

# Case Study for Enhanced Accident Tolerance Design Changes

Steven Prescott  
Curtis Smith  
Tony Koonce

June 2014



U.S. Department of Energy  
Office of Nuclear Energy

**DISCLAIMER**

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

# **Case Study for Enhanced Accident Tolerance Design Changes**

**Steven Prescott  
Curtis Smith  
Tony Koonce**

**June 2014**

**Idaho National Laboratory  
Idaho Falls, Idaho 83415**

**<http://www.inl.gov>**

**Prepared for the  
U.S. Department of Energy  
Office of Nuclear Energy  
Under DOE Idaho Operations Office  
Contract DE-AC07-05ID14517**

## SUMMARY

The ability to better characterize and quantify safety margin is important to improved decision making about Light Water Reactor (LWR) design, operation, and plant life extension. A systematic approach to characterization of safety margins and the subsequent margin management options represents a vital input to the licensee and regulatory analysis and decision making that will be involved. In addition, as research and development in the LWR Sustainability (LWRS) Program and other collaborative efforts yield new data, sensors, and improved scientific understanding of physical processes that govern the aging and degradation of plant systems, structures, and components (SSCs) needs and opportunities to better optimize plant safety and performance will become known. To support decision making related to economics, reliability, and safety, the Risk Informed Safety Margin Characterization (RISMC) Pathway provides methods and tools that enable mitigation options known as risk informed margins management (RIMM) strategies.

The methods and tools provided by RISMC are essential to a comprehensive and integrated RIMM approach that supports effective preservation of margin for both active and passive SSCs. In this report, we discuss the methods and technologies behind RIMM for an application looking at enhanced accident tolerance design changes for a representative nuclear power plant. The focus area of this case study is an investigation of advanced 3D modeling and simulation specifically representing external (i.e., tsunami) and internal (as a result of the tsunami) flooding. We look at potential plant modifications and evaluate, using the RISMC approach, the implications to safety margin for the various strategies. Results are obtained by integrating probabilistic elements of a scenario (where components may fail either stochastically or due to the flood) with mechanistic elements for the flood evolution as it impacts the plant site and key buildings.

# CONTENTS

SUMMARY .....	ii
FIGURES .....	iv
ACRONYMS .....	v
1. BACKGROUND .....	1
2. RISMIC ANALYSIS .....	3
2.1 Overview .....	3
2.2 Bayesian Frequency Analysis.....	5
2.3 Plant SSC Response to Initiator .....	7
2.4 3D Facility Model .....	10
2.5 3D Physics Scenario Simulation .....	10
2.6 Optimal Facility Modifications .....	11
3. Results .....	13
3.1 Computation Recourses and Next Steps.....	17
4. CONCLUSIONS .....	19
5. REFERENCES .....	20
Appendix A –Simulating Scenarios .....	16

## FIGURES

Figure 1: Representation of the Interaction of Degradation Mechanisms That May Impact Plant.....	1
Figure 2: Steps of the Analysis to Model Tsunami Initiating Events .....	3
Figure 3. The key steps of the RISMCM methodology.....	4
Figure 4: Results of the Bayesian Extreme Value Analysis Compared to a Simpler Poisson Model (bars represent 90% intervals while the point represents the mean) .....	6
Figure 5: Example of a Fault tree (top) and Event Tree (bottom) used in traditional PRA modeling. ....	8
Figure 6: State diagram example. ....	9
Figure 7: 3D model of a nuclear reactor facility to be used for simulation testing.....	10
Figure 8: Water penetration points such as doors or ventilation panels.....	11
Figure 9: Facility Model Modifications .....	12
Figure 10: Measuring tsunami wave crest height using 12 million particles.....	13
Figure 11: Flow path of a 19 meter tsunami measuring vent penetration points.....	13
Figure 12: Flow rates for 19 meter tsunami.....	14
Figure 13: Flow rates for 28 meter tsunami.....	15
Figure 14: Water movement through facility for a 19 meter tsunami just reaches the reactor bay door. ...	16
Figure 15 : Results for 38 meter tsunami only have the bay door. ....	17

## ACRONYMS

GEV	Generalize Extreme Value
INL	Idaho National Laboratory
LOSP	loss of offsite power
NOAA	National Oceanic and Atmospheric Administration
PRA	probabilistic risk assessment
RIMM	Risk Informed Margins Management
RISMC	Risk Informed Safety Margin Characterization
SSC	system, structure, and component
LWR/LWRS	light water reactor/sustainability
SBO	station blackout

# Case Study for Enhanced Accident Tolerance Design Changes

## 1. BACKGROUND

The purpose of the Risk-Informed Safety Margin Characterization (RISMC) Pathway is to support plant decisions for risk-informed margins management, with the aim to improve economics and reliability and sustain safety of current nuclear power plants. The goals of the RISMC Pathway are twofold: (1) develop and demonstrate a risk-assessment method coupled to safety margin quantification that can be used by nuclear power plant decision makers as part of their margin recovery strategies; and (2) create an advanced RISMC toolkit that enables a more accurate representation of a nuclear power plant safety margin. In order to carry out the research and development needed for the RISMC Pathway, the Idaho National Laboratory (INL) is performing a series of case studies that will explore methods and tools-development issues. In this report, we show a case study focused on demonstrating the RISMC approach using a representative nuclear power plant. As part of the demonstration, we describe how mechanistic and probabilistic safety calculations are integrated and used to quantify margin recovery strategies as a part of Risk Informed Margins Management (RIMM).

The ability to better characterize and quantify safety margin holds the key to improved decision making about light water reactor design, operation, and plant life extension. A systematic approach to the characterization of safety margin and the subsequent margin management represents an input to the licensee and regulatory analysis and decision making that will be involved. In addition, as research and development in the LWRS Program and other collaborative efforts yield new scientific understanding of aging and degradation, opportunities to better optimize plant safety and performance will become known. This interaction of degradation understanding and potential impacts to plant margins are shown in Figure 1.

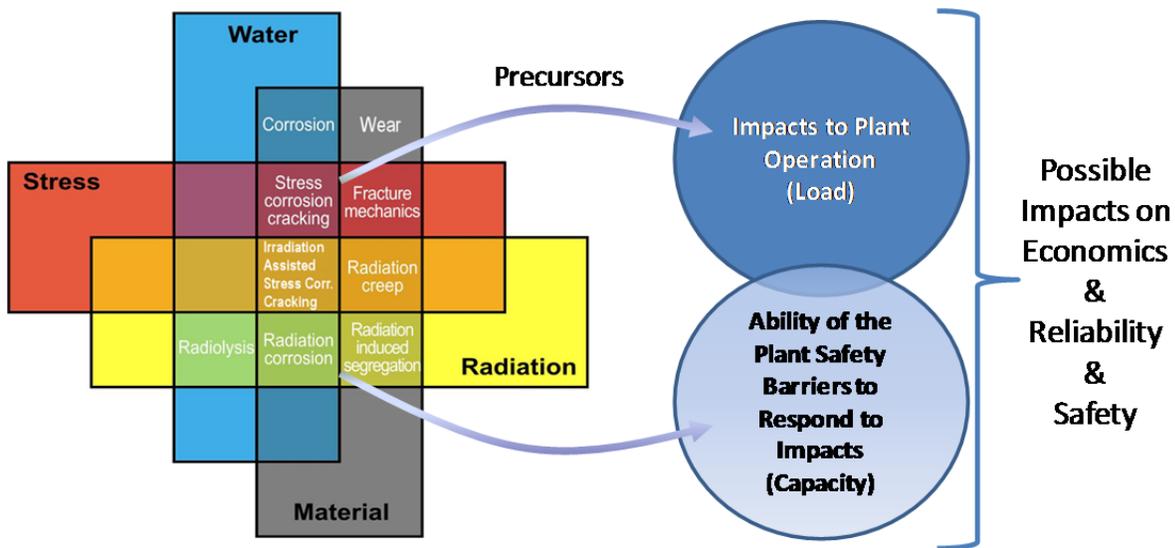


Figure 1: Representation of the Interaction of Degradation Mechanisms That May Impact Plant

## Operations and Safety Barriers If Left Unmitigated

In this report, we describe the approach used for the RISMIC process for enhanced accident tolerance design changes – that is proposed modifications (i.e., design changes) to the plant that will help it to withstand potential upset conditions (i.e., accident tolerance). To demonstrate technical issues and solutions, we use a representative nuclear power plant that is located near the sea in order to consider potential external events such as loss of offsite power (LOSP) or a tsunami. The methods described in this report would also be applicable to other initiating events such as transients and external events such as river/rainfall flooding.

