INL/MIS-24-77521

ADVANCED REACTOR SAFEGUARDS & SECURITY

Allocating Performance Margin Using Mult Attribute Top Event Prevention Analysis

PRESENTED BY

Bob Youngblood Supported by Dave Blanchard and Mihai Diaconeasa

May 15, 2024

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

Task Overview

- The present task is part of a broader effort to understand better how to apply modern modeling techniques to understanding, and ameliorating, cyber risk at nuclear power plants.
  - The premise is that the most efficient way to do this involves being selective about what we protect.
  - It's combinatorial optimization. (See SAND83-0085, Combinatorial Optimization with Boolean Constraints, Hulme and Worrell)
- The scope of the present task is to carry out an analysis demonstrating the following points:

1. Framing of risk management decisions can beneficially consider multiple attributes (multiple performance figures of merit, or FOMs) rather than just public safety. Risk management expenditures can do more good if they are based on a broader set of objectives.
   - To illustrate this, a baseline risk model has been developed, addressing both severe accident risk and risk to "generation."
2. Given risk model results for the attributes of interest, a technique called Top Event Prevention Analysis (TEPA) is a useful way to select a combination of assets to protect.
   - Preliminary Top Event Prevention Analysis has been carried out on the baseline risk model.
3. Because "probability" is problematic in modeling adversarial scenarios, we need to consider an alternative concept, such as "margin."
   - This will be undertaken in coming months.

Team

- Bob Youngblood, PI
- Mihai A. Diaconeasa
  - Assistant Professor of Nuclear Engineering, North Carolina State University
- Dave Blanchard
  - Applied Reliability Engineering, Inc. (AREI)
  - Dave rescued Top Event Prevention Analysis from obscurity, and has applied it for many clients in the safety domain.
  - The model used in this work has been developed by Dave, based on a plant model that originated with one of his clients
  - The commercial software needed to do Top Event Prevention Analysis was developed by Dave in collaboration with Dick Worrell, author of SETS

