Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria

doi: 10.3850/ESREL2026061419_esrel26-p26113-cd

Generation Risk Assessment: System Design, Economic Impacts and Importance Measures

Curtis Lee Smith
Department of Nuclear Science and Engineering, Massachusetts Institute of Technology , USA.
E-mail: curtis@mit.edu

Emanuele Borgonovo
Department of Decision Sciences, Bocconi University, ItalyE-mail: emanuele.borgonovo@unibocconi.it

Probabilistic risk assessment (PRA) is the systematic process of constructing a model representing risks from hazards. A complete PRA identifies the scenarios that may lead to an undesired outcome, the likelihood of said scenarios, and the magnitude of the consequences. The scope of PRA can address a variety of undesired situations that may occur at a facility. One specific situation of interest is for cases where electrical power generation is lost. This case, loss of electricity generation, is evaluated using a Generation Risk Assessment (GRA).
In a PRA, it is first determined ”what can go wrong” by identifying hazards that may facilitate off-normal conditions or initiating events. Then, a scenario model for each initiating event that describes how the nuclear facility will respond to the off-normal condition is created. Next, the model is populated by assigning likelihoods for the initiating event and failures of applicable systems, components, software, or operators. The plant response modeling includes structures, systems, component (SSC) failures, and human error conditions.
A GRA uses a similar approach to modeling. First, the conditions that initiate a loss of electrical generation are determined. Then these conditions are evaluated in a scenario model to represent the off-normal condition. One element of GRA models, though, is they are time-dependent for a variety of factors including seasonal elements, demand conditions, and repair/restoration processes following a loss of electrical production.
Given the specificity of GRA, we need a specialised methodology to assess the importance of SSCs and gather insights through sensitivity analysis. We address the extension of traditional importance measures within this framework first. We then study the application of novel methods to manage the simultaneous presence of multiple and dynamic outputs.

Keywords: Generational Risk, GRA, Importance Measures, Reliability Analysis, Complex Systems Simulation.

1. Introduction

Probabilistic risk assessment (PRA) is the systematic process of constructing and quantifying a model representing risks from hazards, wherein either (or both) the likelihood and the consequences are treated probabilistically. A complete PRA identifies the scenarios that may lead to an undesired outcome, the likelihood of said scenarios, and the magnitude of the consequences. The scope of PRA can address a variety of undesired situations that may occur at a facility. One specific situation of interest is for cases where electrical power generation is lost. This case, loss of electricity generation, is evaluated using a Generation Risk Assessment (GRA).

In a PRA, it is first determined ”what can go wrong” by identifying hazards that may facilitate off-normal conditions (initiating events – Kaplan and Garrick (1981)). A scenario model for each initiating event that describes how the nuclear facility will respond to the off-normal condition is created. Then, the model is populated by assigning likelihoods for the initiating event and failures of applicable systems, components, software, or operators. The plant response modeling includes structures, systems, component failures, and human error conditions.

A GRA uses a similar approach to modeling. First, the conditions that initiate a loss of electrical generation are determined. Then these conditions are evaluated in a scenario model to represent the off-normal condition. One element of GRA models, though, is that they tend to be time-dependent for a variety of factors including seasonal elements, demand conditions, and repair/restoration processes following a loss of electrical production. Consequently, trying to represent the changes to a facility through time using static models such as fault trees and event trees becomes problematic and may result in models that are difficult to understand and maintain. Furthermore, time-dependent approaches such as Markov models become quite large as the number of elements increases which, for real systems, tends to be numerous, thus limiting their application in practice. For our application, the general process we used, and that which is described in this paper, is shown in Figure 1.

The focus of this paper is to provide an example of a GRA modeling approach, details of the model, baseline results, and design-specific sensitivity analysis for a hypothetical advanced reactor design using a state-based simulation-based approach.

