Use of Risk Insights in Support of Security and Safeguards Operation and Design

Ricky L. Summitt, PE
Principal PRA Engineer
ENERCON Services, Inc

Introduction

The use of Probabilistic Safety Assessment (PSA) to risk-inform existing nuclear power plant (NPP) licensing bases has been proven effective and offers a means to substantially reduce plant operating costs by accounting for the deterministic conservatisms. For current generation nuclear power plants, the cost of security represents one of the highest recurring operating costs. The need to address multiple adversary constructs and scenarios results in a need to address many low likelihood scenarios with the same rigor as those found to be significant. Further, the target set definition does no consider quantitative factors such as equipment reliability and adversary intent. For future designs, it is possible to optimize security while considering risk-informed attributes in the design and operations.

An evolutionary improvement in estimation of security posture would be to consider a true risk perspective that addressed the likelihood of the scenario, the likelihood of target acquisition leading to an adverse condition such as core damage, and the potential for significant offsite consequence. However, at the present time, some of the elements require additional development and a complete integration of the risk informed process may not be easily applied within the regulatory construct.

An alternative is to utilize the existing tools and knowledge from the PSA to inform specific topics associated with the assessment of security posture. Insights from the PSA are already being used to help bound target set development for current plants. This paper expands that process to consider a refinement of the target set process to allow for easier protection of key targets that provide the most benefit based on a ranking system using the most important targets and target sets to simplify the final target sets to be protected.

Mapping PSA Insights to Vulnerability and Target Set Development

The development of the security response and protocols are based to a large part by the desire to deny the adversary access to key areas of the facility that contain systems, equipment, or material that is necessary to prevent the undesired outcome of sabotage or theft.

The design of the current NPPs generation did not consider security aspects in relation to equipment location, delay tactics, and barrier construction. For the next generation designs, there is the ability to utilize risk insights to strengthen the safety, security, and safeguards. One such aspect is strategic placement of targets that deny adversary success. For example, it is not unusual for some current reactor designs to find all pumps of a specific system collocated in the same room or nearby rooms that provide optimal.

In the traditional method for target sets, the targets are not categorized in terms of operational reliability or adversary vulnerability. It usually involves identification of a list of components to be challenged by a specific scenario. A multitude of scenarios are developed providing a comprehensive target listing. Another approach is to identify the specific functions required to either maintain a safe-stable state or to preclude theft of materials. This can be expressed at a high level by Figure 1.

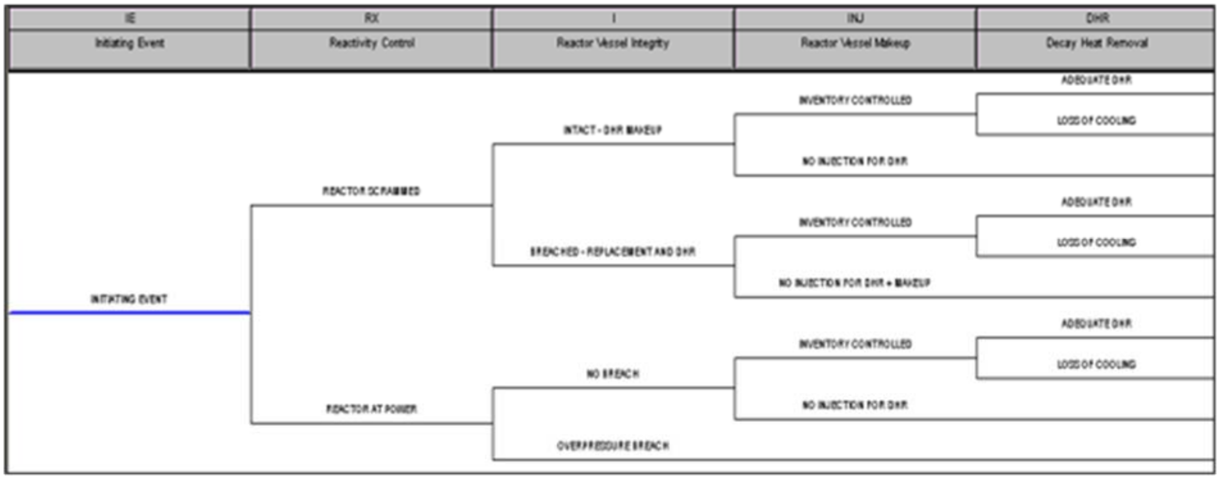

Figure 1. Generic Functional Safe and Stable PSA Event Tree

For security, the initiating event is replaced with incursion onto the site. Only the top branch is success since all functions are successful. It is possible to enter lesser states with partial success, but these are not typically addressed with respect to target set development. Each function can be expanded to define the necessary systems as shown in Figure 2.

