Abstract

Title of Document:	AN EVENT CLASSIFICATION SCHEMA FOR CONSIDERING SITE RISK IN A MULTI-UNIT NUCLEAR POWER PLANT PROBABILISTIC RISK ASSESSMENT
	Suzanne Schroer, Master of Reliability Engineering, 2012
Directed By:	Professor Mohammad Modarres, Department of Mechanical Engineering

Today, probabilistic risk assessments (PRAs) at multi-unit nuclear power plants consider risk from each unit separately and do not formally consider interactions between the units. These interactions make the operation of multiple units dependent on each other and should be accounted for in the PRAs. In order to effectively account for these risks in a multi-unit PRA, six main dependence classifications have been created: initiating events, shared connections, identical components, proximity dependencies, human dependencies, and organizational dependencies. This thesis discusses these six classifications that could create dependence between multiple units. As a validation of the classification, this thesis will also discuss multi-unit events that have occurred in operating plants. Finally, this thesis will present existing methodologies that could be used to quantify unit-to-unit dependencies in the PRA for each classification.

AN EVENT CLASSIFICATION SCHEMA FOR CONSIDERING SITE RISK IN A MULTI-UNIT NUCLEAR POWER PLANT PROBABILSTIC RISK ASSESSMENT

By

Suzanne Schroer

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Master of Science
2012

Advisory Committee:
Professor Mohammad Modarres, Chair
Professor Ali Mosleh
Dr. Nathan Siu

Acknowledgements

I would like to thank Dr. Mohammad Modarres for his guidance during my academic pursuits at the University of Maryland. His direction, challenges, and reassurance have truly been outstanding. I would also like to thank all the faculty in the School of Engineering, especially those in the Risk and Reliability Department who contributed to my graduate education. Furthermore, my colleagues in the Department have helped me learn how to be a student again. In addition, this research would not have been possible without the support of the Nuclear Regulatory Commission's Graduate Fellowship Program and the staff in the Office of New Reactors and the Office of Nuclear Regulatory Research. Finally, my family and friends have been a constant encouragement; without their support, revisions, and incredible patience, none of this would have been possible. Mom and Matt, I cannot thank you enough.

Table of Contents

Table of Figures

Table of Tables

List of Acronyms

Advisory Committee on Reactor Safeguards	ACRS
Auxiliary Feedwater	AFW
Advanced Notice of Proposed Rulemaking	ANPR
Bayesian Belief Network	BBN
Binary Decision Diagram	BDD
Binomial Failure Rate	BFR
Computer-Aided Fault Tree Analysis	CAFTA
Core Damage Frequency	CDF
Dynamic Master Logic Diagram	DMLD
Emergency Containment Filter	ECF
Emergency Core Cooling System	ECCS
Emergency Diesel Generator	EDG
Fire Induced Vulnerability Evaluation	FIVE
Gaussian Process Regression	GPR
International Atomic Energy Agency	IAEA
Large Early Release Frequency	LERF
Licensee Event Report	LER
Loss of Offsite Power	LOOP
Multiple Greek Letter	MGL
U.S. Nuclear Regulatory Commission	NRC
Performance Influencing Factor	PIF
Probabilistic Risk Assessment	PRA
Reactor Oversight Program	ROP
Seismic Margin Assessment	SMA
Significance Determination Process	SDP
Socio-Technical Risk Analysis	SoTeRiA
Staff Requirement Memorandum	SRM
Standardized Plant Analysis Risk	SPAR
Standby Gas Treatment	SGT
Station Blackout	SBO
Structure, System, or Component	SSC
System Analysis Programs for Hands-On Integrated Reliability Evaluations	SAPHIRE

Chapter 1 Introduction

1.1 Background

Currently, multi-unit site risk is not being formally nor adequately considered in either the regulatory or the commercial nuclear environment [1, 2, 3], despite the fact that the question of multi-unit accidents is not one of possibility, but of probability [3]. These types of accidents are significant and do need to be addressed [3]. Fleming, Arndt, Omoto, Jung, et al. have recommended ideas to deal with different facets of a multi-unit probabilistic risk assessment (PRA) [3, 4, 5, 6]; however, there are still no well-established, comprehensive methods for considering multi-unit site dependencies when creating a PRA [7].

In the regulatory arena, the U.S. Nuclear Regulatory Commission (NRC) has been discussing how to address the issue of multi-unit nuclear power plant PRAs for many years. After the Chernobyl accident, the 1981 lessons learned report included four recommendations that dealt with multi-unit accidents. Many of these recommendations came about because noble gas and airborne volatiles were found to have been transported to the other three units onsite during the accident through a shared ventilation system. It was recommended that control room habitability, contamination outside of the control room, smoke control, and shared shutdown systems be looked at more fully [8]. Then, in 1995, the Commission committed to expand the uses of PRA [9]. For several years, the conversation did not focus on multi-unit PRA; however, discussions began again in 2002 and 2003 and resulted in a 2005 NRC staff recommendation to the Commission to endorse an integrated risk analysis [10, 11, 12]. The NRC staff presented the Commission with three options to deal with this so-called integrated risk: 1) take no action, 2) quantify

the integrated risk at the site for new reactors that were being built, or 3) quantify the risk for all reactors at a site. The staff recommended that the Commission choose Option 3, which would require nuclear power plants to quantify the risk of all units on a reactor site [12]. The Advisory Committee on Reactor Safeguards (ACRS) suggested, however, that quantifying the integrated risk from all *new* reactors onsite would be a better option. In the Staff Requirements Memorandum (SRM), the Commission directed the staff to create an Advanced Notice of Proposed Rulemaking (ANPR) and to consider the ACRS's recommendations [13]. Also in 2005, the staff recommended that any modular reactor designs should account for the integrated risk posed at multi-unit sites. In 2006, the NRC staff returned with the ANPR and noted that they would be discussing the issue of integrated risk with external stakeholders [14]. The result of all this was NUREG-1860, which presented an approach to integrated risk that only necessitated that the risk from new reactors be "limited" and did not provide prescriptive guidelines [15]. In 2008, the NRC also indicated that it would be creating loss of offsite power (LOOP) models for its Standardized Plant Analysis Risk (SPAR) program that would address multi-unit effects [16], but such a model is not yet complete. Currently, the NRC is in the early stages of an effort to create an integrated Level 3 PRA that includes the effects of multiple units, as well as the risk from all radiation sources onsite, such as the spent fuel pool [17].

In the nuclear industry, many advances have been made in multi-unit risk analysis; however, solutions generally focus on only one facet of the PRA at a time and do not consider other concurrent events. For example, one issue that has been looked at in more detail with respect to multi-unit PRAs is station blackout (SBO). SBO events are considered to have a high conditional core damage probability [6]. They are, however,

one of the most complicated events to analyze, even for a single unit, because of the interdependencies in the electrical systems [6]. Because of this complex nature, there is a high probability of underestimating the SBO frequency if the dependencies between multiple units are not modeled correctly [6]. For instance, the model developer must take into account that some systems, such as swing diesel generators, may be completely unavailable to one of the units during a simultaneous SBO or LOOP event [6].

Another area that has been looked at by the industry with respect to multi-unit PRAs is seismic events [1]. One methodology looked at correlations between sister units and component fragility across the site; however, severe accident damage that could interfere with emergency operation of other undamaged units was not addressed [1]. Another study found that having crossties for emergency diesel generators (EDGs) during seismic events lowered the core damage frequency (CDF) of a single unit, the CDF of a two-unit site, and the frequency of nearly simultaneous core damage [18]. This study did not, however, evaluate the other dependencies that may exist on a two-unit site. Although some issues of multi-unit risk have been looked at in greater detail, no integrated approach exists and key limiting assumptions have still been made, such as the assumption of a single dependency, such as the aforementioned seismic events, between the units.

The Seabrook Multi-Unit PRA is one of the only multi-unit PRAs existing to date and was created in 1983 [19]. First, initiating events were classified into three categories: those that will always affect multiple units, those that will sometimes affect multiple units, and those that are independent. From those initiating events that affected multiple units, dominant initiating events were chosen for quantification. These events included

LOOP, a truck crash into transmission lines, earthquakes, and flood of service water pumps. Next, a plant model was developed for the two-unit station and accident sequences frequencies were estimated. This plant model accounted for the occurrence of zero, one, or two accidents in a given year, the possibility of concurrent accidents, and potential for common cause failures. Common cause failures in the Seabrook PRA included design errors, human errors, plant mismanagement, and environmental stresses. The accident sequences were quantified by using explicit and parametric models. The parametric model that was used was the beta factor, and the beta factor was "subjectively" estimated. Finally, the frequency of events that affected both units was calculated as:

$$CDF_T = 2CDF_I - CDF_C \qquad \text{Eq. 1.1.1}$$

where CDF_T is the total site CDF, CDF_I is the CDF of a single unit, irrespective of the other unit onsite, and CDF_C is the frequency of a core damage event on both units concurrently. There was also some work done beyond a Level 1 PRA, and it was found that single reactor events had the greatest contribution to releases, despite the fact that concurrent accidents had the highest amount of release per event [19].

1.2 Analysis Options

There are two basic ways to create a multi-unit PRA. One method is to develop an entirely new multi-unit PRA, and the other is to integrate existing single-unit PRAs. The possible prohibitive cost of developing a PRA and the potential technical impediments of creating a state-of-practice multi-unit PRA make the latter method more feasible practically and potentially economically because of the ability to utilize existing data and models. There has been at least one attempt to construct a comprehensive methodology

that would create a simplified multi-unit PRA by integrating multiple single-unit PRAs into a multi-unit PRA [4]. It consists of the following seven basic steps:

1. Find the dominant sequences for the "baseline" plant. The baseline plant is simply the plant that will act as the anchor point for this process.
2. Modify the initiating event frequencies and basic event failure probabilities of the baseline plant to account for another plant.
3. Modify the initiating event frequencies and basic event failure probabilities of the subsequent plant to account for the baseline plant.
4. Develop a multi-unit PRA using only the dominant sequences identified in Step 1.
5. Create a Level 2 PRA for these plants.
6. Create a Level 3 PRA for these plants.
7. Repeat the process for each additional plant [4].

This methodology requires the user to define many of the intermediate steps and create a Level 3 PRA for each unit at the site; additionally, it does not give prescriptive guidelines on how the initiating event frequencies and basic event probabilities should be adjusted to account for other units onsite. Since this method requires the analysis of each accident sequence, it is much more resource intensive than simply analyzing classes of accident sequences which, under the proposed classification schema in this thesis, can be accomplished.

Since there are approximately one hundred systems in a nuclear power plant, there are many ways in which two or more units can be connected [20]. In order to truly address a

multi-unit PRA, one first must be able to understand all of the avenues in which units could be coupled. The multi-unit methodology proposed here defines a unit as a reactor core and its front-line and support systems, structures, and components (SSCs). That is, a unit at a traditional nuclear power plant would be everything inside of the primary containment building and power generation and supporting systems, and for small modular plants, a unit would be considered one module.

1.3 Motivation

The motivation for this thesis was the lack of formalized guidance for creating a multi-unit PRA, which reflects the risk of circumstances that may affect multiple reactors at one site. Additionally, with small, modular reactors, where the plants are designed to have many inter-connected units, preparing for licensing, the NRC will be forced to address this issue.

The events at Fukushima Daiichi also showed how important multi-unit events can be. On March 11, 2011, the largest earthquake Japan has ever experienced caused damage to six units' system at the Fukushima Daiichi Nuclear Power Station. Forty-one minutes later, the first of seven tsunamis hit the site. Even more damage to all three units occurred, including the loss of the shared intake. Three of the six units had been operating at the time of the earthquake, and these units subsequently lost all cooling to their reactor cores. Despite the restoration of partial cooling, there was still hydrogen accumulation on these three units. Two units experienced a hydrogen explosion, and one also leaked hydrogen into an adjacent building causing a third unit to have a hydrogen explosion. This shows just a few of the potential interactions that can occur at a multi-

unit nuclear power plant [21]. The risk community must determine the best way to address multi-unit site risk.

1.4 Objectives

The classification proposed in this thesis will attempt to explore the wide breadth of potential dependencies that occur at multi-unit sites and will allow multiple, independent, single-unit PRAs to be integrated into a single multi-unit PRA. This, in turn, will allow the site CDF to be evaluated. In reality, CDF can be calculated relative to a unit, a site, an owner utility, a country, a class of reactor designs (e.g., Mark-I boiling water reactors), or many other grouping variables. Dependencies do exist in each group and are different from one another. This paper, however, will focus only on the site CDF. A discussion on the definition of this site CDF can be found in Section 1.5. To calculate this site CDF, one can utilize existing single-unit PRAs and combine them using the proposed event classification and methodologies discussed in this thesis. These classifications and methodologies will allow multi-unit accidents to be considered in a comprehensive manner. This approach should be successful whether the multiple units are nearly identical or unique, as is the case when more than one reactor design or vintage exists at a site. The only difference between these will be the amount of sequences that are placed into each classification.

1.5 Definition of Site CDF

Defining the site CDF is not an arbitrary process and is not simply the addition of each unit's marginal CDF because, as discussed, each unit does not operate fully segregated from other units onsite. Dependencies between most all units exist because they are beneficial from a safety, economic, or engineering perspective. In order to quantify a

multi-unit PRA, a new metric must be defined. In this thesis, the site CDF is used as this metric. Before site CDF can be defined, however, core damage needs to be defined. The use of the term "core damage" is somewhat subjective. The IAEA states that core damage for a light water reactor is often defined as exceeding the design basis limit of any of the fuel parameters [22]. The NRC's SPAR models, on the other hand, define core damage as uncovery of the reactor fuel [23]. Others have defined core damage as the uncovery and heatup of the fuel to the point where "severe" fuel damage is anticipated [24]. Still others state that the definition of core damage is consistent world-wide and defined as local fuel temperature above 2200 °F, which is the regulatory limit defined in 10 CFR 50.46(b)(1) [25]. No matter which definition is chosen, it must be kept consistent throughout the PRA. That is, when the single-unit PRAs are combined into the multi-unit PRA, the definition of core damage cannot change. The definition of core damage *frequency* as used in the single-unit PRA, however, must change as the single-unit PRAs are integrated into one multi-unit PRA.

There are three different ways that the CDF for a multi-unit can be calculated. The traditional method is to look at the frequency of core damage per unit, per year irrespective of the operating states of other units. Another is to examine the frequency of one unit having core damage while assuming the other units do not experience core damage (i.e., exactly one core damage). The final approach is to look at the frequency of multiple concurrent core damages.

This lends itself to two ways by which the site CDF can be calculated. The first is by calculating *the frequency of exactly one core damage event occurring per site per year*. That is, the frequency of one unit having a core damage event during a year, while the

other units do not. The other is to calculate *the frequency of multiple core damages occurring nearly simultaneously per site per year*. That is, the frequency of one unit experiencing a core damage event during a year, while another unit is also experiencing a core damage event. All combinations of these cases lead to the definition of site CDF, which is *at least one core damage per site per year*. The CDF for exactly one core damage event occurring per site year would be, for example, the frequency of unit 1 only experiencing a core damage event or only unit 2 experiencing a core damage event; this would be either the dark or light section in Figure 1, respectively. Whereas, the frequency of multiple core damage events would be the intersection area of Figure 1. The sum of the areas would represent at least one core damage event.

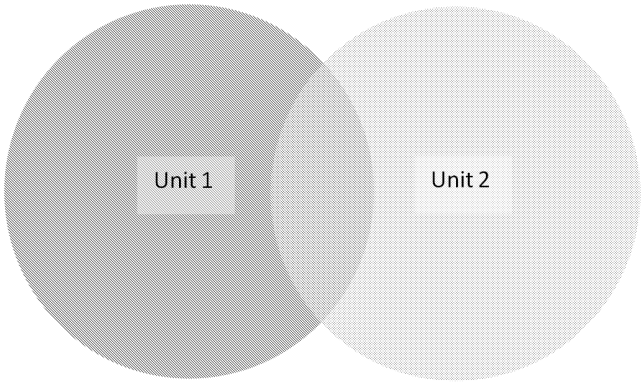

Figure 1: Venn Diagram of Core Damage Frequency

Both calculations can be useful for a nuclear power plant operator to know. Calculating the frequency of exactly one core damage would allow the nuclear power plant to compare to the NRC safety goal for CDF [26]. Additionally, this type of calculation could be used for importance calculations and risk-informed modifications such as in the technical specifications and for components in the reliability assurance program. If the plant, however, wanted to be able to expand the Level 1 PRA to a Level 2 or 3 PRA, then knowing the probability of nearly simultaneous core damage, which would maximize the

potential release, would be more beneficial. This allows the plant to understand SSCs that are important to severe accident progression as well as evaluate options for emergency planning. If expanded to a Level 2 PRA, this calculation would also allow the plant to compare their site large early release frequency (LERF) to the NRC safety goal for LERF [26] or simply large release frequency for new reactors [27]. As previously mentioned, this concept can also be extended to estimate CDF with respect to a plant owner, a vendor, or any other organizational commonality.

Chapter 2 Classifications

2.1 Introduction

To gain an accurate view of a multi-unit site's risk profile, the CDF for the site rather than the unit should be considered. There are many types of events that could create a dependency between multiple units from a risk perspective. In order to effectively account for these risks when looking to create a multi-unit PRA, six main commonality classifications have been established: initiating events, shared connections, identical components, proximity dependencies, human dependencies, and organizational dependencies. An illustration of these classes can be seen in Figure 2. Additionally, there is a seventh class, independent events, which does not affect multiple units. Since this thesis is focused on the mulit-unit dependencies, the discussion of the seventh class will be limited.

