INL/EXT-11-23479
Revision 1

Risk Informed Safety Margin Characterization Case Study: Selection of Electrical Equipment To Be Subjected to Environmental Qualification

M3LW-12IN0702012 "Expansion of Trial Method and Case Study and Improvements"

D. Blanchard (AREI)
R. Youngblood (INL)

April 2012

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

Idaho National Laboratory

INL/EXT-11-23479
Revision 1

Risk Informed Safety Margin Characterization Case Study: Selection of Electrical Equipment To Be Subjected to Environmental Qualification

D. Blanchard
R. Youngblood

April 2012

Idaho National Laboratory
Light Water Reactor Sustainability
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CONTENTS

TABLES

ACRONYMS

AC	alternating current
AFW	auxiliary feedwater
AOV	air-operated valve
CCW	component cooling water
CDF	computational fluid dynamics
CST	condensate storage tank
DM	Decision Maker
DoE	Department of Energy
EQ	environmental qualification
HPSI	High-Pressure Safety Injection System
IA	instrument air
LOCA	loss-of-coolant accident
LOFW	loss of feedwater
LPSI	low-pressure safety injection
LWRS	Light Water Reactor Sustainability
MOV	motor-operated valve
MSIV	main steam isolation valve
NPSH	net positive suction head
NRC	Nuclear Regulatory Commission
PORV	power-operated relief valve
PRA	probabilistic risk analysis
PWR	pressurized water reactor
RCS	reactor coolant system
RISMC	Risk-Informed Safety Margin Characterization
SGTR	steam generator tube rupture
SRV	safety relief valve
SSC	system, structure, or component
SW	service water
TEP	Top Event Prevention

1. INTRODUCTION

Reference 1 discussed key elements of the process for developing a margins-based "safety case" to support safe and efficient operation for an extended period. The present report documents (in Appendix A) a case study, carrying out key steps of the Reference 1 process, using an actual plant Probabilistic Risk Assessment (PRA) model.

In general, the margins-based safety case helps the decision-maker manage plant margins most effectively. It tells the plant decision-maker such things as what margin is present (at the plant level, at the functional level, at the barrier level, at the component level), and where margin is thin or perhaps just degrading. If the plant is safe, it tells the decision-maker why the plant is safe and where margin needs to be maintained, and perhaps where the plant can afford to relax.

As discussed in Reference 1, the details of the safety case need to be considered collectively. Functional margin in a given system, structure, or component (SSC) matters (or not) depending on what alternative means the plant has to accomplish the given SSC's function, should it fail. For that reason, it is necessary to have a clear picture of what SSC's are being counted on collectively in order to assess the significance of a given SSC's performance margin.

The case study in Appendix 1 focuses on environmental qualification (EQ) of electrical equipment in containment. Age-related degradation of cables (such that they become more susceptible to harsh environments) is cited in numerous discussions of extended operation as an important issue. Which cables matter? For which cables do we need ongoing assurance of performance (specifically under harsh environmental conditions)? Replacement of all cables is a daunting prospect. Being able to focus on a subset of cables, while still maintaining plant-level safety and efficiency even if the other cables degrade, would be very useful. The case study shows how to do this.

2. OVERVIEW OF THE CASE STUDY

Table 1 recapitulates Reference 1 steps for developing a margins-based "safety case," and states briefly how the case study in Attachment 1 addressed each step.

As stressed in Reference 1 and Appendix 1, a key issue in safety case formulation is the plant-level safety performance delivered collectively by the SSCs chosen to be in the safety case. In this report, choosing the set of SSCs that is necessary and sufficient to satisfy the safety objectives is referred to as the "selection problem." A tool for validly doing the selection problem (effectively, deciding where resources will be allocated to assure SSC performance margin) is "prevention analysis." [2] Prevention analysis was originally formulated to do a comprehensive facility Q-list problem: to apply Boolean optimization to the selection problem at the plant level. However, the case study shows how to target the prevention analysis to focus on a single issue (in this case, environmental qualification of cables), while validly performing the selection problem at the plant level.

Table 1. Case Study Information.

	Safety Case Development Steps (Reference 1)	How Addressed in Attachment 1 Case Study
1	Begin with a set of safety thresholds and goals in mind. This is not to pre-empt the decision-maker's authority, or to force the analysis to prescribe an answer, but rather to steer analysis and uncertainty reduction to the most important areas.	In the case study, the current level of risk as quantified in the plant's existing Level 1 PRA was taken as baseline. The objective is to maintain the baseline more efficiently.
2	Working within a "success-path" framework, identify SSCs needed for economically successful plant operation. This will best be done through laboratory-industry collaboration. This will include elements of the regulatory safety case, since a regulatory shutdown is inconsistent with economic plant operation. As used here, the regulatory safety case is identified with the license renewal safety case, which is to say that it includes SAR safety case SSCs plus SSCs needed to comply with other important regulations such as the Blackout Rule. This will also include elements of the Risk-Informed Safety Case that are not necessarily in the Regulatory Safety Case. From a formal point of view, these SSCs can be identified straightforwardly through a process of considering the key functions performed by the success paths credited in the Risk-Informed Safety Case. For an example of what is meant by this, refer back to Figure 2 [of Reference 1]. Finally, depending on industry input, this set of SSCs may include SSCs that are NOT part of the risk-informed safety case, but are needed for economics. Large secondary-side SSCs may be cases of this. The recommended thought process for this step is an adaptation of "prevention analysis." Prevention analysis is a tool for allocating performance (margins) over SSCs so as to achieve performance	This step was the major focus of the case study. The case study applied the technique called out in this step ("prevention analysis"), and applied the technique to the plant's current Level 1 PRA, including SSCs in the various safety categories mentioned in this step.

	objectives (such as safety) in a balanced and cost-effective way. The wording of this step is not meant to suggest developing an exhaustive inventory of every SSC involved in production or safety, for downselect in Step 2 below. The idea is to scope the capability that needs to be maintained. Functional success paths are adequate for this purpose, provided that they are specified in sufficient detail to allow an engineer to determine whether a given SSC is "in" or "out."	
3	From the SSCs identified in Step 2, downselect for Risk-informed Safety Margins Characterization (RISMC) purposes to SSCs whose cost issues and technical issues warrant attention within the RISMC effort. This, too, will best be done through laboratory-industry collaboration. For purposes of the rest of the analysis, impute nominal margins (nominal failure probabilities) to the SSCs NOT to be examined within RISMC. This bullet is meant to acknowledge the reality that on a parts-count basis, most issues will be dealt with by plant owners without the need for much analysis, and many other issues will be dealt with by industry organizations without resort to DoE Laboratory help. Moreover, license renewal commits licensees to numerous efforts to manage safety margins in certain areas. In the interest of efficient use of resources, the RISMC program needs to focus on relatively high-stakes issues that are beyond the scope of license renewal and/or require significant analysis, including application of research results from other pathways. The reactor vessel is an example of an SSC that warrants attention within RISMC. It plays a key role in the regulatory safety case because it is a primary boundary to radioactive release. It has a large replacement cost. It plays a role in economic performance because the vessel is monitored closely, and if vessel margins are found to be eroding with respect to regulatory safety criteria, significant cost to the licensee will be incurred, almost certainly long before there is a significant threat to the	This case study was formulated to focus on a particular issue, namely, environmental qualification of aging (and presumably degrading) cables. As stressed in several places above, it is invalid to focus on a particular set of SSCs without regard to the *collective* safety performance of that set. Some previous analyses of issues of this kind have tried to perform SSC selection based on component "importance measures." Such a process does NOT address the safety performance of the resulting SSC selection. In this case study, it was shown how to validly choose a subset of cables whose individual functional margins in harsh environments are sufficient for plant safety, as part of an overall complement of SSCs having the property that maintaining their individual performance margins is necessary and sufficient for maintaining margin at the plant level. This subset turned out to be small relative to the number of cables modeled. For efficiency of the case study, a conservative simplifying assumption was made: that a harsh environment failing one particular cable would fail all similar cables. For that reason, the case study demonstrates *sufficiency* of the selected groups of cables, but it is possible, even though a significantly reduced collection can be shown to maintain the baseline, that some