## 2. RISMIC ANALYSIS

### 2.1 Overview

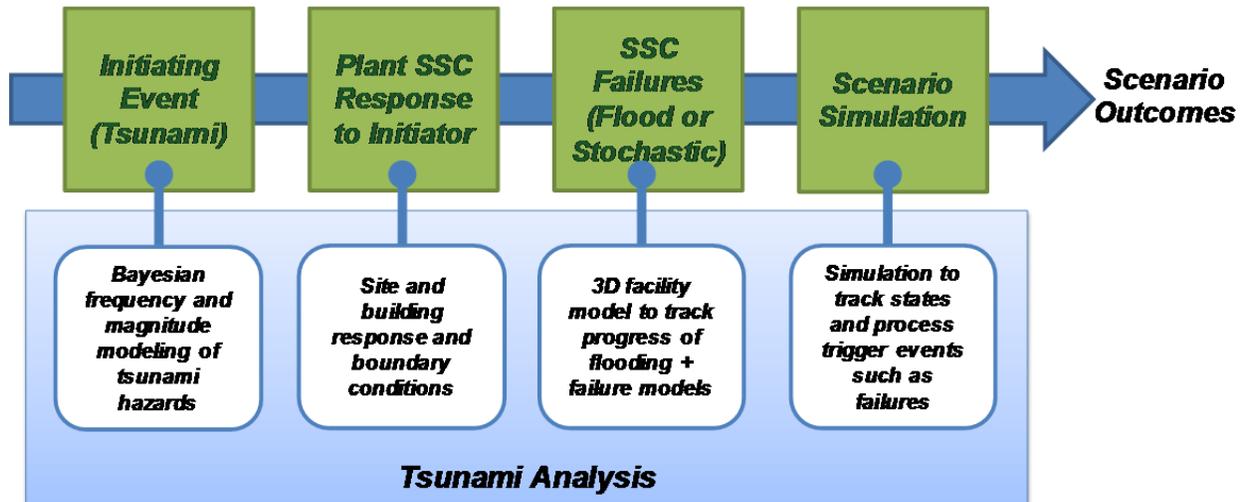


Figure 2: Steps of the Analysis to Model Tsunami Initiating Events

Traditional probabilistic risk assessment (PRA) includes Bayesian frequency analysis combined with system fault trees in a static model. To get a more complete picture of what outcomes are likely for a given scenario, we must be able to include a dynamic or stochastic representation of the model. It should have “real world” behavior that can then be used in the deterministic model to give a final outcome (or end state) for the given facility and scenario. This real world behavior can be represented through 3D modeling of a facility and execution of a scenario through a physics simulation engine for different impacts such as fire, floods, winds, earthquakes, etc. In this report, we demonstrate how we can add these types of 3D simulation techniques and use them to do improve analysis and investigate cost effective modifications to increase the safety of the facility specific to flooding impacts.

The overall analysis approach we used for RIMM is captured in the generic RISMIC methodology steps (see Figure 3), taken from (Smith, Rabiti, & Martineau, 2013).

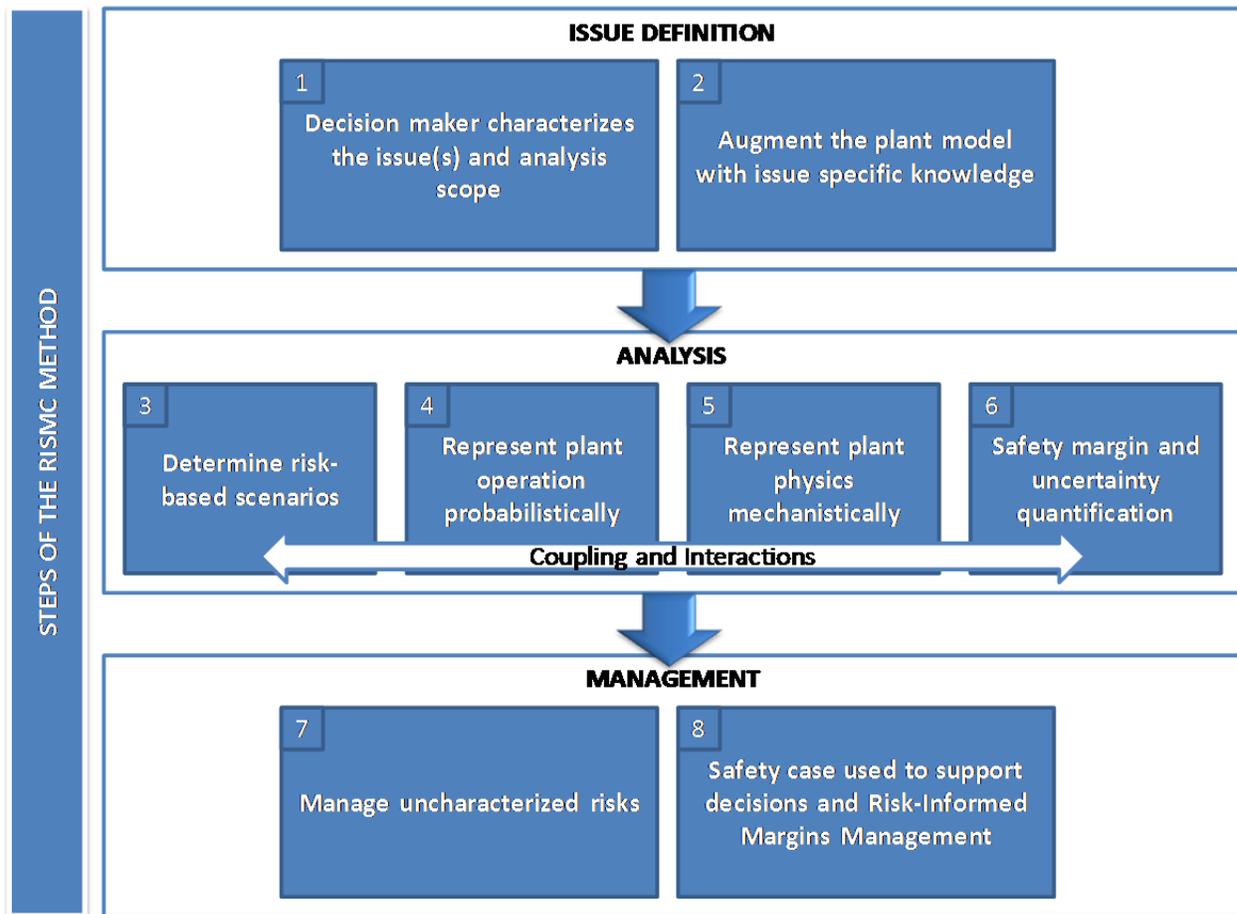


Figure 3. The key steps of the RISMC methodology.

The following steps (shown at a high level above) are to be carried out for each potential design modification under consideration. Note that these steps have been formulated to enable a direct comparison between RIMM alternatives. Explanatory information of the RISMC analysis steps are provided below:

1. Formulate an issue space that includes steady-state and accident condition space. Formulate definitions of functional failure in terms of key performance parameters. This step includes incorporating the boundary conditions for the types of tsunamis under consideration.
2. Conduct a tailored failure modes and effects analysis to establish which induced failure modes need to be simulated in order to address the performance parameters identified above. This step includes consideration of potential failures of SSC from traditional stochastic failure modes (e.g., fails to start, fails to run) and failures from the flood itself.
3. Choose applicable scenarios to analyze, including normal and off-normal conditions. This step includes traditional scenarios such as loss-of-offsite power (LOSP), station-blackout (SBO), and external flooding.
4. Formulate models, including uncertainties, for the plant boundary conditions that will occur during each applicable scenario. This step includes the creation of simulating the stochastic

- failures (see Appendix A for information on this simulation process) and the arrival of a tsunami of a certain magnitude (e.g., height and volume of water entering the plant site).
5. Couple the probabilistic behavior to applicable mechanistic models. This step includes linking the probabilistically-generated scenarios (including the tsunami arrival) with 3D site and building models in order to represent the possibility for flooding.
  6. Simulate scenarios in order to quantify for the desired figures of merit. This step includes running multiple scenarios for multiple configurations (representing different possible accident tolerant design changes) and tracking user-prescribed metrics such as the degree of damage, probability of core damage, or water ingress into critical buildings.
  7. Perform sensitivity analysis to determine limitations and drivers of the analysis. For this step, expert judgment may be required in order to determine where unknowns may be important to decision making.
  8. Quantify performance results such as the probability of failure consistently across RIMM alternatives. This step provides the overall results of the analysis.

## 2.2 Bayesian Frequency Analysis

The Bayesian interpretation of probability theory underlies modern risk assessment. Permeating through all of risk assessment, Bayes' theory provides a basis for formulating and manipulating event probabilities, initiating frequencies, and model parameter uncertainties. Specifically, Bayes provided a technique to process evidence based upon conditional probabilities. In its simplest form, Bayes' equation states:

$$p(\theta|x) = p(\theta)p(x|\theta)/p(x)$$

where  $p(\theta | x)$  is the posterior probability distribution of event (or hypothesis)  $\theta$ ;  $p(\theta)$  is the prior probability distribution (i.e., what is known about the outcome prior to gathering operational evidence);  $p(x | \theta)$  is the chance of observing a particular outcome or set of evidence (given  $\theta$ ); and  $p(x)$  is the unconditional probability of the evidence  $x$  (given any  $\theta$ ). Note that in the general case, we have a set of events or hypothesis and, for these cases,  $\theta$  should be replaced by  $\theta_i$ .

