of the reactor trip and ESF actuation, the CCF of the RPS have an effect on the reactor trip and ESF actuation echelons simultaneously. However, the functions of diverse means for ATWS mitigation and ESF actuation such as the APS, PNMS, and manual switches are not impaired by the CCF of the RPS.

2.3.4 Manual operator action

The SRM on SECY-93-087 [2] requires that independent and diverse displays and manual controls be available so that operators can initiate a system-level actuation of critical safety functions. In conformance with this requirement, diverse and independent sensor channels, displays, and manual controls from the RPS are provided to maintain the reactor safely against DBEs concurrent with a software CCF of the RPS.

2.4 D3 Evaluation of I&C Systems for DBEs

The effects of an RPS software CCF on the DBEs are determined in this section. It is assumed that the automated reactor trip and ESF actuation functions of the RPS are inoperable owing to a software CCF. The PAMS is also assumed to fail as the same PLC is used for the PAMS and RPS. This analysis investigates whether diverse means can cope with each DBE safely even though the RPS fails to perform automated safety functions, and the analysis results are summarized in Table III.

Table III. D3 evaluation chart for DBEs of RR-1

Design Basis Events	Mitigation Functions Required of I&C Systems and Diverse Means against RPS CCF			
	Reactor Trip	SBVs Open	CIDs Close	Monitoring and Display
Startup event during power operation	APS	-[1]	-	IPS
Startup event during training operation	APS	-	-	IPS
Inadvertent withdrawal of a control absorber rod during power operation	APS	-	-	IPS

[1] This mitigation function is not required for the corresponding DBE.

Inadvertent withdrawal of a control absorber rod during training operation	APS	-	-	IPS
Insertion of cold water	APS	-	-	IPS
Inadvertent withdrawal of an experimental target	APS	-	-	IPS
Failure of all PCS pumps	APS	-	-	IPS
Failure of one PCS pump	APS	-	-	IPS
One PCS pump shaft seizure	APS	-	-	IPS
Flow blockage of a channel in a fuel assembly	PNMS	-	PNMS	IPS
Flow blockage of a fuel assembly	APS PNMS	-	PNMS	IPS
Failure of all SCS pumps	APS	-	-	IPS
Rupture of PCS pipe	-	Manual	-	IPS
Failure of a PCS pump casing	-	Manual	-	IPS

As shown in Table III, when any DBE occurs concurrently with a software CCF of the RPS, the reactor trip and ESF actuation functions of the RPS can be superseded by other systems that are not affected by the CCF. The reactor status also can be continuously displayed to operators through the IPS including OWSs and LDPs that are irrelevant to the RPS CCF. As loss of coolant accidents such as a "Rupture of PCS pipe" and "Failure of a PCS pump casing" in Table III requires a manual opening of the SBVs using manual actuation switches equipped in the MCR, a suitable HFE analysis should be performed to demonstrate that sufficient available time, information, and human-system interfaces (HSIs) are provided for operators to conduct the required manual actions.

2.5 Crediting Manual Operator Actions as a Diverse Means

To use manual operator actions as a diverse means to actuate the SBVs, the manual actions are credited using the methodology defined in Appendix 18-A of NUREG-0800 [4]. It should be demonstrated that the "time available" to perform the required manual actions is greater than the "time required" for the operator to perform the actions.

To estimate the time available for the manual actions, a safety analysis for the rupture of a PCS pump casing concurrent with an RPS CCF is performed using the RELAP5/MOD3 code for the thermal hydraulic transient analysis. The time taken for the reactor pool level to decrease to the minimum pool level for the natural core cooling after the rupture event is calculated with the assumption that the SBVs are not opened.

To estimate the time required for the manual actions, the time required for individual task components is evaluated based on the HFE analysis in accordance with the methodology provided in ANSI/ANS 58.8 [5]. The time required to be analyzed is divided into several sub-intervals, and the total time required for the manual SBVs open is calculated. As a unique alarm for this event is provided in the MCR, the time of the alarm generation and time taken for individual manipulations are analyzed in detail.

The HFE analysis for the required time shows that the time required for the manual action is less than the available time obtained from the thermal hydraulic transient analysis. To validate the result of the

HFE analysis, the operator response time is measured through the HFE validation of the HSIs of the RR-1. The validation of the operator response time is performed under conditions that approximate the accident situation as closely as possible. As a result, all of the operating teams complete the required manual action within the available time after the occurrence of the simulated accident. The measured time for each team is less than the time estimated by the HFE analysis. From the result of the validation test, it can be concluded that the operators can manually open the SBVs correctly and reliably in the time available when a rupture of a PCS pump casing accident occurs concurrently with a software CCF of the RPS.

3 D3 ANALYSIS FOR I&C SYSTEMS OF RR-2

The structure of the I&C systems of the RR-2 is almost the same as that of the RR-1. Therefore, the only major differences between the two research reactors are described in this section.

The PAMS of the RR-2 is composed of field instruments and hardwired indicators without digital signal processing units, whereas the PAMS of the RR-1 is implemented based on the same PLC with the RPS. Therefore, the PAMS is unaffected by a software CCF of the RPS in the RR-2.