	public. This outcome would be an NRC/PRA success story, but not a utility success story. Finally, for reasons documented in Materials Pathway reports, the Materials pathway is paying significant attention to the vessel, and their findings need to be folded into a state-of-knowledge assessment of vessel margins.	cables included are not strictly *necessary*.
4	For each SSC selected in Step 3, determine a level of allocated performance needed to satisfy performance requirements for economical plant operation. There are at least two aspects of this: physical SSC capability (e.g., load-bearing), and a threshold failure probability that the SSC should beat. (Example: the SSC should withstand a pressure of X with a failure probability < 1E-m.) SSCs may have two distinct levels of allocated performance. SSCs that are not part of the safety case, but are needed for economical operation, have allocated performance levels corresponding to what is needed for economical operation. SSCs that are part of the regulatory safety case may have multi-faceted performance allocation; one allocated performance level relates in some way to regulatory limits, and another is the level of performance targeted by the system owner to achieve economical operation. Falling short of the regulatory allocation brings unwelcome regulatory attention, up to and including shutdown; falling short of the economics-based allocation may not cause regulatory problems, but (by definition) is inconsistent with economical operation. Note that a lack of margin *to* the regulatory limit can cause shutdown well before there is any real threat to the public. Again, the vessel is an example of this.	For cables, it was argued that elaborate quantification of their performance state was unwarranted; given a harsh environment, we can assume for purposes of analysis that they are either good or bad. Also, if the performance of the cables needs to be good, the failure probabilities of the components with which the cables are associated provide a comparative basis for establishing how good performance needs to be: each cable failure probability should be small compared to the component that it supports.
5	Analyze the current performance capability of each subject SSC. This should be analyzed in terms of the "logo:" loads on the SSC need to be analyzed, and the performance of the SSC given these loads should be analyzed.	The case study did not complete this step, but made a start. The five accident sequence types each have profiles that would constitute the initial step of defining the loads on the cables. However, this information was not used in the present work.

6	Compare each SSC's current performance capability with the performance allocation.	This generic step was formulated to address attributes such as flowrate or probability of fail to run. In this case study, cable performance was modeled as a simple Boolean variable; if the cable is not qualified for a given harsh environment; it is assumed failed, given that environment.
7	Determine whether a suitable life extension safety case is currently viable (whether current SSC performance is consistent with input goals on aggregate performance). If a suitable safety case can be developed, then develop it. If further optimization is worthwhile (tweaking of goals and/or allocations), then iterate the above steps. If a life extension safety case is not currently viable, identify the reasons why not, and report to the decision maker.	For a focused issue such as cables, the conclusion is a bit more restricted. The case study explicitly demonstrated that selecting a particular set of cables in conjunction with a specific set of other plant SSCs, and maintaining those cables' EQ and those other plant SSCs' nominal behavior, maintains plant safety. From results such as this, the overall plant safety case is straightforwardly developed.

3. SUMMARY

Because the case study has been carried out on a current PRA of a currently-operating plant, detailed component-level results cannot be provided in a report that is to be distributed widely. However, tables of high-level results are provided in the case study.

Table 1 of Attachment A of Appendix 1 provides a list of component groups whose selection (by prevention analysis) for continued EQ will maintain plant safety, even if unselected groups degrade significantly. As discussed in Appendix 1, prevention analysis provides more than one alternative for doing this; the table simply shows the result for one of those ways (one involving the smallest number of cable groups, suggesting a lower cost of cable EQ). The table compares this selection with the selection one would make based on so-called "importance measures." Later, in Attachment C of Appendix 1, the safety performance of these two selections is compared. It is seen that the prevention-analysis-based selection of a subset of cable groups essentially maintains plant safety (as measured by core damage frequency), even if unselected groups degrade significantly, while the safety performance of the importance-measure-based selection is quite a bit worse.

4. NEXT STEPS

Methodologically, the value of Prevention Analysis for safety case development is confirmed. However, Prevention Analysis as illustrated in Appendix 1 is just a first step. Enhancements of two kinds are needed to Prevention Analysis in order to make it most effective for this application.

Prevention Analysis develops multiple alternative solutions to the problem of selecting a group of SSCs whose performance "prevents" every cut set. A method for comparing these solutions against each other is needed, even if we do not improve on the current discrete-valued treatment of SSC performance.

The case study treats cable performance in terms of binary variables; it does not quantify cable performance or environmental harshness in terms of continuous variables. Work of this kind has been done previously to address issues of seismic capacity in a facility design. It may be appropriate to develop Prevention Analysis in this way.

5. REFERENCES

1. R. W. Youngblood, RISMC-Based Process for Life Extension "Safety Case" Development, M3LIN10RIS1510202.
2. R. W. Youngblood, "Applying Risk Models To Formulation Of Safety Cases," **Risk Analysis 18,** No. 4, p. 433 **(**August 1998), and references contained therein.

Appendix A

Risk Informed Safety Margin Characterization Case Study

Selection of Electrical Equipment to be Subjected to Environmental Qualification

Applied Reliability Engineering, Inc

Report No. IN11-01-01 Rev 1
April, 2012

Risk Informed Safety Margin Characterization Case Study

Electrical Equipment Qualification

Table of Contents

1. Background

A harsh environment is considered to be a common mode challenge to nuclear power plant components exposed to that environment, even across different component types. Considerable resources are expended on qualification of safety related equipment that may be exposed to such environments with the intent of assuring that these components are capable of performing their safety functions given the environmental challenge. 10CFR50.49 requires licensees to develop a list of electrical equipment 'important to safety' that could be subject to a harsh environment following a design basis event [1]. Regulatory Guide 1.89 [2] describes acceptable methods for meeting 10CFR50.49. Environmental parameters to be considered for design basis events include temperature, pressure, humidity, submergence, chemical effects, and radiation. Synergistic effects of the environmental parameters are to be taken into consideration. Aging to end-of-life conditions are to be considered in qualification testing. Finally, margin to account for uncertainties in the environmental conditions, test instrumentation and analyses are to be considered. Testing requirements developed in IEEE 323 [3] are endorsed. This standard includes the environmental parameters noted above and recommended acceptable margins for use in qualification testing. Electrical equipment included in qualification programs encompasses not only safety-related components relied upon to operate following design basis events but also non-safety related components potentially useful in post accident monitoring in accordance with Regulatory Guide 1.97 [4].

As a part of current license extension efforts to 60 years of operation, licensees explicitly consider aging of components that fall within the scope of the electrical equipment qualification program. This license-extension-related-aging-management review often relies on the practices of the existing qualification program. This generally entails maintaining the normal operating environment in which the components are located and refurbishment or replacement of electrical equipment within the assumptions of the testing program, as opposed to monitoring the material state of parts that may be subject to age related degradation.

As licensees consider whether to operate their plats beyond 60 years, the LWRS program RISMC "pathway" includes an effort that considers SSC aging within the concept of "margin." This concept refers not only to the margin in individual SSCs' capability to meet the functional

challenges posed to them, but also to margin in overall integrated plant design including its response to a full spectrum of transients and accidents.

In order to examine SSC aging from an environmental qualification perspective, a case study has been defined that illustrates how the state of knowledge regarding SSC margin can be characterized given the overall integrated plant design. The case study is intended to demonstrate a method for deciding on which SSCs to focus, which SSCs are not so important from an environmental qualification margin standpoint, and what plant design features or operating characteristics determine the role that environmental qualification plays in establishing a safety case on which decisions regarding margin can be made. This report documents progress to date on that case study.

The subject of the case study is a PWR with a large dry containment. Within the scope of the study are the SSCs located in the containment including mechanical and electrical equipment whose performance could be affected by a harsh environment (this includes not only active components such as motors and solenoid valves, but mechanical equipment that may have elastomers such as pneumatic operators and instrumentation and passive components such as cables). The case study does not limit itself to components on the EQ list. Consideration is also given to potential non-safety related mitigating features that can be credited in limiting the impact of accident sequences leading to harsh environments which may not be addressed in the EQ program.

To generate early insights, the initial look at this PWR considers Level 1 accident sequences of the internal events PRA. The scope of the Level 1 internal events accident sequences includes a spectrum of sequences which would be part of the design basis as well as sequences that would be considered to be beyond the design basis.

The approach taken in performing this evaluation is relatively straightforward and includes the following four steps:

Identify components explicitly modeled in the PRA that are located inside containment

Characterize the environmental profiles to which components inside containment would be exposed for different accident sequences

Modify PRA models to include explicit failure modes associated with component exposure to a harsh environment

Quantify accident sequences and identify components important from an environmental qualification perspective.