It should be noted that the term  $p(x | \theta)$  represents a probabilistic model – the probability of seeing a particular observation conditional upon  $\theta$ . The other two terms on the right side of Bayes' Theorem,  $p(\theta)$  and  $p(x)$ , are probability distributions. For the analysis in this report, we need to determine the initiating event frequency for tsunamis since we wish to simulate (and potentially prevent damage by using RIMM) a variety of potential events. Consequently, we will investigate a probabilistic model that will represent the arrival frequency of different magnitude (i.e., heights) tsunami events.

In our simulation model, we actually use a variety of probabilistic events; a component fails to start; a component fails to run; the frequency of a tsunami; etc. While these events describe different situations for different contexts, one underlying feature they all exhibit is the fact that they are all conditional probabilities or frequencies.

The first step in the analysis is to perform Bayesian analysis of initiating events for the frequency of tsunami events. The goal of the Bayesian modeling for extreme event initiators (e.g., tsunamis) is to gain insight as to the expected tsunami height for various return periods given historical data, and to make predictions as to the expected tsunami heights for longer return periods for a given location. The desired result is a distribution of expected tsunami heights for various return periods (i.e., yearly, every 10 years, every 100 years, etc.) based upon observed historical events.

For this analysis, historical tsunami data for this study was obtained from the National Oceanic and Atmospheric Administration (NOAA). The data is available for download from the NOAA website, [http://www.ngdc.noaa.gov/hazard/tsu\\_db.shtml](http://www.ngdc.noaa.gov/hazard/tsu_db.shtml). The download file contains details for all known tsunamis world-wide from 2000 B.C. to present, including; maximum wave height, magnitude and location of seismic initiating event, and other attributes.

The case analyzed and discussed in this section includes all known historical tsunami events affecting the north-east portion of Japan as an example of the types of events that may occur for a site located on the coast. In order to obtain these data from the large data file from NOAA, all tsunamis affecting Japan were retained from the overall data file. Screening the data resulted in data ranging from 1611 to 2013, 403 years.

The historical data was sufficient in developing wave heights for *observed* return periods, but unable to predict maximum wave heights to be expected for longer return periods. An “extreme value paradigm” is used in order to extrapolate observed data for estimation of the predicted return period wave heights for longer periods (i.e., 10,000 years and 100,000 years). Specifically, the generalized extreme value (GEV) family of distributions is used to perform an asymptotic extrapolation of the known data. For this hypothetical example, we created an OpenBUGS script to perform the Bayesian inference, building upon the GEV modeling as described in Chapter 13 of (Kelly & Smith, 2011). The results of this analysis are shown in Figure 4.

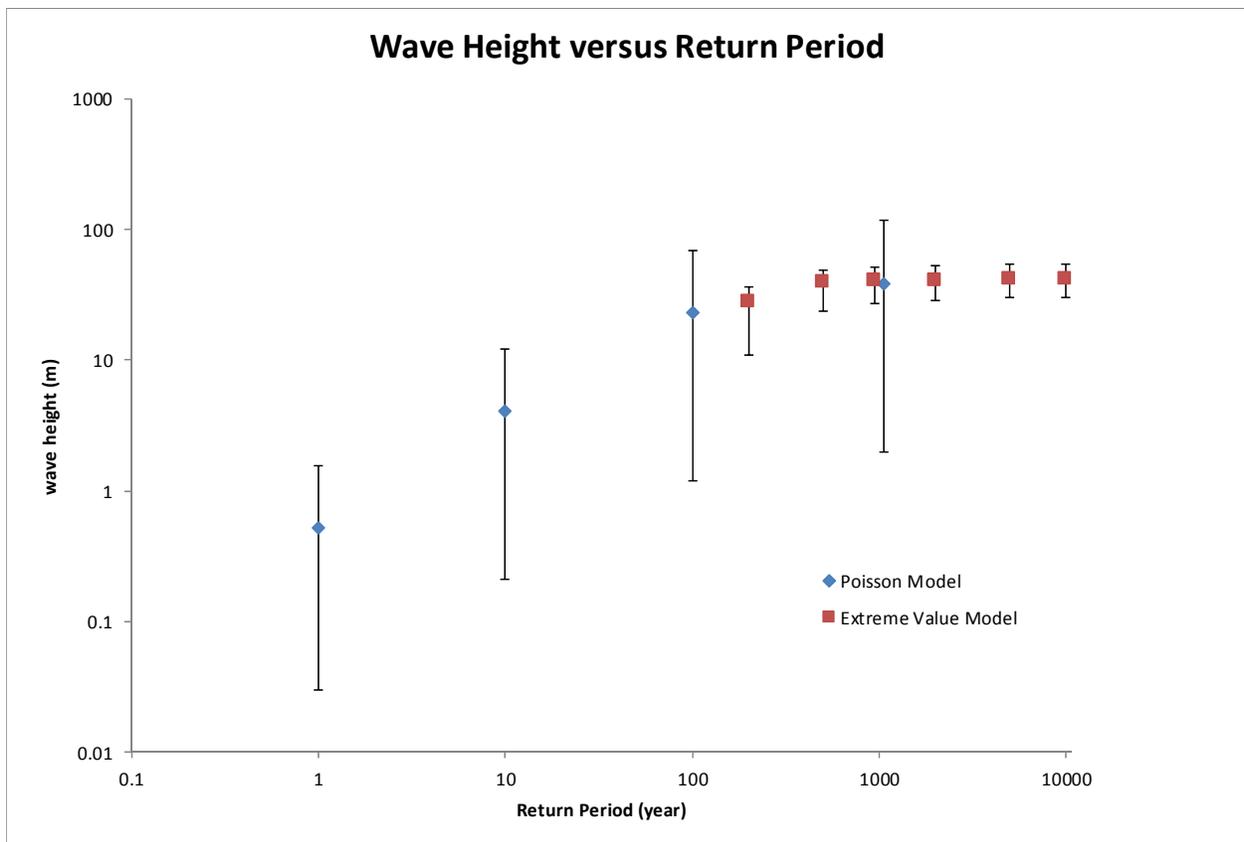


Figure 4: Results of the Bayesian Extreme Value Analysis Compared to a Simpler Poisson Model (bars represent 90% intervals while the point represents the mean)

## 2.3 Plant SSC Response to Initiator

Most PRA plant modeling is made up of components with different failure modes, probabilities, and rates. Typically, these components are grouped into various systems and then are modeled together (in different combinations) as a “system” with logic structures to form fault trees (see Figure 5). Applicable fault trees are combined through scenarios, typically represented by event tree models (see Figure 5). Though this method gives us failure results for a given model, it has limitations when it comes to time-based dependencies or dependencies that are coupled to physical processes which may themselves be time-dependent. For example, if we wish to consider potential component or system failures as a result of a flooding event, the details of the flood (when, where, and how much) become very important and are quite difficult to represent in static models such as fault trees. As we describe in this and later sections, instead of using traditional static models, we couple probabilistic simulation of components to mechanistic analysis representing the flooding event in order to determine which (if any) components fail, when they fail, what caused their failure, what impact these failures have on associated systems, and what impact system failures have on the overall plant.

