Risk-Informed Safety Margin Characterization Case Study: Use of Prevention Analysis in the Selection of Electrical Equipment to Be Subjected to Environmental Qualification

D. P. Blanchard[a] and R. W. Youngblood[b]
[a]Applied Reliability Engineering, Inc. (AREI), San Francisco, California USA*
[b] Idaho National Laboratory (INL), Idaho Falls, Idaho, USA

Abstract: Age-related degradation of electrical equipment is cited in numerous discussions of extended nuclear power plant operation as an important issue. Which SSCs matter? For which SSCs do we need ongoing assurance of performance? Replacement of all components and cables is a daunting prospect. Being able to focus on a subset of SSCs from an environmental qualification (EQ) perspective, while still maintaining plant-level safety and efficiency even if the other components and cables degrade, would be worthwhile.

This paper summarizes a case study that examines SSC aging for components within a PWR large dry containment. The case study illustrates how an understanding of SSC margin can be characterized given the overall integrated plant design, and was developed to demonstrate a method for deciding on which SSCs to focus, which SSCs are not so important from an environmental qualification margin standpoint.

The method chosen for selection of SSCs important to aging and environmental challenges is known as Top Event Prevention (TEP) or Prevention Analysis. TEP is a Boolean method for optimal selection of SSCs (that is, those combinations of SSCs both necessary and sufficient to meet a predetermined selection criterion) and allows demonstration that plant-level safety can be maintained by the collection of selected SSCs alone.

Keywords: Prevention Analysis, TEP, environmental qualification, RISMC

1. INTRODUCTION

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 as well as numerous non-safety electrical equipment that may be exposed to such environments with the intent of assuring that those components are capable of performing their intended functions given the environmental challenge [1-4].

As licensees consider operating their plants well beyond the original license term, equipment aging becomes an increasingly important issue, including age-related degradation of components and cables (such that they become more susceptible to harsh environments). The DOE's Light Water Reactor Sustainability (LWRS) program includes a Risk Informed Safety Margin Characterization (RISMC) effort that considers system, structure and component (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.

* *dblanchard@ar-eng.com*

In order to examine SSC aging from an environmental qualification perspective, a case study was defined [5] that illustrates how the state of knowledge regarding SSC margin can be characterized given the overall integrated plant design. The case study demonstrates 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 paper summarizes the results of that case study.

The approach taken in performing this evaluation was relatively straightforward and included the following four steps:

Identify components explicitly modeled in the internal events probabilistic risk assessment (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 the case study, the latter step was performed through use of Top Event Prevention (TEP) or Prevention Analysis, a technique based on Boolean optimization. An overview of the TEP methodology is presented in Attachment 1 along with a simple example. A test of the effectiveness of the subset of SSCs selected by TEP along with a comparison with more traditional importance measures demonstrates certain important advantages of TEP for this environmental qualification related application.

2. CASE STUDY PLANT DESCRIPTION

The plant selected for the case study is a two-loop pressurized water reactor (PWR) with a large dry containment.

Case Study Plant Systems

The plant has two steam driven feedwater pumps and three auxiliary feedwater (AFW) pumps (two motor and one turbine driven). Primary system pressure relief includes three code safeties and two large power operated relief valves (PORVs), either one capable of supporting feed and bleed operation. Reactor inventory control consists of three low volume charging pumps, two high pressure safety injection (HPSI) pumps and three low pressure safety injection (LPSI) pumps. Containment heat removal consists of three fan coolers (CAC) and two containment spray (CSS) trains.

Support systems include two essential buses normally aligned to offsite power and backed up by two automatic emergency diesel generators (EDG) and one manually operated diesel that can be aligned to either bus.

Case Study Plant PRA

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

- 50 initiating events (including the following, some of which may lead to harsh environments)
  - Four ranges of loss of coolant accident (LOCA) break sizes
  - Steam line breaks (inside and outside containment)
  - Steam generator tube rupture (SGTR)
  - Interfacing system LOCA
  - Transients (with the potential for feed and bleed operation)
    - Turbine trips, Loss-of-feedwater (LOFW), etc.
    - Loss of support systems (service water (SW), instrument air (IA)),etc
    - Loss of ac buses (essential and non-essential)
    - Loss of instrument ac buses, dc buses

- Consequential initiating events
  - Transient induced LOCA (e.g., primary coolant pump seal LOCAs, pressurizer safety relief valve (SRV) challenges, failure of letdown isolation)
  - Transient induced steam line breaks (e.g., stuck open steam dump valves)

- 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 and
  - Control room indication for credited operator actions

3. IDENTIFICATION OF COMPONENT GROUPS

The first step in the case study is to identify all of the individual components explicitly modelled 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.