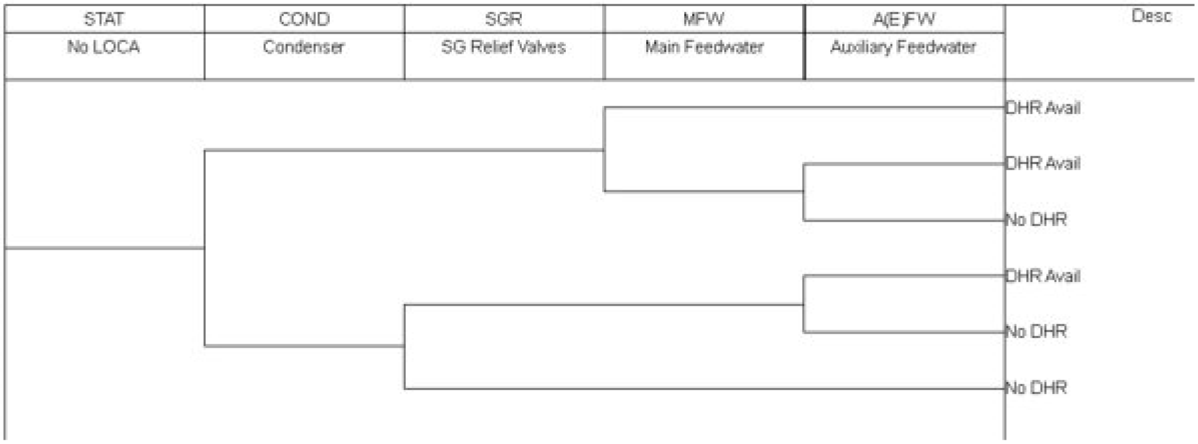

Figure 2. Example Decay Heat Removal Function – PWR Design

The more detailed function event tree defines several success states that can then be used to compare options. For example, main feedwater and auxiliary feedwater form like functions and either could be used for the target set. The more reliable or lower vulnerability system can be selected leading to similar level of protection with higher chance of success. Once the systems are selected, then the subsystems can be considered. For auxiliary feedwater that may include three operational trains as shown in Figure 3.