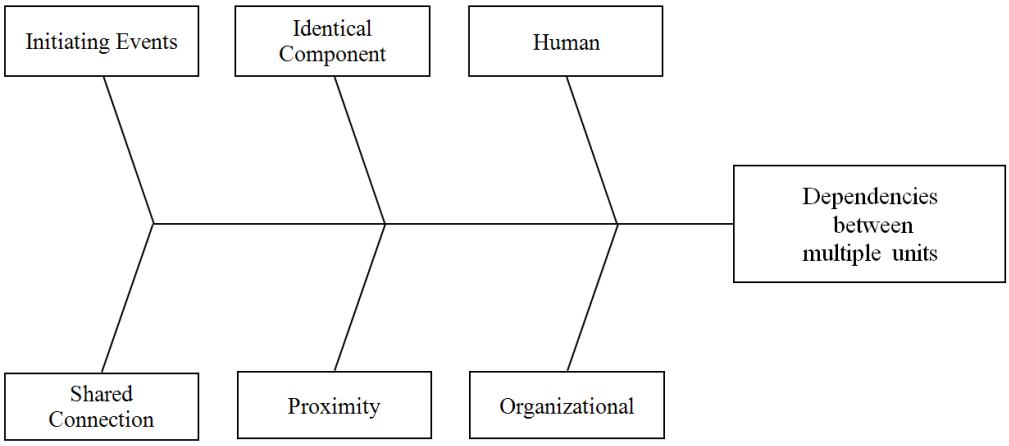

Figure 2: Commonality Classification of Events

The first step in the proposed process is to sort the events in the single-unit accident sequences into the seven classifications, which are introduced briefly here, but explored in greater detail in the following sections. The first classification, initiating events, refers

to single events that have the capacity to affect multiple units of a nuclear power plant site. The initiating event class is divided into two subclasses: definite and conditional. The second classification, shared connections, refers to links (piping, cables, power divisions, etc.) between components that physically connect multiple units. The shared connection class is divided into three subclasses: single SSC, time sequential, and standby sharing. The third classification, identical components, represents components that are the same design for multiple units. This class is considered in single-unit PRAs under "common cause" failures among SSCs. The fourth classification, proximity dependencies, occurs when one or more environments are shared among multiple units' SSCs and have the ability to adversely affect their operation. The fifth class, human dependencies, refers to commonalities that may be created from a person's interaction with an SSC. The human dependency class is divided into two subclasses: pre-initiating event and post-initiating event. The sixth class, organizational dependencies, occurs when an organization connects multiple units (through programs such as operating and emergency procedures, reliability assurance, surveillance procedures, training, simulators, etc.), typically through either a logical error or a permeating culture. Additionally, there is a seventh category of events, SSCs, and human actions that are completely independent. Once the sequences have been sorted, each classification can be considered. This allows the data set to be reduced from one hundred systems, as previously mentioned, to just seven classifications that need to be analyzed. A discussion of each classification is provided in the next section. It should be noted that in the proposed form, this classification schema is not mutually exclusive. Specific coupling

factors, such as manufacturing attributes or component internal parts, could be assigned to each class, in order for the proposed classification to be made more exclusive [28].

2.2 Initiating Events

The first class, initiating events, represents those single events that have the capacity to affect multiple units of a nuclear power plant site. Not all initiating events that are incorporated into a typical nuclear power plant PRA will affect more than one unit on a site, although several have that capability. These initiating events can be divided into two subclasses, events that will always affect multiple units, referred to as "definite" events, and events that will only affect multiple units under certain circumstances, referred to as "conditional" events [19]. These subclasses are illustrated in Table 1. The initiating events used in Table 1 are taken from NUREG/CR-6928 and IAEA-TECDOC-1341 [29, 30].

Table 1: Examples of Initiating Event Subclasses

Definite	Conditional
Loss of Offsite Power	Loss of Emergency Service Water
Loss of Ultimate Heat Sink	Loss of Condenser Vacuum
Station Blackout	Loss of Component Cooling Water
	Loss of Feedwater
	Loss of DC Bus
	Loss of Instrument Air
	Steam Generator Tube Rupture

Those events that will always affect multiple units include loss of offsite power and loss of the ultimate heat sink Those events that have the potential to affect multiple units

under certain circumstances include loss of service water, and loss of condenser vacuum. Examples of circumstances that may cause the conditional initiating events are loss of cooling water intake, which may be associated with certain loss of coolant vacuum or loss of service water events, or different turbine missile trajectories, which would change the affect they have on one or multiple units. It should be noted that depending on the site and reactor design, these subclasses may include different initiating events from those listed in Table 1. For example, if there are no connections in the instrument air system, then events involving instrument air would be classified as independent, rather than a conditional initiating event as seen in Table 1.

2.3 Shared Connections

The second class, shared connections, refers to links that physically connect SSCs of multiple units. These connections may be in three different sub-classes [31, 20]. The first subclass is a single SSC. This occurs when multiple units rely on a single SSC for simultaneous support. Two examples are using the same plant exhaust stack or having a common header for safety injection. The second subclass is time sequential sharing or cross-connected SSCs. This is when an SSC is able to fully support any single unit; however, it is not capable of simultaneously supporting multiple units. This often occurs between electrical power supplies at nuclear power plants. The third subclass is standby sharing. Standby sharing occurs when multiple units share a standby or spare SSC that can only be used to support a single unit. This approach is commonly seen for safety systems such as emergency diesel generators and fire water systems. A more comprehensive list of systems that may be shared can be found in Table 2 [20].

Table 2: Examples of Shared System Subclasses

Single SSC	Time Sequential	Standby
Plant Stack	Startup Auxiliary Transformer	Standby AC Power Systems, including diesel generators
Intake Structure	Diesel Generator	Standby Pumps
Control Room	Spent Fuel Pool Cooling and Clean-Up System	B.5.b Equipment: Portable components
Diesel Generator Building	Chemical and Volume Control System	
Refueling Floor*	Vital 125V DC Control Power System	
Water Treatment Building	Offsite Power System	
Fire Protection System	Auxiliary Feedwater System	
Independent Fuel Storage Installation	Boron Recovery System**	
Makeup Water Treatment System	Component Cooling Water	
Potable and Sanitary Water System	Service Water	
Plant Communication System	Compressed Air	
Reactor Building Crane	Recirculating Cooling Water	
Auxiliary Building	Residual Heat Removal	
Turbine Building	Condenser Circulating Water	
Emergency Gas Treatment System		
Auxiliary Steam System**		
Ultimate Heat Sink		
Condensate Storage Tank		
Post-Accident Sampling System		
Switchyard		

* Denotes systems specific to boiling water reactors
**Denotes systems specific to pressurized water reactors

2.4 Identical Components

The third class, identical components, represents components that have the same design, operation, and operating environment for multiple units. This means that the components are designed, installed, and maintained nearly identically and are operated in the same manner making them susceptible to traditional common-cause failures that are considered for single units. This not only includes conventional components, but also digital instrumentation and control systems and software.

2.5 Proximity Dependencies

The fourth class, proximity dependencies, can be manifested in several different ways. Proximity dependencies occur when a single environment has the potential to affect multiple units. This common environment could be either intentionally or unintentionally created. The proximity could be within a room, positions between or within systems, or occur because of the site layout. Additionally, conduits and doors may connect otherwise independent areas. If, for example, certain components of the chemical and volume control system for multiple units were in the same room, a fire or other event could affect multiple units. Likewise, if there was an explosion onsite and two units were located very close together, the same explosion could affect both units.

2.6 Human Dependencies

The fifth class, human dependencies, can also be manifested in a variety of ways. Human dependencies occur when a person's interaction with a machine affects multiple units. This could be an operator, a maintenance team member, a member of an installation crew, or the like. Human dependencies are split into two subclasses, pre-initiating event and post-initiating event actions. Table 3 illustrates some of these potential dependencies.

Table 3: Examples of Human Dependency Subclasses

Pre-Initiating Event	Post-Initiating Event
Missing surveillances	Misalignment of breakers after LOOP or SBO
Maintenance cleaning	Misalignment of valves after transient
Identical installations	Mental slip because of lack of attention to other units after an event
Transposition errors	
Identical maintenance actions	

Human actions that occur before an event typically create latent conditions. For instance, in currently operating plants the same maintenance team could perform the same task and create the same failure environment on multiple units. Human actions that occur after an event typically have immediate consequences. One example would be in small modular reactors where the same operator controls multiple plants at once. As he is responding to a situation on one unit, he may not notice or be able to control an evolving situation on another unit.

2.7 Organizational Dependencies

The sixth class, organizational dependencies, has a number of different facets. Organizational dependencies occur when an organization somehow connects multiple units, typically by some sort of logic error or culture that permeates the organization. Although human and organizational dependencies are closely related, there is delineation between the two, which lies in the root cause of the failure. Human dependencies are dependencies that are caused by the man-machine interaction, while organizational dependencies are often human actions caused by the logic or culture of the organization. In this case, the organization could refer to a department at the plant, the plant itself, or

the vendor that supplies components to the plant. These dependencies occur because the same logic or culture exists across an entire group, which affects multiple units and, at times, multiple sites. Examples of these dependencies can be seen in Table 4.

Table 4: Examples of Organizational Dependencies

Incorrect procedure that has been mirrored for multiple units
Latent design issue that affects multiple units
Incorrect calculation that is used on multiple units
Incorrect technical specifications that have been mirrored for multiple units
Incorrect vendor guidance that has been applied to multiple units.
Incorrect engineering judgment that has been applied to multiple units
A misinterpretation of guidance or requirements that affects multiple units
A misunderstanding of system configuration or function that affects multiple units
Poor safety culture, which leads to errors of judgment and execution across the organization
Lack of adequate training and skills for events that affect multiple units

Examples of organizational dependencies would be if the engineering department makes the same incorrect assumption on calculations for multiple units or if equivalent procedures are used between two units. Another could be only having one fire brigade for the entire site. Furthermore, organizational dependencies could exist if the same vendor provides equipment and guidance for multiple units. Using the same guidance from a vendor on multiple units could create a dependency across units, for example.

2.8 Independent Events

The seventh class, independent events, represents those events that do not create a dependency between multiple units. This class only includes events whose occurrence and effect are limited to a single unit. Any events or SSCs that do not fall into the

previously discussed categories would fall into this classification. For example, a loss of coolant accident would be an independent event. Additionally, the majority of the SSCs for each unit would be in this category.

Chapter 3 Analysis of Past Multi-Unit Events

3.1 Introduction

In order to verify that the proposed classification encompasses all potential events that may link multiple units, Licensee Event Reports (LERs) that were submitted to the NRC were analyzed. Events that affected multiple units were classified into each of the classes and subclasses. The LERs were also examined to see if there was an official NRC finding from the event. NRC findings were analyzed because they evaluate the risk significance of the event. Also in the course of the analysis, dependencies beyond the site, such as dependencies caused by vendor guidance, were noted.

3.2 Licensee Event Reports

To confirm that the created classification includes all potential events that may link multiple units, all LERs that were submitted to the NRC from 2000 through 2011 were evaluated. LERs are submitted to the NRC after plant abnormalities in accordance with guidelines prescribed in 10 CFR 50.73. These LERs discuss the apparent root causes of the events and actions that will be taken by the licensee. It should be noted that LERs include both existing conditions (i.e., latent conditions) that have been found, that is conditions that were discovered before becoming events, and events that have occurred at the plant, that is conditions that were not caught before causing an event. Three-hundred-ninety-one of 4207 total LERs affected multiple units on a site, which amounts to 9% of all LERs submitted between 2000 and 2011. This represents a significant number of multi-unit issues that happen every year; however, 91% of the events belonged to the seventh event classification, independent events. Each multi-unit LER was reviewed individually to determine the cause of the dependency between the units. It should be

noted that the dependency was not always the root cause of the plant abnormality. For example, in some instances a maintenance member did not follow procedure while working on a common system. The dependency link in these cases was not the human error, but rather the fact that the system was common to multiple units. The most common link between multiple units was organizational dependencies. These included everything from symmetrical procedures and technical specifications across units to vendor and departmental logic errors. This accounted for 41% of the 391 multi-unit LERs. Single shared SSCs were the next most common link and accounted for 28% of the multi-unit LERs. Table 5 outlines further the breakdown of classifications. Additionally, it should be noted that while the majority of LERs only affected two units, twenty-nine LERs (7% of the multi-unit LERs) affected three units. Appendix 1 has a full listing of all the LERs that were analyzed with the classification and subclass assigned.

Table 5: Multi-Unit Licensee Event Report Classifications from 2000-2011

Classification	*Percentage of Total*	*Example LER*
Initiating Event	6.91%	
Definite	3.84%	Severe weather caused a LOOP event that resulted in the automatic scram of three units *[32]*.
Conditional	3.07%	Divers working on Unit 2 piping became unresponsive, so Unit 1 was tripped due to concern for diver safety *[33]*.
Shared Connection	34.27%	
Single	27.62%	Two units had to be shut down because of macro fouling in the shared intake *[34]*.

Time Sequential	5.88%	An auxiliary feedwater (AFW) pump was found to be inoperable. The AFW system is shared between two units. One dedicated train for each unit and a swing train *[35]*.
Standby	0.77%	The standby EDG was aligned during testing. The operators did not recognize this system alignment, and did not correctly start emergency service water pumps to prevent auto start during the testing *[36]*.
Identical component	10.49%	Neutron flux monitor channels were spliced incorrectly on two units *[37]*.
Proximity	4.60%	It was identified that fire damage in the cable spreading room may prevent the ability to safely shutdown two units *[38]*.
Human	3.07%	
Pre-Initiating event	2.81%	The same maintenance team incorrectly installed hydrogen ignition system igniter glow coils on two units *[39]*.

Post-Initiating event	0.26%	After an electrical transient, the operators did not correctly close breakers, which resulted in a condition in which two out of four emergency buses per unit would not have automatically received power from their respective EDGs in the event of a LOOP *[40]*.
Organizational	40.66%	A calculation for high-energy line breaks that was used for multiple units was found to have errors *[41]*.

3.3 NRC Findings

Under the NRC's Reactor Oversight Process (ROP), inspection findings are evaluated under the Significance Determination Process (SDP) and assigned a color that indicates its safety significance [42]. Findings with very low safety significance are labeled "green." "White" findings have low to moderate safety significance, "yellow" findings have substantial safety significance, and "red" findings have high safety significance. For violations that are not subject to the SDP, a severity level is assigned in accordance with the NRC Enforcement Policy [43]. Violations with very low safety significance are "Severity Level IV." "Severity Level III" violations have moderate safety significance, "Severity Level II" violations have significant safety significance, and "Severity Level I" have serious safety significance. Of the 391 LERs determined as multi-unit events, the NRC cited eight as official findings (two red, one yellow, two white, two green, and one Severity Level III violation), which equates to two percent of the multi-unit LERs. Four findings were linked to organizational factors, two to shared SSCs, one to identical

equipment, and one to human action. Table 6 maps the finding to the appropriate LER and event classification.

Table 6: NRC Findings and Corresponding Classes

LER Identifier	Multi-Unit PRA Classification	Description of Event	Finding
259/2009-003	Shared system; single SSC	The shared standby gas treatment (SGT) system relay failed, causing the SGT system to be inoperable for all three units onsite [44].	Green
266/2002-005	Shared system; time sequential	The flow restricting orifices on the shared AFW system pumps were found to have the potential to be simultaneously clogged. The AFW system is shared by two units [45].	Red
387/2002-005	Human; pre-initiating event	Two consecutive maintenance mechanics filled a dry shielded canister with argon gas, rather than helium gas. This event could have had adverse effects on stored spent fuel [46].	Severity Level III
260/2000-002	Organizational	Inadequate safe shutdown instructions had the potential to render the residual heat removal pumps inoperable on two units during a fire event [47].	Green
266/2001-005	Organizational	An error in the emergency operating procedures resulted in the potential to intensify an accident that had loss of instrument air on two units [48].	Red
269/2002-001	Organizational	An incorrect calculation resulted in the inability to adequately control the pressurizer heater from the Standby Shutdown Facility on three units, which could result in the loss of pressure control during events when the Standby Shutdown Facility is needed [49].	White
528/2004-009	Organizational	Procedures did not contain necessary requirements for Emergency Core Cooling System (ECCS) piping voids for three units. The voids that were created could have caused the ECCS to be inoperable during a loss of coolant accident [50].	Yellow
250/2005-004	Identical Equipment	The same fuse type was installed on two units' emergency containment filter (ECF) fan. After two back-to-back blown fuses, the licensee identified that the fuse design was not acceptable. The ECF is designed to remove radioactive iodine in the case of an accident [51].	White

Not only were dependencies found between multiple units on a single site, but there were also several instances that affected more than one site. There were two occurrences of

Westinghouse Nuclear Safety Advisory Letters that caused multiple sites to reach the threshold of submitting an LER, one in 2002 [52, 53, 54, 55] and again in 2009 [56, 57, 58, 59]. The Westinghouse letter in 2002 alerted sites that the steam generator low-low level setpoint for a reactor trip was potentially non-conservative, while the 2005 letter warned sites that in Modes 3 and 4 there could be vapor in the ECCS during a loss of coolant accident. Additionally, two sister plants, located in different sites, had two separate instances of events that affected both plant sites. The first event in 2005 occurred while local leak rate tests were performed during core alterations or movement of irradiated fuel within containment were in progress, thereby creating direct access from the containment atmosphere to the outside atmosphere [60]. This condition had existed on both sites, each with two units. The second, which occurred in 2010, could have caused the loss of the component cooling system safety function at both sites [61].

This analysis shows that not only do multi-unit precursor events occur, but also they can have significant consequences. Evaluation of LERs over an eleven-year period shows that almost ten percent of events that occur at nuclear power plant sites affect multiple units. Furthermore, using NRC findings as an indicator, eight of those events (2%) had safety significance. Additionally, the aforementioned classification accurately captured all the possible events as evident in the LERs and was found to be complete.

Chapter 4 Methodologies

4.1 Introduction

Four different methodologies have been identified that can be used to quantify the six classes of unit-to-unit dependencies. These methodologies are combination, parametric, causal-based, and extension methodologies. In some cases, the implementation of the methodology will vary depending on whether exactly one core damage or nearly simultaneous core damage is being calculated. The details of the differences of these two CDF definitions can be found in Section 1.5. Nonetheless, the basic logic will be the same no matter which probability is being calculated. In cases where the more detailed logic is appreciably different, the implementation of these two separate calculations will be discussed. The combination method simply requires combining existing single-unit PRAs into a multi-unit PRA. The parametric methods rely on a parameter, or several parameters, that are related to a conditional probability for all units. The causal-based method would require that all events be mapped back to a root problem, whether it is a physical failure or an organizational deficiency. The extension method would only require some existing portions of the PRA to be developed further. There is also a special case of the extension method, which uses existing methodologies for external events and applies them to a broader subset of events. For calculations in this thesis, CDF_1 and CDF_2 will represent the single unit CDFs from the existing single-unit PRA of a two-unit site, which have been previously calculated irrespective of the failures or events on other units.

4.2 Combination

For some classes and subclasses, the only thing that needs to be done to create a multi-unit PRA is to combine the existing single-unit PRAs. The items (SSCs, initiating events, etc.) that are already common to multiple plants will always be common; they simply need to be represented as one item in the multi-unit PRA so that they are not double counted in the quantification of the site CDF, LERF, etc. For these items, there will be no effect on the site CDF (i.e., the site CDF is the CDF of one unit multiplied by the number of units on the site); however, the importance of the items may increase in the final risk importance measures. For example, if the following cutsets were obtained for each unit of a two-unit site where *b* was a shared component between the units and I_i represents the initiating events:

Unit 1	Unit 2
$I_1 abc$	$I_4 zby$
$I_2 def$	$I_5 xwv$
$I_3 gbh$	$I_6 ubt$

and the CDF of each unit was as follows:

$$Q_{CDF1} = I_1\, abc + I_2\, def + I_3\, gbh \qquad \text{Eq. 4.2.1}$$

$$Q_{CDF2} = I_4\, zby + I_5\, xwv + I_6\, ubt \qquad \text{Eq. 4.2.2}$$

where Q_{CDF} is the quantification of the CDF. For the remainder of this thesis, when CDF is used in an equation, it will imply Boolean logic. Then the site CDF of exactly one core damage could be calculated as:

$$CDF_T = CDF_1 \bullet \overline{CDF_2} + \overline{CDF_1} \bullet CDF_2 \qquad \text{Eq. 4.2.3}$$

This can be treated as:

$$CDF_T=CDF_1+CDF_2 \quad \text{Eq. 4.2.4}$$

by using house events during the model development. House events "switch" between true and false to account for conditional success of the other unit. Alternatively, the equation above can be used by combining the marginal CDFs, and using the complement events. In this approach, a modern PRA software tool, such as System Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) or Computer-Aided Fault Tree Analysis (CAFTA), would need to be used. The use of a house event will be assumed for the remainder of this thesis.