<u>Major active components</u>
- Motor operated valves
- Air operated valves
- Solenoid valves
- PORVs

<u>Major rotating equipment</u>
- Pump motors
- Fans

<u>Instrumentation</u>
- Transmitters
- Switches
- Temp elements
- Signal converters

<u>Miscellaneous</u>
- Power supplies
- Penetration seals

It should be noted that there are many components and their failure modes that are not explicitly modelled in the PRA but are effectively selected for inclusion in the case study as a result of their association with the components that are modelled. 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.

Approximately 140 basic events were selected in this manner to represent the component failures that 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 Table 1. 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 was to develop the general characteristics of the environment associated with the various accident sequences modelled 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., versus time) that can be assumed when considering the response of selected components during these accidents.

LOCAs - Very Small, Small, Medium/Large
Steam line break
Feed and bleed

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. 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 twice, once to produce the accident sequence results as a function of environmental-related events and the second time to test the effectiveness of a minimal set of component groups selected for qualification.

5.1 Initial Accident Sequence Quantification

Initial accident sequence quantification was performed in the same manner that the PRA is quantified for any application. In order to focus on components whose function could be affected by environmental conditions, however, it is useful to regenerate the cut sets as a function of the environment related basic events. This was accomplished by setting the 250 environmental qualification events to unity and regenerating the cut sets. Tens of thousands of additional cut sets were generated over those resulting from the base case PRA with up to eleventh order cut sets that included environmental-related basic events.

5.2 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. A probabilistic or a deterministic approach could be taken in identifying a subset effective in managing core damage frequency.

Probabilistic Selection Of Environmental Basic Events

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 the cut sets that were a function of environmental-related 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 [6, 7]. (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 study.) 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). Table 2 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 PRA. 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.

Deterministic Selection Of Environmental Basic Events

An alternate method of identifying important environmental related basic events employs a deterministic criterion for selection of important events in the PRA. A method available for the selection of components in such a deterministic manner is Top Event Prevention (TEP) or Prevention Analysis [8-14]. TEP 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). A TEP analysis can be probabilistic in nature, deterministic, or a blend of both. 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.

- 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. The criterion employed was similar to the single failure criterion. 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. For an environmental-related basic event to be considered low in probability, the components in that group would need to be subject to an environmental qualification program.

Application of TEP to the case study yielded more than 180,000 prevention sets. Each prevention set was over 400 basic events in length. 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. For purposes of illustration, a prevention set was selected having the lowest number of harsh-environment-related basic events. These environmental-related events in the selected prevention set represented 17 of the original component groups defined in Table 1. Table 1 notes which component groups are found in the selected prevention set.

A probabilistic test of the effectiveness of preventing the selected 17 groups of harsh-environment related events 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). Table 2 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.

6. 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.

6.1 Component Groups For Which Qualification Margin May Be Worthwhile

The following discusses a few the seventeen selected component groups and the reasons that a characterization of the behaviour of the components within these groups under harsh conditions may be worthwhile. Note that some of the groups are non-safety related and perform functions that are considered to be beyond the design basis.

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. 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 are required to support feed and bleed operation. 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 PORVs would be required to be functional throughout the rest of the event, once feed and bleed was initiated.)

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. 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.)

6.2 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.

Reactor pressure control

Pressurizer sprays are 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 (low pressure injection)

LPSI motor operated valves (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.

7. 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.).

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 known as TEP.

TEP 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. (TEP 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 seventeen 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.

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.

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”, U.S. Nuclear Regulatory Commission, 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,” U.S. Nuclear Regulatory Commission, June 2006.

[5] 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 and R. Youngblood, April 2012.

[6] NUMARC 93-01.Rev. 2, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", April 1996.

[7] NEI 00-04, Rev 0, “10CFR50.69 SSC Categorization Guideline”, 2005.