In this report, the latter step is done in two ways for purposes of comparison:

1. A traditional, importance-measure-based way
2. Using Prevention Analysis, a technique based on Boolean optimization.

The comparison demonstrates certain important advantages of Prevention Analysis for this application.

2. Case Study Plant Description

The plant selected for the case study is a two-loop PWR with a large dry containment. Plant features that influence the safety case for this plant, and a brief description of its PRA, follow.

Case Study Plant Systems

Secondary heat removal

Three AFW pumps (two motor driven, one turbine driven)

Small CST (requires makeup after 6 hours of decay heat removal)

Two steam driven feedwater pumps (pumps are lost on steam line isolation, safety injection, etc)

Two condensate pumps (capable of injection once either steam generator has been depressurized)

RCS Pressure Relief

Three code safety valves

Two large PORVs (either capable of depressurizing reactor for feed and bleed – block valves normally closed, so not a source of LOCA should PORV spuriously operate)

Reactor inventory makeup

Two intermediate head HPSI pumps (requires AFW for small LOCA)

Three LPSI pumps

Three charging pumps (low volume)

Containment heat removal

Two containment spray headers

Three containment atmospheric coolers

Equipment cooling

Three component cooling water pump trains, two heat exchangers

Three service water pumps, two essential headers and one non-essential

AC power sources

Two essential buses

Five offsite transmission lines (aligned such that fast transfer is not required to power essential buses)

Three diesel generators, two automatic and one manual (manually controlled diesel can feed either ac power division, but not both)

DC power

Two divisions with four hour capacity

Case Study Plant PRA

The internal events PRA for this PWR has the following characteristics:

50 initiating events including

Four ranges of LOCA break sizes

Interfacing system LOCA

SGTR

Steam line breaks (inside and outside containment)

Transients

Turbine trips

LOFW

MSIV closure

Loss of offsite power

Loss of support systems (SW, CCW, IA)
Loss of ac buses (essential and non-essential)
Loss of instrument ac buses
Loss of dc buses

Consequential initiating events are considered subsequent to each transient initiator
Transient induced LOCA (e.g., pressurizer SRV challenges, failure of letdown isolation)
Transient induced steam line breaks (e.g., stuck open steam dump valves)
Reactor coolant pump seal LOCA

System fault trees include extensive modeling of instrumentation and control
Auxiliary Feedwater actuation
Safety Injection Signal
Recirculation actuation
Containment spray and containment atmospheric cooler actuation
Load shed
Emergency ac actuation
Control room indication for credited operator actions

Spurious actuations explicitly modeled (PRA recently updated for purposes of Fire PRA).

Treatment of Equipment Qualification in the Case Study Plant PRA

As is the case for most US nuclear power plant PRAs, the PRA used for this case study does not include basic events that explicitly represent component failures due to environmental related conditions. Rather, the current PRA implements a relatively simple model in treating the effects of a harsh environment. As will be discussed in subsequent sections of this report, the current approach will be modified to facilitate performing the case study.

In the current PRA, if a component is in the equipment qualification program, or is similar to one that is in the program, and the environment to which it is exposed in a given accident sequence does not exceed the temperature profile to which the component is qualified, then the component/failure mode is assigned its normal random failure probability. If the environment to

which the component is exposed exceeds the temperature profile to which the component is qualified, then the component failure mode is assumed to occur with certainty. The step function shown in Figure 1 illustrates this treatment of equipment qualification in the PRA. Examples of the application of this model in the case study plant PRA include steam line breaks outside containment. For these initiating events, equipment located in the room in which the break is assumed to occur are not credited in the analysis.

A more realistic treatment of equipment qualification might be to develop a fragility curve for the component and assign a failure probability based on the magnitude of the challenge to which the component is exposed, peak temperature for example. However, the manner in which equipment qualification testing is performed and documented does not allow for estimation of such a fragility curve. Rather, a representative component is tested to a bounding accident sequence profile and documentation of the successful test is provided. Environmental qualification testing is not statistically significant nor are estimates made regarding the performance of the component under different conditions.

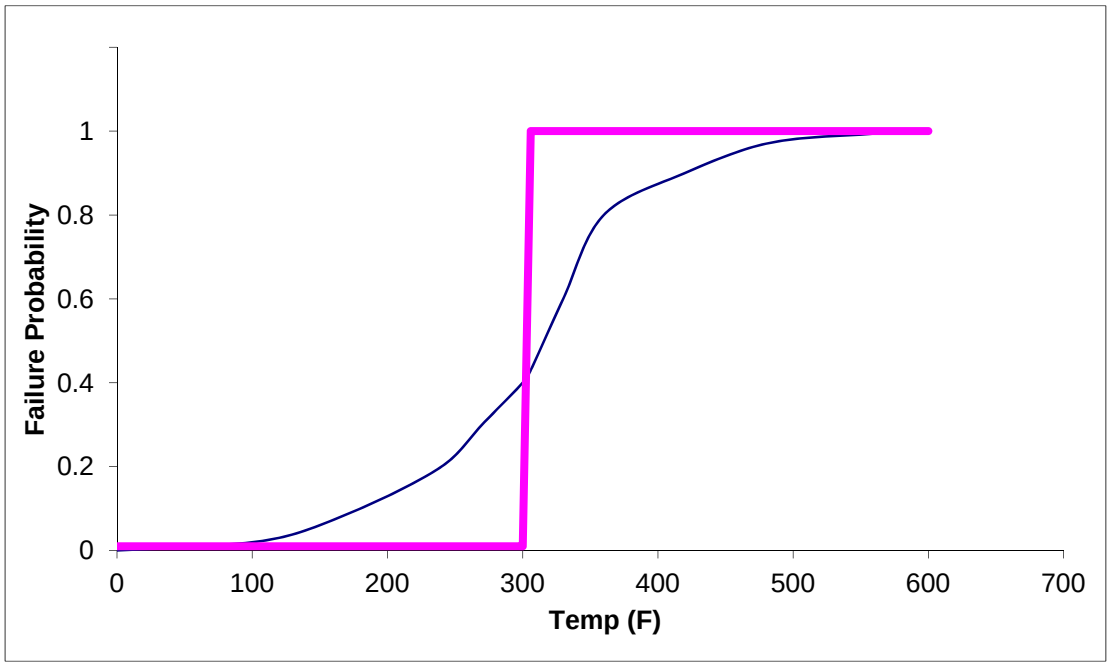


Figure 1 – Treatment of equipment qualification in the case study PRA

This approach to treating harsh environments in PRA is generally considered to be acceptable for several reasons. First, the environment associated with the majority of accident sequences is often in the more benign area of the fragility curve (to the left side of Figure 1). For those events in which the environmental testing profile is exceeded, the environment is often on its way to significantly exceeding the qualification of the equipment (sequences in which containment heat removal failure has failed, for example).

Given these characteristics and the 'best estimate' quantitative approach taken by current PRA methods, it is not clear that having detailed fragilities on components exposed to a harsh environment would make a significant difference in quantification of the accident sequences of the PRA. However, if there were particularly important components that must function when exposed to a harsh environment, the interesting question would be for what subset of components would having fragility information (or alternately providing significant margin) be important.

3. Identification of Component Groups

The first step in the case study is to identify all of the individual components explicitly modeled in the PRA for this PWR and establish their location in the plant. To assist in identifying components located in the containment, the plant staff provided an equipment list that includes the location of each tag id.

Of several thousand components represented in the PRA, over 200 are located in the containment. However, not all of these components are subject to failure were they to be exposed to a harsh environment. Components such as check valves, manually operated valves, tanks, and heat exchangers can be screened from the list. The remaining components are those that contain parts whose performance could be affected by harsh environmental conditions and aging phenomena.

Major active components
- Motor operated valves
- Air operated valves
- Solenoid valves
- PORVs

Major rotating equipment
- Pump motors
- Fans

Instrumentation
- Transmitters (pressure, level)
- Switches (level, limit)
- Temperature elements
- Radiation monitors
- Signal converters (E/P)

Miscellaneous
- Power supplies
- Penetration seals (hatches)

Attachment A contains a summary of the component types and failure modes for components located inside containment for the case study plant and the functions that they provide. Basic events included in the system fault trees associated with each component were then identified. It should be noted that there are many components and their failure modes that are not explicitly modeled in the PRA but are effectively selected for inclusion in the case study as a result of their association with the component types listed in the attachment. Examples include power and control cables, junction boxes, and terminals. The selected basic events effectively can be considered to be modules that not only include the component in question, but supporting subcomponents needed for the component to function.