The CDF of exactly one unit can now be represented as:

$$Q_{CDFT} = I_2\,def + I_5\,xwv + (I_1\,abc + I_3\,gbh + I_4\,zby + I_6\,ubt) \quad \text{Eq. 4.2.5}$$

$$Q_{CDFT} = A+B \quad \text{Eq. 4.2.6}$$

where

$$A = I_2\,def + I_5\,xwv \quad \text{Eq. 4.2.7}$$

$$B = I_1\,abc + I_3\,gbh + I_4\,zby + I_6\,ubt \quad \text{Eq. 4.2.8}$$

and A represents cutsets that do not contain the shared component and B represents cutsets with the shared component (i.e., component b in this example).

4.3 Parametric

Another methodology that may be used for certain classes of dependencies is parametric methods. Parametric methods are commonly used in traditional single-unit PRAs for common cause failure events. These methods include the alpha or beta factor and multiple Greek letter (MGL) models. The parameters that are created using these methods are used to quantify conditional probabilities of events. For parametric

modeling, the details of the logic will be slightly different for calculating the probability of exactly one core damage and the probability of nearly simultaneous core damage.

If the probability of exactly one core damage is being calculated, then the CDF of a two-unit site can be represented as:

$$CDF_1 = A_1 + B_1 \quad \text{Eq. 4.3.1}$$

$$CDF_2 = A_2 + B_2 \quad \text{Eq. 4.3.2}$$

where A represents cutsets that do not contain the affected components and B represents cutsets with affected components. Then, the CDF for exactly one core damage could be represented as:

$$CDF_T = CDF_{1+}\ CDF_2 \quad \text{Eq. 4.3.3}$$

$$CDF_T = A_1 + A_2 + \rho\ B_1 + B_2 \quad \text{Eq. 4.3.4}$$

$$CDF_T = A_1 + B_1 + A_2 + B_2 \quad \text{Eq. 4.3.5}$$

where ρ is a dimensionless parameter multiplier that accounts for the increased probability of B_1 and B_2 occurring together because of the dependency.

If, however, the probability of nearly simultaneous core damage was being calculated, then the site CDF would be represented as:

$$CDF_T = (A_1 + B_1) \bullet (A_2 + B_2) \quad \text{Eq. 4.3.6}$$

$$Q_{CDFT} = I_1 Pr(A_1)\ I_3 Pr(A_2) + I_1 Pr(A_1) I_4 Pr(B_2) + I_2 Pr(B_1)\ I_3 Pr(A_2) + I_3 Pr(B_1)\ I_4 Pr(B_2) \quad \text{Eq. 4.3.7}$$

where I represents the initiating events and where

$$Pr(B_i) = Pr(B_i \mid C)\ Pr(C) + Pr(B_i \mid \quad Pr(\quad \text{Eq. 4.3.8}$$

where C is the root event that causes dependence (coupling factor). Assuming the conditional probability when C does not happen is approximately the same as the non-conditional probability of failure by the rare event approximation yields,

$$Pr(B_i) = Pr(B_i \mid C)\ Pr(C)+Pr(B_i)\ (1-Pr(C)) \qquad \text{Eq. 4.3.9}$$

then substituting Equation 4.3.9 into Equation 4.3.7 yields,

$$\begin{aligned} Q_{CDFT} = {} & I_1Pr(A_1)\ I_3Pr(A_2)+ I_1Pr(A_1)I_4[Pr(B_2 \mid C)\ Pr(C)+Pr(B_2)\ (1-Pr(C))]+ I_3Pr(A_2)I_2[Pr(B_1 \mid C)\ Pr(C)+Pr(B_1)\ (1-Pr(C))] + \\ & I_2[Pr(B_1 \mid C)\ Pr(C)+Pr(B_1)\ (1-Pr(C))]\ I_4[Pr(B_2 \mid C)\ Pr(C)+Pr(B_2)\ (1-Pr(C))] \end{aligned} \qquad \text{Eq. 4.3.10}$$

and factoring out Pr(C) yields,

$$\begin{aligned} Q_{CDFT} = {} & I_1Pr(A_1)\ I_3Pr(A_2)+ I_1Pr(A_1)I_4[Pr(B_2) + Pr(C)(Pr(B_2 \mid C)-Pr(B_2))]+ I_3Pr(A_2)I_2[Pr(B_1) + Pr(C)(Pr(B_1 \mid C)-Pr(B_1))] + \\ & I_2[Pr(B_1) + Pr(C)(Pr(B_1 \mid C)-Pr(B_1))]\ I_4[Pr(B_2) + Pr(C)(Pr(B_2 \mid C)-Pr(B_2))] \end{aligned} \qquad \text{Eq. 4.3.11}$$

and incorporating the parameter ρ yields,

$$\begin{aligned} Q_{CDFT} = {} & I_1Pr(A_1)\ I_3Pr(A_2)+ I_1Pr(A_1)I_4[(1-\rho)Pr(B_2) + \rho(Pr(B_2 \mid C)-Pr(B_2))]+I_2[(1-\rho)Pr(B_1) + \rho(Pr(B_1 \mid C)-Pr(B_1))]\ I_3Pr(A_2)+ I_2[(1-\rho)Pr(B_1) + \rho(Pr(B_1 \mid C)-Pr(B_1))]\ I_4[(1-\rho)Pr(B_2) + \rho(Pr(B_2 \mid C)-Pr(B_2))] \end{aligned} \qquad \text{Eq. 4.3.12}$$

where ρ is a constant and the defined parameter that represents the probability of condition C existing.

In order to estimate the aforementioned parameters, a number of different parametric models could be used. Parametric models can be divided into two major categories: shock models and nonshock models [62]. While nonshock models look at basic event probabilities for random independent causes of single component failures, shock models also consider common cause "shocks" that impact the system at a certain frequency. The only shock model that has been used in nuclear power plant PRAs is the binomial failure rate (BFR) model [62]. Due to its complexity, however, it is not widely used.

The alpha factor, beta factor, and MGL models are nonshock methods and are currently used in nuclear power plant PRAs [62]. Within nonshock models there are two categories, identified as single parameter and multiple parameters models. The beta factor is a single parameter model. The alpha factor and MGL models are multiple parameter models, which means that they introduce more than one parameter to help calculate the conditional probabilities. This allows for partial dependencies between more than two components. The parameters in the MGL model have no direct relation to observable data, whereas the alpha factor model parameters, on the other hand, are estimated from observable data [62]. Currently nuclear power plants rely almost completely on the alpha and MGL models to model common cause failures because they strike a balance between complexity and accuracy.

The Seabrook Multi-Unit PRA used the beta factor [19]; however, there is not much information on how parameters currently used in single-unit PRAs would translate to multi-unit PRAs. Use of the beta factor in a multi-unit PRA may be problematic, given the conservatism that occurs when the common cause failure group is higher than four [62]. The other current parametric models may not adequately address multi-unit PRAs because they use parameter estimators that assume that when one train of a system is challenged, all similar trains are also challenged [62]. This is oftentimes not the case for multi-unit events. For example, during a single-unit reactor trip, the supporting systems for that unit will be called upon while other units' systems usually continue with normal operation. New parametric methods may need to be developed to accurately capture the conditional probabilities present in multi-unit PRAs.

4.4 Causal-based

Another methodology that may be used to model certain classifications is causal-based modeling. Causal-based modeling is simply another method to solve for the probability of the dependence existing (or Pr(C) in Equations 4.3.8-12). This type of modeling may take many forms such as process modeling techniques, regression-based techniques, deterministic dynamic techniques, or Bayesian belief networks [63]. Depending on which causal model is used, there may be no need to differentiate between the probability of exactly one core damage and nearly simultaneous core damage events.

There are many different types of dynamic deterministic methods. Two forms are dynamic event trees and dynamic fault trees. Dynamic event trees and fault trees were developed to utilize the advantages of state-space models, which are models that are not systemically oriented, while keeping the representation of the static trees by using dynamic gates to establish interaction among components and modify their failure attitude [64]. When using dynamic event trees and fault trees, the fault trees are developed first, followed by the dynamic event trees [65]. An example of these dynamic gates can be seen in Figure 3.

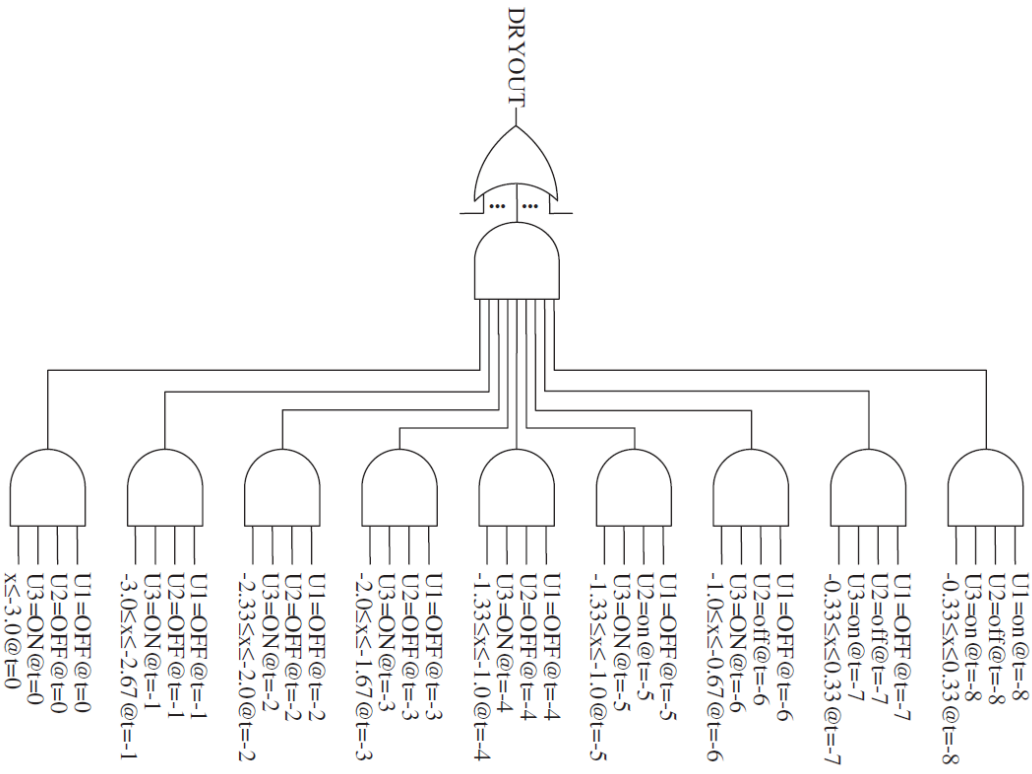

Figure 3: Dynamic AND Gate [65]

Dynamic event trees and fault trees are susceptible to extremely large numbers of algorithms because the resolution cannot be performed with Boolean algebra [64]. Dynamic event trees are similar to conventional event trees, except the branching times are determined from a system simulator through user-defined branching rules and associated probabilities. Branching rules can be used to model the uncertainty in the hardware/human/process behavior [65]. For example, if the system requires a valve to open when the pressure is above a preset limit, a branching rule could be created that the valve either opens or fails when the system pressure, as determined by the system simulator, reaches the predefined set point. This branching ensures relevant possibilities are captured for different scenarios [65]. Dynamic fault trees account for the timing of

failure events by using deductive logic to identify event sequences leading to a specified top event [65].

Dynamic master logic diagrams (DMLDs) are another form of dynamic deterministic methods that can be used to model failures or the potential for failures in real time. A DMLD can combine physical relationships, Boolean relationships, and fuzzy logic[1] into a single diagram [66]. Figure 4 shows a simple diagram of a DMLD that represents the amount of components that can be powered from three sets of batteries. In Figure 4, the Pr(C) would be the output of the "Number of Components that Can be Powered" box.

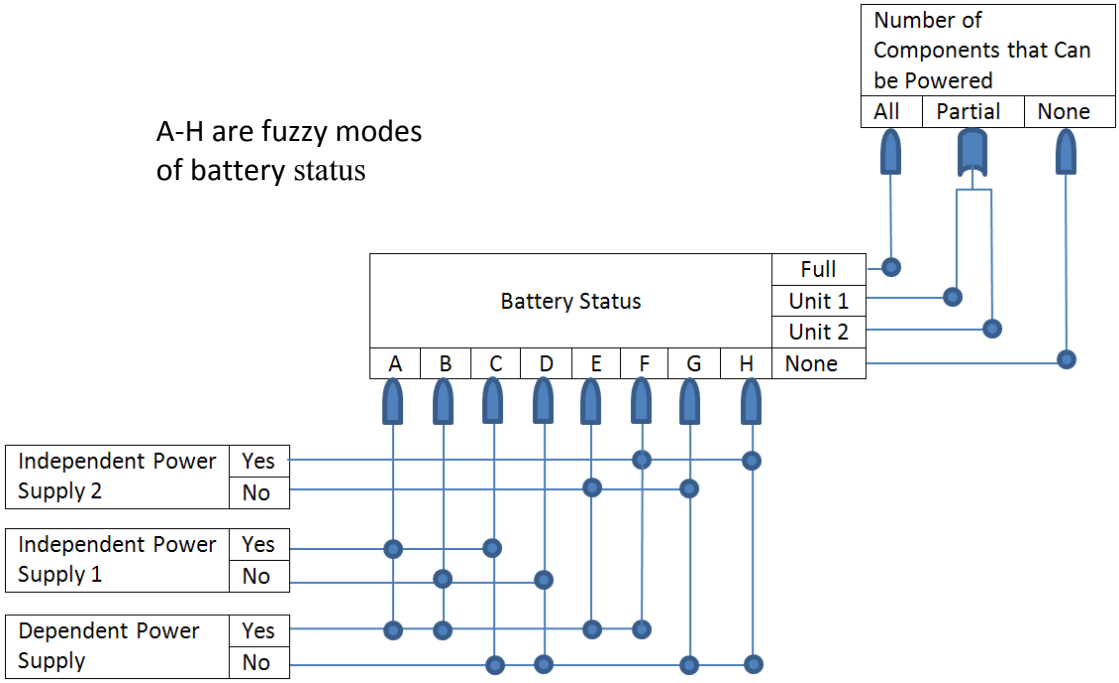

Figure 4: Dynamic Master Logic Diagram

Another causal model, a binary decision diagram (BDD), consists of nodes, which have exactly two output nodes (either 0 or 1). These nodes are then placed in a network to

[1] Fuzzy logic: "a form of mathematical logic in which truth can assume a continuum of values between 0 and 1." [90]

illustrate the relationships between the components. All of the nodes feed into two final states, either 0 or 1, that is operation or failure [67]. An example of a BDD can be seen in Figure 5. In Figure 5, Pr(C) would be the probability of A occurring.

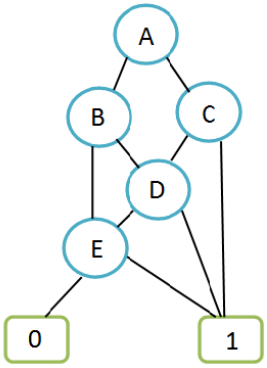

Figure 5: Binary Decision Diagram

The Socio-Technical Risk Analysis (SoTeRiA) method uses a causal-based method to create an organizational safety risk framework that maps the organizational roots of risk [68]. This model would allow organizational failures to be mapped into existing PRAs. Mohaghegh has also developed a method that uses a causal-based method to integrate a Probabilistic Physics-of-Failure model into a traditional nuclear power plant PRA [69]. A physics-of-failure model allows underlying physical failure methods (e.g., wear, fatigue fracture, creep, etc.) to be incorporated into risk models [70]. Using physical models allows not only failures, but also potential failures to be observed. A physics-of-failure approach would likely need to be combined with some other sort of model, such as a DMLD or Bayesian Belief Network (BBN) in order to get the full value of such a model. Value would also be added, by using the approach with a traditional event tree, fault tree PRA.

The most established causal-based techniques are BBNs. They are also the most versatile, as they can be combined with any of the other causal based methodologies [63]. A BBN is a directed acyclic graph or influence diagram that models relationships of a set of variables, as seen in Figure 6 [71]. In Figure 6, Pr(C) would be both the probability of A and B occurring.

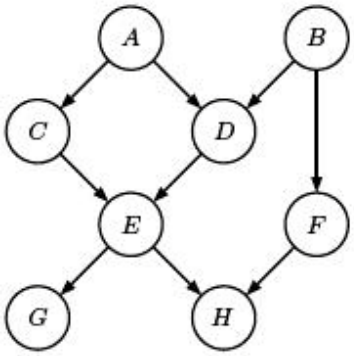

Figure 6: Directed Acyclic Graph [72]

The nodes of the graph (A through H) represent random variables, and the links represent relationships between these probabilistically determined variables [71]. BBNs also allow dissimilar information to be combined, such as qualitative information like that from expert panels, as well as quantitative data [73]. There are four basic steps to creating a BBN [74]:

1. Define a decision node; that is, the main node
2. Define the evidence nodes, which are those nodes that are related to the main node, whether indirectly or directly
3. Define the relationship between the evidence nodes and the decision node
4. Quantify each link

In open source literature, no examples of BBNs being used in nuclear power plant PRAs were found, but causal-based methods have been used in a variety of areas such as artificial intelligence [72]. Despite their low use, there are methods that have been developed to integrate causal-based methods into traditional nuclear power plant PRAs, such as the aforementioned SoTeRiA and physics-of-failure model.

4.5 Extension of Current PRA

Another methodology that could be used to quantify the event classifications is to merely extend the current breadth of the existing PRA. This approach would simply extend the traditional PRA model, which typically consists of a combination of event trees and fault trees. For the extension method, it would be necessary to determine at the outset whether nearly simultaneous core damage events were going to be calculated or if only the probability of exactly one core damage would be the focus. If the model only considers exactly one core damage, the extension method could be completed as described below; however, if nearly simultaneous core damage events were to be included, then the model developer would need to take special care to add in top events that include scenarios that lead to nearly simultaneous core damage. The first step in this process would be to identify initiating events that are not in the existing single-unit PRAs [75]. For example, some scenarios from one unit's Level 2 PRA may actually create an initiating event for another unit's Level 1 PRA. These new initiating events would have to be determined on a plant-by-plant basis. In many other cases, there may not be any new initiating events to identify. This would be true for the SSCs that are currently included in PRA models for nuclear power plants. Then, event trees would be developed for the new initiating events and extended for those initiating events that were in the single-unit PRAs [75]. For

example, for a LOOP initiating event, the top events may need to include failure of one unit's EDGs, failure of another unit's EDGs, and failure of both units' EDGs, rather than simply having one top event for EDG failure. By adding these top events, the PRA is then further modified to account for multi-unit dependencies. If necessary, fault trees would then be developed for the new top events of the event trees. Also, if needed, basic event probabilities would be evaluated. Finally, the model would be quantified [75].