[8] R. W. Youngblood, “Applying Risk Models To Formulation Of Safety Cases,” Risk Analysis 18, No. 4, p. 433, August 1998.

[9] J. R. Schaefer, R. B. Worrell, P. Szetu, “Implementation of an Air-Operated Valve Program at Northern States Power Company”, 8th International Conference on Nuclear Engineering (ICONE8), April 2000.

[10] 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.

[11] P. Szetu, S. Hesler and W. Reuland, “Risk-Informed Turbine Missile Analysis for a BWR 4”, Proceedings of PSA '05, Sep 2005.

[12] G. B. Varnado , R. B. Worrell, and D. P. Blanchard, “Risk-Informed Physical Security”; Dynamic Allocation of Resources, Proceedings of PSA '05, Sep 2005

[13] B. A. Brogan, R. B. Worrell and D. P. Blanchard, “Focusing the Circuit Analysis Effort in Transitioning to NFPA-805 using Top Event Prevention (TEP)”, Proceedings of PSA ’08, Sep 2008.

[14] R. Torok and D. Blanchard, “Risk Insights Associated with Digital Upgrades”, PSAM10, June 2010.

Table 1: 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 TEP); refer to Table 2.

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	✓	
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	Fail to deenergize	✓	✓

Component Group / Failure Mode			*Importance Measures*	*Prevention Set*
	Letdown flow			
	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		
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		

Table 2: 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 TEP*[*] *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 1 – Overview of Top Event Prevention Analysis (TEP)

Definitions and general concepts associated with Top Event Prevention analysis and the generation of prevention sets are described in this attachment. An overview of the steps in the TEP process is provided along with a simple example.

General Concepts and the Steps in TEP

Regardless of how it is obtained, the Boolean expression under consideration will be called **the top event expression**, and we will assume it takes the form of its minimal cut sets. **A prevention set** is a collection of basic events which, if they all do not occur, precludes the occurrence of the top event. Thus, a prevention set contains at least one basic event from every top event minimal cut set. A prevention set is **minimal** if it ceases to be a prevention set when any of its basic events are removed.

The idea of prevention sets can be extended to include a level of prevention. A **prevention set of level L** contains at least L basic events from each top event minimal cut set, and it is **minimal** if it ceases to be a prevention set of level L when any of its events are removed. Besides specifying a level of prevention, one can indicate which of the basic events are to count toward the prevention level. Basic events that count toward L are **credited events**; those that do not count toward L are **excluded events**. (Examples of events that the analyst may wish to exclude from the analysis include those having a high probability of failure.) Thus, prevention sets of level L contain at least L credited events from every top event minimal cut set, and minimal prevention sets of level L cease to be prevention sets of L credited events if any of their events are removed. For example, level 1 prevention sets contain at least one credited event from every minimal cut set in the top event expression; level 2 prevention sets contain at least 2 credited events from every top event minimal cut set, etc.

In general, Top Event Prevention Analysis comprises four steps:

(1) Build and solve a model to obtain the top event expression.

(2) Choose a prevention level L, and specify the events that are to be credited toward prevention or, conversely, those that are to be excluded.

(3) Generate an expression for each top event minimal cut set that represents prevention of the cut set by L credited events.

(4) Form the Boolean product of the expressions generated for each of the minimal cutsets and expand and simplify this product to obtain all minimal prevention sets of level L.

As noted above, the output of a TEP analysis takes the form of prevention sets. Prevention sets have the following 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. Specifying a level of prevention (L) results in each prevention set containing multiple (L) success paths.
- 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 the occurrence of the top event. Components not included in a prevention set are not needed to prevent the top event.
- Multiple prevention sets are often generated as a part of a TEP analysis. Therefore, each prevention set by itself is a complete solution. The analyst needs to select only one prevention set to have identified a sufficient set of components necessary to prevent the top event.
- Prevention sets can be tested to determine their effectiveness with respect to cut sets that likely were truncated in obtaining the top event expression developed to begin the analysis. To test the effectiveness of a prevention set on truncated minimal cut sets, the models used to obtain the top event expression are solved again crediting basic events that are in the chosen prevention set without crediting those that are not. Additional cut sets generated as a part of this test can be appended to the original cut sets to regenerate the prevention sets and produce components making up complete success paths needed to prevent the top event.