2. GRA Modeling Approach

The GRA provides ways to focus on how a power generation system may not meet their intended operational outcomes. To perform a GRA, we need detailed information and associated modeling approaches for a variety of technical elements, including:

- Potential initiating events internal and external to the system that may affect the system in a way that would interrupt or degrade electricity production
- The components and their characteristics (including failure rates and economic impacts) that may contribute to system and plant performance for loss of electrical production
- Models to represent the scenarios leading to off-normal conditions
- Models to represent the down time following an off-normal condition until the time that electricity production is resumed
- Models to represent the economic consequences of lost electricity generation and other impacts such as replacement costs of failed equipment

From the GRA, several metrics are typically produced:

- The drivers and their impact to power generation economics
- The overall system failure frequency (how many down times might we see in one year)
- The overall system unavailability (what is the time that electricity production is interrupted compared to the total time the facility could have produced electricity)

For the hypothetical reactor GRA evaluation, a fault tree derived from the reactor PRA was created where only components that have a “fails to run” failure mode and could potentially cause loss of electricity generation (e.g., by tripping the reactor) were included. This initial fault tree approach was simply used to first scope-out the model and start to identify applicable failure conditions. However, the time-dependence aspect and economic consequences are difficult to include in a fault tree type of model. For example, timing of multiple events such as parallel component failures, multiple simultaneous repairs, and long-duration restoration all need to be considered. Consequently, the scoping fault tree can only used for initial exploration so a systems simulation code was used instead. Note that Markov models were not considered due to the complexity seen as the number of components and states increases.

The system simulation failure and economics modeling aspect are addressed through the use of the EMRALD open-source simulation tool. This tool is under development at the Idaho National Laboratory (and released through GitHub) with the goal of representing complex systems using risk and reliability analysis approaches. (INL (2024)) EMRALD focuses on a couple of important characteristics, including: (a) providing a simplifying modeling approach using states and a modern browser- based editor; (b) allowing the user to couple other software tools including

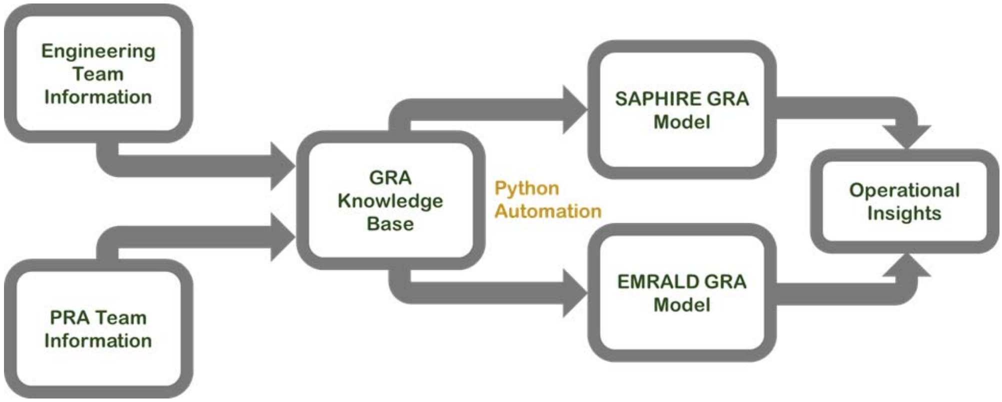

Fig. 1. The GRA model development process

physics simulations; (c) calculating detailed time-based sequence of system and component state-space evolution, and (d) allowing traditional aspects of reliability analysis such as fault trees. The analysis of EMRALD models takes place through a separate module that performs the probabilistic simulation. EMRALD adopts standard approaches such as the use of JSON for storing all modeling information.

As part of the model development automation, a reactor knowledgebase was created that is queried by the automation process to create specific elements of the GRA model. Within the GRA knowledgebase, the following items are represented

- Components and their associated system, subsystem, and ID
- Component upset condition failure modes and failure rates
- Restoration time categories for all components
- References used to support quantitative information

One important element of the GRA model is the time it takes to restore a component following a failure. The restoration times were represented by the following categories:

- Short (less than 24 hr)
- Medium (24-72 hr)
- Long (72-168 hr)
- Very Long (1 week - 1 month)
- Extended (1 month - 6 months)
- Indefinite (more than 6 months)
- Restore Following Grid LOOP
- Restore Following Plant-centered LOOP
- Restore Following Switchyard LOOP
- Restore Following Weather LOOP

Each of the components was assigned to one of the categories above. Note that a future enhancement to the GRA model would be to include a more complicated model for resource utilization and restoration time that could incorporate the type of failure.