The failure mode for each selected basic event was reviewed and a judgment made as to whether a harsh environment could cause such a failure. Further screening of a number of failure modes was performed as a part of this review. For example, valves that were already in position to perform their function, and the failure of these valves would lead to their remaining in this position, were not considered to be contributors to functional failure of the valves as a result of a harsh environment. Solenoid valves which would have to spuriously energize in order to fail were screened because a harsh environment was not considered to be a significant source of hot shorts. Basic events that remain after this screening include active components which must change position (e.g., MOV or AOV fails to change state), motors that fail to continue to run (e.g., fans, pumps), transmitters that may not send a sufficiently accurate signal (e.g., pressurizer pressure or steam generator level), solenoid valves which must remain energized or AOVs which must remain pressurized to perform their intended function. Approximately 140

basic events were selected in this manner to represent the component failures which could occur due to a harsh environment for components located inside containment.

A final grouping was undertaken for the basic events that were selected as representing the components and failure modes that could occur due to a harsh environment inside the containment. This final grouping reflects that environmental effects are common cause challenges to the components that are exposed to them. A grouping of identical components that perform the same function was performed so as to recognize that if one component in a group were to fail as a result of harsh environmental conditions, then it was highly likely that the other members of that group that perform the same function also would fail. The 140 basic events representing components inside containment and their failure modes that were assumed to occur due to environmental challenges were placed into the approximately fifty component groups shown in Attachment A. Each component group represents one to eight components and their corresponding harsh-environment-related failure mode.

4. Characterization of the Accident Sequence Environment

The next step in the analysis is to develop the general characteristics of the environment associated with the various accident sequences modeled in the PRA. For the purpose of the case study, the conditions associated with five different accident types are considered in terms of the harsh environment that each may impose on components in the containment. These five accident types each will have an environmental 'profile' (e.g., pressure, temperature, etc. vs time) that can be assumed when considering the response of selected components during these accidents.

Very small LOCA
Small LOCA
Medium/Large LOCA
Steam line break
Feed and bleed

It is noted that several of these accident types represent a number of possible sources of harsh environmental conditions. Small LOCA, reactor coolant pump seal LOCA and stuck open pressurizer SRVs all have similar profiles, for example. For the purpose of the case study, harsh environments due to these events will be tracked as though they would induce similar

environments. The basic events in the cut sets would be used to determine the accident sequences that generate these environments. In addition, it should be recognized that selected accident sequences could result in environments associated with more than one of the above accident sequence types (a steam line break could evolve into a small LOCA through the pressurizer, for example). Each of the above accident sequence types are tracked to help identify which accident sequences may evolve into multiple and/or more severe environmental challenges.

Considering the approximately fifty component groups and their associated failure modes that potentially could occur when exposed to a harsh environment, along with the five environmental 'profiles' defined above, yields roughly 250 component group environmental condition combinations which must be reflected in the case study. Each of these 250 combinations is represented by a unique environmental related basic event and incorporated into the fault trees of the PRA for the case study.

5. Modification to PRA Logic Models to Incorporate Harsh Environment Effects

As noted earlier, failure modes associated with degraded environmental conditions are often modeled implicitly in PRAs. For the purpose of the case study, the PWR PRA used in the analysis was modified such that environmentally induced failure modes were modeled explicitly.

Incorporating the environmental related basic events into the system fault trees was relatively straightforward. First, fault tree logic was created for each of the component groups listed in Attachment A. This fault tree logic is simply represented by the union (OR) of the five environmental basic events for each component group described in the preceding sections. Attachment B shows example environmental fault tree logic for a HPSI MOV. The intersection (AND) of each environmental basic event is taken with a flag[1] representing the environmental challenge. The union of this fault tree logic is then taken with each of the individual basic events that make up the component group.

[1] A "flag" is essentially a house event, used in multi-purpose fault trees to switch model logic "on" or "off" depending on the scenario being analyzed.

For any given accident sequence, the flags associated with a given environmental challenge can be set to True or False depending on the conditions associated with the specific branch being analyzed for that accident sequence. For example, the flag representing a medium or large LOCA would be set to True for all accident sequence branches of the medium or large LOCA event trees. These same flags would be set to False for transient, small LOCA and steam line break event trees. Slightly more complicated to implement are the flag settings for feed and bleed. This flag would need to be set to False at the beginning of transient sequences in which the success of AFW is yet to be determined and yet be set toTrue subsequent to failure of AFW reflecting the initiation of feed and bleed.

The methods for setting flags are dependent on the software used for accident sequence quantification. Most commonly used accident sequence software have provisions for establishing flag settings at any level of the analysis; event tree, accident sequence, fault tree or branch. These existing techniques are sufficient for implementing the case study related harsh environment fault tree logic reflected in Attachment B.

6. Accident Sequence Quantification

On incorporating the harsh environment related logic into the system fault trees for the case study plant, accident sequence quantification was performed. Generation of accident sequence cut sets was performed three ways for different purposes:

- Base case accident sequence quantification in which every component group in the containment is assumed to be qualified.
- Generation of cut sets as a function of the harsh environment basic events depicted in Attachment B.
- Accident sequence quantification selecting an optimal subset of the environmental basic events as candidates for environmental qualification while failing all other environmental related basic events to see how effective the selected subset is in managing safety.

Base case accident sequence quantification

Initial accident sequence quantification was performed much in the same way that the PRA used in the case study is quantified for any application. For the base case, all environmental-related basic events were set to False. Effectively, this is equivalent to assuming that all components in the containment are qualified for a harsh environment.

The quantitative accident sequence results for the base case are shown in Table 1 of Attachment C. The core damage frequency is broken up into accident classes which represent functional accident sequence types that contribute to the potential for core damage.

The internal events core damage frequency for this plant is just over 2E-5/year. It is dominated by small LOCA with failure of injection or recirculation. SGTR events in which the affected steam generator is not isolated and station blackout events round out the top 75% of the core damage frequency for this plant. This distribution of core damage frequency among functional accident sequence type is typical for PWRs.

Cut set generation as a function of harsh environment events

In order to focus on components whose function could be affected by environmental conditions, it is useful to regenerate the cut sets as a function of the environment related basic events. This could be done probabilistically, similar to how the base case accident sequence quantification was performed with the modification that the harsh environment related basic events are set to unity in order to force them into the cut sets without their contributing to truncation. However, an additional method of generating the harsh environment related cut sets also was used.

To focus the analysis on components for which environmental qualification may be an issue, the cut sets were generated using 'deterministic truncation', which was performed simply by counting the number of low probability (e.g., P_f <0.05) random failures that would have to occur before the components potentially affected by a harsh environment would play a role in providing adequate core cooling. If multiple random failures occurred in a cut set, the need to consider other elements corresponding to component that could be affected by environmental conditions was not considered to be significant. On the other hand, combinations of environment-related basic events that lead to core damage by themselves following an initiating event would be important to retain for further evaluation. In this regard, cut sets were generated truncating those with two or more low probability random failures (non-environmental related basic events). The result of this quantification generated more cut sets containing environmental basic events than would be expected if a probabilistic truncation had been performed. These deterministically-generated cut sets were then combined with the cut sets

generated probabilistically to produce final cut sets as a function of harsh environment related events.

The result of this combined probabilistic and deterministic quantification produced over 30,000 cut sets containing up to eleven basic events besides the initiating event. Cut sets containing the environmental basic events such as those shown in Attachment B contain one to five such events.

