Multiattribute Risk Analysis Techniques in a Cyber Security Application

David Blanchard[a], Robert W. Youngblood[b], Mihai A. Diaconesea[c]
[a]Applied Reliability Engineering, Inc., Burlingame, CA, USA
[b]Idaho National Laboratory, Idaho Falls, ID, USA
[c]North Carolina State University, Raleigh, NC, USA

Abstract: Risk methods routinely are applied to issues having a single defined outcome (e.g., core damage, release, lost generation, etc.) but do not generally consider combining model results to identify integrated solutions to managing risk across a spectrum of consequences. This paper describes the status of work directed at development of methods for combining models representing multiple differing end states in order to address the risks measured using these models across their associated consequences. The problem statement is cyber security related, that is, what are the minimal number of digital assets in a nuclear power plant that are worthwhile protecting from a cyber attack? The models for a full scope internal events PRA from a hypothetical current generation PWR are used along with fault tree logic developed in support of a generation risk assessment. Among the methods employed in the work is Top Event Prevention Analysis (TEP). Prevention analysis is a Boolean technique that identifies minimal combinations of success paths meeting user specified prevention criteria. As opposed to focusing on digital assets classified as 'safety-related', prevention analysis highlights those in critical success paths irrespective of their classification, potentially allowing relaxation of controls on some safety-related assets and at the same time focusing efforts on more risk significant assets that may be overlooked with traditional deterministic approaches alone. To ensure a wide spectrum of system functions were considered, all of the breakers included in the models were assumed to be candidates for exhibiting the effects of digital misbehaviors. Systematic events representing the misbehavior of the breakers were incorporated into the fault trees and the results regenerated as a function of these systematic events. Prevention analysis has been completed on the cyber oriented cut sets for both core damage and several systems required to support plant operation. Of hundreds of breakers included in the models, only roughly a third were found to be sufficient in managing both generation risk and limit the frequency of core damage. The effectiveness of protecting only this subset of breakers from a cyber attack was analyzed. The design features of the plant that result in the selection of the subset of breakers is under review.

Keywords: multi-attribute risk, cyber security optimization, prevention analysis, TEP

1. INTRODUCTION

Framing of risk management decisions can beneficially consider multiple attributes (i.e, multiple performance figures of merit, or end states) rather than just public safety (e.g., core damage or release frequency). Risk management expenditures will be more effective if they address a broader set of considerations. The present study is intended in part to illustrate this point.

In this study, an evaluation of the combined risks associated with both severe accidents and generation are evaluated for the purpose of selecting a minimal set of components that are effective in managing both. In addition, the evaluation focuses on management of both severe accident and generation risks under the conditions of a potential cyber attack, making the evaluation challenging from a probabilistic perspective.

To perform this multi-attribute cyber related risk evaluation,

- A baseline risk model has been developed for a pressurized water reactor (PWR) with a large dry containment typical of the current generation of plants. The risk model addresses both severe accident risk and risk to electrical generation. An important class of basic events representing digital related behaviors (systematic events) [1-3] has been added to the model, accounting for possible effects of cyber attack.
- Given risk model results for the attributes of interest, a technique called Top Event Prevention Analysis (TEP) [4-6] is a useful way to set directions in management of cyber risk. Preliminary Top

Event Prevention Analysis has been carried out on the baseline risk model modified to include systematic events.

In this paper, the following topics are addressed.

Section 2 introduces the baseline risk model (including both severe accident as well as generation risks) and enhancements to it that were directed at incorporation of cyber related effects in the form of systematic events.

Section 3 introduces Top Event Prevention Analysis which was used to identify a minimal subset of systematic events on which to focus cyber security. Section 4 summarizes results obtained so far and Section 5 discusses conclusions and possible further research.