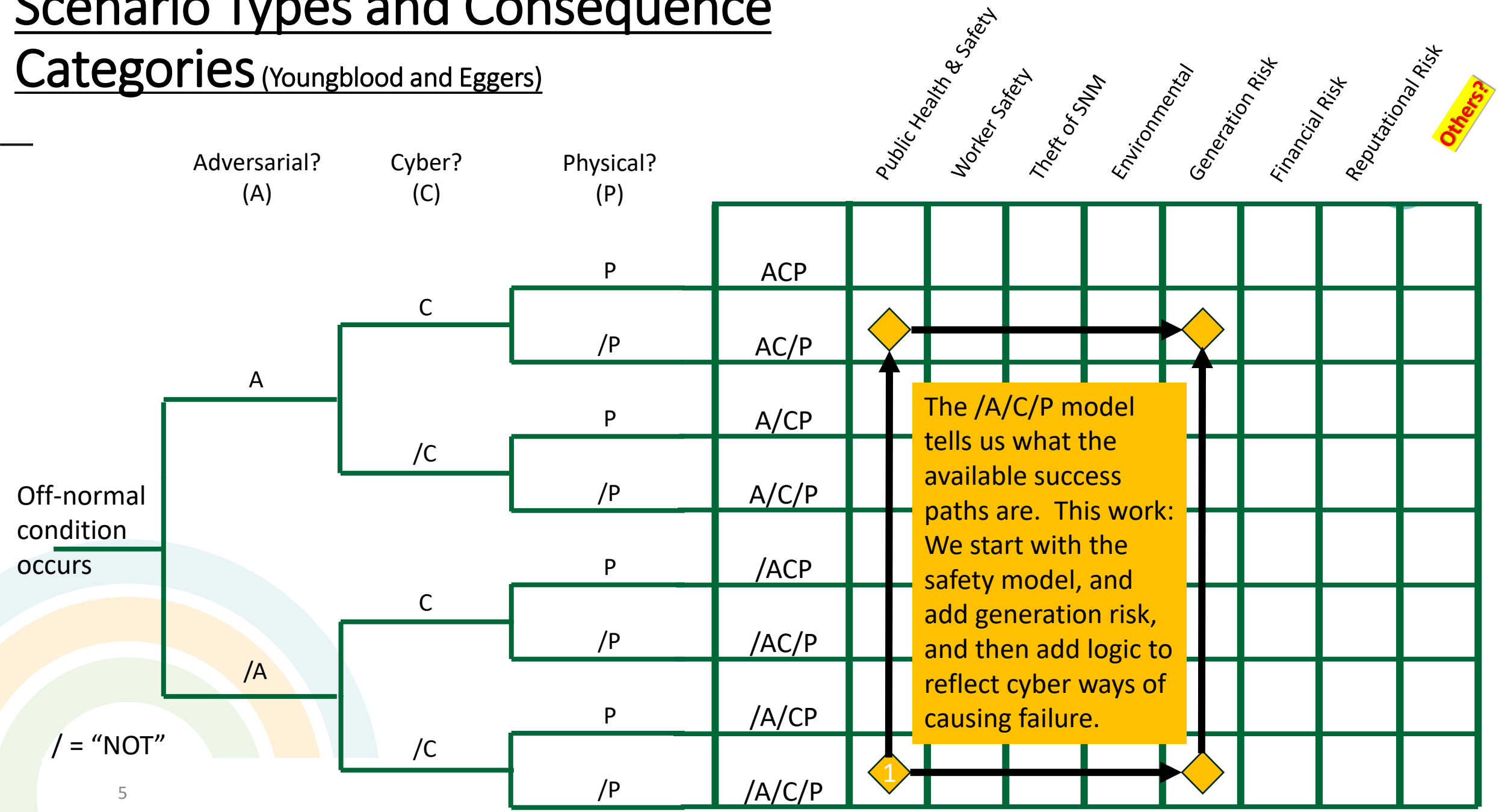
Multiattribute?

What do we mean by “Multiattribute?”

=> Considering Different Consequence Types (not just severe accident risk)

We will see later that there are synergies between preventing safety problems and preventing interruption of plant generation.

Scenario Types and Consequence Categories (Youngblood and Eggers)



Top Event Prevention Analysis?

What is “Top Event Prevention Analysis?” (”Prevention Analysis” for short)

=> It’s a way of choosing what subset of assets to

- Protect
- Assure
- QA
- …

} … Based on plant-level requirements on safety, availability, …

Risk Analysis vs. Top Event Prevention Analysis

Usual Application of Risk Analysis

Need To Predict This → Characterize This → Model This

$$\text{Freq (Damage State)} = \sum_{IE} \text{Freq (IE)} * P(\text{Damage State} \mid IE)$$

Prevention Analysis

Infer Target From Policy → Characterize This → Solve For Requirements On This: Which SSCs To Include, What Failure Probability...

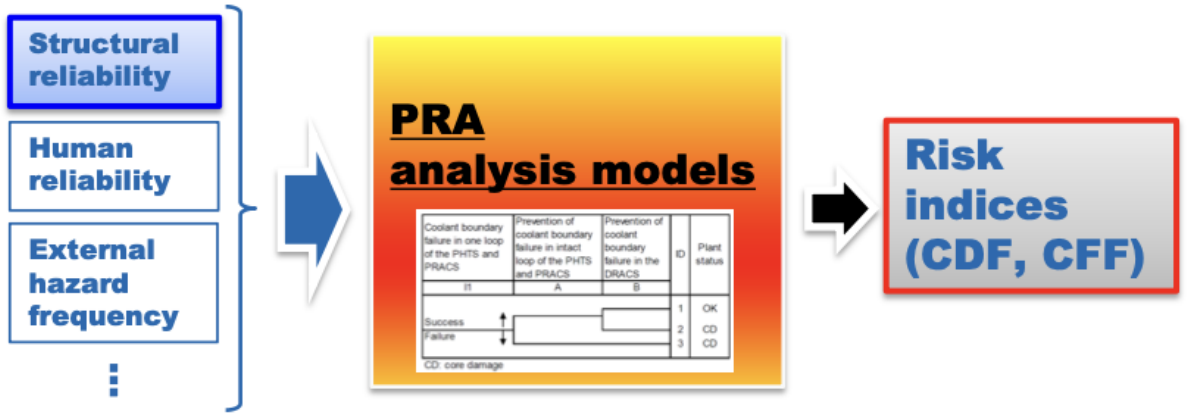
$$\text{Freq (Damage State)} = \sum_{IE} \text{Freq (IE)} * P(\text{Damage State} \mid IE)$$