Selection of a subset of harsh-environment basic events and testing their effectiveness

Not all of the environment-related basic-related events that are found in the cut sets generated above need to be prevented in order to assure a reasonably low core damage frequency. A method for selecting the most important of these harsh-environment basic events is needed. Similar to generating the cut sets as a function of environmental basic events, a probabilistic or a deterministic approach could be taken in identifying a subset effective in managing core damage frequency.

a. Probabilistic selection of environmental basic events

A common probabilistic approach to the identification of important components is to use importance measures. The cut sets produced above reflect the distribution of risk from the original PRA plus a significant additional number of cut sets that are a function of the various harsh environments that may occur throughout the accident sequences. Importance measures were developed based on these combined cut sets. Table 2 of Attachment C shows importance measures for harsh-environment-related basic events. Typically, in importance measure based risk-informed applications, components having a Fussell-Vesely measure greater than 0.5% or a Risk Achievement Worth greater than 2 are candidates for being considered as important [5, 6][2]. (Note that as the harsh environment related events have an assigned failure probability of 1.0, Risk Achievement Worth does not play a role in determining their importance for the case

[2] It is recognized that the environment-related events developed for the case study are common cause events that effectively reflect failure at the system level. The risk significance thresholds for system level common cause events typically are at 5% for the Fussell-Vesely measure of importance and 20 for Risk Achievement Worth [6]. However, as described in Section 4, the component groups were broken up into five separate basic events each representative of a different accident sequence environment. Therefore, component level importance measure thresholds were used in identifying risk significant component groups, as opposed to at the system level, even though use of component level thresholds might be somewhat conservative.

study at this point.) Attachment C Table 2 shows which basic events meet the above criterion: fifteen harsh-environment-related basic events, representing thirteen of the 50 groups of components, are identified by importance measures as being important from a harsh-environment and possible equipment qualification perspective.

A probabilistic test of the effectiveness of the basic events in the thirteen environment groups was performed by regenerating the accident sequence cut sets after setting each of the environmental related basic events in these groups to False (effectively assuming that they were environmentally qualified) and leaving the environmental basic events in the other groups set to a failure probability of 1.0 (assuming that they would fail on exposure to a harsh environment). It should be noted that, in this probabilistic test, if any one of the environmental related basic events for a given component group met risk significance thresholds (e.g., FV > 0.5%), then the components in that group were assumed to be qualified for all environments (e.g., a high importance for very small LOCAs resulted in the assumption that the components would be qualified for very small, medium and large LOCAs, feed and bleed and steam line breaks as well). Attachment C Table 1 shows the results of the accident sequence quantification for this test. The core damage frequency for this case is several times higher than that of the base case. The majority of the increase appears to be associated with transient-initiated events that evolve into sequences in which the containment environment becomes degraded (e.g., feed and bleed) and the larger break size LOCAs. It is clear that lowering the importance measure threshold when selecting environmental related basic events (and place the components associated with those basic events in an equipment qualification program) may be necessary if the core damage frequency is to be maintained near its base case value.

b. Deterministic selection of environmental basic events

An alternate method of identifying important environmental related basic events considers how the cut sets that are a function of these events were generated. A deterministic criterion was used to produce cut sets that included less than two random failures in addition to the environmental events. Those cut sets having two or more random (non-harsh environment related) events were truncated. A similar criterion could be developed for identification of the potentially important environmental basic events. That is, which of the environment-related basic events in the cut sets need to be prevented in order to assure that each cut set is prevented by at least two reasonably low failure probability events?

A method available for the selection of components in such a deterministic manner is Top Event Prevention (TEP) or prevention analysis [7, 8]. Prevention analysis uses Boolean methods to perform a systematic examination of the accident sequence cut sets of a PRA to identify subsets of the basic events found in those cut sets whose collective prevention is effective in maintaining acceptable results (in this case, minimal degradation of CDF with respect to the baseline). Prevention analysis can be probabilistic in nature, deterministic, or a blend of both. If it were possible to guarantee SSC performance absolutely (failure probability =0), the single-failure criterion would be unnecessary, and prevention analysis would dissolve into simple identification of individual success paths. Because it is not possible to guarantee performance absolutely, defense in depth is part of reactor safety practice. Accordingly, prevention analysis allows for formulating prevention criteria in different ways, and identifies combinations of success paths that satisfy the analyst-imposed prevention criterion. The subsets of components (or prevention sets) identified as important to the PRA have several characteristics:

- A prevention set consists of complete paths of equipment which, if they operate successfully, will assure the accomplishment of the safety functions modeled in the PRA. TEP results are presented in terms of success paths, in this regard.
- Each prevention set emerging from TEP is minimal with respect to the prevention criterion. That is, only those components contained in a prevention set are necessary to assure an adequate level of protection from core damage or large early releases. It can be demonstrated that components not included in a prevention set are not important to safety, if all elements of the prevention set receive appropriate treatment.
- Multiple prevention sets are often generated as a part of a TEP analysis. Each prevention set by itself is a complete solution. Only one prevention set need be selected to identify the success paths that are important to preventing core damage or large early releases.

As noted above, a deterministic defense-in-depth related criterion was implemented for the identification of harsh-environment related basic events that were important to the results of the PRA for the case study. In this regard, cut sets were considered to be adequately prevented if two or more low-probability failures were required for any given initiating event before core damage would occur. In the application of TEP to the cut sets of the PRA, events credited toward prevention of each cut set included not only random failures but harsh environment related basic events as well.

Application of TEP to the case study yielded more than 180,000 prevention sets. Each prevention set was over 400 basic events in length. *(Note that the PRA was modularized before accident sequences quantification, so many "basic events" are modules actually containing multiple basic events).* Prevention sets generally contain many basic events each, because each prevention set represents a combination of success paths, and each success path consists of many individual components. Given the prevention-set criterion that each cut set should be prevented by at least two failures, the case study prevention sets each comprise at least two success paths for each initiating event.

Within each prevention set is a combination of random failures and basic events representing failure of components due to harsh environmental conditions that were added as described in the preceding sections. The number of environment-related basic events in the prevention sets ranges from 45 to 52. For purposes of illustration, a prevention set was selected having the lowest number of harsh-environment-related basic events. These 452 events represent 17 of the original component groups defined in Attachment A. Attachment A notes which of the component groups are found in the selected prevention set.

A probabilistic test of the effectiveness of preventing the 45 harsh-environment related basic events in the selected prevention set was performed by regenerating the accident sequence cut sets after setting each of the selected basic events to False (effectively assuming that they were environmentally qualified) and leaving the remaining environmental basic events set to a failure probability of 1.0 (assuming that their failure was guaranteed on exposure to a harsh environment). Note that, in this sensitivity study, only those environmental related events in the prevention sets were credited in the analysis. In other words, if a component were assumed to be qualified for a small LOCA, then it may also be qualified for a very small LOCA environment but it would not necessarily be qualified for a steam line break , medium or large LOCA. Table 1 of Attachment C shows the results of the accident sequence quantification for this test. It is noted that the core damage frequency is within 10% of the base case core damage frequency, suggesting that the selected components would be successful in managing core damage risk were they to be subject to an environmental qualification program that was effective in preventing them from failing if exposed to a harsh environment. This is not necessarily the most effective prevention set; it was simply chosen for illustration.

7. Explanation of the results

Of the roughly fifty component groups located in the containment of the case study plant that potentially could be affected by harsh environmental conditions during various accident sequences considered in the internal events PRA, only seventeen of the groups appear to be important with respect to maintaining the core damage frequency at an acceptable level, assuming adoption of the overall prevention strategy implied by selection of the particular prevention set selected in the preceding section. It is these seventeen component groups for which margin with respect to qualification of the equipment to withstand the expected harsh environments may be most valuable or, alternately, for which development of an environmental fragility curve may be useful.

a. Component groups for which qualification margin may be worthwhile

The following discusses the seventeen component groups and the reasons that a characterization of the behavior of the components within these groups under harsh conditions may be worthwhile.

Steam generator instrumentation

Two sets of steam generator level transmitters are shown to be important with respect to environmental qualification. The first set is responsible for automatic actuation of auxiliary feedwater, whereas the second set is associated with the feedwater control system and is credited in the PRA only as backup instrumentation used by the operators to manually initiate makeup to the steam generators in the event that automatic actuation does not occur. The accident sequence environment for which qualification of this instrumentation is important is associated with small LOCAs and steam line breaks inside containment. *(Note that the feedwater-related steam generator level instrumentation is a backup to the AFW related automatic instrumentation. A sensitivity study might show that the backup instrumentation may be significantly less important to qualify for harsh environments than the automatic instrumentation).*

Steam generator pressure instrumentation is used to isolate the steam generators during a steam line break. Failure to isolate the steam generators results in loss of the steam supply to the turbine driven AFW pump. *(Note that this steam generator pressure instrumentation is*

required only immediately following the initiating event, and is not required to function for a significant period of time under harsh environmental conditions).