2. DESCRIPTION OF BASELINE RISK MODEL AND ENHANCEMENTS

Baseline Risk Model

A plant risk model has been formulated to support the present work. For the purpose of this paper, we refer to this model as the "Grizzly Gulch Generating Station" (GGGS) model. GGGS is a PWR having a large dry containment and a complement of systems typical of that plant type and its vintage (Generation II). The GGGS severe accident model is based on typical fault-tree / event-tree models developed from a hybrid of several real, but unnamed, PWRs.

The GGGS generation risk model (GRA) is developed from the severe accident model, revising system logic to reflect the differences in system alignment and success criteria necessary to support normal plant operation. An EPRI generation risk assessment methodology was adopted to develop the GRA logic [7].

Appendix A provides information describing the results of both the GGGS PRA and GRA by initiating event.

Model Enhancements to Address Cyber Attack

Addressing cyber attack risk was accomplished after the initial formulation of the severe accident and generation models by incorporating "systematic events"[1] into the fault trees.

Because this work is intended to be illustrative, a practical shortcut was adopted in modeling the effects of a cyber attack. Rather than embarking on an exercise to identify and model all possible digital components that might exist at GGGS (a realistic but imaginary plant), the cyber related modeling focused on the potential effects of a cyber attack, specifically, the mispositioning of circuit breakers that may be actuated and controlled by digital assets. All breakers and their failure modes, whether active (fail to open/close when needed – FTO/FTC) or spurious (open/close when not called upon to actuate – FTRO/FTRC) were considered to reflect possible cyber attack effects. Modeling circuit breakers covers a wide variety of system functions having diverse effects on the plant. Furthermore, incorporation of systematic events representing cyber effects could be performed in a semi-automated way, allowing project effort to focus on solving the computational challenges associated with running the model and interpreting the results.

Figures 1 and 2 illustrate the incorporation of systematic events representing the potential effects of a cyber attack into the GGGS fault trees. Figure 1 shows a portion of the emergency ac power breaker logic. Breaker "152-DGA" links Diesel Generator A to Emergency Bus A. This breaker is normally open, but when power from Diesel Gen. A is needed, that breaker needs to close to provide power to the emergency bus. A cyber event interfering with its control signal can cause the breaker to remain open when needed. Moreover, to prevent overloading the diesel generator, other breakers (152-SGB-A1 and 152-SGB-A2) that supply Emergency Bus A from the station power transformer and switchyard transformers connected to offsite power need to open. The control circuit for breaker 152-DGA includes permissive logic that would preclude

[1] In this paper, the potential effects of a cyber attack are represented by systematic events. The term "systematic event" refers to a component behaviour that is deterministic in nature rather than probabilistic. In the presence of specific conditions, the component always behaves (or misbehaves) in a specific way. Because "probability" is problematic in modelling adversarial scenarios, the methodology for treating cyber induced systematic events attempts to bound the uncertainty of the likelihood and extent of the effects of the attack.

breaker 152-DGA from closing were a cyber event to prevent breaker 152-SGB-A1 or 152-SGB-A2 from opening when there was no power from an offsite power source.

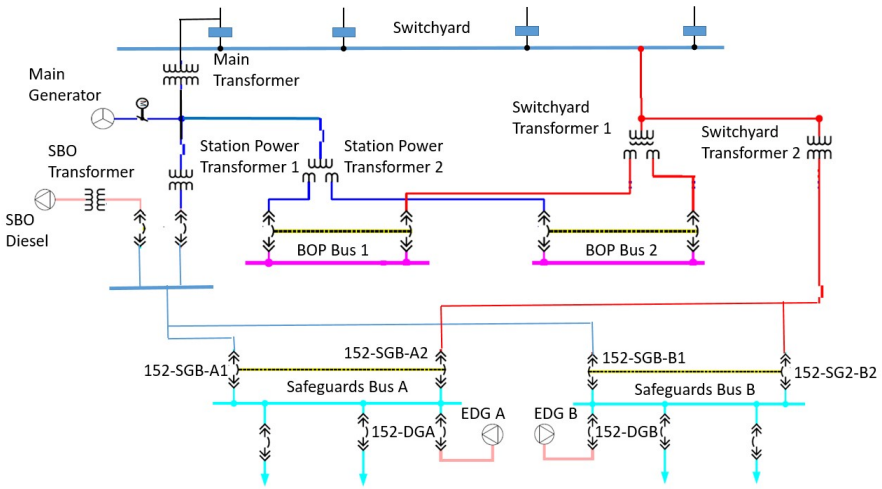


Figure 1. Emergency AC Power Distribution (GGGS)