3. EMRALD GRA Modeling Approach

EMRALD is simulation software that represents plant states, failure context, time, outage durations, and associated consequences. Since the model is a simulation of potential future events, it provides detailed plant transition timing and causal failure information. The EMRALD GRA model consists of:

- Simulation starting and boundary conditions
- Internal initiating events including loss of off-site power
- Component failure states
- Component restoration states
- Return to full power state
- Overall plant electrical production state as a function of time

- Consequences when reaching specific states

The EMRALD GRA model is run many times to determine potential plant behavior. From the many simulation runs, a data postprocessing step is performed to obtain results and operational insights. To begin a simulation we first create the facility starting points and a timer to defines the overall ”mission time” by which we will measure operational output and downtimes. This initial setup is shown in Figure 2 where we start the reactor at time t=0 and we start the mission time timer at t=0. For this example, the mission time is defined to be 1 year.

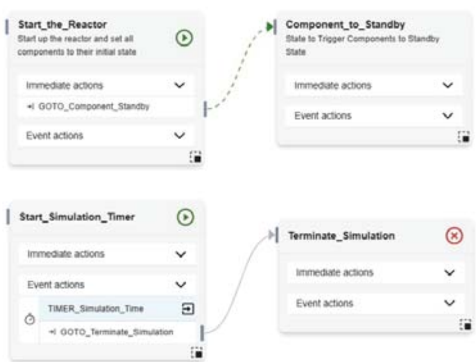

Fig. 2. Simulation setup in EMRALD.

Once the simulation starts, we need to track the status of the facility. Figure 3 shows the EMRALD diagram that activates all applicable components and then checks to see when one or more components fail. If enough components fail, as determined by their use in the facility, the production of electricity may be interrupted. This interruption state is captured by the ”System_Failed” state. Following a facility power interruption, the reactor will be restarted which itself takes some time and is represented by the state ”Reactor_Restart.”

Each component in the GRA model is represented by both a working and failed state. This modeling approach is shown in Figure 4. In this model, we determine times-to-failure and restoration times that provide state transition times.

Fig. 3. EMRALD model to check the overall facility status.

In this example, we represented a total of 73 key components including coolant pumps, heat exchangers, piping, electrical equipment, sensors, safety systems, and power supplies.

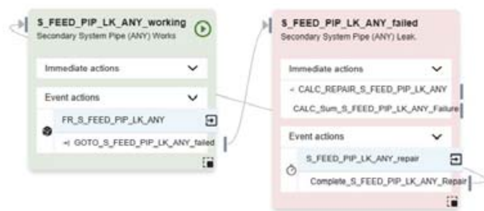

Fig. 4. Example of one of the components in the GRA EMRALD model.

4. Data Analysis of EMRALD GRA

Once the EMRALD GRA model has been created and debugged, the simulation is run many times to determine overall component and facility performance. To perform the data analysis and importance measure determination, we used a combination of custom Python and HTML-based analysis tools.

First, we created a Python tool to parse through the EMRALD simulation output and plot the component and system failure frequencies versus unavailability. The results of this initial analysis shows (see Figure 5), for each component or the overall system (in grey), its respective unavailability (x axis) for lost electricity production compared to its failure frequency (y axis). From this figure, we can see a comparison of individual components where worse-performing components will appear in the upper right part of the figure indicating they have both a large unavailability (causing the system to not produce power) and fail often (high failure frequency).