Safety Applications

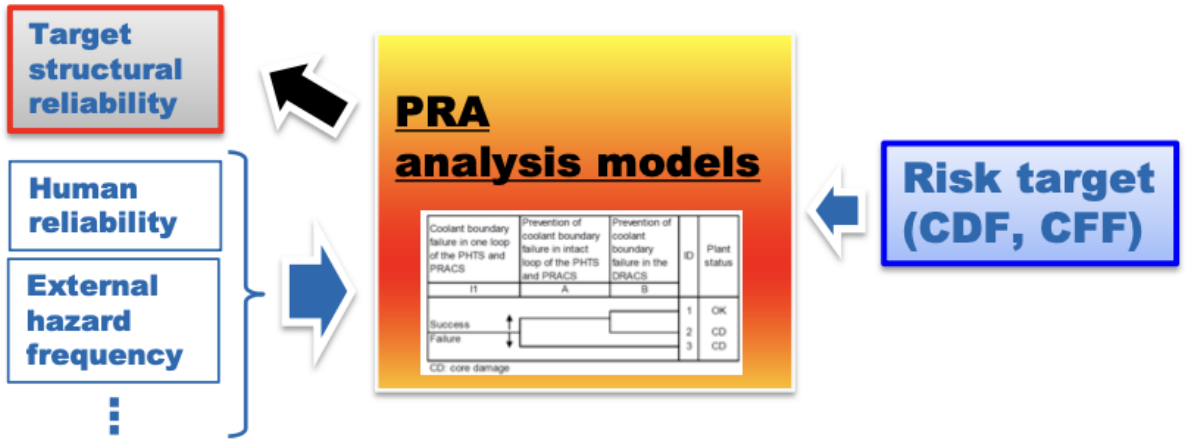
… And Apply Engineering Knowledge To Determine What Engineering Requirements To Apply To Achieve Desired Performance Profile

Key Technical Elements: Derivation of Component Level Target Reliability (App. I)

- Probabilistic Risk Assessment (PRA) is usually used to integrate the individual reliabilities into the risk index.



- The developed method uses PRA **in a reverse way** to derive component level structural reliability from the plant level risk target.



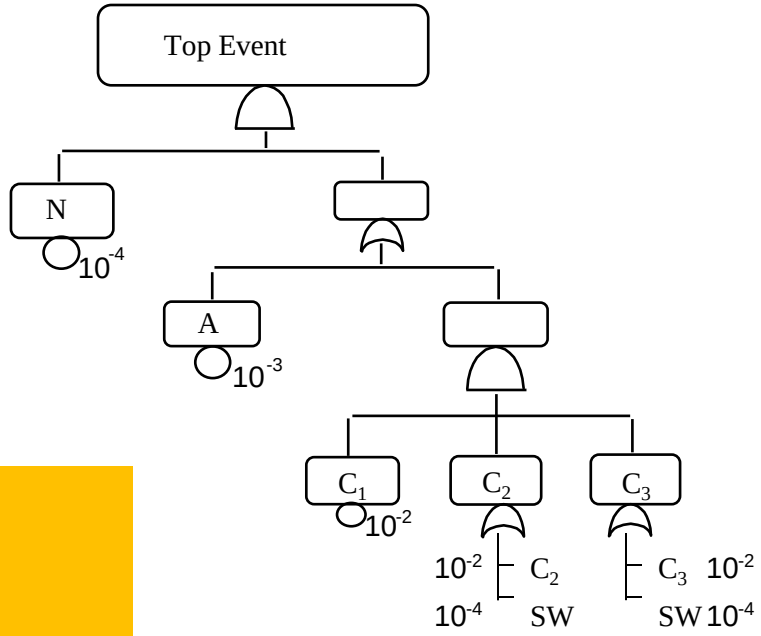
Kurisaka, K., Nakai, R., Asayama, T., and Takaya, S., 2011, "Development of System Based Code (1) Reliability Target Derivation of Structures and Components", J. Power Energy Syst., Vol. 5, pp.19-32. DOI: 10.1299/jpes.5.19