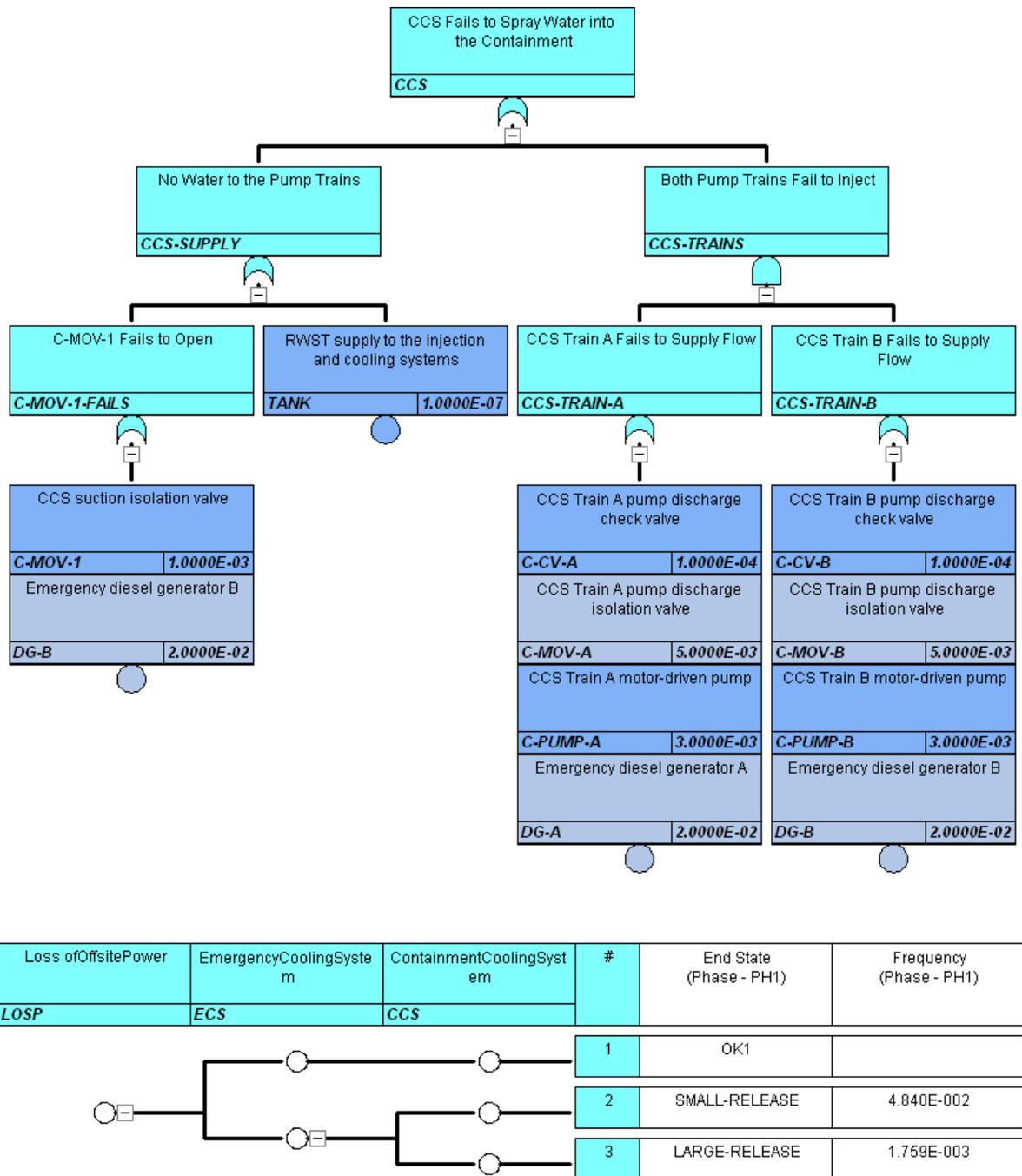


Figure 5: Example of a Fault tree (top) and Event Tree (bottom) used in traditional PRA modeling.

Typical PRA modeling can easily be converted into an equivalent “State Diagram.” (See Figure 6) The new model converges to the same results by evaluating multiple stochastic iterations. A state diagram model allows for incorporation of time related interactions such as those from 3D Physics simulations.

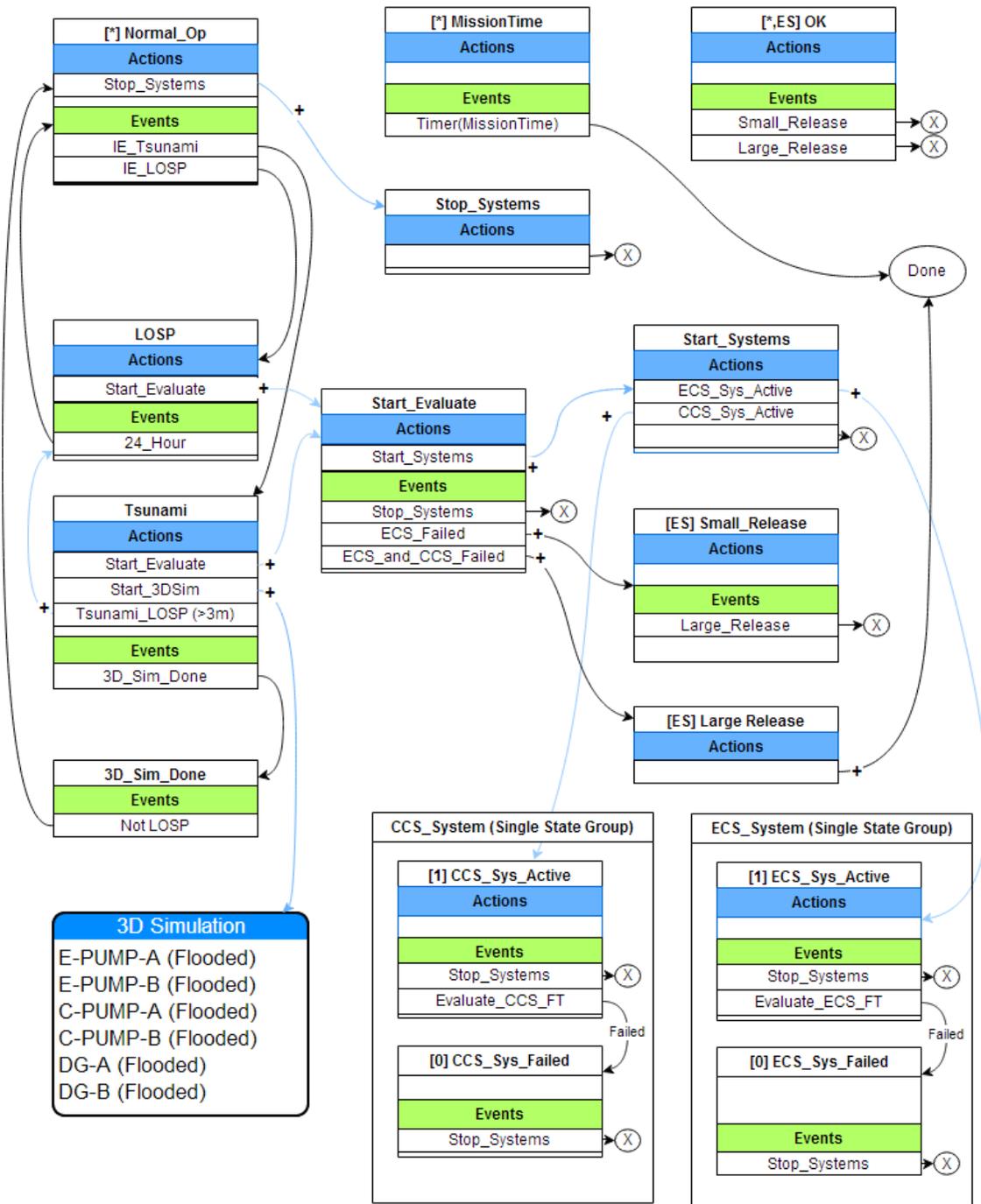


Figure 6: State diagram example.

For this scenario we converted the “Advanced Demo” model originally created using SAPHIRE into a state diagram model and added an initiating event for a tsunami. The frequency and magnitude of the tsunami wave is determined through the Bayesian Analysis discussed in section 2.2.

## 2.4 3D Facility Model

For this advanced analysis, a detailed 3D model or models of the facility must be created. This model not only consists of the buildings and structures of the facility but it also includes any components that can be affected by any of the desired scenarios. The models of a facility can be broken up into different sections or just different level of details in order to optimize run times for the various scenarios. For our example we have a cross section of the facility which includes one turbine and reactor building. Then we created a more detailed model of the reactor and diesel generator building for more detailed analysis of component failures. An example of the detail level for the 3D site model is shown in Figure 7.

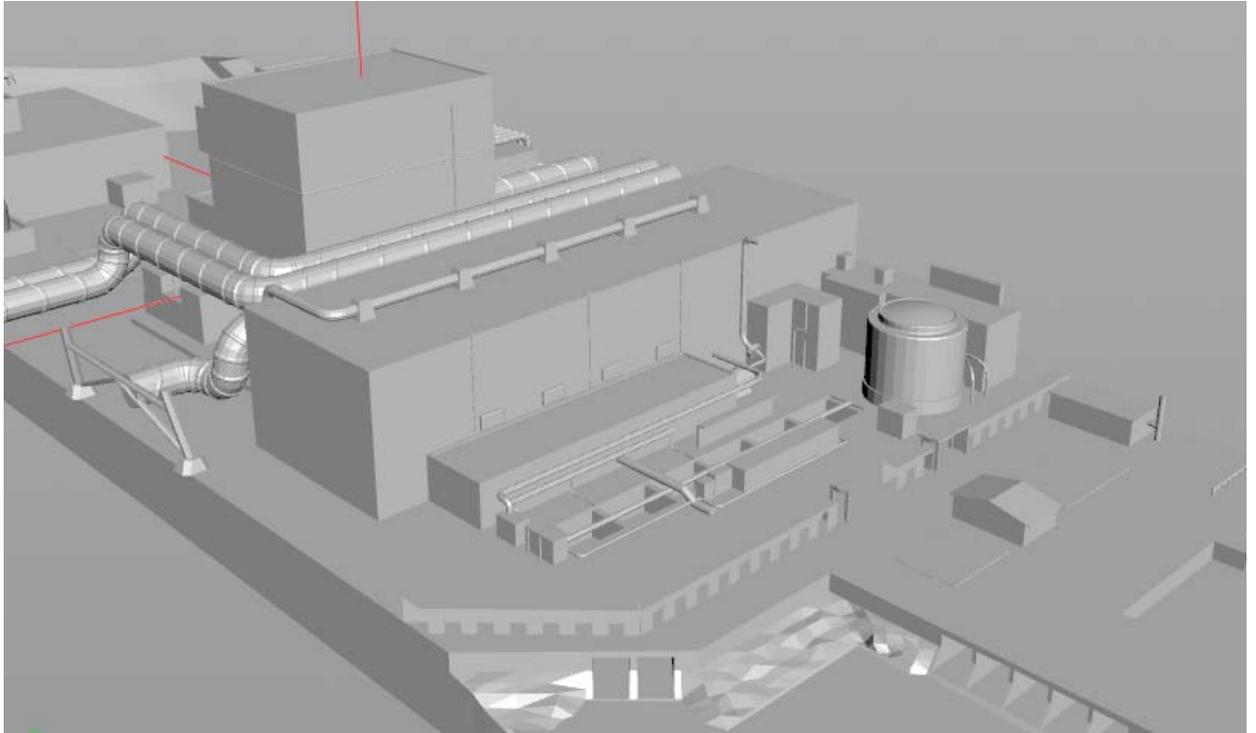


Figure 7: 3D model of a nuclear reactor facility to be used for simulation testing.