In Figure 2, fault tree logic for aligning the diesel generator to Emergency Bus A is shown. The unshaded events represent the original fault tree logic. The events shaded light blue show systematic events that have been added to the model to reflect the effects of a cyber attack. Cyber related systematic events are incorporated simply by taking the union of the systematic event with the basic event representing the random failure of the breaker it is assumed to affect.

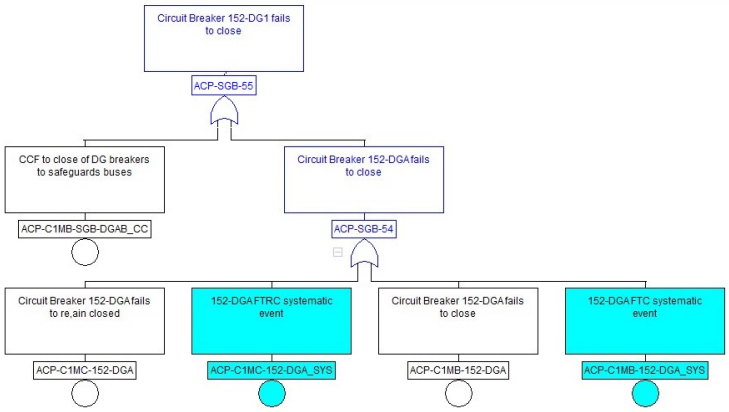


Figure 2. Emergency Bus A Diesel Generator Breaker Fault Tree Logic (GGGS)

Over 300 breakers are included in the GGGS severe accident model. As a number of the breakers have multiple failure modes (FTO/FTC/FTRO/FTRC), roughly 450 systematic events were incorporated into the GGGS fault trees in the manner described above. Attachment A provides a breakdown of the breakers included in the GGGS models by failure mode. No attempt was made to quantify the likelihood that a cyber attack would result in the mispositioning of the affected breakers (i.e., each systematic event was assigned a probability of 1.0). As illustrated inTable 1, the addition of so many systematic events to the model resulted in a combinatorial explosion of the number of minimal cut sets generated as a function of the systematic events.

Table 1. GGGS severe accident results (with and without cyber related systematic events)

	# Cut Sets	Truncation	CDF (min cut upper bound)
No systematic events (base case)	36 thousand	1E-12/yr	9E-6/yr*
With systematic events	7.5 million	1E-7/yr, order 10	NA**

*estimated distribution: mean 2.8E-5/yr, 5% 4.2E-6/yr, 50% 7.1E-6/yr, 95% 5.3E-5/yr

**A large fraction of minimal cut sets simply consist of an initiating event and multiple systematic events

Over 130 breakers are included in the systems modelled to measure generation risk. Those having multiple failure modes result in the addition of roughly 200 systematic events to the GGGS GRA fault trees. Like the severe accident model, this resulted in a significant increase in the number of GRA minimal cut sets generated as a function of systematic events.

Table 2. GGGS generation risk results (with and without cyber related systematic events)

	# Cut Sets	Truncation	Frequency (min cut upper bound)
No systematic events (base case)	9 thousand	1E-12/yr	0.58/yr* (10 initiators in Attachment A)
With systematic events	530 thousand	1E-10/yr	NA**

*estimated distribution: mean 0.7/yr, 5% 0.4/yr, 50% 0.5/yr, 95% 1.5/yr
**A large fraction of minimal cut sets simply consist of multiple systematic events

3. TOP EVENT PREVENTION ANALYSIS

Top Event Prevention Analysis ("Prevention Analysis" for short, or sometimes "TEP") is a method for driving PRA models in order to answer a particular kind of question: based on the PRA model, what is the minimal subset of failure events appearing in the PRA model that we need to prevent, in order to satisfy plant-level criteria on safety, availability, reliability, or other metric quantified by the PRA? That is: on which basic events do we need to focus prevention resources, including special treatment?