A special case of extension methodologies that could be employed is one that is similar to those that are currently used to model and quantify external events. There are several external event methodologies that are used for nuclear power plants, and, depending on which of these external event methodologies is chosen, in addition to any other methodologies used in conjunction with them, the necessity of differentiating between exactly one core damage and nearly simultaneous core damage events will vary. For the most part, since event trees and fault trees are created, the model developer will need to ensure the inclusion of top events that could lead to nearly simultaneous core damage, if that is the goal of the evaluation.

The NRC's methodology for external events includes an initial evaluation, then a screening or bounding analysis, followed by a qualitative and then quantitative analysis. If necessary, a detailed analysis can be performed on the remaining events [76]. The initial evaluation involves a site walk down to identify any areas that may be susceptible to dependencies. During external event evaluations, this evaluation typically focuses on a single category of external events (e.g., seismic events, fire, and floods) that could affect a unit. The screening analysis involves a qualitative look at what events could realistically occur. For typical external event evaluations, an event frequency of 1×10^{-07}

per reactor year or lower is screened out from further evaluation [77, 78]. The qualitative analysis would then focus on the consequences of those events that have not been screened out. If the consequences were small, then those events could also be screened out. The events that remain would then be quantitatively analyzed to determine their effect on the site's risk profile. If a more detailed analysis still needed to be completed for some events, such as a fire propagation model, then this analysis could be completed for those specific events.

Another option would be the International Atomic Energy Agency's (IAEA) external event methodology, which has seven basic steps. The first two are to identify the external event and the postulated plant conditions. Then, scenarios and external event classifications are developed, followed by identification of design parameters and loading schemes. Next, safety SSCs are identified, and it is determined if their safety function is affected by the identified external events. If necessary, design modifications are made so that all safety-related SSCs are functional during external events [79].

For both fire and seismic events, there are special means to create traditional event tree-fault tree PRAs. These approaches could also be used for a multi-unit PRA. A two-part approach is typically used for a fire PRA. First, as with other external events, a screening analysis is done to identify important fire locations. In the second phase, those important fire locations are analyzed, usually with the combination of a traditional event tree-fault tree approach and more detailed fire propagation, damage, and suppression models [80, 81]. For a seismic PRA, the basic event probabilities for components are varied depending on their seismic fragilities [82]. For example, an event tree is created for a seismic event of a certain magnitude, and the basic event probabilities are updated to the

expected failure rate given that specific magnitude of earthquake. The same is then done for different magnitude seismic events. Then the event tree results are combined to illustrate the plant's seismic risk.

The Fire Induced Vulnerability Evaluation (FIVE) is similar to the fire PRA method with the goal of exposing fire vulnerabilities so that their risk can be reduced. FIVE looks at the propagation of the fire if barriers or penetration seals fail, and unlike the fire PRA method, typically gives full credit to areas that are in compliance with 10 CFR Appendix R [80].

The Seismic Margin Assessment (SMA) method is similar to a seismic PRA; however, the scope is limited. There are four basic steps to performing a SMA. First, a single earthquake magnitude is chosen to evaluate. The chosen level for currently operating reactors is typically at or below 0.3g peak ground acceleration, although as high as 0.5g has also been used in more recent SMAs. Then a walk down is performed to identify important SSCs, and those items identified are screened, just as in a seismic PRA. Finally, fragility of the items that have not been screened is evaluated. The screening process and further evaluation are only done for the chosen magnitude of earthquake, thus creating a bounding earthquake that the plant must be able to survive [83].

When using these methodologies to evaluate multi-unit dependencies, as with parametric and causal-based methods, a combination or hybrid of the external event methodologies could be used. For the FIVE and SMA models, this would need to take place, as their aim when used exclusively is not mean for PRA quantification. Alternatively, a single method could be chosen to evaluate the multi-unit dependencies.

Chapter 5 Applying Methodologies

5.1 Introduction

The four methodologies that have been presented in the previous section are not applicable to all of the classifications. Certain methodologies are more appropriate for certain classifications. Additionally, while some methods may be applicable, they realistically may not be possible because of either lack of data or availability of more developed techniques. This chapter will discuss the applicability and practicality of using the methodologies for each of the classifications.

5.2 Initiating Events

As discussed previously, there are two different subclasses of the initiating events classification: definite and conditional. The definite initiating events that will always affect multiple units would only need to use the combination methodology to be integrated into a multi-unit PRA. The extent that the definite initiating event affects multiple units will vary depending on the initiating event. Since the single-unit PRAs should contain all of the potential initiating events, they would simply need to be combined. For example, if the following cutsets were for a two-unit site where I_d represents the definite initiating event and I_1, I_2, and I_3 represent other initiating events:

Unit 1	**Unit 2**
$I_d abc$	$I_2 zyx$
$I_1 def$	$I_d swv$
$I_d ghi$	$I_3 ult$

And the CDF of each unit was as follows:

$$Q_{CDF1} = I_d abc + I_1 def + I_d ghi \qquad \text{Eq. 5.2.1}$$

$$Q_{CDF2} = I_2 zyx + I_d swv + I_3 ult \quad \text{Eq. 5.2.2}$$

Then the total CDF of exactly one core damage could be calculated as:

$$CDF_T = CDF_1 + CDF_2 \quad \text{Eq. 5.2.3}$$

$$Q_{CDFT} = I_1 def + I_2 zyx + I_3 ult + (I_d abc + I_d ghi + I_d swv) \quad \text{Eq. 5.2.4}$$

$$Q_{CDFT} = I_1 def + I_2 zyx + I_3 ult + I_d\,(abc + ghi + swv) \quad \text{Eq. 5.2.5}$$

$$CDF_T = A + B \quad \text{Eq. 5.2.6}$$

where A represents events not affected by the definite initiating event, B represents events affected by the definite initiating event, and

$$A = I_1 def + I_2 zyx + I_3 ult \quad \text{Eq. 5.2.7}$$

$$B = I_d(abc + ghi + swv) \quad \text{Eq. 5.2.8}$$

For conditional initiating events, two methodologies may be appropriate. One would be a parametric method, which would require creating a parameter or several parameters that represent the conditional probability of the initiating event affecting multiple units. As discussed previously, the metric of interest (exactly one core damage event or nearly simultaneous core damage) will change the implementation of a parametric model. For example, if A represents events not affected by the initiating event, B represents events that may be affected by the initiating event, then the CDFs for a two-unit site would be:

$$CDF_1 = A_1 + B_1 \quad \text{Eq. 5.2.9}$$

$$CDF_2 = A_2 + B_2 \quad \text{Eq. 5.2.10}$$

And if the probability of exactly one core damage was being calculated, then the site CDF would be:

$$CDF_T = CDF_{1+} CDF_2 \quad \text{Eq. 5.2.11}$$

$$CDF_T = A_1 + B_1 + A_2 + B_2 \quad \text{Eq. 5.2.12}$$

$$CDF_T = (A_1 + A_2) + \rho (B_1 + B_2) \quad \text{Eq. 5.2.13}$$

where ρ is a dimensionless parameter multiplier that accounts for the increased probability of B_1 and B_2 occurring together because of common initiating event.

If however, the nearly simultaneous core damage was being calculated for the same two-unit site, then the site CDF, from Equation 4.3.12, would be:

$$Q_{CDFT} = I_1 Pr(A_1)\, I_3 Pr(A_2) + I_1 Pr(A_1) I_2 [(1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] + I_3 Pr(A_2) I_2 [(1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))] + I_2^2 [(1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))]\, [(1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] \quad \text{Eq. 5.2.14}$$

where I represents the initiating event, C represents the existence of the conditional initiating event, and ρ is a constant that represents the probability of the conditional initiating event affecting multiple units.

The other option for conditional initiating events would be to use a causal methodology, which would map the root cause of the dependency that would possibly be created through that initiating event. For example, if the initiating event was loss of service water, then the loss could be mapped in a directed graph like the one in Figure 7.

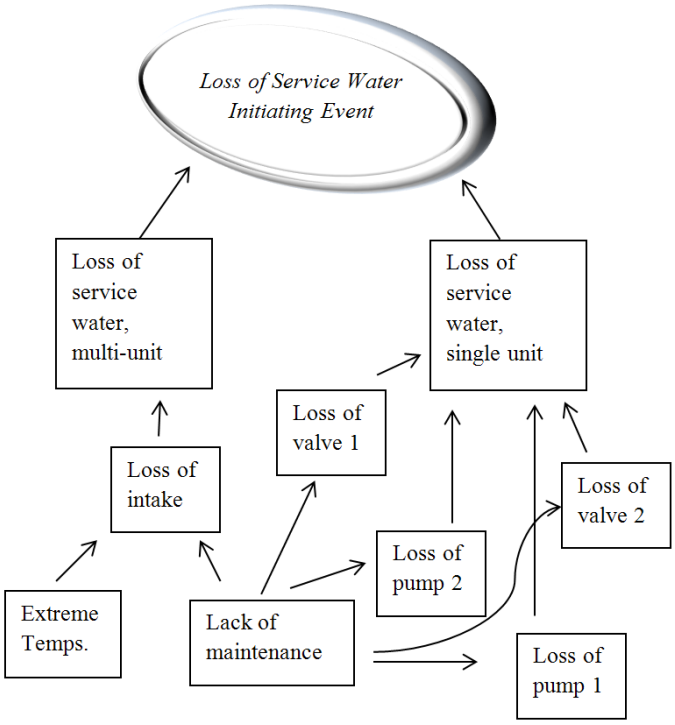

Figure 7: Loss of Service Water Causal Network

This causal network could be expanded as much as necessary. For example, the loss of pump one could be expanded using a physics-of-failure model or these nodes could simply be linked to existing fault trees.

Using a parametric method would be practicable as there are many established methods for using parametric methods in nuclear power plant PRAs; however, since some initiating events occur so infrequently, the dataset could be skewed. Furthermore, using a parametric method would require the user to data mine, as currently there are no established databases for how frequently events affect multiple units. Using a causal-based method would most likely require more effort than a parametric method, but there would be a lower likelihood of having biased results because the dataset should be more robust. In addition, the causal-based network could be simplified or expanded to

accommodate whatever data was available. Conversely, there are no well-established causal methods for nuclear power plants as there are for parametric methods.

5.3 Shared Connection

There are three different subclasses of the shared connection classification: single SSC, time sequential, and standby, as discussed previously. The single SSC dependencies would only need to use the combination methodology to be integrated into a multi-unit PRA. Since the single SSC should be modeled in all of the single-unit PRAs, they would simply need to be combined. For example, if the following cutsets for a two-unit site, where *b* was the shared component between the units, were:

Unit 1	**Unit 2**
$I_1 abc$	$I_4 zby$
$I_2 def$	$I_5 xwv$
$I_3 gbh$	$I_6 ubt$

And the CDF of each unit was as follows:

$$Q_{CDF1} = I_1\, abc + I_2\, def + I_3\, gbh \qquad \text{Eq. 5.3.1}$$

$$Q_{CDF2} = I_4\, zby + I_5\, xwv + I_6\, ubt \qquad \text{Eq. 5.3.2}$$

Then the total CDF for exactly one unit could be calculated as:

$$CDF_T = CDF_1 + CDF_2 \qquad \text{Eq. 5.3.3}$$

$$Q_{CDFT} = I_2\, def + I_5\, xwv + (I_1\, abc + I_3\, gbh + I_4\, zby + I_6\, ubt) \qquad \text{Eq. 5.3.4}$$

$$CDF_T = A + B \qquad \text{Eq. 5.3.5}$$

where A represents cutsets that do not contain the shared component and B represents cutsets with the shared component. For a shared system, rather than merging cutsets, the event trees would need to be combined in a similar fashion.

For time sequential sharing dependencies, three methodologies would be appropriate. One would be a parametric method, which would require creation of a parameter to represent the conditional probability that the SSC is available for each unit. As previously discussed, the metric of interest (exactly one core damage event or nearly simultaneous core damage) will change the implementation of a parametric model. For example, if A represents events that do not contain the shared components and B represents events that contain the shared components, then the CDFs for a two-unit site would be:

$$CDF_1 = A_1 + B_1 \qquad \text{Eq. 5.3.6}$$

$$CDF_2 = A_2 + B_2 \qquad \text{Eq. 5.3.7}$$

And if the probability of exactly one core damage was being calculated, then the site CDF would be:

$$CDF_T = CDF_{1+} CDF_2 \qquad \text{Eq. 5.3.8}$$

$$CDF_T = A_1 + B_1 + A_2 + B_2 \qquad \text{Eq. 5.3.9}$$

$$CDF_T = (A_1 + A_2) + \rho\,(B_1 + B_2) \qquad \text{Eq. 5.3.10}$$

where ρ is a dimensionless parameter multiplier that accounts for the increased probability of B_1 and B_2 occurring together because of shared components.

If, however, the nearly simultaneous core damage was being calculated for the same two-unit site, then the site CDF, from Equation 4.3.12, would be:

$$Q_{CDFT} = I_1 Pr(A_1)\, I_3 Pr(A_2) + I_1 Pr(A_1) I_4 [(1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] + I_3 Pr(A_2) I_2 [(1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))] + I_2 [(1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))]\, I_4 [(1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] \quad \text{Eq. 5.3.11}$$

where I represents the initiating event, C represents the existence of the shared components, and ρ is a constant that represents the probability of the shared components affecting multiple units.

If an entire system was shared, then a house event would need to be created in the PRA to reflect the conditional probability of the system being available. This house event would change the basic event probabilities of the components in the shared system using a developed parameter.

Use of a causal methodology would map the root cause of events that could cause the SSC to become unavailable simultaneously. This causal network could be very simple, as in Figure 8, or it could map all failure modes down to the failure mechanism, such as fatigue or wear. In the figure, a two-unit site is represented that has a dedicated EDG for each unit and a swing EDG that can service either unit. The accuracy of using such a model would be proportional to the detail of the model created, if appropriate intermediate modeling assumptions are made.

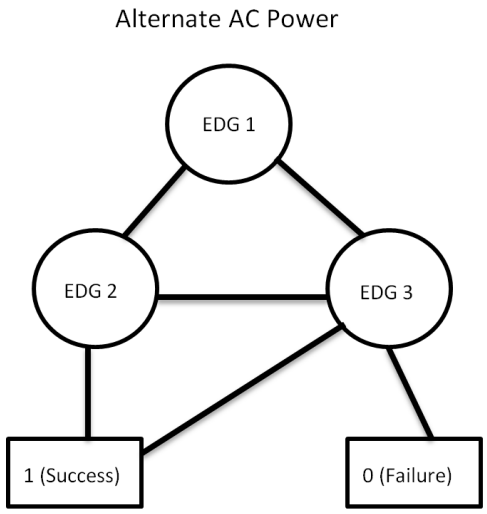

Figure 8: EDG Binary Decision Diagram

The third option would be to incorporate the SSC into existing event trees, which would require the assumption of a dominant unit. For example, to account for the dependencies between a two-unit site that has two main EDGs and a swing diesel, it could be represented as:

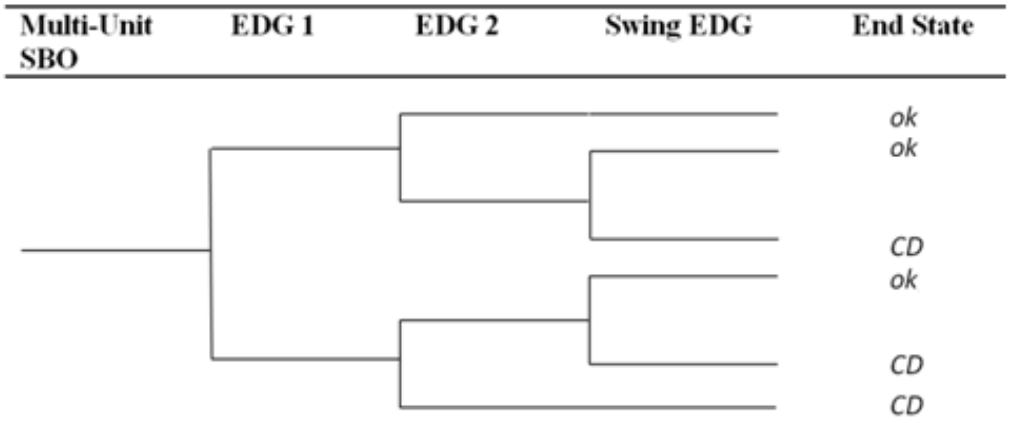

Figure 9: EDG Event Tree

where "CD" is core damage on at least one unit, and "ok" indicates both units have successful use of the diesels. This same approach could be used whether it was a component, structure, or system that was shared.

Depending on the SSC, the parametric data could overemphasize certain failure mechanisms, but there should be enough data available for active components. However, a parametric approach makes it difficult to truly account for the time-sensitive nature of these types of shared systems. Using a causal methodology would likely require the most effort, and depending on the SSC, there could be a lack of data in order to form a causal network. It would be important to use a dynamic causal network that could account for the time-sequential sharing aspect. The detail of the chosen causal method, as outlined previously, would determine the model accuracy. Incorporation into the existing PRA would require the least amount of effort; however, the accuracy would be compromised, since the assumption would have to be made that one unit would be the primary unit. Additionally, latent errors in the single-unit PRAs could be carried into the multi-unit PRA.

For standby systems, two methodologies would be appropriate: causal modeling and incorporation into existing event trees. Using a causal methodology would simply map which events could cause the SSC to become unavailable simultaneously, just as in the time-sequential sharing. It would not, however, be important to have a dynamic causal network because the timing of the event would not greatly influence the availability of the system. Also, just as in time-sequentially shared SSCs, shared standby systems could be incorporated into the existing event trees. If one of the standby systems was incorporated into existing event trees, again, one unit would have to be assumed to be the primary unit [6]. Using a causal methodology could prove difficult, depending on the SSC and the degree of detail used. Whereas, incorporation into existing fault trees would

not require much effort, but the accuracy of the PRA may be compromised, just as in the time-sequential sharing.

5.4 Identical Component

For the identical component class, two methodologies could be used to model this dependency. Parametric modeling is one option and would likely be an extension of the current common cause failure model used for the single-unit PRAs. As discussed previously, the metric of interest (exactly one core damage event or nearly simultaneous core damage) will change the implementation of a parametric model. For example, if A represents events that do not contain an identical component and B represents events that contain an identical component, then the CDFs for a two-unit site would be:

$$CDF_1 = A_1 + B_1 \qquad \text{Eq. 5.4.1}$$

$$CDF_2 = A_2 + B_2 \qquad \text{Eq. 5.4.2}$$

And if the probability of exactly one core damage was being calculated, then the site CDF would be:

$$CDF_T = CDF_{1+}\, CDF_2 \qquad \text{Eq. 5.4.3}$$

$$CDF_T = A_1 + B_1 + A_2 + B_2 \qquad \text{Eq. 5.4.4}$$

$$CDF_T = (A_1 + A_2) + \rho\,(B_1 + B_2) \qquad \text{Eq. 5.4.5}$$

where ρ is a dimensionless parameter multiplier that accounts for the increased probability of B_1 and B_2 occurring together because of identical components.