## 2.5 3D Physics Scenario Simulation

With these 3D models, various scenarios can be created that use a physics engine to simulate real world interactions and determine potential outcomes based upon the physics. As stated earlier, for this example we will be analyzing different tsunami events. To do this we first used a section of the facility and created different large waves with simulated water particles. When running a simulation model, the particles flow and move very similar to (or representative of) how real water would behave in a real facility (see Figure 8). Using a large facility model, potential water flow into various facility buildings or structures can be determined by monitoring the water at the penetration points such as doors and vents. By running this larger model with different tsunami levels we can extrapolate data for waves in between the simulated levels. General seepage amounts could also be added by understanding the height of the water impinging upon leak paths such as doors or penetrations. The flow tracking and water monitoring conditions can then be used for more detailed simulations inside facility buildings to determine what component failures occur for randomly sampled tsunami events. These dynamic simulation results are

then included into the nominal risk model to give better overall PRA results. Once we have the results from these simulations, we can use them as a baseline to compare with any changes we make to the facility in order to determine the efficacy of potential accident tolerant design changes.

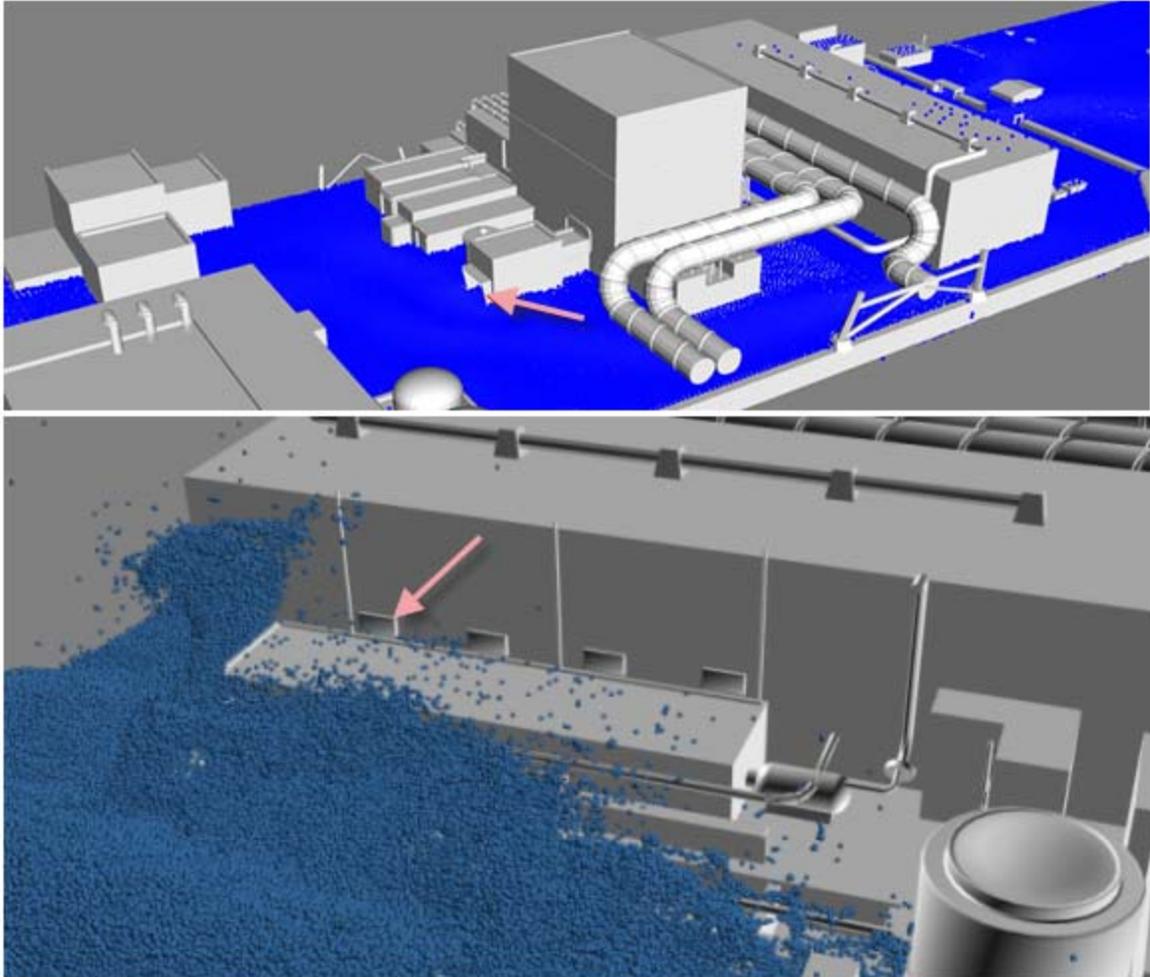


Figure 8: Water penetration points such as doors or ventilation panels.

## 2.6 Optimal Facility Modifications

Using the baseline results from the existing facility, different modifications can be made and tested to determine which modifications give the improved results (and the degree of safety improvement) for a variety of simulations. In our initial design change, we have moved the intake vents from the side wall of the building to the top of the building, thereby reducing a potential ingress path for water from large tsunami events (see Figure 9). In the second design change, a standard exterior door was replaced with a more substantial (i.e., submarine-type) door. With each of these design changes to the model, the water penetration into the facility buildings is recalculated given various tsunami waves. The building simulations also need to be run in order to determine any component failures.