From the importance measure analysis simulation work we have reported previously (Borgonovo and Smith (2025)), we created an HTML-based tool that can read the detailed output file from EMRALD that complies all states (both for the components and system) and performed a detailed analysis using the approach found in (Borgonovo and Smith (2025)). The key features of this HTML tool are:

- Parsing the raw EMRALD data into a tabular (e.g., Excel) format
- Determination of average failure state times
- Plotting state arrival times
- Detailed importance measure calculation including Fussell-Vesely, Risk Achievement Worth, Risk Reduction Worth, and Barlow-Proschan
- Bootstrap analysis to evaluate results convergence

An example of the state arrival time plot is shown in Figure 6 where we show the time of system failure for each iteration (where 10,000 iterations were used). This plot illustrates the randomness of stochastic failures where some components may fail early in the operating cycle while other components may fail late.

To perform the importance measure calculation, there are four steps to follow:

Step 1: Select which state(s) represents system failure Step 2: Select which states to calculate importance measures for Step 3: Click "Calculate Importance Measures" Step 4: View the resulting importance measures showing which states most contribute to system failure

An example of the importance measures for the primary pumps and heat exchangers are shown in Figure 7.

Lastly, a bootstrap analysis is performed to determine how the calculated results converge for each type of importance measure. This step is vital in determining how accurate the numerical results are reported since they are based on a Monte Carlo simulation approach. We first show the Fussell-Vesely results (Figure 8) for the three primary pumps and then the Barlow-Proschan results (Figure 9) for the same pumps. Based upon the graphical results, it appears that the Barlow-Proschan calculation is 'more noisy' as compared to the Fussell-Vesely calculation. The reason for this insight is that the Barlow-Proschan importance measure quantifies a component's critical role in a system's reliability and is defined as the probability that the component's failure causes system failure. As such in a simulation approach, the Barlow-Proschan is conditional upon cases where the component failure time is the same as the system failure time (which is a small subset of all of the potential component and system failure cases). Thus, getting a significant number of the events required in the numerator of the Barlow-Proschan calculation calls for a large number of simulations to achieve convergence.

5. Economics Modeling

While the details of the economics modeling for the specific facility we evaluated are proprietary, we provide an example of how the economic losses from component failures can be evaluated. First, during the simulation, each time a component is failed, the economic impacts is recorded and then averaged over all of the iterations. The impacts that can be tracked include the downtime resulting in lost electricity generation, the labor costs to respond to the failure, and replacement costs of the new or refurbished components.

As an example of the economic modeling, we assigned hypothetical costs that result from each of the component failures where longer duration outages result in increased costs. For this example, the shortest duration outages were assumed to cost \$50,000 (USD) while the longest duration (of indefinite length) was assumed to cost \$10,000,000 (USD). Using this range of costs in the simulation, we found that the average yearly economic impact from component failures was \$198,000 (USD) per year.

6. Conclusions

We demonstrated the ability to simulate impacts and outages of a complex system through a GRA model. This approach used a state-based Monte