If, however, the nearly simultaneous core damage was being calculated for the same two-unit site, then the site CDF, from Equation 4.3.12, would be:

$$Q_{CDFT} = I_1 Pr(A_1)\, I_3 Pr(A_2) + I_1 Pr(A_1) I_4[(1-\rho)Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] + I_3 Pr(A_2) I_2[(1-\rho)Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))] + I_2[(1-\rho)Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))]\, I_4[(1-\rho)Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] \quad \text{Eq. 5.4.6}$$

where I represents the initiating event, C represents the existence of the identical components, and ρ is a constant that represents the probability of the identical component commonality affecting multiple units.

Using a causal methodology would model the physics-of-failure of the component [69]. For example, if the same type of compressor was used on both units, a causal network like the one in Figure 10 could be used for all compressors at the plant. The equations at the bottom of the figure show the actual physics of the failure of the compressor.

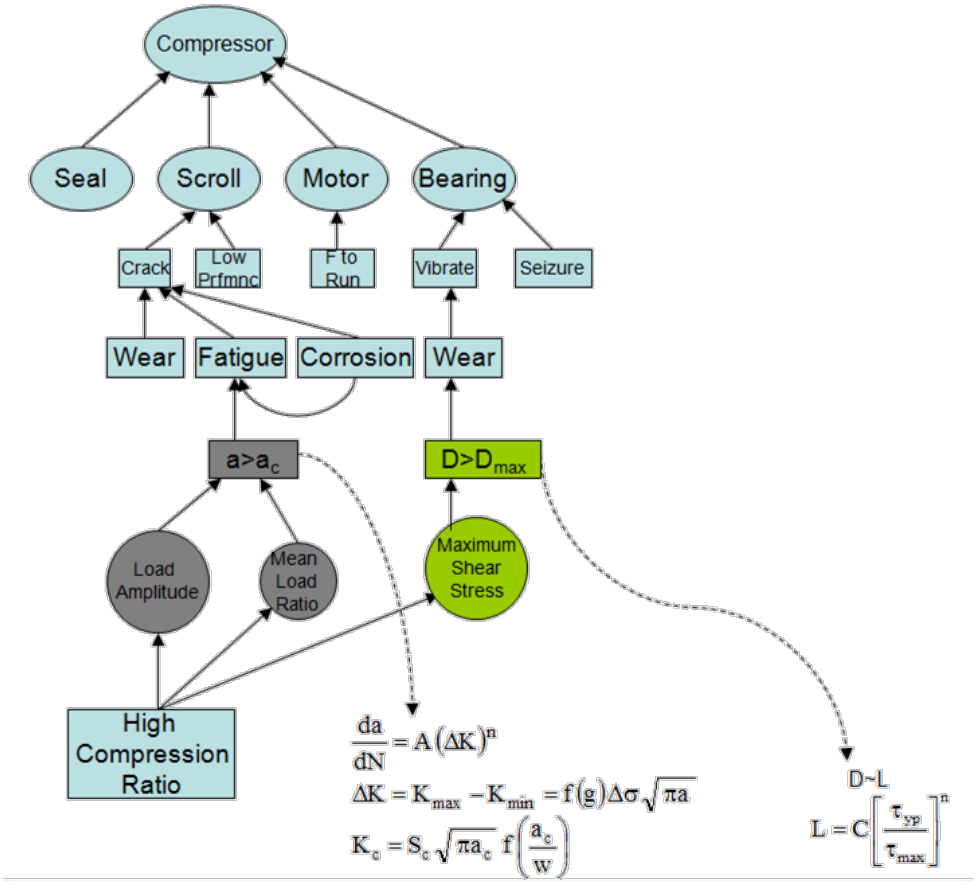

Figure 10: Compressor BBN (based on original figure by M. Modarres, 3 May 2010)

Using a parametric method would almost certainly be more consistent with the rest of the PRA and require the least amount of effort; however, it could also perpetuate any existing problems in the single-unit PRAs. Additionally, for larger component groups current parametric methods may not be sufficient. In these cases, new parameters would need to be developed to accurately account for common cause failure. Using a causal-based method would require more effort, but for most components, there should be enough data to map the physical failure of the component.

5.5 Proximity Dependency

For the proximity class, one methodology could be used. This would be to extend the single-unit external events PRA. This method would only be viable if every unit onsite had an external event PRA. For example, if a fire PRA had already been completed for each unit, then the fire zones that had been identified could be reconsidered for a multi-unit affect. The same thing could be done for seismic events and other external events. The focus would simply shift from the effect of these events on a single unit to the effect on multiple units.

This extension could also occur by using one of the external event models presented in Section 4.5. A single model or a combination of these models could be developed to accurately reflect a site's risk profile. For example, if a site had a high frequency of tornadoes, then the proximity dependencies analysis could be more focused on the effect of high wind events.

Extending the current external events PRA may not capture all of the dependencies because of the state of the existing PRA. Using a methodology similar to existing

external event methodologies would require a more in-depth analysis; however, it would allow the analysis to be done while the entire site was considered, rather than just one unit, and would not contain any previous bias that may have occurred during the single-unit external events analysis.

5.6 Human Dependency

As previously discussed, the human dependency class has two subclasses: pre-initiating event and post-initiating event. For the pre-initiating event subclass, two methodologies would be appropriate. A parametric methodology would require creation of a parameter or several parameters that represent the conditional probability of a human error occurring given the occurrence of another event. As discussed previously, the metric of interest (exactly one core damage event or nearly simultaneous core damage) will change the implementation of a parametric model. For example, if A represents events that do not contain the human action and B represents events that contain the human action, and the CDFs for a two-unit site are:

$$CDF_1 = A_1 + B_1 \qquad \text{Eq. 5.6.1}$$

$$CDF_2 = A_2 + B_2 \qquad \text{Eq. 5.6.2}$$

Then, if the probability of exactly one core damage was being calculated, the site CDF would be:

$$CDF_T = CDF_{1+} CDF_2 \qquad \text{Eq. 5.6.3}$$

$$CDF_T = A_1 + B_1 + A_2 + B_2 \qquad \text{Eq. 5.6.4}$$

$$CDF_T = (A_1 + A_2) + \rho\,(B_1 + B_2) \qquad \text{Eq. 5.6.5}$$

where ρ is a dimensionless parameter multiplier that accounts for the increased probability of B_1 and B_2 occurring together because of the human action.

If, however, the nearly simultaneous core damage was being calculated for the same two-unit site, then the site CDF, from Equation 4.3.12, would be:

$$Q_{CDFT} = I_1 Pr(A_1)\, I_3 Pr(A_2) + I_1 Pr(A_1) I_4 [(1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] + I_3 Pr(A_2) I_2 [(1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))] + I_2 [(1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid C) - Pr(B_1))]\, I_4 [(1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid C) - Pr(B_2))] \quad \text{Eq. 5.6.6}$$

where I represents the initiating event, C represents the existence of the human action, and ρ is a constant that represents the probability of the human action affecting multiple units.

A causal methodology would simply map the root cause of the human failure. For example, physical factors, memorized information, and mental states could be considered, as seen in Figure 11 [84]. This figure considers internal and external performance influencing factors (PIFs) and operator behavior (by looking at information, decision, and action). If causal modeling was used, there would be no reason to separate pre-initiating event and post-initiating event human actions; however, the delineation would be necessary for a parametric methodology, as the conditional probabilities would be very different.

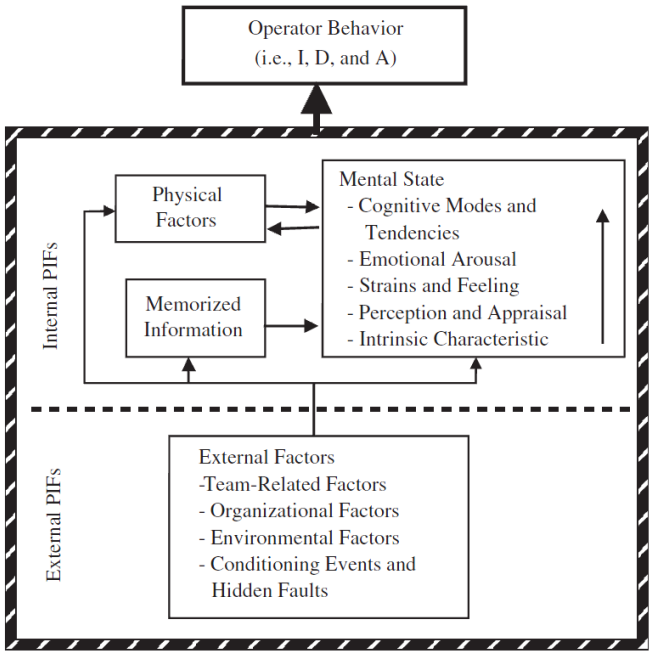

Figure 11: Factors that Affect Human Performance [84]

For the post-initiating event subclass, there are also two methodologies that would be appropriate. The first, a parametric methodology, would require creation of a parameter that represents the conditional probability of a human event occurring given that an initiating event had occurred and a human failure event had also occurred. Again, the metric of interest (exactly one core damage event or nearly simultaneous core damage) will change the implementation of a parametric model. For example, if A are events not affected by the initiating event, B are events that are affected by the initiating event but not the human action, C are events that are affected by the initiating event and the human action, and the following CDFs for a two-unit site were:

$$CDF_1 = A_1 + B_1 + C_1 \qquad \text{Eq. 5.6.7}$$

$$CDF_2 = A_2 + B_2 + C_2 \qquad \text{Eq. 5.6.8}$$

And if the probability of exactly one core damage was being calculated, then the site CDF would be:

$$CDF_T = CDF_{1+}\, CDF_2 \qquad \text{Eq. 5.6.9}$$

$$CDF_T = A_1 + B_1 + C_1 + A_2 + B_2 + C_2 \qquad \text{Eq. 5.6.10}$$

$$CDF_T = (A_1 + A_2) + \rho\,(B_1 + B_2) + \tau\,(C_1 + C_2) \qquad \text{Eq. 5.6.11}$$

where ρ is a dimensionless parameter multiplier that accounts for the increased probability of B_1 and B_2 occurring together because of common initiating event and τ is a dimensionless parameter multiplier that accounts for the increased probability of C_1 and C_2 occurring together because of both the human action and the initiating event.

If, however, the nearly simultaneous core damage was being calculated for the same two-unit site, then the site CDF, using the same logic as was used in Equations 4.3.6-12, would be:

$$\begin{aligned} Q_{CDFT} = {} & I_1 Pr(A_1)\, I_3 Pr(A_2) + I_1 Pr(A_1) I_2[(1-\rho) Pr(B_2) + \\ & \rho(Pr(B_2 \mid D) - Pr(B_2))] + I_1 Pr(A_1) I_2[(1-\tau) Pr(C_2) + \tau(Pr(C_2 \mid E) - Pr(C_2))] \\ & + I_3 Pr(A_2) I_2[(1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid D) - Pr(B_1))] + \\ & I_3 Pr(A_2) I_2[(1-\tau) Pr(C_1) + \tau(Pr(C_1 \mid E) - Pr(C_1))] + I_2^2[(1-\rho)(Pr(B_1) + \\ & \rho(Pr(B_1 \mid D) - Pr(B_1)))((1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid D) - Pr(B_2))) + \\ & ((1-\rho) Pr(B_1) + \rho(Pr(B_1 \mid D) - Pr(B_1)))((1-\tau) Pr(C_2) + \\ & \tau(Pr(C_2 \mid E) - Pr(C_2))) + ((1-\tau) Pr(C_1) + \\ & \tau(Pr(C_1 \mid E) - Pr(C_1)))((1-\rho) Pr(B_2) + \rho(Pr(B_2 \mid D) - Pr(B_2))) + \\ & ((1-\tau) Pr(C_1) + \tau(Pr(C_1 \mid E) - Pr(C_1)))\, ((1-\tau) Pr(C_2) + \\ & \tau(Pr(C_2 \mid E) - Pr(C_2)))] \end{aligned} \qquad \text{Eq. 5.6.12}$$

where I is the initiating event, D is the existence of the initiating event, E is the concurrent existence of the initiating event and the human action, ρ is a constant that represents the probability of the initiating event affecting multiple units, and τ is a constant that represents the probability of the initiating event and the human action affecting multiple units.

The second option would be a causal methodology that would simply map the root cause of the human error. This approach, as discussed previously, would not be any different than the causal method chosen for the pre-initiating event subclass.

For either the pre-initiating event or the post-initiating event subclass, the use of a parametric model would be extremely difficult as there is virtually no assimilated data for the effect of human actions at a nuclear power plant. A causal-based method would require a significant amount of effort as the root cause of a human action would need to be determined; nonetheless, there are codes that have been developed for this purpose [84]. However, the evaluation of past events could be challenging. For example, there would have to be an evaluation as to whether the incorrect valve installation was because the maintenance team did not think safety was important, because they were not paying attention to the task, or because they were simply not qualified to perform the installation. For the causal-based method, it would also be necessary to use expert judgment to quantify the network.

5.7 Organizational Dependency

For the organizational classification, two different methodologies could be used. One would be to create a traditional PRA model of organizational factors and incorporate organizational factors into the existing single-unit fault trees. If this methodology was chosen, it would also be appropriate to use a parametric methodology to represent the conditional probability of an event given that an organizational failure has occurred.

The second methodology would be to create a causal model of organizational factors. This method would map the organizational failures to potential equipment or human

failures. For example, the safety culture and organizational culture would be considered to map the different relationships as seen in Figure 12 [63].

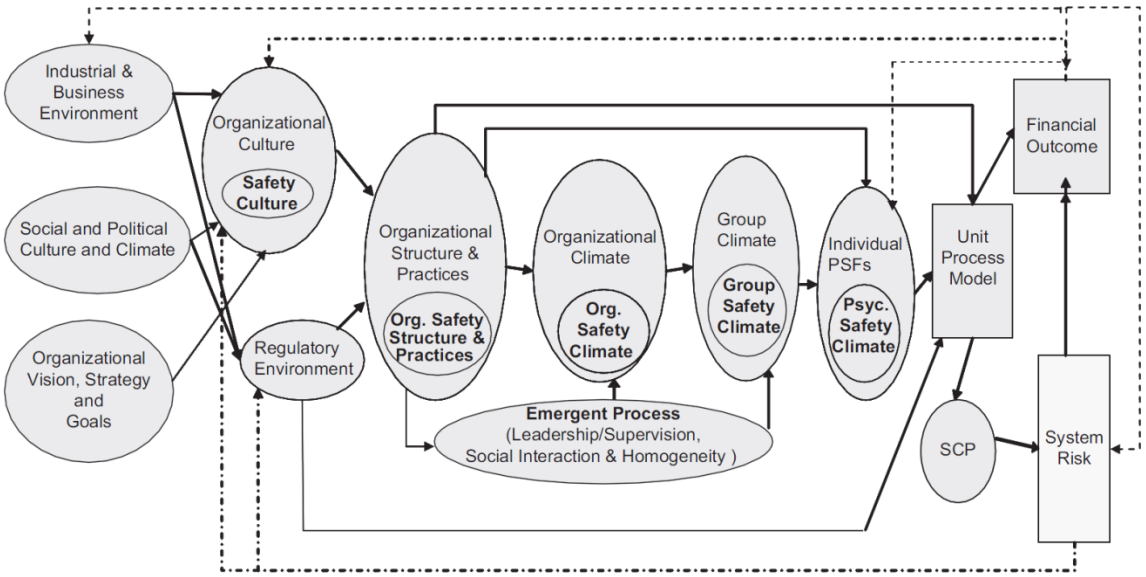

Figure 12: Factors that Affect Organizational Performance [63]

A parametric method would be extremely difficult to quantify, as there is no data currently collected at nuclear power plants to identify organizational failures. Given the integral nature of organizational factors, using a causal model would be the preferred and most complete methodology. There are methods, such as SoTeRiA, that could be used [63]. However, no matter what method is chosen, it will be difficult to quantify the factors and relationships that affect organizational performance as it is an extremely complex and often subjective issue.

Chapter 6 Conclusions and Recommendations

6.1 Conclusions

Currently, multi-unit nuclear power plant PRAs consider the risk from each unit separately and do not consider combination events between the units. To gain an accurate view of the site's risk profile, the CDF for the site rather than the unit must be considered. This thesis has presented a classification system that utilizes existing single-unit PRAs and combines them into a multi-unit PRA. Six main commonality classes that can cause multiple units to be dependent have been presented: initiating events, shared connections, identical components, proximity dependencies, human dependencies, and organizational dependencies. A seventh class, independent events, was only marginally discussed because it does not address dependencies between the units.

This thesis has also discussed multi-unit events that have occurred at U.S. nuclear power plants and the potential consequences of those events. It was found that nine percent of reportable events an eleven-year period affected multiple units. Furthermore, two percent of those that affected multiple units were safety significant. Additionally, it was found that multi-site issues have occurred in the United States.

Four methodologies were examined that could quantify classifications: combination, parametric, causal-based, and extension methods. The applicability and practicality of using the methods for each classification was also discussed. A summary of the applicability of the methods for each classification can be seen in Table 7. As discussed in Chapter 5, these methodologies are not unconditionally applicable. For example, for human dependencies, in order for a parametric model to be used, data would have to be gathered about the effects of human actions at a nuclear power plant.

Table 7: Applicability of Methodologies for Each Classification

Classification and Subclasses	*Applicable Methodology*
Initiating Event	
Definite	Combination
Conditional	Parametric or causal
Shared Connection	
Single	Combination
Time Sequential	Parametric, causal, or extension
Standby	Causal or extension
Identical component	Parametric or causal
Proximity	Extension
Human	
Pre-initiating event	Parametric or causal
Post-initiating event	Parametric or causal
Organizational	Extension or causal

6.2 Recommendations

Future areas of research could include analyzing each methodology for each of the proposed classifications, as seen in Table 7, to determine the most appropriate technique, technical impediments, as well as the need for any expansions. Additionally, a feasibility study could be done to combine existing single-unit PRAs using the current state-of-practice methods. This could also be done for nontraditional reactor technologies such as small modular reactors and advanced reactor technologies.

Before a feasibility study could be done, the dependencies of each component of the plant would need to be identified in some sort of dependency matrix. This is already typically done for single-unit PRAs; traditionally, only hard physical connections were included, such as a motor-operated valve needing to have power from a predefined source. These matrices allow the PRA model developer to know what to consider when creating the PRA. This same thing would need to be done for proximity, human, and organizational dependencies. For proximity dependencies, room location, nearby doors and conduits,

and the location with respect to other units onsite would need to be noted. For human dependencies, the operator or the maintenance team member responsible for the action, as well as whether the action occurs before or after the event would need to be noted. For organizational dependencies, the department responsible for the system, the procedures used when operating the component, and the training that is given on the SSCs would need to be noted.

Furthermore, as discussed in Chapter 5, some of the methodologies require a larger body of knowledge, as well as more advanced techniques, before they are feasible for use in nuclear power plant PRAs. Additionally, if the classification proposed in this thesis was extended to a Level 3 PRA or used for severe accident management, consideration would need to be given to sites with different reactor types, as the severe accident progression would vary for each unit.