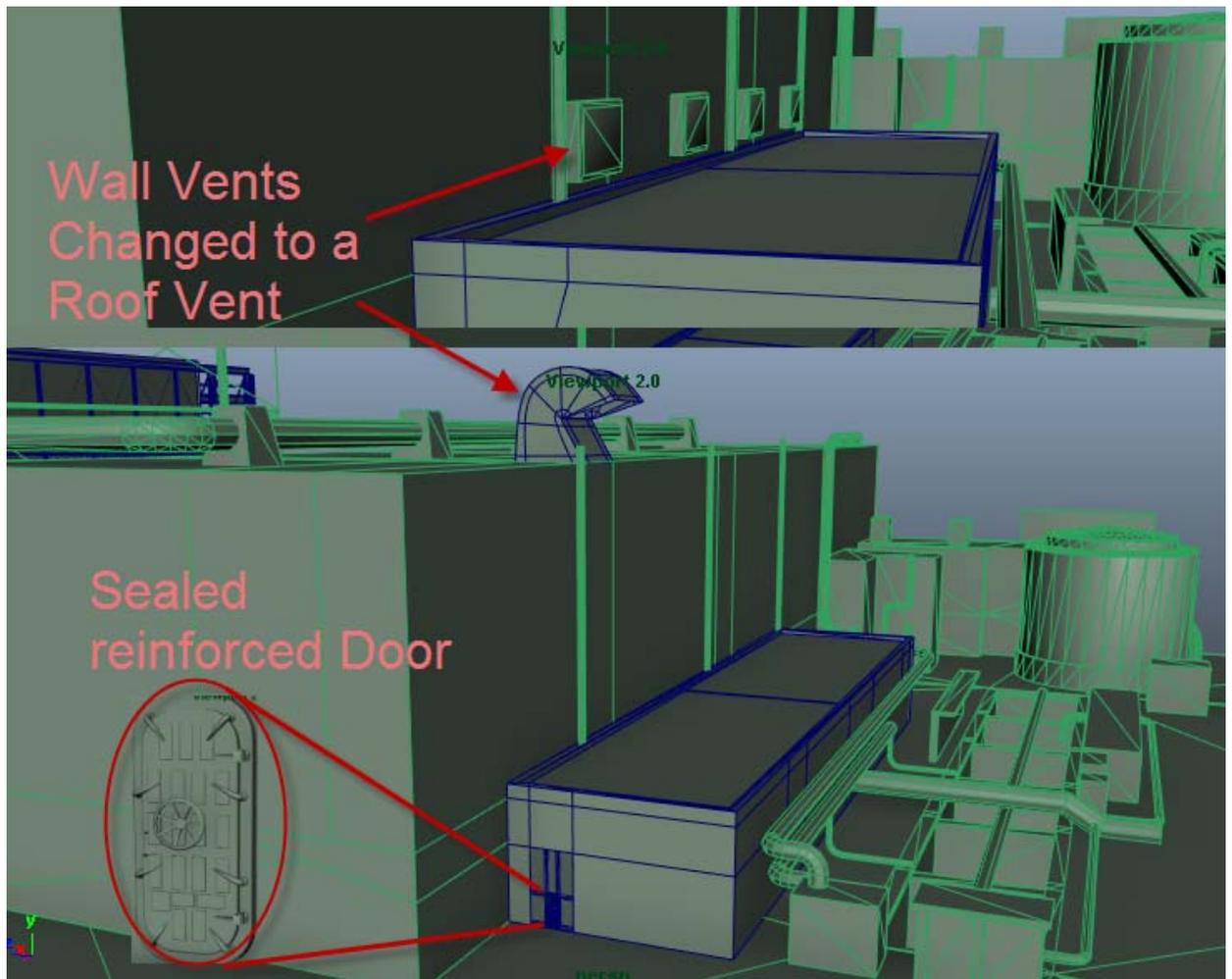


Figure 9: Facility Model Modifications

The simulation results based upon the accident tolerant design changes can tell us two things. First, what level of a tsunami can our changes protect against, if any. Second with PRA integration we can determine, how much the modifications reduce overall risk level. Note that in real cases, many different design changes can be tested to determine a cost effective and viable solution. In this demonstration case for potential accident tolerant design changes related to flooding external events, we only considered a subset of possible changes.

### 3. Results

For our initial analysis, we have tested different tsunami heights and measured the water level at the reactor building loading door, vents into the generator room, and an exterior man door into the generator room. These simulations used 12 million particles to determine flow paths and flood heights at any time and location in the facility.

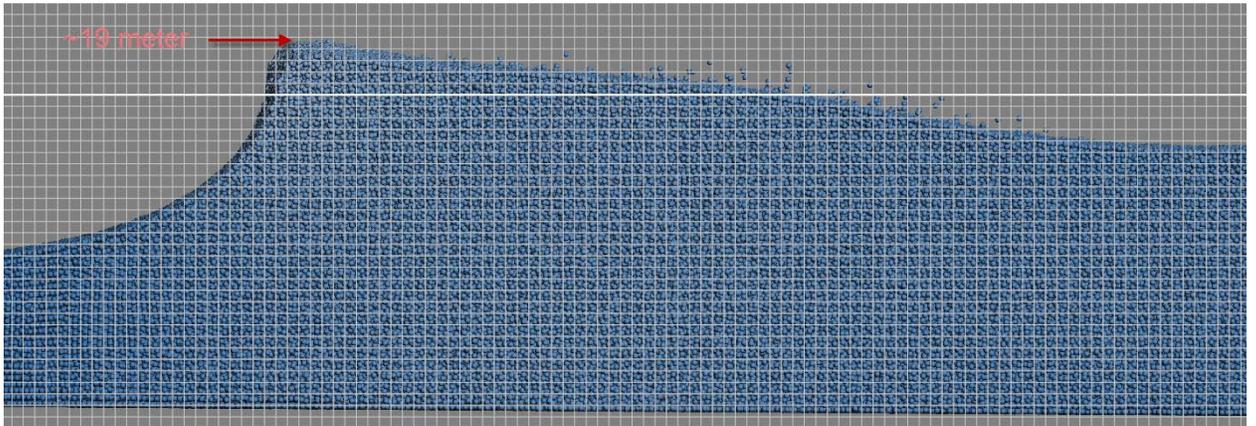


Figure 10: Measuring tsunami wave crest height using 12 million particles.

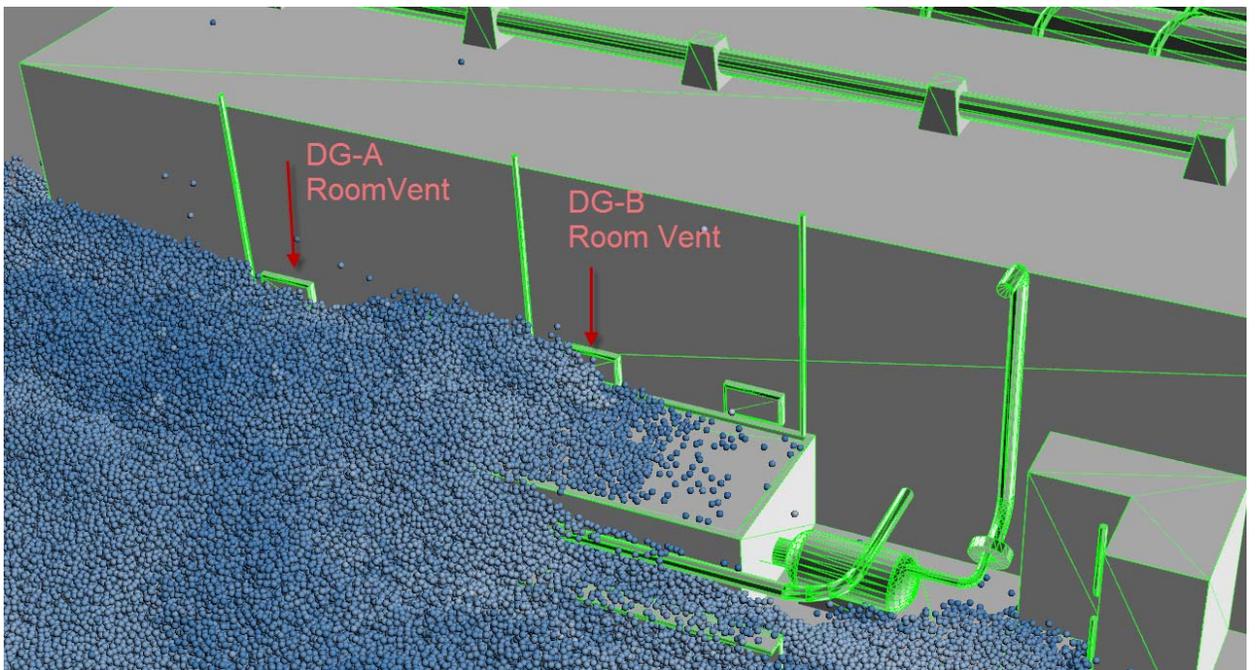


Figure 11: Flow path of a 19 meter tsunami measuring vent penetration points.

The simulation calculations shown below are an approximation of flow from water height pressure only not including wave impact pressures (see appendix 1.3). The code for getting accurate pressure and velocity on simulation objects is being added currently and will be included in any future simulations. These large model simulations take the most computational resources. Sub simulations, which provide component failures for flooding inside facility buildings, take less time and resources per simulation, but were not completed in this phase.

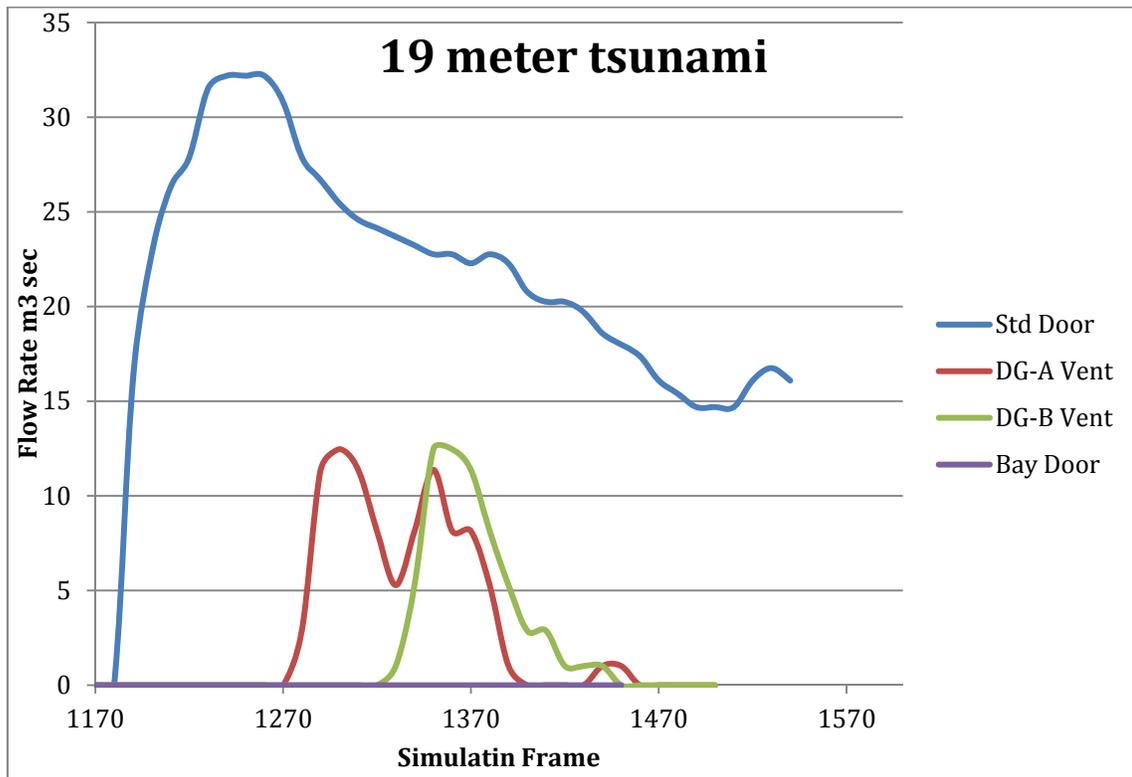


Figure 12: Flow rates for 19 meter tsunami.