Prevention Analysis is fundamentally different from the way in which PRA is normally applied, including the application of measures of importance. As shown in the upper half of Figure 3, risk analyses typically begin with a definition of the risk to be avoided (i.e, the Damage State noted above, be it severe accident related or some other undesired outcome such as lost generation). Functions are defined that would prevent or mitigate the undesired outcome and logic developed to model the loss of available systems and human actions that could accomplish those functions (often in the form of event trees and fault trees). The results are summed over all accident sequence types to provide an overall estimate of the risk from that Damage State in terms of likelihood and consequences.

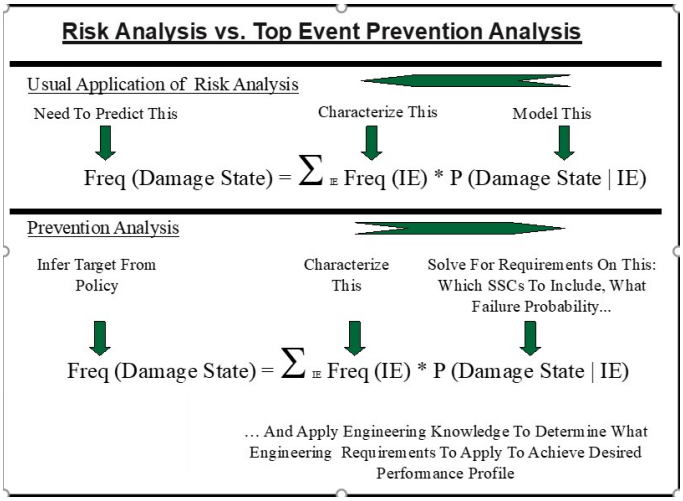


Figure 3. Risk Analysis vs. Prevention Analysis

The lower half of the diagram illustrates how prevention analysis is performed. Beginning with the risk analysis, which is in failure space, the results are converted into success space working backward. The user defines a criterion for preventing each minmal cut set in the Damage State – i.e., a desired level of prevention. The prevention criterion can be probabilistic (e.g., desired frequency of each specific cut set), deterministic (e.g., minimum number of failures needed to prevent each cut set) or a combination of both. The prevention criterion is then used to produce combinations of success paths, or prevention sets, for each minimal cut set. Having defined acceptable ways of preventing each minimal cut set, the product of the prevention sets for all minimal cut sets is taken, expanded and simplified to produce prevention sets for the entire Damage State that is capable of preventing all of the accident sequences.

Past application of the TEP methodology to a several nuclear power plant safety issues are provided in references 4, 5 and 6. The steps in the TEP process were outlined above and consist of the following:

1. Build and solve a model to obtain a Boolean expression that represents the risk of an undesired Damage State (likelihood and consequences).
2. Develop desired prevention criteria (level of prevention, probabilistic and/or deterministic).
3. For each accident sequence minimal cut set, develop an expression that identifies all of the ways that each minimal cut set can be prevented by the defined prevention criterion (prevention sets).
4. Form the Boolean product of the prevention sets for each minimal cut set, expand and simplify the resulting expression. Each term in the resulting expression is a prevention sets for the entire model at the user specified level of prevention.

Prevention analysis was performed on the 7.5 million cut sets described in Section 2 that were generated as function of systematic events. With a significant number of minimal cut sets consisting of only an initiating event and multiple systematic events (set to 1.0), implementing a probabilistic prevention criterion was not practical. A deterministic prevention criterion of level 2 was selected. Requiring the prevention multiple failures in each minimal cut set provides a level of defense in depth in managing risk, particularly for relatively high frequency initiating events (such as loss of feedwater, etc.). Due to the sheer number of minimal cut sets, prevention analysis was performed in several steps.