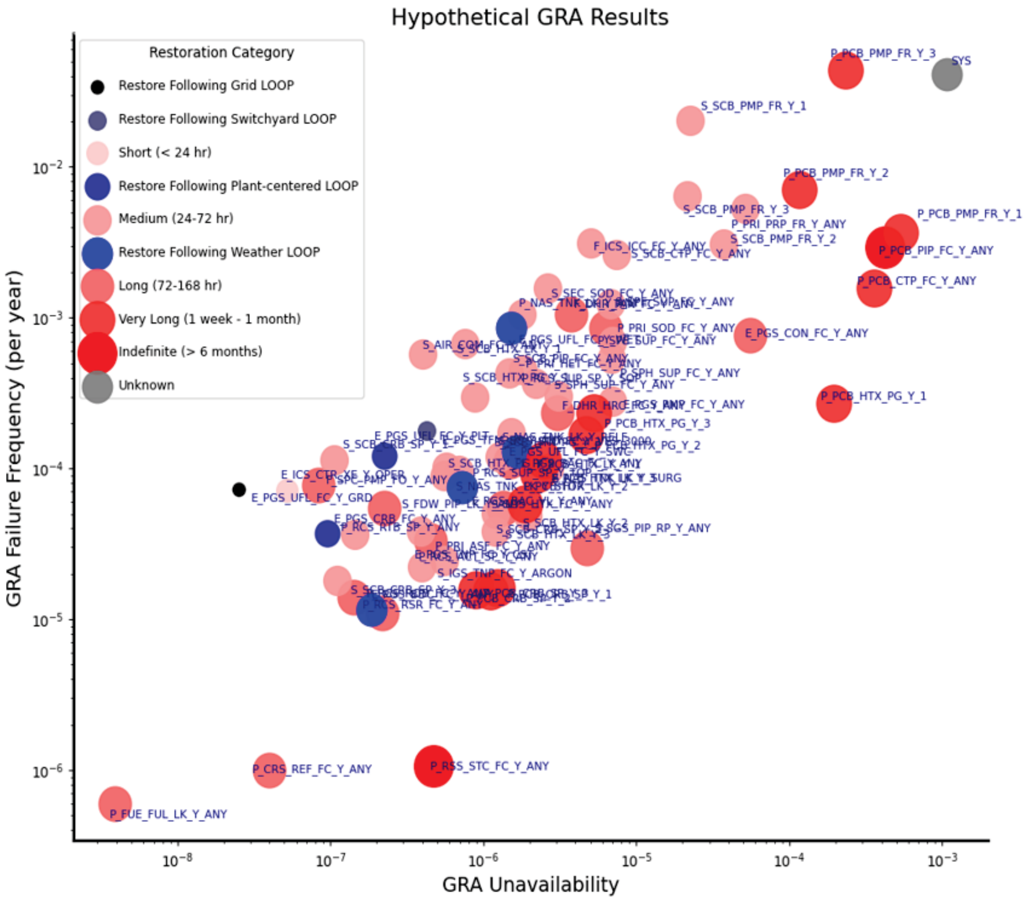

Fig. 5. Failure frequency and unavailability results for the example GRA model.

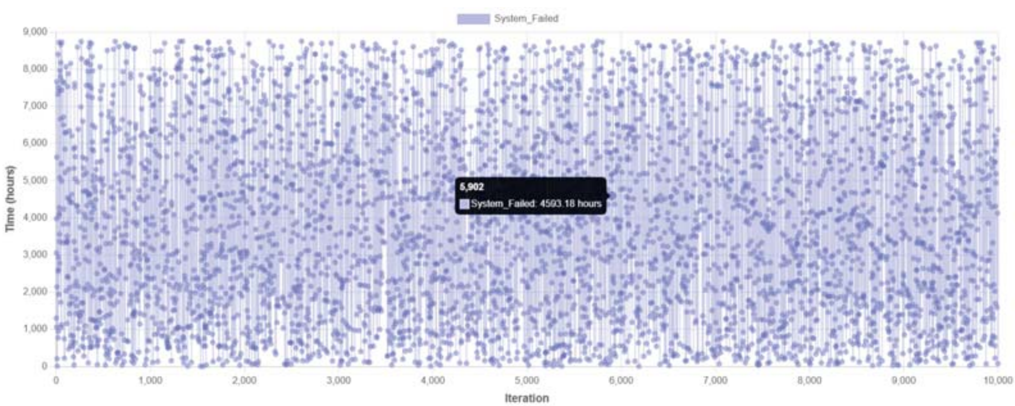

Fig. 6. Tracking system failure state times as a function of simulation iteration.

State Name	Fussell-Vesely (FV)	RAW	RRW	Birnbaum	Barlow-Proschan (BP)
P_BOUNDRY_PMP_FR_2_failed	0.04	1.04	1.00	0.02	0.00
P_BOUNDRY_PMP_FR_1_failed	0.04	1.05	1.00	0.03	0.00
P_BOUNDRY_PMP_FR_3_failed	0.04	1.07	1.00	0.03	0.00
P_BOUNDRY_HTX_PG_2_failed	0.02	2.20	1.01	0.55	0.02
P_BOUNDRY_HTX_PG_3_failed	0.02	2.20	1.01	0.55	0.02
P_BOUNDRY_HTX_PG_1_failed	0.02	2.20	1.01	0.55	0.01
P_BOUNDRY_HTX_LK_2_failed	0.01	2.20	1.01	0.55	0.01
P_BOUNDRY_HTX_LK_1_failed	0.01	2.20	1.01	0.55	0.01
P_BOUNDRY_HTX_LK_3_failed	0.01	2.20	1.00	0.55	0.01

Fig. 7. Importance measures calculated for primary pumps and heat exchangers from the EMRALD simulation.