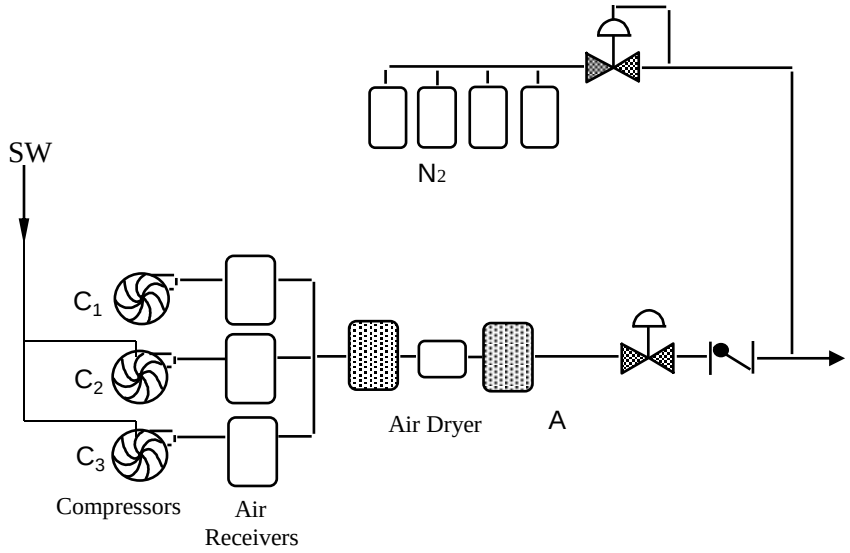
To extend risk analysis to cyber, we need the concept of “systematic event.”

- Operationally, systematic events are ones in which “something happens (e.g., a functional failure occurs) but where no specific component can be ‘blamed.’”
- Rather than occurring randomly, or being caused by other random events, systematic failures are caused by things like flawed design, flawed software, or perhaps by cyberattack.
  - If a circuit breaker is open when it is not supposed to be, this could be due to a physical failure of the breaker, or perhaps an upstream physical failure resulting in an incorrect control signal, or perhaps a cyberattack having corrupted the control signal. The latter case is a “systematic event.”
- Identifying systematic events is a major emphasis of STPA (System-Theoretic Process Analysis). (Beyond the scope of this talk)
- In this work, we will postulate a large class of systematic events, incorporate them into a risk model, and analyze the resulting scenarios to determine a *combination* of systematic events whose prevention will result in an appropriate level of protection at the facility level.