Appendix 1

Table 8: Summary of Multi-Unit LER Classifications

LER Number	Classification	Subclass	Summary
2772001001	Human	Post-Initiator	After an electrical transient, the operators did not correctly close breakers which resulted in a condition in which two out of four emergency buses per unit would not have automatically received power from their respective EDGs in the event of a LOOP.
2372011001	Human	Pre-Initiator	Stop logs were installed on both sides of a bay rendering the containment cooling service water inoperable for two units.
2662000002	Human	Pre-Initiator	Surveillances were missed for emergency core cooling system valves on two units.
3212000001	Human	Pre-Initiator	Water level sensors in the suppression pool were installed incorrectly on two units.
3272009007	Human	Pre-Initiator	A technical specification required action was missed for two units.
3612003001	Human	Pre-Initiator	Technician performing work on Unit 3 misidentified a reference terminal and made a connection to a relay for Unit 2, which caused a reactor trip at Unit 2. Unit 3 was defueled.
3612007003	Human	Pre-Initiator	Flow meters for ultimate heat sink were not calibrated correctly causing incorrect adjustments on two units.
3872002005	Human	Pre-Initiator	Two consecutive maintenance mechanics filled a dry shielded canister with argon gas rather than helium gas. This event could have had adverse effects on stored spent fuel.

LER Number	Classification	Subclass	Summary
4132006003	Human	Pre-Initiator	Igniter glow plug coils were installed incorrectly on two units.
4242007001	Human	Pre-Initiator	Top-mounted auxiliary contact blocks were not installed correctly on two units.
4542005001	Human	Pre-Initiator	Employee falsified surveillance procedures on two units.
5282003004	Human	Pre-Initiator	Control switch contact blocks were incorrectly installed on three units.
2492004006	Identical Component		The shafts of the main turbine generators, which are nearly identical, were found to be cracked on two units.
2502005004	Identical Component		The same inadequate fuse type was installed on two units' emergency containment filter fan.
2652005002	Identical Component		Main steam line electromatic relief valve actuators were damaged because of vibrations on two units.
2692010001	Identical Component		A valve that released foreign material was installed on two units.
2692011004	Identical Component		A specific type of particulate radiation monitor was found to be inadequate, which resulted in three units violating technical specifications.
2752008001	Identical Component		It was found that similar solenoid valves could malfunction on two units because of valve aging.
2772000002	Identical Component		The air coolant and jacket coolant heat exchangers for emergency diesel generators for two units were found to be inadequate.

LER Number	Classification	Subclass	Summary
2802010002	Identical Component		Aluminum conduit seal penetrations that were used on two units were found to be inadequate.
2822000001	Identical Component		Steam exclusion dampers were found to have a potential for failure on two units.
2822001005	Identical Component		The same breaker type, which is susceptible to poor electrical connection, was operated on two units.
2822010004	Identical Component		The same battery chargers, which have the potential to stop providing output, were used on two units.
3062006002	Identical Component		Neutron flux monitor channels were spliced incorrectly on two units.
3162003004	Identical Component		The weight of the ice baskets was found to be below the requirements of the technical specifications on two units.
3172002004	Identical Component		Loose cable connectors on two units' post-accident monitoring systems could have prevented them from fulfilling their safety function.
3212006003	Identical Component		The same valve was used on two units and caused both units to be in violation of technical specifications.
3232002001	Identical Component		Bonnet fasteners used for atmospheric steam dump valves that were susceptible to stress corrosion cracking, were used for two units.
3232003007	Identical Component		Battery chargers for two units were installed with a control circuit design deficiency.

LER Number	Classification	Subclass	Summary
3232005001	Identical Component		The same pressurizer safety valves were used on two units and have a history of random spread lift.
3252005006	Identical Component		The same inappropriate setpoint was used for two units' emergency diesel generators differential overcurrent protective devices.
3252008003	Identical Component		It was found that the design of two identical reactor-building cranes was inadequate.
3252010004	Identical Component		Two units' emergency diesel generators had collector rings that were subject to corrosion.
3382010001	Identical Component		Aluminum conduit seal penetrations were found to be inadequate on two units.
3482001002	Identical Component		Large penetration fire seals that were used on two units were found to be inadequate.
3612002001	Identical Component		Certain relays were found to be susceptible to aging-related failure on two units.
3612006003	Identical Component		The same inadequate electrical logic was used for two units' emergency diesel generators.
3612010004	Identical Component		Emergency diesel generator room emergency fan nose cones were subject to the same corrosive environment on two units.
3622002002	Identical Component		A faulty breaker was installed on two units.
3622006002	Identical Component		An inadequate gasket design was used on two units.

LER Number	Classification	Subclass	Summary
3622007004	Identical Component		A contaminated batch (moisture contamination) of hydraulic dump valves was installed on two units.
3692005001	Identical Component		Containment atmosphere particulate radioactivity monitors were incorrectly operated for two units.
3692006001	Identical Component		Ice condenser floor cooling valves for two units were operated incorrectly.
3692011002	Identical Component		Valves on two units were being operated incorrectly.
3742002002	Identical Component		The same type of potentiometer, which was not designed adequately, was used on two units' emergency diesel generators.
3872002002	Identical Component		The same inadequate valve was used on two units' main steam isolation valves.
3872003007	Identical Component		The oil used for maintaining the core spray pumps was changed for two units. This change, because of the interaction with the old oil, caused foaming in the pumps.
4132007001	Identical Component		Certain associated circuits, which are used, were found to be inadequate on two units.
4132007002	Identical Component		The same inadequate submarine hatch design was used for two units.
4242006002	Identical Component		Problems were identified with a specific transmitter type that was used on two units.
4462001001	Identical Component		Problems were identified with a light socket that was used on two units.
4552005001	Identical Component		Software that is common to two units was found to have a logic fault.

LER Number	Classification	Subclass	Summary
5282001003	Identical Component		Control element assemblies with similar design and operation were found to have cracks on three units.
2662000010	Initiating Event	Conditional	Divers working on Unit 2 piping became unresponsive, so Unit 1 was tripped due to concern for diver safety.
2752007001	Initiating Event	Conditional	A loss of offsite startup power caused two units' emergency diesel generators to start.
2962005003	Initiating Event	Conditional	An electrical disturbance caused two units to have a reduction in power.
3242003004	Initiating Event	Conditional	A turbine trip on Unit 2 caused an electrical transient, which affected some Unit 1 systems.
3252006007	Initiating Event	Conditional	An electrical disturbance caused two units' emergency diesel generators to start.
3382009004	Initiating Event	Conditional	A human-induced loss of offsite power caused two units to trip.
3612001002	Initiating Event	Conditional	An electrical disturbance caused two units to trip.
3612008002	Initiating Event	Conditional	An electrical disturbance caused two units to trip.
3612008003	Initiating Event	Conditional	An electrical disturbance caused two units to trip.
3732001001	Initiating Event	Conditional	An electrical disturbance caused two units to have a reduction in power.
3872002006	Initiating Event	Conditional	A fire caused a partial loss of offsite power, which affected two units.
4132007003	Initiating Event	Conditional	An electrical disturbance caused two units' emergency diesel generators to start.
4452003003	Initiating Event	Conditional	An electrical disturbance caused two units to trip.

LER Number	Classification	Subclass	Summary
4982003001	Initiating Event	Conditional	An electrical disturbance caused two units to trip.
5292004003	Initiating Event	Conditional	An electrical disturbance caused two units' emergency diesel generators to start.
2372005003	Initiating Event	Definite	A loss of offsite power caused two units to enter a limiting condition of operation.
2592011001	Initiating Event	Definite	Severe weather caused a loss of offsite power event, which caused three units to trip.
2692007001	Initiating Event	Definite	An electrical disturbance at a switching station caused an electrical disturbance, which caused two units to trip.
2752001001	Initiating Event	Definite	An external fire caused an electrical disturbance, which caused emergency diesel generators to start at two units.
2752011003	Initiating Event	Definite	A tsunami warning caused temporary relocation of plant personnel at two units.
2772003004	Initiating Event	Definite	An offsite electrical grid disturbance caused two units to trip.
2802003004	Initiating Event	Definite	A hurricane caused an electrical disturbance, which caused two units to trip.
2962004002	Initiating Event	Definite	A lightning strike on the grid caused an electrical disturbance, which caused speed perturbations on two units' main turbines.
3252000001	Initiating Event	Definite	A human-induced loss of offsite power caused two units' emergency diesel generators to start.
3382011003	Initiating Event	Definite	A seismic event, which led to a loss of offsite power event, caused two units to trip.

LER Number	Classification	Subclass	Summary
4132006001	Initiating Event	Definite	A loss of offsite power caused two units to trip.
5282004006	Initiating Event	Definite	A loss of offsite power caused three units to trip.
2372005001	Organizational		A symmetrical design deficiency was found on two units.
2372009007	Organizational		A symmetrical design deficiency was found on two units.
2502000002	Organizational		Symmetrical procedures used on two units were found to cause both units to be in violation of technical specifications.
2502000003	Organizational		A symmetrical design deficiency was found on two units.
2502006008	Organizational		A test methodology that was used for two units was found to be inadequate.
2502010001	Organizational		A symmetrical design deficiency was found on two units.
2542005001	Organizational		A symmetrical design deficiency was found on two units.
2592011010	Organizational		A symmetrical design deficiency was found on two units.
2602000002	Organizational		A vendor-supplied analysis that was used to develop procedures on two units was found to be incorrect.
2602002003	Organizational		A vendor-supplied analysis that was used for algorithms on two units was found to be incorrect.
2602003004	Organizational		A design deficiency that affected two units was found.
2652001002	Organizational		A design deficiency that affected two units was found.

LER Number	Classification	Subclass	Summary
2662000005	Organizational		An analysis used for two units' procedures was found to be inadequate.
2662000008	Organizational		Symmetrical procedures that were used for two units were found to be inadequate.
2662001001	Organizational		Symmetrical procedures used on two units were found to be deficient.
2662001003	Organizational		An unanalyzed condition was found by which the internal pressure may exceed the design pressure of containment for two units.
2662003001	Organizational		Symmetrical procedures used on two units were found to be incorrect.
2662005001	Organizational		The fire organization plan used for two units was found to be inadequate.
2662005002	Organizational		The fire organization plan used for two units was found to be inadequate.
2662005003	Organizational		A vendor-supplied calculation that was used for setpoints for two units was found to be incorrect.
2662005004	Organizational		Symmetrical procedures used on two units were found to be deficient.
2662005005	Organizational		Calculations used for two units’ electrical distribution systems were found to be incorrect.
2662005006	Organizational		A calculation that was used to demonstrate regulatory compliance for two units was found to be incorrect.
2662005007	Organizational		Symmetrical procedures used on two units were found to be deficient.
2662007008	Organizational		A calculation that was used for setpoints on two units was found to be incorrect.

LER Number	Classification	Subclass	Summary
2662010003	Organizational		Symmetrical procedures used on two units were found to be inadequate.
2692000004	Organizational		Symmetrical technical specifications for three units were found to be inadequate.
2692000005	Organizational		Symmetrical procedures used on two units were found to be deficient.
2692001001	Organizational		An analysis, which was used in technical specifications for three units, was found to be inaccurate.
2692002001	Organizational		A symmetrical design deficiency was found on three units.
2692006002	Organizational		Drawings and field walk downs that were used for safety function analysis for three units, were found to be inaccurate.
2692011006	Organizational		A symmetrical design deficiency was found on two units.
2702011001	Organizational		A vendor-supplied calculation that was used for two units was found to be incorrect.
2722000004	Organizational		An engineering evaluation that was used for two units was found to be incorrect.
2722002001	Organizational		A vendor-supplied calculation that was used for setpoints for two units was found to be incorrect.
2722005001	Organizational		Symmetrical procedures used on two units were found to be defective.
2752000006	Organizational		Symmetrical procedures used on two units were found to be deficient.
2752002001	Organizational		A vendor-supplied calculation that was used for setpoints for two units was found to be incorrect.

LER Number	Classification	Subclass	Summary
2752010003	Organizational		An inadequate understanding of the design of two units' offsite power systems caused both units to be in violation of technical specifications.
2752010004	Organizational		Symmetrical procedures used on two units were found to be defective.
2752011002	Organizational		A symmetrical design deficiency was found on two units.
2772005002	Organizational		Analyses of interim configurations for three units were found to be insufficient.
2772010004	Organizational		An operational assumption that was used for two units was found to be inadequate.
2772011002	Organizational		A symmetrical design deficiency was found on two units.
2802003006	Organizational		A symmetrical analysis that was used for two units was found to be insufficient.
2822000002	Organizational		Vendor-supplied fuel for two units was found to have higher fuel pellet densities than assumed in the spent fuel pool criticality analysis.
2822001001	Organizational		Symmetrical procedures used on two units were found to be deficient.
2822003002	Organizational		A fire analysis that was used for two units was found to be inadequate.
2822007002	Organizational		A fire analysis that was used for two units was found to be inadequate.
2822007003	Organizational		A fire analysis that was used for two units was found to be inadequate.
2822009004	Organizational		An analysis used for two units' residual heat removal system was found to be inadequate.

LER Number	Classification	Subclass	Summary
2822009006	Organizational		A high-energy line break analysis that was used for two units was found to be incorrect.
3152000002	Organizational		A symmetrical design deficiency was found on two units.
3152000003	Organizational		A symmetrical design deficiency was found on two units.
3152000006	Organizational		A misinterpretation of technical specifications for two units' emergency diesel fuel oil system caused both units to be in violation of technical specifications.
3152001002	Organizational		Symmetrical procedures used on two units were found to be deficient.
3152005002	Organizational		An inadequate understanding of technical specifications for two units' emergency diesel generators caused both units to be in violation of technical specifications.
3152008003	Organizational		An inadequate understanding of technical specifications for two units' essential service water system caused both units to be in violation of technical specifications.
3162002002	Organizational		Symmetrical procedures used on two units were found to be deficient.
3172000003	Organizational		Symmetrical procedures used on two units were found to be deficient.
3172002002	Organizational		Symmetrical procedures used on two units were found to be deficient.
3172005003	Organizational		A vendor-supplied power calculation that was used for two units was found to be incorrect.

LER Number	Classification	Subclass	Summary
3172006003	Organizational		A high-energy line break analysis that was used for two units' procedures was found to be incorrect.
3182008001	Organizational		A vendor-supplied calculation that was used for setpoints for two units was found to be incorrect.
3212001003	Organizational		A vendor-supplied analysis, which was used for setpoints for two units, was found to be incorrect.
3212002003	Organizational		A vendor-supplied calculation that was used for setpoints for two units was found to be incorrect.
3212006001	Organizational		Symmetrical procedures used on two units were found to be deficient.
3252003002	Organizational		A vendor-supplied calculation that was used for two units was found to be incorrect.
3252005001	Organizational		A software parameter change that was completed on two units was found to be incorrect.
3252006006	Organizational		Inadequate understanding of the design of two units led to both units' technical specifications to be non-conservative.
3272002001	Organizational		A vendor-supplied calculation that was used for setpoints for two units was found to be incorrect.
3272006001	Organizational		The same logical error was applied to two units' fire analysis, which could have caused damage to reactor coolant pumps in certain postulated fires.

LER Number	Classification	Subclass	Summary
3342000001	Organizational		Operator guidance for two unit's supplemental leak collection and release system was found to be deficient.
3352000001	Organizational		The original design of two units did not comply with regulatory requirements for fire protection.
3352000003	Organizational		A misunderstanding of regulations caused two units' control room minimum staffing levels to be unmet.
3352006005	Organizational		The original design of two units did not comply with regulatory requirements for fire protection.
3382002002	Organizational		Symmetrical deficient procedures used on two units caused the units to be in violation of technical specifications.
3382005001	Organizational		Symmetrical procedures used on two units were found to be deficient.
3382010003	Organizational		A design deficiency that affected two units was found.
3382011002	Organizational		Symmetrical procedures used on two units were found to be deficient.
3482009002	Organizational		A design calculation that was used for two units was found to be incorrect.
3522008004	Organizational		Symmetrical procedures used on two units were found to be deficient.
3612000001	Organizational		A symmetrical design deficiency was found on two units.
3612000004	Organizational		An analysis for the emergency core cooling system for two units was found to be incorrect.

LER Number	Classification	Subclass	Summary
3612000007	Organizational		An inadequate understanding of technical specifications caused two units to be in violation of technical specifications.
3612000008	Organizational		The control room isolation system, which is common to two units, was actuated.
3612000009	Organizational		Incomplete procedures caused two units to miss surveillances.
3612000012	Organizational		An inadequate understanding of technical specifications for two units' boration flow path caused both units to be in violation of technical specifications.
3612000015	Organizational		Inadequate documentation caused two units' post-accident monitoring instrumentation containment isolation valves to be in violation of technical specifications.
3612002002	Organizational		Symmetrical procedures used on two units were found to be deficient.
3612002003	Organizational		Symmetrical procedures used on two units were found to be deficient.
3612002004	Organizational		Symmetrical procedures used on two units were found to be defective.
3612002005	Organizational		Symmetrical procedures used on two units were found to be deficient.
3612008007	Organizational		Symmetrical procedures used on two units were found to be deficient.
3612010003	Organizational		An inadequate understanding of technical specifications for two units' containment isolation valves caused both units to be in violation of technical specifications.

LER Number	Classification	Subclass	Summary
3612010005	Organizational		A seismic analysis that was used for two units was found to be inadequate.
3612010006	Organizational		The safety culture at a site caused two units to violate technical specifications.
3612011001	Organizational		A misunderstanding of a safety analyses for two units caused two units to have a potential loss of safety function.
3622000001	Organizational		Symmetrical deficient procedures used on two units caused both units to be in violation of technical specifications.
3662001001	Organizational		Symmetrical procedures used for setpoints on two units were found to be deficient.
3692000002	Organizational		Symmetrical technical specifications for two units were found to be inadequate.
3692000003	Organizational		An analysis, which was used for two units' spent fuel pool, was found to be inadequate.
3692007004	Organizational		Symmetrical procedures used on two units were found to be deficient.
3732000001	Organizational		Symmetrical procedures used on two units were found to be defective.
3732000003	Organizational		A symmetrical analysis that was used to calculate setpoints on two units was found to be insufficient.
3732000004	Organizational		Symmetrical procedures used on two units were found to be deficient.
3732010003	Organizational		A seismic analysis that was used for two units was found to be incorrect.

LER Number	Classification	Subclass	Summary
3872000001	Organizational		An inadequate system design led to missed regulatory required testing on two units.
3872000006	Organizational		A symmetrical design deficiency was found on two units.
3872000009	Organizational		An inadequate understanding of technical specifications for two units' containment boundary valves caused both units to be in violation of technical specifications.
3872001001	Organizational		A design analysis that was used for two units was found to be incorrect.
3872001003	Organizational		A power calculation that was used for two units was found to be incorrect.
3872005001	Organizational		A misinterpretation of guidance for two units' containment ventilation caused both units to be in violation of technical specifications.
3872011001	Organizational		A symmetrical design deficiency was found on two units.
4132002004	Organizational		An engineering evaluation that was used for two units' chiller rooms were found to be inadequate.
4242005002	Organizational		A vendor-supplied calculation that was used for setpoints for two units was found to be incorrect.
4452001001	Organizational		Symmetrical procedures used on two units were found to be deficient.
4452001003	Organizational		Symmetrical procedures used on two units were found to be deficient.