Feed and Bleed

The PORVs and pressurizer block valves are required to support feed and bleed operation. As this plant normally operates with the block valves closed, it is necessary to open them to initiate feed and bleed. The initiating events for which the environment would be degraded before block valves were opened are small LOCA and steam line breaks inside containment. The accident sequences in which the PORVs would be required to operate include small LOCA, steam line breaks and feed and bleed operation itself. *(Note that it is not clear when during a steam line break or small LOCA feed and bleed would need to be initiated. Also, PORVs would be required to be functional throughout the rest of the event, once feed and bleed was initiated).*

Letdown isolation

Charging and letdown are normally aligned during power operation. If charging were to be lost during a transient, then isolation of letdown would be required. Accident sequences in which letdown isolation would have to occur in a degraded environment include steam line breaks inside containment. Failure to isolate letdown in this situation would lead to a very small LOCA in addition to the steam line break. *(Note: This is a very slowly evolving accident at worst, and may be able to be dismissed deterministically).*

Reactor inventory control

Both cold-leg injection and hot-leg injection are assumed to be required for LOCAs. Cold-leg injection is the primary means of makeup to the reactor from HPSI during small breaks and during recirculation for the entire break spectrum. Hot-leg injection is assumed to be required long term following a large LOCA to avoid boron precipitation and plate out on the fuel assemblies during recirculation. *(Note that precipitation of boron on fuel assemblies may cause limited blockage and fuel damage, but is not likely to result in widespread core damage).*

Pressurizer pressure is important in assuring reactor inventory control, as it is the primary means of actuating safety injection for the entire range of breaks in the LOCA spectrum. *(Note that pressurizer pressure initiation of safety injection is required early in the event and is not needed once actuation has taken place.)*

Containment control

Either containment coolers or containment sprays are sufficient as the primary means of long term decay heat removal following LOCAs and transients in which feed and bleed is initiated. Failure of containment heat removal can result in heat up of the containment sump water, NPSH problems during recirculation, and long term containment pressure failure. Components from both systems are shown to need safety margin with respect to environmental qualification in the prevention analysis (fans and service water supply and return valves for the containment coolers, pressure sensors for the containment spray system). That both systems are needed for defense-in-depth reasons is due to selected initiating events that defeat a single division of each (loss of a specific AC bus, for example, can result in failure of sufficient coolers that containment spray is the only effective containment heat removal system that remains and vise versa. *(Note that containment coolers would be required to operate throughout the event. Containment pressure sensors, however, are located outside containment and only the internal portion of the sensor exposed to the containment atmosphere, and not the external electronics, would be subject to a harsh environment).*

Large containment penetrations need to be qualified for the environment in containment following LOCAs and feed and bleed operation not just for containment isolation purposes, but in the Level 1 PRA in order to maintain containment overpressure in support of an adequate NPSH during recirculation. *(Note that containment penetrations would need to remain intact throughout the duration of the accident).*

b. Component groups not needing significant qualification margin

Equally important in determining the need for margin is an understanding of the reasons selected component groups do not contribute significantly to the core damage frequency if it assumed that they are not qualified. In this regard there are several component groups that do not appear in the selected prevention set.

Shutdown cooling

For the case study plant, shutdown cooling plays a role in two types of accident sequences.

The first is in preventing the need to make up to the condensate storage tank to maintain AFW operation. This plant has a relatively small CST, and cooling down and aligning shutdown cooling can avoid the need for CST makeup. Cool down and alignment of SDC takes place without a degraded environment in containment, and none of the environmental related basic events appear in these accident sequences.

The second shutdown cooling related scenario is for SGTR sequences in which equalization of reactor and steam generator pressure is not accomplished. Eventual cool down and alignment of shutdown cooling is needed for the sequences before the refueling water storage tank is depleted. As the primary coolant inventory loss is not into the containment for this sequence, no harsh environment exists and environmental qualification plays little role.

Reactor pressure control

Pressurizer sprays are associated with a number of component groups that could be exposed to a harsh environment inside containment. While pressurizer spray facilitates controlled cooldown of the reactor, it is not necessary for achieving a safe stable state following a transient. The accident sequences for which pressurizer spray plays its most significant role is during SGTR in support of reducing reactor pressure to near that of the affected steam generator. Again, because primary coolant loss is not into the containment for SGTR, there is little degradation of the environment that would keep pressurizer spray components from providing their safety function.

Reactor inventory control (charging)

At the case study plant, the charging system has a relatively low capacity (~100gpm) and is not capable of making up for small LOCA or larger break sizes. However, for very small LOCA (less than the capacity of charging pumps) the charging system can serve as an additional high pressure injection system. Charging to the reactor is typically aligned during normal plant operation. No components need to change position in order to provide the reactor inventory function during should a very small LOCA occur. As charging components inside containment are normally aligned for the reactor inventory makeup function, no environmental challenges are likely to affect the system's ability to perform this function.

Reactor inventory control (low pressure injection)

LPSI MOVs are located inside containment and would need to open to support the low pressure injection function during a medium or large LOCA. However, best estimate analysis for the case study plant shows that HPSI in conjunction with initial injection from accumulators will provide adequate core cooling. As HPSI is necessary for the small end of the LOCA break spectrum and as it also can be aligned for recirculation, LPSI injection MOVs simply provide a redundant backup to injection from HPSI.

8. Summary and Conclusions

A methodology has been developed for the purpose of identifying the minimum set of SSCs in a nuclear power plant that need to remain functional when exposed to a harsh environment following an accident. The methodology has been demonstrated for the components located inside containment using a full scope Level 1 internal events PRA for a PWR with a large dry containment.

In performing the demonstration, equipment located inside the containment that could be affected by harsh environments or aging were binned into roughly fifty component groups where a component group was defined as identical components having the same failure mode. Each component group represented one to eight components, including not only equipment with a specific tag id but all supporting hardware or parts that are necessary for the component to perform its function (e.g., junction boxes, power and control cables, penetration assemblies, etc.).

On defining the component groups, a simple characterization of the various accident sequence environments to which equipment inside the containment might be exposed was developed. Accident sequence environment characterization included that from the full spectrum of LOCAs, steam line breaks, and consequential events such as reactor coolant pump seal LOCAs and feed and bleed operation.

Generation of accident sequence cut sets as a function of the component groups and their environmental challenges was performed using the PRA for the case study plant. With these cut sets as input, a minimal prevention set of component groups was then selected, whose implementation would entail formal equipment qualification: that is, demonstrating the ability of

the components within the group to remain functional following exposure to a harsh environment is of significant importance. For purposes of comparing methodologies, this selection was done in two different ways: one way based on traditional importance measures, and the other way using a method called 'prevention analysis.'

Prevention analysis suggested that within one candidate strategy, only seventeen of the original fifty component groups potentially exposed to harsh environmental conditions in the containment for the case study plant need to be qualified to function in these harsh environments. (Prevention analysis presents the decision-maker with different strategic options; the present discussion is based on selection of the strategy requiring EQ of the smallest number of component groups.) Verification of the effectiveness of this subset of the component groups in maintaining an acceptably low core damage frequency was performed by assuming that *all* of the components in *all* of the non-selected component groups failed when exposed to a harsh environment. Making this assumption and regenerating the accident sequence results of the PRA resulted in an increase in core damage frequency of less than 10%, demonstrating that the components within the selected sixteen component groups suffice to be successful in managing core damage risk, if they are subject to an environmental qualification program that is effective in preventing them from failing if exposed to a harsh environment. The analogous exercise performed on the importance-measure-based selection of component groups demonstrated much less successful control of EQ-related core damage frequency.

The components in the seventeen component groups not only are those for which implementation of an environmental qualification program is worthwhile, but are components for which demonstrating margin on the capability of the components to remain functional when exposed to the various harsh environments may be of value. Alternately, characterizing the fragility of the components within these groups to the environmental conditions (temperatures, pressures, humidity, etc.) to which the components may be exposed during an accident may be worthwhile. Regardless, with respect to the component groups that were *not* selected as a part of this case study, it is concluded that the rigor to which environmental qualification is applied to components within these groups appears to be of relatively low importance, nor do these components require significant margin with respect to environmental challenges and/or aging.

This approach is conservative in the sense that the model assumes that if any component in a given group fails as a result of a harsh environment, the whole group fails. Otherwise, the result is as valid and complete as the underlying PRA (in this case, the plant's PRA). It is also stressed that for purposes of illustration, this exercise focused on one particular strategic option offered by prevention analysis; there might be a better option out there, requiring more EQ but having compensating advantages that are beyond the scope of this report.