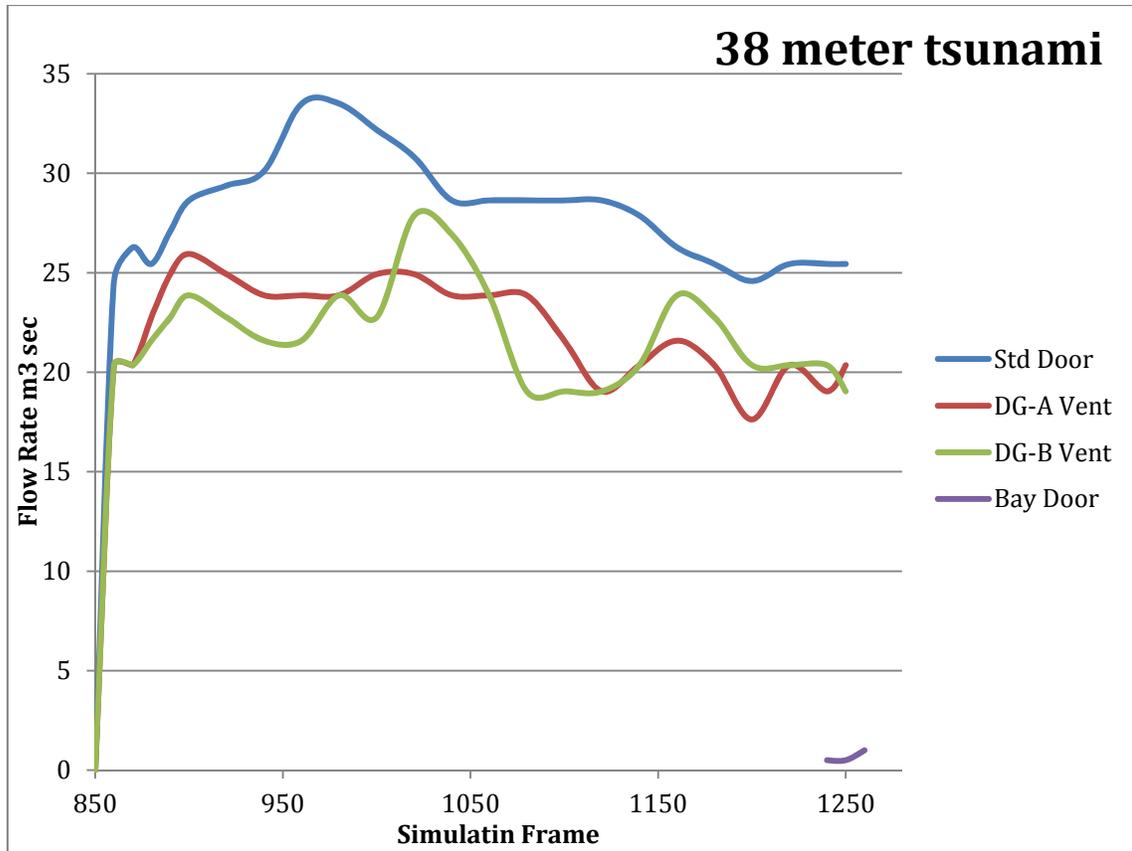


Figure 13: Flow rates for 28 meter tsunami.

The flow rate from the generator man door initially only has gap seepage until door failure. (We are assuming average door failure at 1 psi or 6895 Pascal from tests done by FEMA. This equates to door failure at .75 meters.) Door failure is almost immediate and results in full flow. Venting provides a major access point for both the 19 and 38 meter waves, smaller waves would result in only splash and spray entry. However, small amounts of water in the venting can cause diesel generator failure if it gets in the air intake. Water in the reactor building is also a major concern for larger tsunamis but the simulation shows that anything under a 19 meter wave would not reach the reactor room for this facility model. These results from the original model can then be used as a comparison for any other modifications.

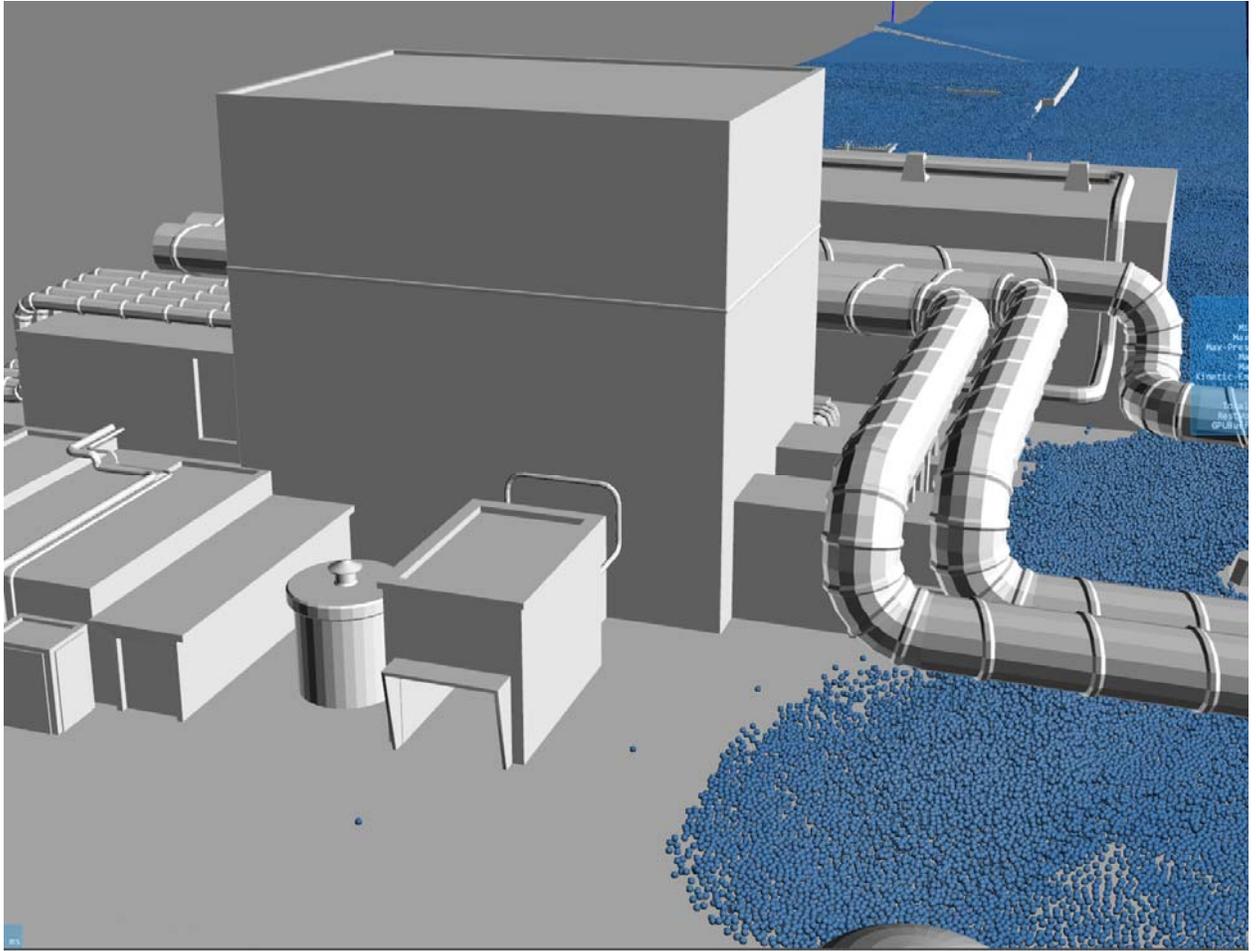


Figure 14: Water movement through facility for a 19 meter tsunami just reaches the reactor bay door.