LER Number	Classification	Subclass	Summary
4452002001	Organizational		An inadequate system design led to two unit's emergency diesel generators being inoperable.
4452010002	Organizational		An inadequate understanding of technical specifications for two units' main feedwater pumps caused both units to be in violation of technical specifications.
4452010003	Organizational		Symmetrical procedures used on two units were found to be deficient.
4452011001	Organizational		Vendor-supplied guidance that was used for calculations for two units was found to be incorrect.
4542000001	Organizational		The in-service testing program used for two units was found to be inadequate.
4542001001	Organizational		A power calculation that was used for two units was found to be incorrect.
4542001002	Organizational		Symmetrical procedures used on two units were found to be deficient.
4542003001	Organizational		An inadequate understanding of two units' filtration system actuation instrumentation (FSAI) caused both units' FSAI to be inoperable.
4542003003	Organizational		A flow calculation that was used for two units was found to be inaccurate.
4542005002	Organizational		Symmetrical procedures used on two units were found to be deficient.
4542005003	Organizational		An inadequate understanding of technical specifications for two units' containment penetrations caused both units to be in violation of technical specifications.

LER Number	Classification	Subclass	Summary
4542005004	Organizational		Symmetrical procedures used on two units were found to be deficient.
4542006002	Organizational		A symmetrical design deficiency was found on two units.
4542008002	Organizational		A design calculation that was used for two units was found to be incorrect.
4542009001	Organizational		Symmetrical procedures used on two units were found to be deficient.
4542011001	Organizational		Vendor-supplied guidance that was used for calculations for two units was found to be incorrect.
4542011003	Organizational		An analysis that was used for the auxiliary feedwater system on two units was found to be incorrect.
4562002003	Organizational		An inadequate understanding of technical specifications for two units' reactor coolant system caused both units to be in violation of technical specifications.
4562003003	Organizational		A vendor-supplied power calculation that was used for two units was found to be incorrect.
4562005001	Organizational		An inadequate understanding of technical specifications for two units' containment penetrations caused both units to be in violation of technical specifications.
4562008001	Organizational		An analysis that was used for the auxiliary feedwater system on two units was found to be incorrect.
4562010006	Organizational		An inadequate understanding of two units' component cooling system caused both units' technical specifications to be inaccurate.

LER Number	Classification	Subclass	Summary
4562010007	Organizational		Vendor-supplied guidance that was used for calculations for two units was found to be incorrect.
4562011004	Organizational		A high-energy line break analysis that was used for two units was found to be incorrect.
4572010002	Organizational		Symmetrical procedures used on two units were found to be deficient.
4982002002	Organizational		An analysis that was used for setpoints for two units was found to be inadequate.
4982003006	Organizational		Symmetrical procedures used on two units were found to be inadequate.
5282000003	Organizational		Symmetrical procedures used on two units were found to be deficient.
5282000004	Organizational		Symmetrical procedures used on two units were found to be deficient.
5282001002	Organizational		A test methodology that was used for three units was found to be inadequate.
5282004005	Organizational		Symmetrical procedures used on two units were found to be deficient.
5282004009	Organizational		Inadequate understanding of the design of three units led to all units' emergency core cooling system to have potentially been unable to fulfill their safety function.
5282005003	Organizational		Vendor-supplied guidance that was used to calculate setpoints for three units was found to be incorrect.
5282007003	Organizational		Symmetrical procedures used on three units were found to be deficient.
5282007004	Organizational		Symmetrical procedures used on three units were found to be deficient.

LER Number	Classification	Subclass	Summary
5282007005	Organizational		Symmetrical procedures used on three units were found to be deficient.
5282009003	Organizational		Symmetrical procedures used on three units were found to be deficient.
5282010002	Organizational		A calculation that was used for three units was found to be incorrect.
5292005005	Organizational		A design analysis that was used for two units was found to be inadequate.
2542000002	Organizational		Inadequate documentation caused two units to be in violation of technical specifications.
4542010001	Organizational		An inadequate understanding of two units' component cooling system caused both units' technical specifications to be inaccurate.
32008001	Proximity		Contraband was attempted to be brought onto a three-unit site.
2602001004	Proximity		Control room habitability was breached because a door was blocked opened.
2662000004	Proximity		A location was identified that could prevent two units from safely shutting down if a fire occurred in the area.
2662007006	Proximity		It was identified that fire damage in the cable spreading room may prevent the ability to safely shutdown two units.
2662010005	Proximity		Multiple high-energy line break barriers for two units were not controlled.
2692000007	Proximity		A radioactive source was lost onsite.

LER Number	Classification	Subclass	Summary
2692002002	Proximity		An engineering evaluation identified the potential for an adverse valve actuation on three units during a design basis fire.
2692003001	Proximity		An engineering evaluation identified the potential for an adverse valve actuation on three units during a design basis fire.
2812006002	Proximity		An unexpected steam valve opening caused siding to detach and contact transformer components. This ultimately led to a loss of offsite power that affected two units.
2822009001	Proximity		Inadequate analysis of hot shorts led to scenarios by which postulated fires could affect two units.
2822009009	Proximity		A radioactive source was lost onsite.
2822010003	Proximity		Battery room door seals for two units were found to be inadequate for postulated flooding scenarios.
2952007001	Proximity		A radioactive source was lost onsite.
3522005001	Proximity		A radioactive source was lost onsite.
4132002005	Proximity		A radioactive source was lost onsite.
4132004003	Proximity		Inadequate analysis of hot shorts led to scenarios by which postulated fires could affect two units.
4242006003	Proximity		A contract employee was given unescorted access to a site without self-disclosing material information.

LER Number	Classification	Subclass	Summary
5282006007	Proximity		The closure of a cubicle door cause a loss of offsite power on two units, which in turn, caused their emergency diesel generators to start.
2372002002	Shared SSC	Single	The smoke purge mode for the control room emergency ventilation system was found to prevent the system, which is common to two units, from performing its safety function.
2372002003	Shared SSC	Single	Manual valve failures prevented the cooling water flow to the control room refrigeration-condensing unit, which is common to two units.
2372002004	Shared SSC	Single	The control room ventilation ductwork, which is common to two units, was breached causing the control room ventilation system to be inoperable.
2372006005	Shared SSC	Single	The emergency ventilation air conditioning system, which is common to two units, was found to be inoperable.
2372008003	Shared SSC	Single	The control room emergency ventilation air conditioning system, which is common to two units, was found to be inoperable.
2502010004	Shared SSC	Single	A radiation monitor that is common to two units was found to be inoperable.
2542000008	Shared SSC	Single	Secondary containment, which is common to two units, was found to be breached.

LER Number	Classification	Subclass	Summary
2542005006	Shared SSC	Single	A control room emergency ventilation air conditioning compressor failed. The control room emergency ventilation air system is common to two units.
2542007003	Shared SSC	Single	The control room ventilation system, which is common to two units, was found to be unable to perform its safety function.
2542008001	Shared SSC	Single	The safe shutdown makeup pump, which is common to two units, was found to be in violation of technical specifications.
2542011003	Shared SSC	Single	The control room emergency ventilation air conditioning system, which is common to two units, was found to be inoperable.
2592009003	Shared SSC	Single	The shared standby gas treatment system relay failed, causing the standby gas treatment system to be inoperable for three units.
2602003005	Shared SSC	Single	A shutdown bus, which supplies power to two units' equipment, was temporarily de-energized.
2602005006	Shared SSC	Single	A low voltage on shutdown battery cells caused two units to be in violation of technical specifications.
2652000001	Shared SSC	Single	A malfunctioning valve caused the safe shutdown makeup pump on two units to be inoperable.
2662000003	Shared SSC	Single	Inadequate controls were found on a temporary penetration for the cable spreading room, which has cables for two units.

LER Number	Classification	Subclass	Summary
2662006001	Shared SSC	Single	The control room emergency ventilation filtration system, which is common to two units, was found to be inoperable.
2692000002	Shared SSC	Single	The control room cooling chiller, which is common to three units, was found to be inoperable.
2692000003	Shared SSC	Single	The control room cooling chiller, which is common to three units, was found to be inoperable.
2692004004	Shared SSC	Single	The control room ventilation system booster fan, which is common to two units, was found to be inoperable.
2692005001	Shared SSC	Single	The emergency power path auxiliary power source, which is shared by three units, was found to be inoperable.
2692006003	Shared SSC	Single	Foreign material was found in suction piping, which could have adversely affected reactor building spray pumps on three units.
2692009001	Shared SSC	Single	Spent fuel assemblies were found to be improperly stored in a spent fuel pool that is shared by two units.
2692011003	Shared SSC	Single	The standby shutdown facility, which is shared by three units, was found to be inoperable.
2722001005	Shared SSC	Single	The control room emergency air intake dampers, which are common to two units, were found to be inoperable.
2752001002	Shared SSC	Single	A differential relay tripped which caused the emergency diesel generators at two units to start.

LER Number	Classification	Subclass	Summary
2752006001	Shared SSC	Single	An unusually large number of dead birds were found on the bar racks associated with the cooling water intake for two units.
2752011006	Shared SSC	Single	The control room envelope, which is common to two units, was lost.
2752011007	Shared SSC	Single	The control room envelope, which is common to two units, was found to be inadequate.
2752011008	Shared SSC	Single	A design vulnerability was found in the control room ventilation system, which is common to two units.
2772003002	Shared SSC	Single	Inoperability of the standby gas treatment filter train, which is used for two units, caused a condition that is prohibited by technical specifications.
2772006004	Shared SSC	Single	A flooding vulnerability was found in the emergency diesel generator building carbon dioxide suppression room, which is common to two units.
2772010002	Shared SSC	Single	An improperly fastened rod hanger resulted in the inoperability of a subsystem of the emergency service water, which is a system common to two units.
2772011005	Shared SSC	Single	The qualified offsite power circuit, which is common to two units, was found to be inoperable.
2802000002	Shared SSC	Single	The effect of ventilation fans on the control room boundary, which is common to two units, resulted in a technical specification violation.

LER Number	Classification	Subclass	Summary
2802001002	Shared SSC	Single	The control room chillers breakers, which are common to two units, were found to have an improper trip rating.
2802005002	Shared SSC	Single	Radiation monitors that are common to two units were found to be inoperable.
2802008002	Shared SSC	Single	A failure of a breaker failure lockout relay resulted in a simulated loss of offsite power, which caused two units' emergency diesel generators to start.
2802009001	Shared SSC	Single	An emergency service water pump, which services two units, was found to be inoperable.
2802009002	Shared SSC	Single	An emergency service water pump, which services two units, was found to be susceptible to flooding.
2812003001	Shared SSC	Single	A shorted main generator lead caused automatic actuations on two units.
2822000005	Shared SSC	Single	The cooling water strainer backwash valves, which are common to two units, were not tested.
2822002001	Shared SSC	Single	The auxiliary building special vent zone boundary, which is shared by two units, was found to be degraded.
2952011001	Shared SSC	Single	A fuel rod storage canister was found to be improperly stored in a spent fuel pool that is shared by two units.
3012006002	Shared SSC	Single	Spent fuel assemblies were found to be improperly stored in a spent fuel pool that is shared by two units.
3012011003	Shared SSC	Single	The removal of a safeguards rack caused standby emergency power for two units to be inoperable.

LER Number	Classification	Subclass	Summary
3132001003	Shared SSC	Single	The control room emergency ventilation system radiation monitors, which are common to two units, were found to be inoperable.
3152000005	Shared SSC	Single	The auxiliary building crane was operated over the spent fuel pool, which is shared by two units, without proper alignment of the spent fuel ventilation system.
3152001005	Shared SSC	Single	The rod control cluster assembly was operated in violation of technical specifications over the spent fuel pool, which is shared by two units.
3152003003	Shared SSC	Single	Two units had to be shut down because of macro fouling in the shared intake.
3162000011	Shared SSC	Single	The spent fuel exhaust ventilation system, which is common to two units, was found to be inoperable.
3172006001	Shared SSC	Single	An emergency diesel generator tripped causing two units to be in violation of technical specifications.
3172011002	Shared SSC	Single	A diesel generator battery charger failed causing two units to be in violation of technical specifications.
3172011003	Shared SSC	Single	An emergency diesel generator was found to be inoperable causing two units to be in violation of technical specifications.
3212006004	Shared SSC	Single	A lack of understanding of the design caused the control room boundary, which is common to two units, to be in violation of technical specifications.

LER Number	Classification	Subclass	Summary
3212009006	Shared SSC	Single	The main control room air conditioner, which is common to two units, was found to be inoperable.
3212010002	Shared SSC	Single	The main control room air conditioner, which is common to two units, was found to be inoperable.
3212010003	Shared SSC	Single	The main control room environmental control system boundary, which is common to two units, was found to not be single failure proof as required.
3252000002	Shared SSC	Single	A small amount of chlorine gas escaped the chlorination system and caused the control room emergency ventilation system, which is common to two units, to actuate.
3252000003	Shared SSC	Single	A small amount of chlorine gas escaped the chlorination system and caused the control room emergency ventilation system, which is common to two units, to actuate.
3252005004	Shared SSC	Single	A loss of electrical power to an emergency bus, along with an air compressor failure, caused the control room emergency ventilation systems, which is common to two units, to be inoperable.
3252006001	Shared SSC	Single	The control room emergency ventilation and air conditioning, which is common to two units, were found to be inoperable.
3252006003	Shared SSC	Single	The control room emergency ventilation, which is common to two units, was found to be inoperable.

LER Number	Classification	Subclass	Summary
3252006005	Shared SSC	Single	The control room emergency ventilation, which is common to two units, was found to be inoperable.
3252007001	Shared SSC	Single	A crosstie breaker, which is used by two units, was found to be inoperable.
3252008002	Shared SSC	Single	The control room air conditioning system, which is common to two units, was found to be inoperable.
3252008004	Shared SSC	Single	A control room emergency ventilation subsystem did not perform as expected in a post-maintenance test, causing entry into a limiting condition of operation for two units.
3272009006	Shared SSC	Single	The auxiliary building gas treatment system, which is common to two units, was found to be inoperable.
3272009008	Shared SSC	Single	Spent fuel assemblies were found to be improperly stored in a spent fuel pool that is shared by two units.
3272011001	Shared SSC	Single	The control room air conditioning system, which is common to two units, was found to be inoperable.
3342008001	Shared SSC	Single	The control room envelope intake, which is common to two units, was found to be in violation of technical specifications.
3382002001	Shared SSC	Single	The waste gas decay tank oxygen analyzer, which is common to two units, was found to be in violation of technical specifications.
3522005002	Shared SSC	Single	A trip of a transformer caused the trip of an offsite power source, which caused automatic actuation of two units' components.

LER Number	Classification	Subclass	Summary
3522006001	Shared SSC	Single	A spurious actuation of the fire suppression system caused the trip of an offsite power source, which caused automatic actuation of two units' components.
3522006004	Shared SSC	Single	A faulty calculation that was used for a voltage regulator could have resulted in the loss of two offsite circuits.
3612000003	Shared SSC	Single	The control room emergency air cleanup system, which is common to two units, was found to have operated outside of the design basis.
3612000005	Shared SSC	Single	The control room emergency air cleanup system, which is common to two units, was found to be outside of its design basis.
3612000010	Shared SSC	Single	The control room emergency cleanup system, which is common to two units, was found to not be seismically qualified.
3612001003	Shared SSC	Single	One train of the control room emergency cleanup system, which is shared by two units, was found to be inoperable.
3612005003	Shared SSC	Single	Relay setting for the degraded grid voltage protection system could have caused early separation from offsite power for two units.
3612007006	Shared SSC	Single	A loose electrical connection caused the emergency chilled water system, which is shared by two units, to be inoperable.
3692009001	Shared SSC	Single	The nuclear service water system, which is common to two units, was found to be inoperable.

LER Number	Classification	Subclass	Summary
3692010001	Shared SSC	Single	The control room area chilled water system, which is common to two units, was found to be inoperable.
3692011001	Shared SSC	Single	Two units had to be shut down because of macro fouling in the shared intake.
3732005001	Shared SSC	Single	A single failure vulnerability of a current transformer was found that would have caused a loss of offsite power at two units.
3872000010	Shared SSC	Single	The control room emergency outside air supply, which is common to two units, was found to be inoperable.
3872002001	Shared SSC	Single	The control structure chiller, which is common to two units, was found to be inoperable.
3872003002	Shared SSC	Single	The standby gas treatment system, which is common to two units, was found to be inoperable.
3872003003	Shared SSC	Single	The standby gas treatment system, which is common to two units, was found to be inoperable.
3872003004	Shared SSC	Single	The control room emergency outside air supply and the control room floor cooling system, which are common to two units, were found to be inoperable.
3872008001	Shared SSC	Single	High exhaust radiation monitors, which are common to two units, were found to be inoperable.
4132000003	Shared SSC	Single	The control room ventilation system, which is common to two units, was found to be inoperable.

LER Number	Classification	Subclass	Summary
4132001003	Shared SSC	Single	The control room ventilation system, which is common to two units, was found to be inoperable.
4132003002	Shared SSC	Single	The loss of a vital inverter caused the nuclear service water system, which is shared by two units, to be inoperable.
4132007004	Shared SSC	Single	The control room area chilled water system, which is common to two units, was found to be inoperable.
4452001002	Shared SSC	Single	The primary plant ventilation system, which is common to two units, was found to be in violation of technical specifications.
4452003004	Shared SSC	Single	The control room air conditioning system, which is common to two units, was found to be inoperable.
4462010001	Shared SSC	Single	A fault occurred on a startup transformer that caused automatic actuations on two units.
4542000002	Shared SSC	Single	The control room ventilation system, which is common to two units, was found to be in violation of technical specifications.
4542005005	Shared SSC	Single	Improper tank cleaning caused the ultimate heat sink water makeup system, which is common to two units to be inoperable.
4542007002	Shared SSC	Single	An ultimate heat sink pipe leak, which is common to two units, caused both units to shut down due to technical specification requirements.

LER Number	Classification	Subclass	Summary
4562003001	Shared SSC	Single	The unit common control room ventilation system filtration system actuation instrumentation radiation monitors, which are common to two units, were found to be inoperable.
4562006002	Shared SSC	Single	The main control room ventilation envelope, which is common to two units, was found to be inoperable.
4562010005	Shared SSC	Single	The control room outside air intake, which is common to two units, was found to be inoperable.
4982010004	Shared SSC	Single	A switchyard bus de-energized causing a loss of offsite power for two units.
5282007002	Shared SSC	Single	An unanalyzed condition during a control room fire caused three units to be in violation of technical specifications.
5282011001	Shared SSC	Single	A protective relay actuation on a startup transformer caused a loss of offsite power on two units.
5282011003	Shared SSC	Single	A control room essential filtration misalignment caused three units to be in violation of technical specifications.
2662001004	Shared SSC	Standby	Redundant standby emergency power supplies were not started in compliance with technical specifications.
3272010001	Shared SSC	Standby	A common spare breaker was incorrectly installed, which caused two units to be in violation of technical specifications.