While the case study was limited to just those components located inside containment, the proposed approach is sufficiently straightforward that it can be applied to any component types located in a nuclear power plant that may be exposed to harsh environmental conditions during an accident or subject to aging. The methodology is sufficiently systematic that the specific accident sequences that result in the need for qualification of individual components, and hence their associated environmental conditions, can be identified. Just as important, the method supports development of the engineering rationale as to why components are or are not selected as being important from an aging perspective or during harsh environmental conditions. Using the methodology of this case study, this engineering rationale can be documented in terms of plant specific design features and operating characteristics that drive the results.

9. References

1. 10 CFR 50.49, “Environmental qualification of electric equipment important to safety for nuclear power plants.”
2. Regulatory Guide 1.89, Rev. 1, “Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plant”, 1984.
3. IEEE Standard 323-1983, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”
4. Regulatory Guide 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” June 2006.
5. NUMARC 93-01.Rev. 2, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", April 1996.
6. NEI 00-04, Rev 0, “10CFR50.69 SSC Categorization Guideline”, 2005.
7. R. W. Youngblood, “Applying Risk Models To Formulation Of Safety Cases,” Risk Analysis 18, No. 4, p. 433, August 1998.
8. R. A. White and D. P. Blanchard, Development of a Risk-Informed IST Program at Palisades Using Top Event Prevention, Proceedings of ICONE10, April 2002.

Attachment A Component Groupings

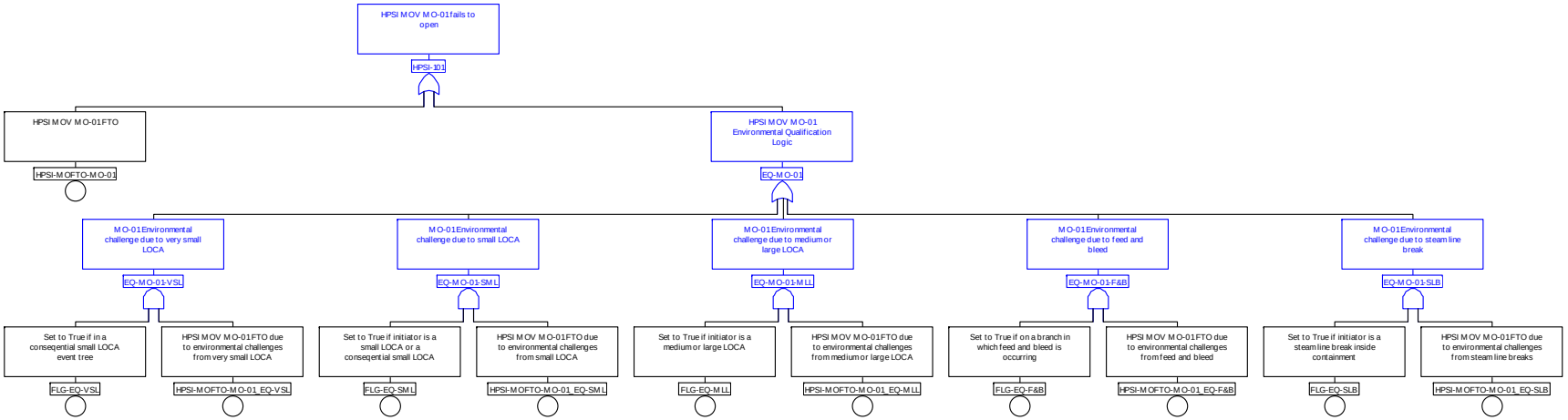
This table lists component groups and failure modes considered in this case study. The columns on the right indicate whether a given group was selected for EQ within the two methods applied (importance measures and prevention analysis); refer to Attachment C, Table 1.

Component Group / Failure Mode			*Importance Measures*	*Prevention Set*
Auxiliary feedwater				
	SG level transmitters AFW actuation	Fail to function	✓	✓
	SG level transmitters Feedwater control (operator information)	Fail to function	✓	✓
	Pressure transmitter Steam generator isolation	Fails to function		✓
Shutdown cooling				
	MOV Shutdown cooling	Fails to open		
	Limit switch LPSI MOV	Fails to remain closed		
	Pressure transmitter LPSI suction	Fails to function		
Reactor Pressure Control				
	AOV Pressurizer spray	Fails to open		
	AOV Pressurizer spray	Fails to remain open		
	Solenoid valve Pressurizer spray	Fails to energize		
	Solenoid valve Pressurizer spray	Fails to remain energized		
	Pump Primary coolant	Fails to run		
	Block valve Pressurizer	Fails to open		✓
	PORV Pressurizer	Fails to open		
	PORV Pressurizer	Fails to remain open		✓
	Pressure transmitter Pressurizer (operator information)	Fail to function		
Reactor inventory control (charging/letdown)				
	AOVs Letdown flow	Fail to open		
	AOVs Letdown isolation	Fail to close	✓	✓
	AOVs Letdown flow	Fail to close	✓	

Component Group / Failure Mode			*Importance Measures*	*Prevention Set*
	AOVs Charging makeup	Fail to close		
	AOVs Charging makeup	Fail to remain closed		
	E/P transducer Letdown flow	High output		
	E/P transmitter Letdown flow	Fails to function		
	Solenoid valve Letdown flow	Fail to deenergize	✓	✓
	Solenoid valve Letdown isolation	Fail to energize	✓	
	Solenoid valve Charging makeup	Fail to energize		
	Solenoid valve Letdown flow	Fail to energize		
	Solenoid valve Charging makeup	Fail to remain energized		
	Temperature element Letdown htx	Fails to function	✓	
	Level transmitter Pressurizer	Fails to function		
	Pressure transmitter Letdown pressure	Fails to function		
	E/P transmitter Letdown control	Fail to function		
	Valve position controller Letdown control	Fail to function		
Reactor inventory control (safety injection)				
	Limit switch HPSI MOV	Fails to close		
	Limit switch HPSI MOV	Fails to remain closed		
	MOV Hot-leg injection	Fails to open		✓
	MOV Cold-leg injection	Fails to open	✓	✓
	MOV Hot-leg injection	Fails to close		✓
	MOV LPSI	Fails to open		
	Pressure transmitter Pressurizer	Fails to function	✓	✓
	MOV SIT	Fails to remain open		

Component Group / Failure Mode			*Importance Measures*	*Prevention Set*
Containment control				
	Fan Containment cooler	Fail to start		
	Fan Containment cooler	Fail to run	✓	✓
	AOVs SWS to containment coolers	Fail to open	✓	✓
	Solenoid Valve SWS to containment coolers	Fail to deenergize	✓	✓
	Pressure Transmitter Containment pressure		✓	✓
	Radiation monitor Containment	Fail to remain energized		
	Seal Equipment hatch	Fails to remain closed		✓
	Hatch Fuel transfer tube	Fails to remain closed		✓
	Flange ILRT penetration	Fails to remain closed		

Attachment B Example Environmental Qualification Fault Tree Logic



Attachment C
Table 1 Accident Sequence Quantification Results

Accident Sequence Type	*Base case CDF (1/yr)*	*Qualify components selected using importance measures* CDF (1/year)*	*Qualify components selected using prevention analysis* CDF (1/year)*
Transient with reactor at high pressure and failure of injection	1.7E-6	5.9E-5	1.7E-6
Transient with reactor at high pressure and failure of recirculation	8.4E-7	3.3e-6	8.4E-7
Station Blackout	2.9E-6	2.9E-6	2.9E-6
Containment Heat Removal Failure	9.5E-7	9.5E-7	9.8E-7
LOCA with reactor at high pressure and failure of injection	5.2E-6	6.3E-6	5.8E-6
LOCA with reactor at high pressure and failure of recirculation	4.1E-6	2.2E-5	5.0E-6
LOCA with reactor at low pressure and failure of injection	2.2E-7	3.4E-5	2.8E-7
LOCA with reactor at low pressure and failure of recirculation	1.7E-6	4.3E-5	1.7E-6
Anticipated Transient without SCRAM	6.9E-8	6.9E-8	6.9E-8
Steam Generator Tube Rupture	6.0E-6	6.0E-6	6.0E-6
LOCA Outside Containment	1.7E-8	1.7E-8	3.9E-8
Total	2.4E-5	1.8E-4	2.5E-5

*Accident sequence quantification performed with all environmental failure basic events having high importance or in the selected prevention set to False (as though they were qualified) and the remaining environmental failure basic events failed ($P_f = 1.0$).