TEP Step 1. Selection of systematic events for beakers with active failure modes (FTO/FTC)

- The initial prevention analysis was performed on the core damage minimal cut sets and focused on selection of a minimal subset of systematic events for breakers with active failure modes (FTO/FTC).
- In selecting basic events to be prevented, preference was given to selecting low probability random failures over systematic events. A level of prevention of 2 was specified as noted above.
- Expansion and simplification of the prevention sets was performed resulting in hundreds of thousands prevention sets each hundreds of variables in length
- The resulting prevention sets were reviewed, and a prevention set with the fewest number of systematic events selected for further processing.

Table 3. Selection of severe accident cyber related systematic events
(breaker active failure modes)

Maximum number of prevention sets	127 thousand
Number of variables in selected prevention set	229
Number of systematic events in selected prevention set	36 out of a total of 155 systematic events representing breaker active failure modes

TEP Step 2. Selection of additional systematic events for beakers with passive failure modes (FTRO/FTRC)

- The next step in the prevention analysis is performed including the core damage minmal cut sets that contain systematic events with passive failure modes (FTRO/FTRC).
- In selecting basic events to be prevented, preference was given to preferentially selecting not only low probability random failures but the 36 breaker active failure systematic event selected in TEP Step 1. As before, a deterministic level of prevention of 2 was specified.
- Expansion and simplification of the prevention sets was performed once again resulting in hundreds of thousands prevention sets each hundreds of variables in length
- The resulting prevention sets were reviewed, and a prevention set with the fewest number of systematic events selected, this time containing systematic events representing breakers with both active and passive failure modes

Table 4 – Selection of severe accident cyber related systematic events
(breaker active and passive failure modes)

Maximum number of prevention sets	111 thousand
Number of variables in selected prevention set	235
Number of systematic events in selected prevention set	149 out of a total of 451 systematic events representing breaker active and passive failure modes

TEP Step 3. Selection of additional systematic events for beakers in the generation risk assessment (GRA)

- The prevention analysis moves on to the generation risk assessment and includes all systematic events with breaker failure modes, either active or passive.
- In selecting basic events to be prevented, preference was given to preferentially selecting not only low probability random failures but the 149 active and passive breaker systematic events selected in TEP Step 3. However, the deterministic level of prevention is reduced to 1 as a number of generation related systems are known to have single point vulnerabilities.
- Expansion and simplification of the prevention sets was performed once again resulting in hundreds of thousands prevention sets each hundreds of variables in length
- The resulting prevention sets were reviewed, and a prevention set with the fewest number of systematic events selected, this time containing systematic events representing breakers with both active and passive failure modes.

Table 5. Selection of generation risk cyber related systematic events
(breaker active and passive failure modes)

Maximum number of prevention sets	millions
Number of variables in selected prevention set	329
Number of systematic events in selected prevention set	56 out of a total of 199 systematic events in the GRA representing breaker active and passive failure modes (18 additional systematic events are selected for the GRA that were not among 149 systematic events selected for the severe accident models).

4. TESTING AND REVIEW OF THE RESULTS

Up to this point in the analysis, deterministic criteria alone have been used in the selection of a minimum subset of systematic events as candidates for managing the risk associated with a cyber attack from both a severe accident and loss of generation perspective. Of the more than 450 breaker related systematic events added to the models, 149 were selected as important to severe accident risk and 56 to generation risk (38 systematic events being common to both sets of consequences).

In this section, a review of these results is presented in the form of a probabilistic test of the effectiveness of the selected systematic events in managing severe accident and generation risk.