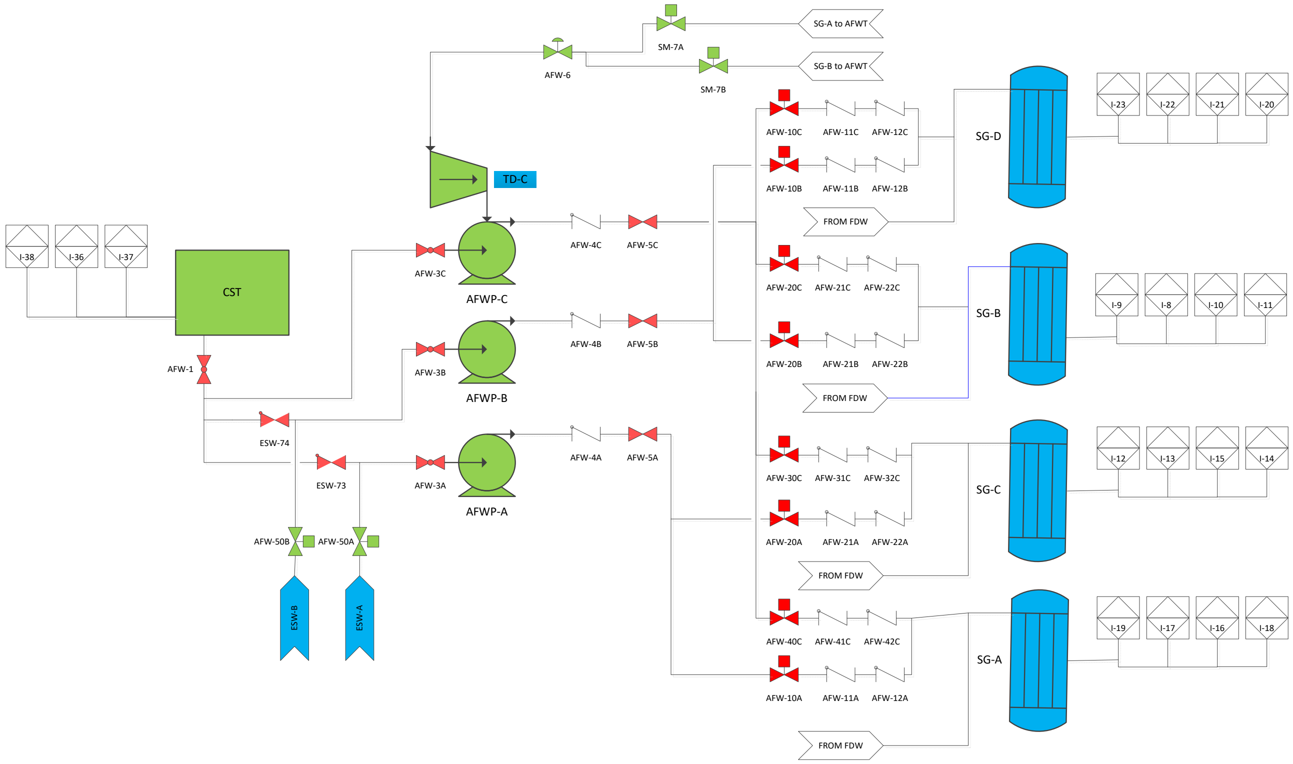

Figure 3. Example Auxiliary Feedwater System – 4 Loop Plant

The basic events in the traditional PSA model can be mapped to the master component for each modeled component. Once completed, the PSA model represents component level faults. The component faults can then be mapped to the associated plant physical location. From this substitution the location model is defined. An example of the process is Table 1.

Table 1. Example Transition from PSA Failure Mode to Location

PSA Model Failure Mode	Associated Component	Associated Location
Motor-operated valve NI-34 fails to open	Motor-operated valve NI-34	AB-305

The model created from this process identifies the combinations of locations that could result in the undesired event and provides a physical construct of the model. The next step involves conversion of the model from a failure model to a success model. This is done by altering the gate logic to represent the complement term. Essentially this involves altering the “AND” logic to “OR” logic and the reverse. With the success logic developed the next step defines the ranking system.

Considerations for Ranking Target Sets

To develop the success results, the model is quantified setting the location events to 1.0. This provides the combinations of locations that, if successfully defended would preclude any consequence. By using a simple importance tool such as Fussell-Vesely importance for the elements of the success results, a ranking scheme can be developed for each location and groups of locations. The location importance can be identified by:

$$L_j = \frac{\sum CS_j}{\sum CS}$$

In this equation CS_j defines a cut set with specific location, L and CS indicates the total cut sets. The value L_j can take values from 0.0 to 1.0. Those with the highest values, closest to 1.0, are the most critical to defend because they preclude the highest number of potential adversary scenarios. Those with the lowest values are candidates for removal. For example, if a partial listing of the results indicated the success paths listed in Table 2.

Table 2. Example Success Paths

Success Path	Locations			
1	AB-305	AB-100	AB-190	AB-403
2	RX-102	TB-300	AB-305	AB-403
3	AB-303	AB-305	DG-101	DG-201
4	TB-200	TB-300	AB-100	DG-101

Using the equation and the results, the location important can be determined and the locations can be defined. A sample is produced in Table 3.

Table 3. Ranking of Locations based on Success Path Outcome

Location	Occurrence	Importance	Rank
AB-305	3	4	0.75
AB-100	2	4	0.50
DG-101	2	4	0.50
TB-300	2	4	0.50
AB-403	2	4	0.50
AB-100	1	4	0.25
AB-190	1	4	0.25

From this initial assessment, AB-305 has the highest ranking. The next step examines the scenarios to define the most collocated scenario for the highest ranking. Observation of the listing identifies #3 as the most collocated (33% of all AB-305 results).

Table 4. Physical Security Defense Basis

3	AB-303	AB-305	DG-101	DG-201
	Adjacent		Adjacent	

Based on this assessment, success can be achieved for 25% (0.75 x 0.33) of the identified paths by protecting two areas within the plant in this simple example. This process can be repeated to identify some level of acceptable performance, for example, 95% success. Physical security measures can be reduced for locations that consistently result in a combination of low ranking and complex defense can be relaxed. In contrast, high ranking areas are candidates for refinement. This can be used to define locations for detection, fighting positions, and delay features. It can also be used to optimize the placement of security forces and the immediate response.

Improvements to Design to Reduce Target Set Vulnerability

The same process can be applied to the next generation plants to optimize physical security features and physical plant layout. The information developed in the prior section can be analyzed to determine what equipment should be collocated and equipment that should be separated. If the model is solved at the component level, the same process can be repeated and a ranking developed.