Dave Blanchard

Top Event Prevention Analysis: Simple Example





Safety Domain

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

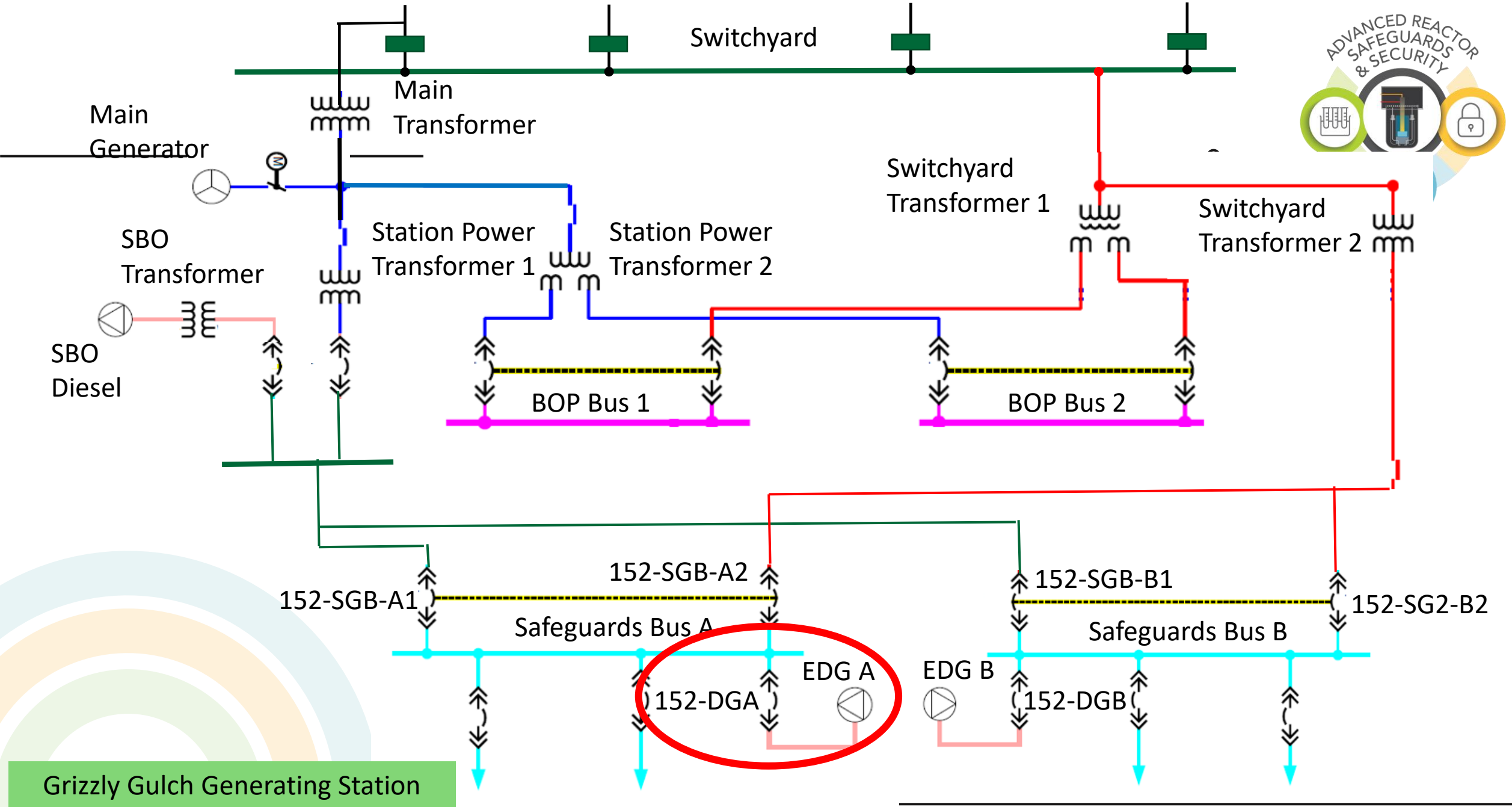
N * A +
N * C_1 * SW +
N * C_1 * C_2 * C_3.

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.