As noted in the introduction to this paper, a quantitative risk analysis of a cyber event must recognize uncertainties not only with respect to the frequency of a cyber attack but also the extent of its effect on digital assets in the plant. To address these uncertainties, several simplifying assumptions were made to estimate the quantitative impact of the cyber attack particularly with respect to the systematic events incorporated into the GGGS severe accident and generation risk models:

- Systematic events in the selected prevention set were set to False in the risk models.
  Treating systematic events in this manner assumes that digital assets represented by the selected systematic events are made subject to design and programmatic controls associated with a cyber security program. While such a program may not completely eliminate the potential for cyber related misbehaviours of the affected components, the controls effectively are assumed to result in relatively low likelihood of loss of the function provided by the digital assets as compared to the random failure probabilities associated with the components that they actuate or control.
- Systematic events that are not a part of the selected prevention set were set to True in the risk models.
  This assumption is relatively bounding in that
  - Systematic events that were not selected are considered not to be subject to protection under a cyber security program and their associated components are assumed to fail to perform their functions with certainty during a cyber attack.

- The entire set of unprotected systematic events are assumed to fail to perform their functions following a cyber attack.

The application of the above two simplifying assumptions to the minimal cut sets for the GGGS severe accident and GRA models is summarized in the second row of the following two tables.

Table 6 – Cyber related severe accident risk quantitative results

	# Cut Sets	Truncation	Core damage frequency
No systematic events (base case)	36 thousand	1E-12/yr	9E-6/yr
With systematic events using TEP (prevention level = 2) 149 systematic events (selected) – False 302 systematic events (not selected) – True	7.5 million	1E-7/yr, order 10	3E-4/yr (more than a factor of 30 over the base case)
With 10 additional systematic events selected using importance measures - False			2.5E-5/yr (within a factor of 3 of the base case)

Table 7 – Cyber related generation risk quantitative results

	# Cut Sets	Truncation	Reactor trip frequency
No systematic events (base case)	9 thousand	1E-12/yr	0.58/yr
With systematic events using TEP (prevention level = 1) 56 systematic events (selected) – False 143 systematic events (not selected) – True	530 thousand	1E-10/yr	36/yr (a factor of 60 greater than the base case)
With 7 additional systematic events selected using importance measures - False			0.65/yr (within 15% of the base case)

In the above tables, the term ‘selected’ implies that the digital assets associated with these systematic events are subject to a cyber security program that limits the vulnerability of the assets to a cyber attack.

As reflected in the second rows of the above tables, the systematic events that were selected deterministically using prevention analysis begin to manage risk, but the frequency of core damage and plant trips remain more than an order of magnitude above the base case. A review of the dominant contributors to this increase reveals the following:

- 95% of the increase in core damage frequency comes from systematic events found in the accident sequences for three initiating events
  - Very small LOCA (VSLOCA)
  - Steam generator tube rupture (SGTR)
  - Loss of offsite power (LOOP)
- 98% of the increase in reactor trip frequency comes from systematic events in two systems
  - Main condenser
  - High voltage switchgear buses

Returning severe accident and generation risk to near their base case frequencies requires the addition of systematic events to a cyber security program beyond those selected deterministically. A relatively straightforward approach to selection of these additional systematic events was taken through the generation of importance measures.

The systematic events that had not been selected by prevention analysis were all set to True in the severe accident and generation cut sets as they were assumed not to be subject to protection in a cyber security program. Examining the unselected systematic events having the highest Fussell-Vesely importance[2] resulted in the following;

[2] As Fussell-Vesely represents the fraction of current total risk to which an event contributes, this measure of importance was used to identify the systematic events which would have the greatest effect on reducing cyber risk if selected for protection under the cyber security program.

- Only 10 additional systematic events of high importance needed to be selected to address a large fraction of the increase in risk from the VSLOCA, SGTR and LOOP accident sequences
- 7 additional systematic events of high importance to generation risk were sufficient to address the increase in reactor trip frequency stemming from loss of the main condenser and high voltage switchgear.

The quantitative risk effects of adding these 17 breaker related systematic events to those selected using prevention analysis is reflected in the last rows of Tables 6 and 7 (as well as in Attachment A). Were these breakers be made subject to the controls of a cyber security program, severe accident risk could be returned to within a factor of 3 of the base case core damage frequency and generation risk well within a factor of 2 of the base case reactor trip frequency.