For example, if the component level success paths indicated the following in Table 5.

Table 5. Example Component Success Path Listing

1	EFW-A	DG-A	SWG-A	DC-A		
2	EFW-B	DG-B	SWG-B	DC-B		
3	EFW-C	DC-B	PRZ-B			
4	DG-A	RHR-A	SI-A	DC-A		
5	DG-B	RHR-B	SI-B	SWG-B		
6	SW-A	RHR-A	DG-A	DC-A	SWG-A	

Examining the scenarios, a pattern emerges that the same train of power including the DG, DC, and SWG are critical for many scenarios. It would make sense, therefore, to collate, to the degree possible, the electrical system. In contrast, the EFW trains appear as single items reflecting the ability to provide makeup to the steam generators from any of the sources. To avoid a significant loss that removes 50% of the available success paths, it is logical to separate the EFW pumps by physical barriers such that the adversary pays a time price to accomplish the loss of EFW.

Finally, the power trains represent a significant impact appearing in most all paths due to the reliance of equipment on ac or dc power. Therefore, care should be given to not collocate the power trains. Placing them at different plant elevations with barriers would provide the means for improved security while not resulting in adverse operational characterization.

Improvements and Limitations

The process defined above does not credit the inherent reliability of the component or the adversary goals. Inclusion of these two factors can have a measurable impact on the prior assessments and improve screening.

In general, high reliability components are generally not chosen targets by adversaries. Large physical components such as pumps, major bus work, and onsite power sources are typically targeted. With high reliability and low selection worth, these components can typically be removed from the target list.

When different paths are somewhat identical, such as #1 and #2 from the prior section, component reliability can play a factor in selection for retention. Adjustments can be made to address the selection worth that can increase or decrease the ranking value with the goal of determining the most reliable response to the adversary attack.

However, when addressing the location aspect of the path sets, the reliability of equipment is complicated when more than one target is within the same location. Several approaches could be taken:

- Highest cumulative equipment reliability
- Average of equipment reliability
- Summation of equipment reliabilities

These factors are subject to adversary preference for equipment damage order and is somewhat subjective. The inclusion of the selection worth can provide a means to introduce this variable.

The success paths at the location level are manageable in terms of assessing the ranking of each success path. However, due to the logic construct for most PRA models, the number of success paths at the component level can be significant. To make the project manageable, it may be necessary to develop a mixed model containing both location and equipment events.

The model does not consider the relative time differences between various scenarios. The timing will be based on the adversary path assessment. Regardless of the time involved, each success path provides the locations to be protected. This can be by delay or other feature that terminates the adversary timeline prior to success.

A limitation to this approach is that the risk model only addresses specific systems and equipment that are credited to maintain a safe-stable state given a requirement to cease power operation. Other systems that could influence the ability of the plant to response, area faults such a large pipe breaks, are not clearly specified unless external events are incorporated into the process and mapped to locations in a manner like the components.

A future ranking process could include the number of simulation or other adversary scenarios that incorporate a specific path set. This could provide an addition fraction to refine what path sets may be most challenged and would need to be improved to ensure physical security.

Conclusions

The use of PSA insights can help define the best options of systems and equipment to maintain safety after adversary is neutralized. This is done by a combination of ranking attributes for individual success paths taken from the PSA results.

These same results can be used to collocate and protect the most reliable options and allow for screening of equipment of lesser importance. The access control and physical security posture can be adjusted to concentrate on the best alternatives and reduced for other options. This will maintain adequate security and offer cost savings.

References

1. U.S. Nuclear Regulatory Commission. 10 CFR 73 - Physical Protection of Plants and Materials. 2019.
2. Zamanali, J. and C. Chwasz, Nuclear Power Plant Security Assessment Guide, 2013, NUREG/CR-7145, Information Systems Laboratories, Inc.: U.S. Nuclear Regulatory Commission
3. Brueher, W., et al., Nuclear Security Assessment Methodology for Regulated Facilities - Working Material - NUSAM Working Document of Analysis Working Group (Draft), 2017, IAEA,
4. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.81 Target Set Identification and Development for Nuclear Power Reactors, 2010,
5. Integrated Target Set Development, Restricted, Reliability and Safety Consulting (RSC) Engineers, Inc., RSC 14-75S, December 2017.
6. Risk Ranking of Target Sets and Target Path Sets, Restricted, RSC Engineers, Inc., RSC 14-76S, December 2017.
7. Garcia, M.L., Vulnerability Assessment of Physical Protection Systems, Sandia National Laboratories, 2006.