Attachment C
Table 2 Environmental Basic Event Importance Measures

Note 1: These importance measures were calculated with basic event probability set to 1.
Note 2: **Bold** cells meet risk significance threshold. If any member of a component group is risk significant, then environmental qualification for all environments is assumed in generating the results in the importance measures related column of Table 1.

Component Group / Failure Mode Environment		*Importance Fussell-Vesely*
Auxiliary feedwater		
SG level transmitters AFW actuation	AFW-TLMT-LT-AFW_EQ-F&B	4.4E-03
	AFW-TLMT-LT-AFW_EQ-SLB	**3.1E-02**
	AFW-TLMT-LT-AFW_EQ-SML	**1.3E-01**
	AFW-TLMT-LT-AFW_EQ-VSL	9.5E-04
SG level transmitters Feedwater control (operat or info)	AFW-TLMT-LT-FW_EQ-F&B	4.5E-03
	AFW-TLMT-LT-FW_EQ-SLB	**3.0E-02**
	AFW-TLMT-LT-FW_EQ-SML	**1.2E-01**
	AFW-TLMT-LT-FW_EQ-VSL	9.4E-04
Pressure transmitter Steam generator isolation	MFW-TPMT-PT-SG_EQ-F&B	2.8E-05
	MFW-TPMT-PT-SG_EQ-SLB	2.1E-04
	MFW-TPMT-PT-SG_EQ-SML	3.5E-03
Shutdown cooling		
MOV Shutdown cooling	LPI-MVMA-MO-SDC_EQ-SLB	2.3E-03
	LPI-MVMA-MO-SDC_EQ-SML	1.2E-05
	LPI-MVMA-MO-SDC_EQ-VSL	3.7E-04
Pressure transmitter LPSI suction	LPI-TPMT-PT-SDC_EQ-SLB	2.3E-03
	LPI-TPMT-PT-SDC_EQ-SML	1.2E-05
	LPI-TPMT-PT-SDC_EQ-VSL	3.7E-04
Reactor pressure control		
Block valve Pressurizer	PRV-MVMA-MO-BLK_EQ-F&B	3.0E-03
	PRV-MVMA-MO-BLK_EQ-SLB	6.8E-04
	PRV-MVMA-MO-BLK_EQ-SML	9.6E-04
	PRV-MVMA-MO-BLK_EQ-VSL	3.0E-05
PORV Pressurizer	PRV-RVMD-PRVPORV_EQ-F&B	3.0E-03
	PRV-RVMD-PRVPORV_EQ-SLB	6.8E-04
	PRV-RVMD-PRVPORV_EQ-SML	9.6E-04
	PRV-RVMD-PRVPORV_EQ-VSL	3.0E-05
	PZR-AVMD-CV-PZRSP_EQ-SML	5.8E-07
AOV Pressurizer spray	PZR-KVMC-SV-2117_EQ-SML	5.8E-07
Pump Primary coolant	PZR-PMMG-P-5PCP_EQ-SML	1.7E-06
Reactor inventory control (charging/letdown)		
AOVs/SVs Charging makeup	CVC-AVMC-CV-CHG_EQ-SML	5.8E-07
	CVC-KVMC-SV-CHG_EQ-SML	5.8E-07
AOVs/SVs	**CVC-AVMB-CV-2003_EQ-SLB**	**9.1E-02**

Component Group / Failure Mode Environment		*Importance Fussell-Vesely*
Letdown isolation	CVC-AVMB-CV-2003_EQ-VSL	3.0E-03
	CVC-KVMA-SV-2003_EQ-SLB	**9.1E-02**
	CVC-KVMA-SV-2003_EQ-VSL	3.0E-03
AOVs/SVs Letdown isolation	**CVC-AVMC-CV-2001_EQ-SLB**	**5.9E-02**
	CVC-KVMC-SV-2001_EQ-SLB	**5.9E-02**
Temp element Letdown htx	**CVC-TEMT-TE-0201_EQ-SLB**	**5.9E-02**
E/P transducer Letdown flow	CCS-EPMT-E/P-0203_EQ-SLB	5.7E-04
Valve pos controller Letdown control	CCS-PCMT-POC-0909_EQ-SLB	5.7E-04
AOVs/SVs Letdown flow	CVC-AVMA-CV-LTDN_EQ-SLB	1.2E-05
	CVC-KVMB-SV-LTDN_EQ-SLB	1.2E-05
Level transmitter Pressurizer	CVC-TLMT-LT-PZR_EQ-SLB	1.9E-03
	CVC-TLMT-LT-PZR_EQ-VSL	1.3E-04
Reactor inventory control (safety injection)		
MOV Cold-leg injection	HPI-MVMA-MO-HPSI_EQ-F&B	3.0E-03
	HPI-MVMA-MO-HPSI_EQ-MLL	3.8E-03
	HPI-MVMA-MO-HPSI_EQ-SLB	2.0E-03
	HPI-MVMA-MO-HPSI_EQ-SML	**1.2E-01**
	HPI-MVMA-MO-HPSI_EQ-VSL	1.6E-03
MOV Hot-leg injection	HPI-MVMA-MO-HLI_EQ-MLL	3.8E-03
	HPI-MVMB-MO-HLI_EQ-MLL	3.8E-03
MOV LPSI	LPI-MVMA-MO-LPSI_EQ-SLB	2.3E-03
	LPI-MVMA-MO-LPSI_EQ-SML	1.2E-05
	LPI-MVMA-MO-LPSI_EQ-VSL	3.7E-04
Pres transmitter Pressurizer	SIS-TPMC-PT-PZR_EQ-F&B	1.6E-03
	SIS-TPMC-PT-PZR_EQ-MLL	4.2E-03
	SIS-TPMC-PT-PZR_EQ-SLB	**1.8E-01**
	SIS-TPMC-PT-PZR_EQ-SML	**1.6E-01**
	SIS-TPMC-PT-PZR_EQ-VSL	1.4E-03
Containment control		
Fan Containment cooler	CAC-FNMG-V-1CAC_EQ-F&B	5.9E-04
	CAC-FNMG-V-1CAC_EQ-MLL	3.9E-03
	CAC-FNMG-V-1CAC_EQ-SLB	1.1E-03
	CAC-FNMG-V-1CAC_EQ-SML	1.2E-01
	CAC-FNMG-V-1CAC_EQ-VSL	9.4E-04
AOVs SWS to cont coolers	CAC-AVMA-CV-SWS_EQ-F&B	5.9E-04
	CAC-AVMA-CV-SWS_EQ-MLL	3.9E-03
	CAC-AVMA-CV-SWS_EQ-SLB	1.1E-03
	CAC-AVMA-CV-SWS_EQ-SML	**1.2E-01**
	CAC-AVMA-CV-SWS_EQ-VSL	9.4E-04
Solenoid Valve SWS to cont coolers	CAC-KVMA-SV-SWS_EQ-F&B	5.9E-04
	CAC-KVMA-SV-SWS_EQ-MLL	3.9E-03
	CAC-KVMA-SV-SWS_EQ-SLB	1.1E-03
	CAC-KVMA-SV-SWS_EQ-SML	**1.2E-01**
	CAC-KVMA-SV-SWS_EQ-VSL	9.4E-04
Pres Transmitter	CHP-PSMT-CONT_EQ-F&B	2.7E-03

Component Group / Failure Mode Environment		*Importance Fussell-Vesely*
Cont pressure	**CHP-PSMT-CONT_EQ-MLL**	1.5E-02
	CHP-PSMT-CONT_EQ-SLB	4.4E-03
	CHP-PSMT-CONT_EQ-SML	4.7E-01
	CHP-PSMT-CONT_EQ-VSL	3.5E-03
Seal Equipment hatch	CIS-GKMJ-HATCH_EQ-F&B	3.1E-04
	CIS-GKMJ-HATCH_EQ-MLL	1.1E-04
	CIS-GKMJ-HATCH_EQ-SLB	6.2E-05
	CIS-GKMJ-HATCH_EQ-SML	3.9E-03
	CIS-GKMJ-HATCH_EQ-VSL	4.6E-05
Hatch Fuel transfer tube	CIS-GKMJ-MZ-18_EQ-F&B	3.1E-04
	CIS-GKMJ-MZ-18_EQ-MLL	1.1E-04
	CIS-GKMJ-MZ-18_EQ-SLB	6.2E-05
	CIS-GKMJ-MZ-18_EQ-SML	3.9E-03
	CIS-GKMJ-MZ-18_EQ-VSL	4.6E-05