In summary, using a blend of deterministic (prevention analysis) and probabilistic (importance measures) approaches, a minimal subset of cyber related systematic events in the severe accident and generation risk models for a hypothetical current generation PWR were identified as being capable of managing risk. Of the more than 450 components used to represent the potential effect of a cyber attack, just a little over a third appear to be effective in managing both severe accident and generation risk were they to be protected under a cyber security program.

At the time of the writing of this paper, review of the basis for the selection (or not selecting) each of the systematic events in the GGGS severe accident and generation risk models is in progress.

5. CONCLUSIONS

This paper has discussed analysis of a digital risk problem using a realistic plant model which resembles numerous existing Gen II plant PRAs. Assuming that protecting digital assets from cyber attack is potentially burdensome but arguably necessary: How do we optimize the approach to digital asset protection? Can we choose a subset of assets whose protection does a good job, but may involve a different set of digital assets than those classified as safety related or important to safety?

The premise of the current project is that there is probably benefit to choosing the protection scheme considering the safety problem and the generation-risk problem together, rather than separately optimizing protection for safety and optimizing protection for generation as if the two problems were independent. Results obtained so far suggest that a benefit does exist: a Prevention Set emerging from the joint analysis contains numerous elements that support both safety and generation.

In this analysis, adversary initiated digital related misbehaviors are represented by systematic events. Two characteristics of the digital risk problem combine synergistically to make the problem appreciably more difficult (and candidate solutions more difficult to assess):

- Systematic events represent deterministic behaviors of components that are not random. Using event probability information with systematic events is problematic.
- Adding systematic events to a safety model increases the number of cut sets very considerably.

Having both characteristics in the same problem means that there are many more minimal cut sets, and we lack a method for reasoning about their probabilities in a traditional way. For now, this has driven us to reason about the efficacy of a given prevention set based on the following:

- Systematic events in the selected prevention set were assumed to be subject to protection under a cyber security program and were set to False in the risk models.
- Systematic events that are not a part of the selected prevention set were set to True in the risk models.

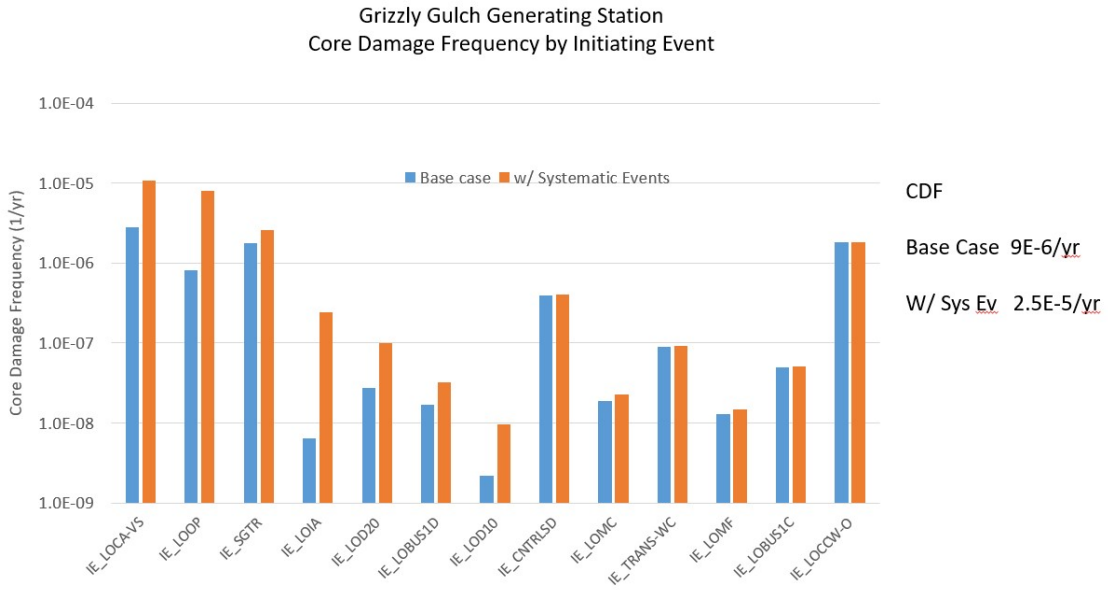
The above exercise is an interesting thought tool, but we cannot prove that the result is bounding. Setting included events to “False” basically assumes that protection is highly effective, but that is, for now, a presumption. Also, we have not yet analyzed common-cause failure. On the other hand, assuming that ALL of the non-selected events ALWAYS fail is extremely pessimistic.