The APS of the RR-2 is designed to perform the reactor trip and ESF actuation functions while the APS of the RR-1 performs only the reactor trip function. Therefore, even when the RPS fails, the automated ESF functions can be performed by the APS, which is diverse from the RPS.

The echelons of defense of the RR-2 are structured as shown in Table IV, and the I&C systems are classified into CCF groups, as shown in Table V.

Table IV. Echelons of defense of the RR-2 I&C systems

Echelon	Safety Class	I&C Systems
Control echelon	Non-safety	RRS, PICS, APS
Reactor trip echelon	Safety	RPS
ESF actuation echelon	Safety	RPS
Monitoring and indication echelon	Safety	PAMS, Manual trip/ESF switches
	Non-safety	IPS (including OWS/LDP), Manual trip/ESF switches

Table V. CCF groups of RR-2 I&C systems

CCF Group (Block)	I&C Systems
Group-1	RPS
Group-2	RRS, PICS, APS
Group-3	IPS(including OWS/LDP)
Group-4	PAMS
Group-5	Manual trip/ESF switches

The I&C systems classified into different CCF groups are designed to be diverse from each other when considering the six aspects of diversity described in Section 2.2, such that internal failures including the effects of software CCFs do not propagate to other groups.

As the APS of the RR-2 performs the same ESF actuation functions with the RPS such as opening SBVs, closing CIDs, and running safety residual heat removal system pumps (SRHRSPs), the required ESF actuations can be covered by the APS even when the RPS fails and the direct initiation of safety functions by the PNMS is not designed for the RR-2.

Table VI shows the D3 evaluation results of the I&C systems for DBEs under the assumption that the automated reactor trip and ESF actuation functions of the RPS are inoperable owing to a software CCF. As shown in Table VI, the required reactor trip and ESF actuation functions for all the DBEs can be performed by the APS when the RPS fails to perform safety functions owing to a software CCF, and the reactor status can be continuously displayed to operators by the PAMS and IPS including OWSs and LDPs.

Table VI. D3 evaluation chart for DBEs of RR-2

Design Basis Events	Mitigation Functions Required of I&C Systems and Diverse Means against RPS CCF				
	Reactor Trip	SBVs Open	CIDs Close	SRHRSP Run	Monitoring and Display
Loss of normal electrical power	-	-	-	APS	IPS, PAMS
Inadvertent withdrawal of a control absorber rod during startup operation	APS	-	-	-	IPS, PAMS
Inadvertent withdrawal of a control absorber rod during power operation	APS	-	-	-	IPS, PAMS
Control rod failure	APS	-	-	-	IPS, PAMS
Influence by experiments and experimental devices	APS	-	-	-	IPS, PAMS
Failure of all PCS pumps	APS	-	-	APS	IPS, PAMS
Failure of one PCS pump	APS	-	-	APS	IPS, PAMS
Reduction in coolant flow due to bypassing of the core	APS	-	-	APS	IPS, PAMS
Shaft seizure of PCS pump	APS	-	-	APS	IPS, PAMS
Flow blockage of a single sub-channel in a fuel assembly	APS	-	APS	-	IPS, PAMS
Flow blockage of a fuel assembly	APS	-	APS	-	IPS, PAMS

Failure of pumps in the secondary circuit	APS	-	-	APS	IPS, PAMS
Breakage of the secondary circuit components	APS	-	-	APS	IPS, PAMS
Rupture of the primary coolant boundary	APS	APS	APS	APS	IPS, PAMS
Failure of the cladding of a fuel element	APS	-	APS	-	IPS, PAMS

4 SUMMARY AND CONCLUSIONS

A case study on a D3 analysis for the I&C systems of two research reactors was conducted for this paper. The I&C systems of the research reactors are classified into four echelons of defense to confirm the defense-in-depth design and the diversity between CCF groups and echelons of defense was analyzed to assure the integrity of the I&C systems against a software CCF of the RPS. As a result of the D3 evaluation for DBEs, it is confirmed that the required safety functions of the RPS can be superseded by other systems unaffected by the CCF when any DBE occurs concurrently with a software CCF of the RPS. As a manual operator action is used as a diverse means in the case of a loss of coolant accident in conjunction with an RPS CCF for RR-1, a suitable HFE analysis was performed to credit the manual operator action.

Through the D3 analysis for the I&C systems of research reactors, the potential vulnerabilities to a software CCF can be identified and the corrective actions such as design modifications should be taken. If any design change that could affect the defense-in-depth of the I&C systems is implemented, the D3 analysis should be carried out iteratively.

5 ACKNOWLEDGMENTS

This work was supported by the National Research Foundation (NRF) of Korea funded by the Ministry of Science, ICT and Future Planning (Grant Code: 2012M2C1A1026912).

6 REFERENCES

1. USNRC, NUREG-0800, Branch Technical Position 7-19, Revision 6, *Guidance for Evaluation of Diversity and Defense-in-Depth in Digital computer-Based Instrumentation and Control Systems* (2012).
2. USNRC, Staff Requirements Memorandum on SECY-93-087, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs* (1993).
3. USNRC, NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems* (1994).
4. USNRC, NUREG-0800, Appendix 18-A, *Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses* (2014).
5. ANSI, ANSI/ANS 58.8, *Time Response Design Criteria for Safety-Related Operator Actions* (1994).