LER Number	Classification	Subclass	Summary
3872007001	Shared SSC	Standby	An emergency service water pump was automatically started due to improper alignment of the standby diesel generator.
2372009003	Shared SSC	Time Sequential	An emergency diesel generator, which is shared by two units, was found to be inoperable.
2502004001	Shared SSC	Time Sequential	Two emergency diesel generators, which can be used by two units, were found to be inoperable.
2502005006	Shared SSC	Time Sequential	An auxiliary feedwater pump, which is shared by two units, was found to be inoperable.
2542000001	Shared SSC	Time Sequential	An emergency diesel generator, which is shared by two units, was inadvertently started.
2542005002	Shared SSC	Time Sequential	An emergency bus, which was cross-tied, tripped causing power to be lost to two units' emergency power.
2592011002	Shared SSC	Time Sequential	A loss of safety function occurred when an emergency diesel generator that is shared by two units lost power.
2662001002	Shared SSC	Time Sequential	The use of an interlock defeat switch in certain scenarios was found to violate two units' technical specifications.
2662001005	Shared SSC	Time Sequential	The auxiliary feedwater system, which is shared by two units, was found to have a potential vulnerability.
2662001006	Shared SSC	Time Sequential	An unanalyzed condition during a fire could have caused two units' shared auxiliary feedwater systems to be inoperable.

LER Number	Classification	Subclass	Summary
2662002003	Shared SSC	Time Sequential	Partial clogging of recirculation orifices could have caused the auxiliary feedwater system, which is shared by two units, to be inoperable.
2772000004	Shared SSC	Time Sequential	A malfunctioning valve caused the emergency service water system, which is used by two units, to have inadequate flow.
2772005003	Shared SSC	Time Sequential	An emergency diesel generator that can be used by two units was not in compliance with technical specifications.
2772011003	Shared SSC	Time Sequential	A delayed relay operation caused an emergency diesel generator, which is common to two units, to automatically start.
2772011004	Shared SSC	Time Sequential	An emergency diesel generator, which is shared by two units, was found to be inoperable.
2802001001	Shared SSC	Time Sequential	An emergency diesel generator, which is shared by two units, was found to be inoperable.
2802005003	Shared SSC	Time Sequential	An emergency service water pump, which is shared by two units, was found to be inoperable.
2802006001	Shared SSC	Time Sequential	The auxiliary feedwater system, which is the same design on two units, was found to have a design error by which certain postulated single failure accidents could render the system inoperable.

LER Number	Classification	Subclass	Summary
2822000003	Shared SSC	Time Sequential	An unanalyzed condition could have caused the essential service (cooling) water system, which is shared by two units, to be inoperable.
2822010001	Shared SSC	Time Sequential	An unanalyzed condition could have caused the cooling water system, which is shared by two units, to be inoperable.
3252009002	Shared SSC	Time Sequential	The loss of power to an emergency bus caused automatic system actuations on two units.
3382003005	Shared SSC	Time Sequential	The inoperability of a hydrogen recombiner caused two units to be in violation of technical specifications.
3692010004	Shared SSC	Time Sequential	Two sub-trains of the starting air system for the emergency diesel generators for two units were cross-tied without complying with the Technical Specifications.
3872007002	Shared SSC	Time Sequential	The residual heat removal system, which is shared by two systems, was found to be inoperable.

References

[1] T. Hakata, “Seismic PSA Method for Multiple Nuclear Power Plants in a Site,” *Reliability Engineering and Safety System,* no. 92, pp. 883-894, 2007.

[2] U.S. Nuclear Regulatory Commission, “Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making (NUREG/CR-6813),” Washington, DC, 2003.

[3] K. N. Fleming, “On the Issue of Integrated Risk-A PRA Practitioner's Perspective,” in *Proceedings of the ANS International Topical Meeting on Probabilistic Safety Analysis*, San Francisco, CA, 2005.

[4] S. Arndt, “Methods and Strategies for Future Reactor Safety Goals,” PhD Thesis, 2010.

[5] A. Omoto, “Design Consideration on Severe Accident for Future LWR (IAEA-TECDOC-1020),” in *Proceedings of a Technical Committee Meeting of the International Atomic Energy Agency*, Vienna, 1996.

[6] W. S. Jung, J.-E. Yang and J. Ha, “A New Method to Evaluate Alternate AC Power Source Effects in Multi-Unit Nuclear Power Plants,” *Reliability Engineering and System Safety,* no. 82, pp. 165-172, 2003.

[7] J. Sandberg, G. Thuma and G. Georgescu, “Probabilistic Safety Analysis of Non-Seismic External Hazards,” Radiation and Nuclear Safety Authority (STUK), Helsinki, Finland, 2009.

[8] U.S. Nuclear Regulatory Commission, “Resolution of Generic Safety Issues: Task CH2: Design (NUREG-0933),” Washington, D.C., 1981.

[9] U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities (60 FR 42622)," Washington, D.C., 1995.

[10] U.S. Nuclear Regulatory Commission, "Plan for Resolving Policy Issues Related to Licensing Non-Light Water Reactor Designs (SECY-02-0139)," Washington, D.C., 2002.

[11] U.S. Nuclear Regulatory Commission, "Policy Issues Related to Licensing Non-Light-Water Reactor Designs (SECY-03-0047)," Washington, D.C., 2003.

[12] U.S. Nuclear Regulatory Commission, “Policy Issues Related to New Plant Licensing and Status of the Technology-Neutral Framework for New Plant Licensing (SECY-05-0130),” 2005.

[13] U.S. Nuclear Regulatory Commission, “Staff Requirements Memorandum-SECY-05-0130-Policy Issues Related to New Plant Licensing and Status of the Technology-Neutral Framework for New Plant Licensing,” 2005.

[14] U.S. Nuclear Regulatory Commission, “Staff Plan to Make A Risk-Informed and Performance-Based Revision to 10 CFR Part 50 (SECY-06-0007),” Washington, D.C., 2006.

[15] U.S. Nuclear Regulatory Commission, “Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing (NUREG-1860),” Washington, D.C., 2007.

[16] Idaho National Laboratory, “The NRC's SPAR Models: Current Status, Future Development, and Modeling Issues,” in *Proceedings of the ANS International Topical Meeting on Probabilistic Safety Analysis*, Knoxville, TN, 2008.

[17] U.S. Nuclear Regulatory Commission, "Staff Requirements Memorandum-SECY-11-0089-Options for Proceeding with Future Level 3 Probabilistic Risk Assessment (PRA) Activities," Washington, D.C., 2011.

[18] K. Muramatsu, Q. Liu and T. Uchiyama, “Effects of Correlations of Component Failures and Cross-Connections of EDGs on Seismically Induced Core Damages of a Multi-Unit Site,” *Journal of Power and Energy Systems,* vol. 2, no. 1, pp. 122-132, 2008.

[19] Pickard Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment-Section 13.3 Risk of Two Unit Station," Prepared for Public Service Company of New Hampshire, PLG-0300, 1983.

[20] M. D. Muhlheim and R. T. Wood, “Design Strategies and Evaluation for Sharing Systems at Multi-Unit Plants Phase I (ORNL/LTR/INERI-BRAZIL/06-01),” Oak Ridge National Laboratory, 2007.

[21] Institute of Nuclear Power Operations, "Special Report on the Nuclear Accident a Fukushima Daiichi Nuclear Power Station (INPO 11-005)," Atlanta, 2011.

[22] International Atomic Energy Agency, "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide No. SSG-3," Vienna, 2010.

[23] U.S. Nuclear Regulatory Commission, "Risk Assessment of Operational Events Handbook: Volume 3-SPAR Model Reviews, Rev. 2," Washington, D.C., 2010.

[24] Bogazici University Nuclear Engineering Department, "PSA Glossary," [Online]. Available: http://www.nuce.boun.edu.tr/psa/psaglossary.html. [Accessed 15 May 2012].

[25] M. Knochenhauer and J.-E. Holmberg, "Guidance for the Definition and Application of Probabilistic Safety Criteria," in *Proceedings of PSAM 10 International Probabilistic Safety Assessment & Management*, Seattle, Washington, 2012.

[26] U.S. Nuclear Regulatory Commission, "Regulatory Guide, 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Washington, D.C., 2002.

[27] U.S. Nuclear Regulatory Commission, "Staff Requirement Memorandum-SECY-90-016-Evolutionary Light Water Reactor Certification Issues and Their Relationships to Current Regulatory Requirements," Washington, D.C., 1990.

[28] U.S. Nuclear Regulatory Commission, "Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding (NUREG/CR-6268)," Washington, D.C., 2007.

[29] U.S. Nuclear Regulatory Commission, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants (NUREG/CR-6928)," Washington, D.C., 2007.

[30] International Atomic Energy Agency, "Extreme External Events in the Design and Assessment of Nuclear Power Plants (IAEA-TECDOC-1341)," Vienna, 2003.

[31] Institute of Electrical and Electronics Engineers, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety System (ANSI/IEEE Std 379-1988), New York , 1988.

[32] Tennessee Valley Authority, Letter to U.S. Nuclear Regulatory Commission, "Browns Ferry Nuclear Plant, Units 1, 2, and 3: Licensee Event Report 50-259/2011-001-00," 2011.

[33] Point Beach Nuclear Plant, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 2000-010-00," 2000.

[34] Duke Energy, Letter to U.S. Nuclear Regulatory Commission, "Duke Energy Carolinas, LLC: Licensee Event Report 369/2011-01, Revision 1," 2011.

[35] Florida Power and Light, Letter to U.S. Nuclear Regulatory Commission, "Turkey Point Units 3 and 4: Reportable Event 2005-006-01," 2005.

[36] PPL Susquehanna, LLC, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 50-387/2007-001-00," 2007.

[37] Prairie Island Nuclear Generating Plant, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 2-06-02," 2006.

[38] Point Beach Nuclear Plant, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 266/301-2007-006-00," 2007.

[39] Duke Energy, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 413/06-003," 2006.

[40] Exelon Nuclear, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 2001-001-00, Peach Bottom Atomic Power Station Unit 2 and 3," 2001.

[41] Exelon Generation Company, LLC, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 2011-004-00," 2011.

[42] U.S. Nuclear Regulatory Commission, "NRC Inspection Manual: Manual Chapter 0609 - Significance Determination Process," Washington, D.C., 2011.

[43] U.S. Nuclear Regulatory Commission, "NRC Enforcement Policy," Washington, D.C., 2011.

[44] Tennessee Valley Authority, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report (LER) 50-259/2009-003," 2009.

[45] Point Beach Nuclear Plant, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 266/2002-003-01," 2002.

[46] PPL Susquehanna, LLC, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 50-387/2002-005-00," 2002.

[47] Tennessee Valley Authority, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report (LER) 50-260/2000-002-00," 2000.

[48] Point Beach Nuclear Plant, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report (LER) 266/2001-005-00," 2001.

[49] Duke Energy, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 269/2002-01, Revision 0," 2002.

[50] Palo Verde Nuclear Generating Station, Letter to U.S. Nuclear Regulatory Commission, "Licensee Event Report 2004-009-01," 2004.

[51] Florida Power and Light, Letter to U.S. Nuclear Regulatory Commission, "Turkey Point Units 3 and 4: Reportable Event 2005-004-00," 2005.

[52] PSEG Nuclear LLC, Letter to U.S. Nuclear Regulatory Commission, "LER 272/02-001-00 Salem Generating Station-Unit 1," 2002.

[53] Southern Company, Letter to U.S. Nuclear Regulatory Commission, "Vogtle Electric Generating Plant-Unit 1 and 2 Licensee Event Report 1-2005-002," 2002.

[54] Tennessee Valley Authority, Letter to U.S. Nuclear Regulatory Commission, "Sequoyah Nuclear Power Plant Units 1 and 2-Licensee Event Report 50-327/2002001," 2002.

[55] Westinghouse Nuclear Safety Advisory Letter 02-3, "Steam Generator Mid-Deck Plate Pressure Loss Issue," 2002.

[56] Exelon Generation Company, Letter to U.S. Nuclear Regulatory Commission, "Braidwood Station, Units 1 and 2, Licensee Event Report 2010-007-00," 2010.

[57] Exelon Generation Company, Letter to U.S. Nuclear Regulatory Commission, "Byron Station, Units 1 and 2, Licensee Event Report 2011-001-00," 2011.

[58] Luminant Power, Letter to U.S. Nuclear Regulatory Commission, "Comanche Peak Nuclear Power Plant, Licensee Event Report 445/11-001-00," 2011.

[59] Westinghouse Nuclear Safety Advisory Letter 09-8, "Presence of Vapor in Emergency Core Cooling System/Residual Heat Removal System in Modes 3/4 Loss-of-Coolant Accident Conditions," 2009.

[60] Exelon Generation Company, Letter to U.S. Nuclear Regulatory Commission, "Braidwood Station, Unit 1, Licensee Event Report 2005-001-00".

[61] Exelon Generation Company, Letter to U.S. Nuclear Regulatory Commission, "Braidwood Station, Units 1 and 2, Licensee Event Report 2010-006-00," 2010.

[62] U.S. Nuclear Regulatory Commission, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment (NUREG/CR-5485)," Washington, D.C., 1998.

[63] Z. Mohaghegh, R. Kazemi and A. Mosleh, "Incorporating Organizational Factors into Probabilistic Risk Assessment of Complex Socio-Technical Systems: A Hybrid Technique Formalization," *Reliability Engineering and System Safety,* no. 94, pp. 1000-1018, 2009.

[64] A. Chiacchio, L. Compagno, D. D'Urso, G. Manno and N. Trapani, "Dynamic Fault Trees Resolution: A Conscious Trade-Off between Analytical and Simulative Approaches," *Reliability Engineering and System Safety 96,* pp. 1515-1526, 2011.

[65] P. Bucci, J. Kirschenbaum, L. A. Mangan, T. Aldemir, C. Smith and T. Wood, "Construction of Event-Tree/Fault-Tree Models from a Markov Approach to Dynamic System Reliability," *Reliability Engineering and System Safety ,* no. 93, pp. 1616-1627, 2008.

[66] Y.-S. Hu and M. Modarres, "Evaluating System Behavior through Dynamic Master Logic Diagram Modeling," *Reliability Engineering and System Safety,* no. 64, pp. 241-269, 1999.

[67] S. B. Akers, "Binary Decision Diagrams," in *IEEE Transactions on Computers, Vol. C-27*, 1978.

[68] Z. Mohaghegh and A. Mosleh, "Incorporating Organizational Factors into Probabilistic Risk Assessment of Complex Socio-Technical Systems: Principles and Theoretical Foundations," *Safety Science,* no. 47, pp. 1139-1158, 2009.

[69] Z. Mohaghegh, M. Modarres and A. Christou, "Physics-Based Common Cause Failure Modeling in Probabilistic Risk Analysis: A Mechanistic Approach," in *Proceedings of the ASME 2011 Power Conference*, Denver, Colorado, 2011.

[70] Z. Mohaghegh and M. Modarres, "A Probabilistic Physics-of-Failure Approach to Common Cause Failures in Reliability Assessment of Structures and Components," in *American Nuclear Society, 2011 Winter Meeting*, Washington, D.C., October 30-November 3, 2001.

[71] P. Trucco, E. Cagno, F. Ruggeri and O. Grande, "A Bayesian Belief Network Modelling of Organisational Factors in Risk Analysis: A Case Study in Maritime Transportation," *Reliability Engineering and System Safety,* no. 93, pp. 823-834, 2008.

[72] F. V. Jensen and T. D. Nielsen, Bayesian Networks and Decision Graphs, Second Edition, New York: Springer, 2007.

[73] B. A. Gran and A. Helminen, "A Bayesian Belief Network for Reliability Assessment," in *SAFECOMP '01 Proceedings of the 20th International Conference on Computer Safety, Reliability, and Security*, London, 2001.

[74] R. Montironi, W. F. Whimster, Y. Collan, P. W. Hamiltion, D. Thompson and P. H. Bartels, "How to Develop and Use a Bayesian Belief Network," *J Clin Pathol,* no. 49, pp. 194-201, 1996.

[75] U.S. Nuclear Regulatory Commission, "PRA Procedures Guide (NUREG/CR-2300)," Washington, D.C., 1983.

[76] U.S. Nuclear Regulatory Commission, "Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150 (NUREG/CR-4840)," Washington, D.C., 1990.

[77] ASME/ANS RA-Sa-2009, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME, New York, NY, American Nuclear Society, Le Grange Park, Illinois: Addenda to ASME/ANS RA-S-2008, February 2009.

[78] U.S. Nuclear Regulatory Commission, "Methods for External Event Screening Quantification Integration and Evaluation Program (NUREG/CR-4839)," Washington, D.C., 1992.

[79] International Atomic Energy Agency, "IAEA Safety Standards Series: External Events Excluding Earthquakes in the Design of Nuclear Power Plants (No. NS-G-1.5)," Vienna, 2003.

[80] U.S. Nuclear Regulatory Commission, "Technical Review of Risk-Informed, Performance-Based Methods for Nuclear Power Plant Fire Protection Analyses-Draft Report for Comment (NUREG-1521)," Washington, D.C., 1998.

[81] U.S. Nuclear Regulatory Commission, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities (NUREG/CR-6850)," Washington, D.C., 2005.

[82] International Atomic Energy Agency, "Probabilistic Safety Assessment for Seismic

Events, IAEA-TECDOC-724," Austria, 1993.

[83] N. Chokshi and J. J. Johnson, "Methodology of Seismic Margin Assessment and Evaluation Examples in the US," in *Presentations from the First Kashiwazaki International Symposium*, Kashiwazaki, Japan, November 24-26, 2010.

[84] Y. Chang and A. Mosleh, "Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents, Part 1: Overview of the IDAC Model," *Reliability Engineering and System Safety,* no. 92, pp. 997-1013, 2007.

[85] U.S. Nuclear Regulatory Commission, "NRC Issues "Yellow" Finding at Palo Verde Nuclear Plant; Proposes $50,000 Fine (ML051010288)," Washington, D.C., 2005.

[86] C. Wang and A. Mosleh, "Qualitative-Quantitative Bayesian Belief Networks for Reliability and Risk Assessment," in *Reliability and Maintainability Symposium, 2010 Proceedings*, San Jose, CA, 2010.

[87] U.S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment of Five U.S. Nuclear Power Plants (NUREG-1150)," Washington, D.C., 1990.

[88] C. W. Kang and M. W. Golay, "A Bayesian Belief Network-Based Advisory System for Operational Availability Focused Diagnosis of Complex Nuclear Power Systems," *Expert Systems with Applications,* no. 17, pp. 21-32, 1999.

[89] M. Modarres, M. Kaminskiy and V. Krivtsov, "7.2 Analysis of Dependent Failures," in *2nd ed. Reliability Engineering and Risk Analysis: A Practical Guide*, Boca Raton, Florida, CRC Press, 2010, pp. 342-351.

[90] Princeton University, "WordNet Search - 3.1," 2005. [Online]. Available: http://wordnetweb.princeton.edu/perl/webwn?s=fuzzy%20logic. [Accessed 13 April 2012].