Simple TEP Example

A simple application of these steps is presented in Figure 1. The figure contains a simple line diagram of a pneumatic system typical of that found in many power plants. It includes a three-train instrument air system backed up by a single train nitrogen supply. Included in the figure are a fault tree and the cut sets and importance measures for each of the components modeled in the system.

A common use of the importance measures is to identify those components that could contribute to the risk associated with this system from two perspectives:

(1) Those components which currently contribute most to the failure of the system (represented by the Fussell-Vesely measure of importance), and

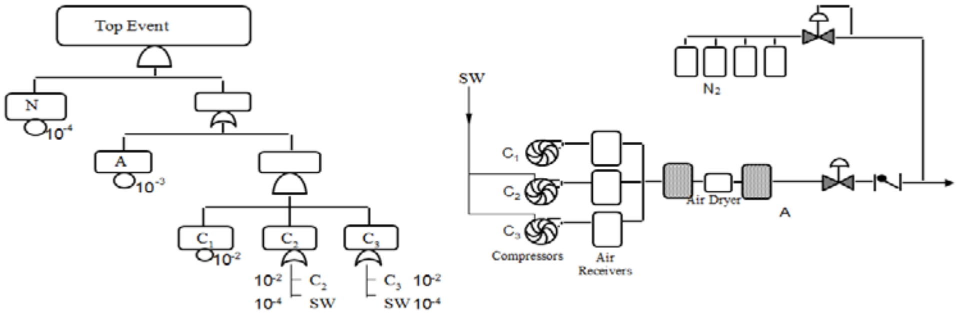
(2) Those components that could potentially contribute significantly if they were to degrade in reliability (represented by Risk Achievement Worth).

In practice, thresholds are often selected for each of these types of measures (e.g., Fussell-Vesely ≥ 0.5% and Risk Achievement Worth ≥ 2) above which the components are considered to be risk significant and thereby subject to focused attention to assure their reliability. Using these thresholds in the example of Figure 1, the entire train of nitrogen and the air filters would be selected as the most important components in this pneumatic supply system. But notice that none of the compressors are identified as being important. This example illustrates a practical limitation of importance measures, that is (due to combinatorial issues), the components they identify are important but those that do not meet the numerical thresholds cannot be stated to be unimportant without further analysis.

Top Event Prevention Analysis differs from the traditional use of importance measures for identifying important contributors to top event occurrence because it finds combinations of events that are necessary and sufficient to prevent the occurrence of the top event to the chosen level. If the components in a prevention set of level L receive focused attention in plant programs to assure their reliability, these components are enough to protect against the occurrence of the top event to level L.

Returning to the simple example in Figure 1, prevention sets have been generated from the cut sets developed for the pneumatic system. A level of prevention of two has been selected for this example. That is, at least two components from each cut set are required to be considered important and subject to focused maintenance or testing to assure that the top event effectively has been prevented. Using this approach, not only is the train of nitrogen identified as being potentially important but the air receivers and at least one air compressor as well. Each prevention set identifies complete paths of equipment needed for the system that is modeled to perform its function, systematically addressing the limitation to importance measures noted above. Further, the method finds every minimal prevention set of level L. Since all prevention sets are found, one can choose from among them a solution that satisfies some additional criteria such as being easier to implement or less costly than other solutions.

Figure 1



10^{-7}	$N * A$
10^{-10}	$N * C_1 * SW$
10^{-10}	$N * C_1 * C_2 * C_3$

	N	A	C_1	C_2	C_3	SW
Fussell-Vesely	1.0	~1.0	10^{-3}	10^{-3}	10^{-3}	10^{-3}
Risk Achievement Worth	10^4	10^3	1.2	1.1	1.1	10

Top Event

$N * A +$
$N * C_1 * SW +$
$N * C_1 * C_2 * C_3$.

Prevention Sets (Level 2)

$(N*A) *$
$(N*C_1 + N*SW + C_1*SW) *$
$(N*C_1 + N*C_2 + N*C_3 +$
$C_1*C_2 + C_1*C_3 + C_2*C_3)$.

Minimal Prevention Sets

$N * A * C_1 +$
$N * A * C_2 * SW +$
$N * A * C_3 * SW$.