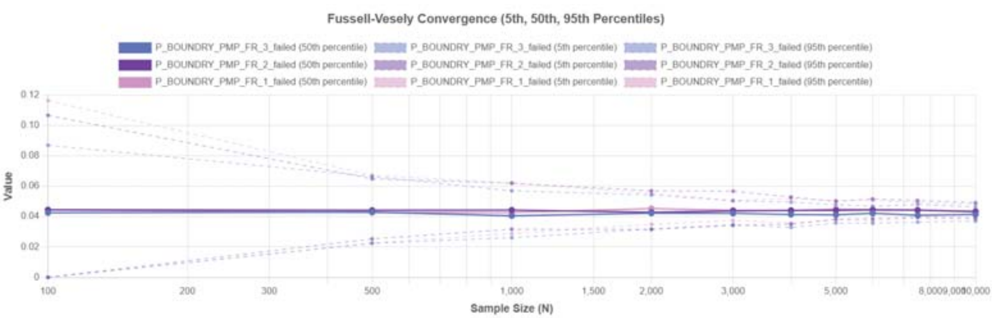

Fig. 8. Bootstrap convergence analysis for the Fussell-Vesely calculation.

Carlo simulation tool called EMRALD. Using this method, we can explicitly see the plant components, states, and transitions from working to failure. We can also sample from uncertainty distributions on any variable in the model allows us to factor in uncertainty directly in the calculation. From the simulation, we can readily extract detailed information such as timing, resources, and causes of failures. The model we created embodies 73 major components yet still takes less than 40 seconds to run 10,000 iterations on a consumer-grade laptop. Since the model itself is built using modules, it is easy to create component-specific diagrams that have unique failure modes and custom repair and restoration models. The detailed simulation output allows for a variety of post-processing data analysis to be performed including importance measure and bootstrap evaluation.

Acknowledgement

We acknowledge the support from our respective Universities in the creation of this paper. We testify that their tables and figures are our own works.

References

Borgonovo, E. and C. Smith (2025). Importance measures from complex reliability simulations. In *35th European Safety and Reliability Conference (ESREL 2025) and the 33rd Society for Risk Analysis Europe Conference (SRA-E 2025)*, pp. 330–337. Research Publishing Services.

INL (2024). The event modeling risk assessment

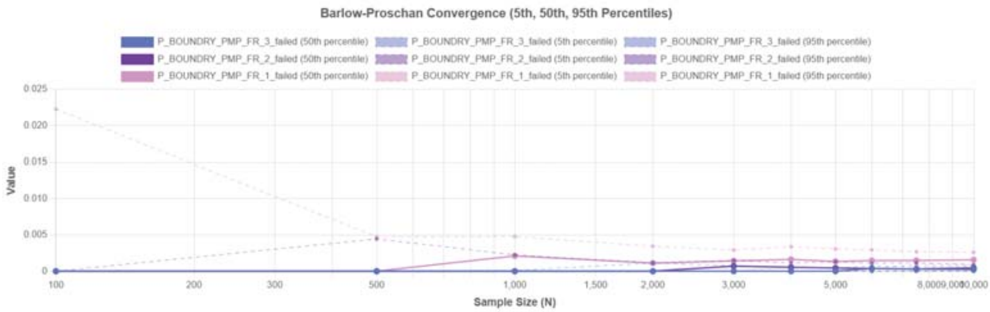

Fig. 9. Bootstrap convergence analysis for the Barlow-Proschan calculation.

using linked diagrams (emrald) open source software.

Kaplan, S. and B. Garrick (1981). On the quantitative definition of risk. *Risk Analysis I*, 11–27.