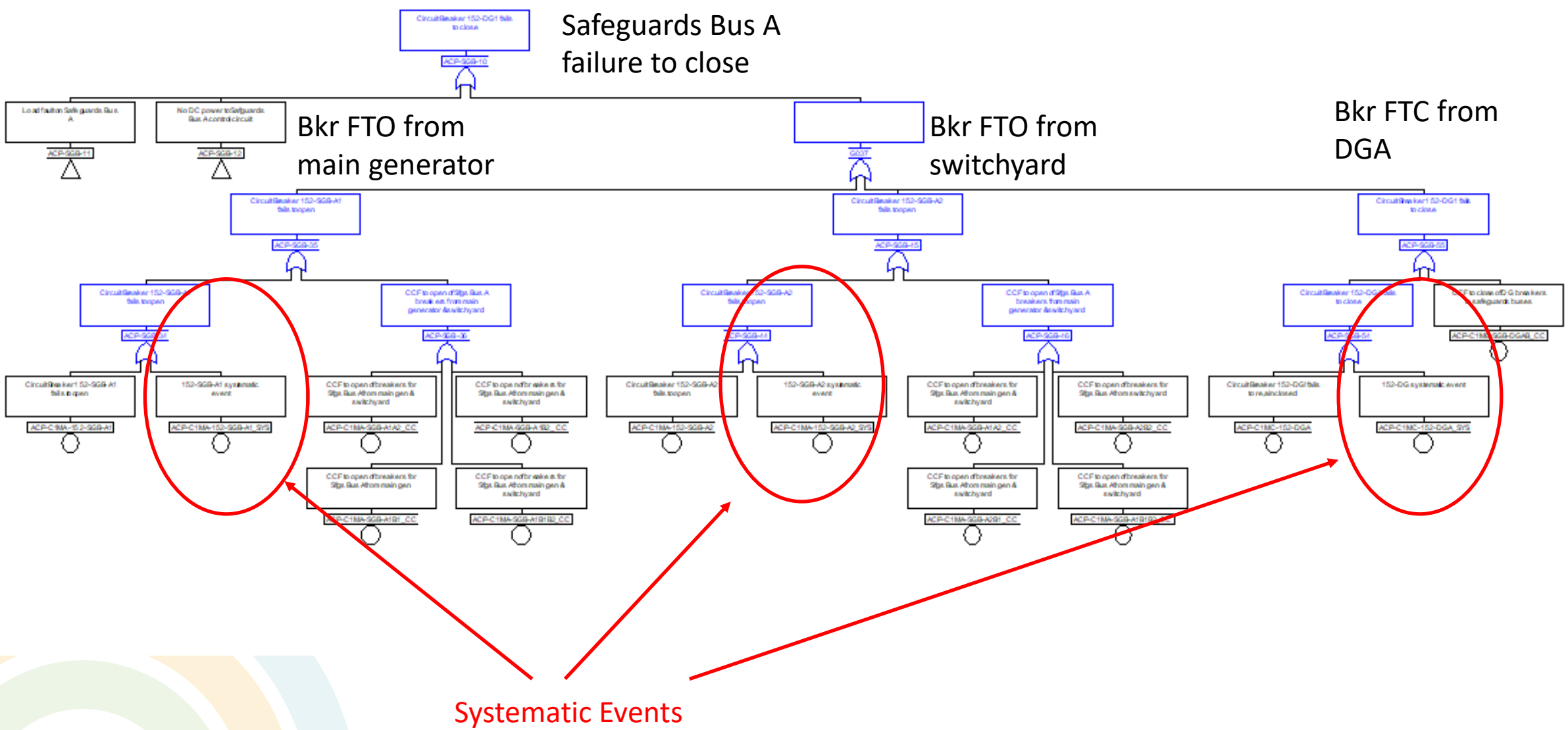
Grizzly Gulch Generating Station
c/o Dave Blanchard