Lack of probability information for adversarially-caused systematic events is not a limitation of Prevention Analysis per se; the issue is inherent in trying to apply scenario-based methods to problems involving systematic events that can be caused by adversaries. Being an extremely effective tool for scenario-based risk management, Prevention Analysis can generate interesting results in this problem despite the explosion in problem size caused by introducing systematic events into the safety model without probability information. Future work will include learning how to think more usefully about the risk management approach for cyber, without the safety domain's traditional approach to probability quantification.

REFERENCES

[1] "Untangling Systematic Failures, Dependencies, and Common Cause Failures in Digital Systems," EPRI, Palo Alto, CA: 2024.
[2] "Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments", EPRI, Palo Alto, CA: 2012, 1025278.
[3] "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," NUREG/CR-7007, ORNL/TM-2009/302, ORNL, 2009.
[4] R. Youngblood and L. Oliveira, "Application of an Allocation Methodology," Proceedings of "PSA '89
[5] R. W. Youngblood and R. B. Worrell, "Top Event Prevention in Complex Systems", Proceedings of the 1995 Joint ASME/JSME Pressure Vessels and Piping Conference, June 1995
[6] Risk Informed Safety Margin Characterization Case Study: Selection of Electrical Equipment To Be Subjected to Environmental Qualification, INL/EXT-11-23479 Rev. 1, April 2012.
[7] "Generation Risk Assessment (GRA) Plant Implementation Guide", EPRI, Palo Alto, CA: 2004. 1008121.

Attachment A – Grizzly Gulch Generating Station Severe Accident and Generation Risk Summary



GGGS GRA Results	Base case GRA freq (1/yr)	Base case SPAR IE freq (1/yr)	selected core damage prevention set *159 systematic events* GRA freq (1/yr)	Systematic events from selected core damage prevention set + Level 1 GRA prev set *18 add'l systematic events* GRA freq (1/yr)	selected core damage prevention set + Level 1 GRA prev set + GRA importance meas *7 add'l systematic events* GRA freq (1/yr)
Loss of FW (total)	0.018	0.022	243	0.015	
Loss of FW (partial)	0.19		730	0.22	
Loss of Main Condenser	0.036	0.025	504	17	0.041
MSIV Closure	0.011		0.028	0.015	
Instrument Air	1.1E-02	7.2E-03	2.7E-02	2.7E-02	
Component Cooling	7.5E-04	5.1E-04	5.5E-03	5.0E-03	
Service Water (BOP)	5.1E-03	1.5E-03	5.0E-03	5.0E-03	
Service Water (CCW htxs)	9.6E-04		4.4E-03	4.4E-03	
Service Water (total loss)	9.4E-04	5.1E-04			
HV Swgr (Trip)/bus	6.0E-02	2.1E-03	1146	3.7	0.063
5 HV buses	3.0E-01		5728	18	0.32

Grizzly Gulch Generating Station – Breaker failure modes representing potential cyber related effects
Switchyard disconnects (345kv)
High voltage breakers (4160vac & 2400vac)
Low voltage breakers (480vac)
Instrument breakers (125vac)
DC breakers (120vdc)

308 breakers total	112 breakers w/ active failure modes	279 breakers w/ passive failure modes
	155 breaker basic events FTO/FTC	296 breaker basic events FTRO/FTRC