DGA breaker to Safeguards Bus A failure to close

Bkr FTO from main generator

Bkr FTO from switchyard

Bkr FTC from DGA



Systematic Events

Grizzly Gulch Generating Station
c/o Dave Blanchard

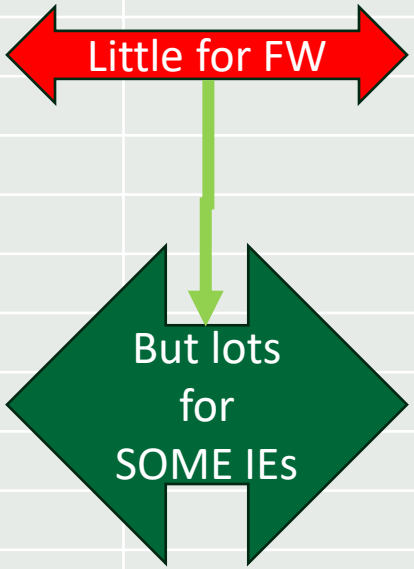
Current Results

"Results"

1. Find a Level 2 Prevention Set (including systematic events) that works fairly well in preventing core damage. Now: what do we have to do in order to address loss of generation?
2. Test the Prevention Set on Generation Risk.
   - Find that it prevents some contributors to loss of generation, but not all.
3. Run Prevention Analysis on Generation Risk cut sets, conditioning the analysis on credit for systematic events already in the selected Core Damage Prevention Set.
4. This process adds more systematic events. Test the new Prevention Set on Generation Risk.
5. Still not ideal. Look at the cut sets that are causing the problem. Identify a few more events whose prevention would address those cut sets.
6. Looks Good!

The fact that the Prevention Set for safety actually helps with generation risk illustrates part of the point of considering the two attributes together. In principle, one could consider generation risk in the original process of formulating the "safety" Prevention Set…

	Base Case (Syst Evs Not Added Yet)		Systematic events from … Selected Core Damage Prevention Set:	Selected Core Damage Prevention Set + Level 1 GRA Prev Set		Selected Core Damage Prevention Set + Level 1 GRA Prev Set + GRA Importance Meas	
GRA results as of 2/29/2024			159 systematic Events (out of 386 added to the model)	18 additional systematic events to help with GRA		7 add'l systematic events	
Selected Core Damage Prevention Set Alone does …							
	GRA freq (1/yr)		GRA freq(1/yr)	GRA freq(1/yr)		GRA freq (1/yr)	
Loss of FW (total)	0.018		243	0.015	Good		
Loss of FW (partial)	0.19		730	0.22	Good		
Loss of Main Condenser	0.036		504	17	Still BAD	0.041	Now OK
MSIV Closure	0.011		0.028	0.015	OK		
Instrument Air	1.1E-02		2.7E-02	2.7E-02	Not Bad		
Component Cooling	7.5E-04		5.5E-03	5.0E-03	So-so		
Service Water (BOP)	5.1E-03		5.0E-03	5.0E-03	Good		
Service Water (CCW htxs)	9.6E-04		4.4E-03	4.4E-03	So-so		
Service Water (total)	9.4E-04						
HV Swgr (Trip)/bus	6.0E-02		1146	3.7	Still BAD	0.063	Now OK
HV Swgr (LOOP w/Tran)	8.8E-02						



How were these metrics quantified?

- We aren't using probabilities for the systematic events. So we can't really "quantify" the risk metrics in the usual way. So where are the frequencies coming from?

A drastic sensitivity study:

- The Prevention Sets are tested in the following way. Note that for a selected Prevention Set, every systematic event is either included, or not. So:
  - Set included breaker systematic events to False (assume they are successfully prevented)
    - Assumes controls and treatment result in low likelihood of failure mode as compared to components the breakers are supporting.
  - Set breaker systematic events that were not included to True
    - Assumes breaker failure modes represented by these systematic events **occur with certainty**.

DRASTIC

Summary

- The model has been developed and exercised. The calculational process works.
- The results displayed seem worthwhile:

➢We can reason qualitatively about the pros and cons of protecting different collections of assets.

  - Reasoning qua**nt**itatively would require probabilities …

- Looking ahead: So far, this crudely equates "number of things protected" to "attack difficulty." Can we do better?
  - "Margin?"
  - Is diversity (prevent cut sets by preventing unlike cut set elements) in the prevention set needed?
  - This is still a research topic (it's the scope of the rest of this FY).