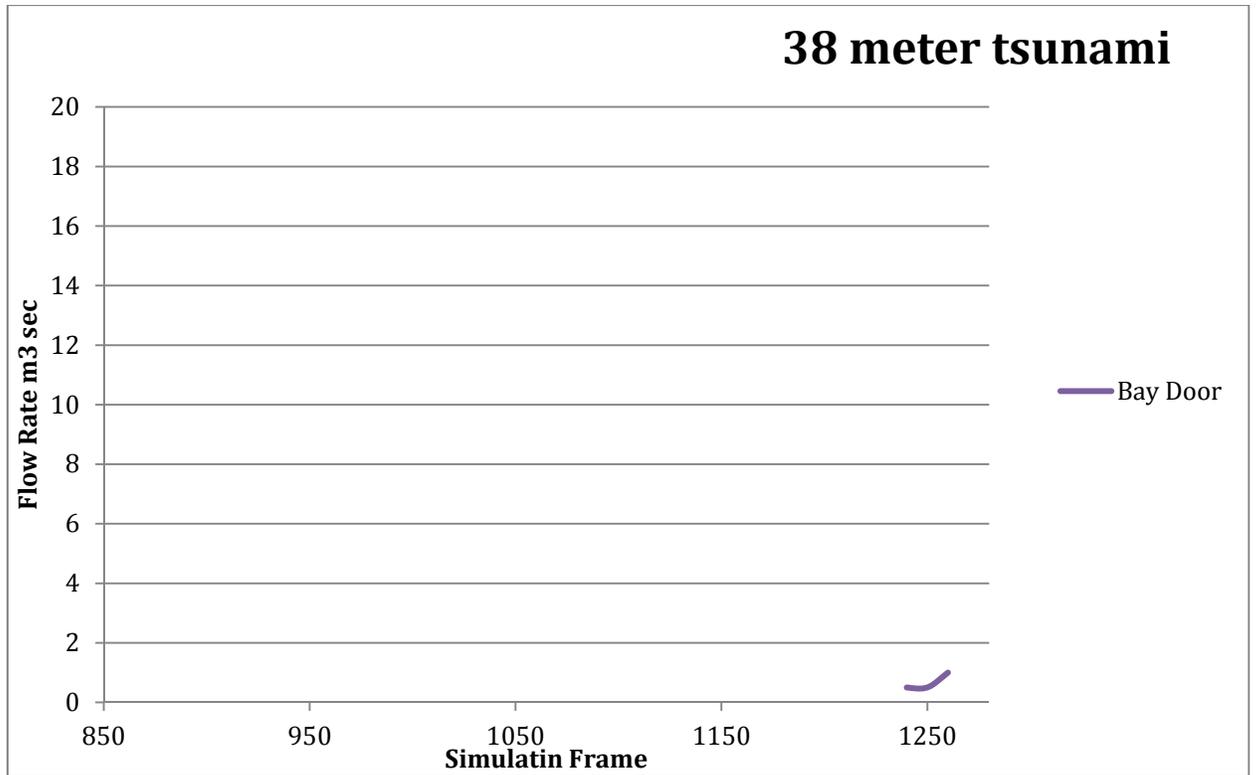


Figure 15 : Results for 38 meter tsunami only have the bay door.

By moving the venting to the top of the building there was no water any water entry from either scenario. Modification of the man door into a sealed hatch or submarine also door eliminated all water flow for any tested tsunami height, because its pressure rating exceeded that of the wave force. The water entering from the reactor bay door is the same as the original, because no protective modifications were made for this entry point (thereby leaving this vulnerability at the facility and may need to be evaluated further). No water reaches the bay door for the 19 meter wave, and in the 38 meter wave the peak height was not reached by the end of the simulated run time.

An analyst can evaluate the data from the various simulations and use the data to demine required changes or even a priority for budget restricted risk asset improvements. For example with this data they may determine that the highest priority change would be to change the standard exterior door to the sealed reinforced door in order to protect against a tsunamis less than 19 meters high.

### 3.1 Computation Recourses and Next Steps

Each tsunami simulation took approximately 80 hours to run on a using 14 threads on seven 2.4 GHz cores Intel i7. The simulation required over 16 Gigabytes of RAM for the fluid particle simulation. New hardware is available to decrease simulation time. With minor modification to the physics engine simulation times could be reduced orders of magnitude using either high end GPU graphics cards or newly released Intel Coprocessors.

Using the calculation results from a range of tsunami simulation samples, we can approximate the flow rates into the facility buildings for any tsunami wave height within our simulation range. Random sampling of a tsunami initiating event can then use these flow rates to run sub simulation and determine component failures inside facilities and incorporate them back into the PRA model.

## 4. CONCLUSIONS

We have carried out a demonstration of the RIMM approach using a representative nuclear power plant as a case study. We showed how mechanistic and probabilistic quantification can be used and extended into the realm of safety margin characterization in order to improve nuclear power plant safety by addressing design changes that focus on accident tolerance.

This case study has pointed to several additional areas of promising research and development related to RIMM. First, we showed how the concept of safety margin provided additional information, both from a quantitative aspect but, more importantly, from an engineering physics understanding – this information could be investigate further in order to potentially optimize the RIMM process. Additional applications include real-time nuclear power plant risk monitors that could respond to near-term upsets such as a potential tsunami, arriving flood or hurricane, or a severe storm. This risk monitor would be the backbone for a general decision support capability for operational decisions.

During the research and development for the case study, issues and lessons learned were encountered. Technical issues included items such as how to represent multiple dependent failures in a simulation framework due to the external event (the tsunami causing an internal flood); how to automate events that called the mechanistic analysis (representing the 3D flooding model); how to integrate probabilistic and mechanistic modeling; and to represent infrequent events using a Bayesian extreme value model.

Several successful outcomes have resulted from performing the case study. The RISMC approach does the following:

- Provides the safety case information to decision makers in order to select design changes for enhanced accident tolerance.
- Develops a significantly improved plant physics approach to represent external and internal flooding.

## 5. REFERENCES

- Kelly, D., & Smith, C. (2011). *Bayesian Inference for Probabilistic Risk Assessment: A Practitioner's Guidebook*. Springer.
- Mosleh, A., Rasmuson, D., & Marshall, F. (1998). *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NRC.
- Smith, C., Rabiti, C., & Martineau, R. (2013). *Risk Informed Safety Margins Characterization (RISMC) Pathway Technical Program Plan*. INL/EXT-11-22977 (revision 1).

# APPENDIX A

## A.1 Simulating Scenarios

### A.1.1 Simulation Approach for Scenarios

One of the weaknesses with “static” type of models such as logic-based event trees is that phenomenology and time may be difficult to represent directly in the model. In these cases, we can turn to more sophisticated analysis techniques. One of the approaches to depict scenarios is through simulation methods.

To represent scenarios, the simulation technique we will describe is that of an approach called discrete event simulation. In general, discrete event simulation is a semi-Markovian technique utilizing both discrete time and discrete space. In discrete event simulation, there are two basic types of simulation approaches, thinning event and event lifetime simulations. These two types of simulation are described in this section.

In the **thinning event simulation** approach, we focus on the determination of the *probability* that the simulation will transition from a state to another state within the next time interval (or time step). Examples of these transition probabilities (within the next incremental time step) are the probability that a pump fails to operate, the probability that a pressure transducer sends a spurious signal, the probability that a component is repaired, and the probability that an initiating event occurs. In a nuclear power plant PSAs, two general types of state transitions are modeled.

We represent state changes “per demand,” where the state transition might be modeled via a binomial aleatory model.

We represent state changes “per time,” where the state transition might be modeled via a Poisson aleatory model and the time step is small.

For those cases where the time is small (which it will be during the event simulation) we can write the Poisson equation as:

$$p(t \leq T \leq (t + \Delta t) | T > t) = \frac{e^{-\lambda t} - e^{-\lambda(t+\Delta t)}}{e^{-\lambda t}} = 1 - e^{-\lambda \Delta t}$$

where

- $\lambda$  = the hazard rate of transitions,
- $T$  = the time until the occurrence of a state transition,
- $t$  = the operational time.
- $\Delta t$  = a small change in operational time.

Consequently, if we are in state A at time  $t$ , given that  $T > t$ , then the probability that we have a failure in the next  $\Delta t$  is given by the equation above. Further, if the product  $\lambda \Delta t$  is small (less than 0.1), then we can rewrite it as

$$p(t \leq T \leq (t + \Delta t) | T > t) = 1 - e^{-\lambda \Delta t} \approx \lambda \Delta t$$

To perform the simulation, we use a Metropolis technique combined with the probability integral transformation theorem. One of the features of probability integral transformation is that we can sample from a cumulative distribution function since the inverse of this function is uniformly distributed from 0 to 1. Within the Metropolis routine, the cumulative distribution  $F(t)$  is uniformly distributed and the “candidate” transition (which we will call the state transition criteria) can be found by solving for  $\lambda$ :

where “Uniform” represents a uniformly distributed from 0 to 1. Consequently, if we know the

$$\lambda = \frac{F(t \leq T \leq (t + \Delta t) | T > t)}{\Delta t} = \frac{\text{Uniform}}{\Delta t}$$

failure rate  $\lambda$  and the time step  $\Delta t$ , we can call a uniform random number generator at each time step to determine if the transition is allowed or not in the scenario simulation.

In the case of the binomial model, if the number of trials is one ( $n = 1$ ) then we have the limiting case which is known as a Bernoulli trial. Since we have only one trial, at most we may have one failure ( $r = 1$ ). Thus, the binomial model reduces to

$$p(r = 1) = p$$

where  $r$  is the number of failures and  $p$  is the probability of a failure per trial. Here, we have a simple state transition criteria for the Metropolis routine, namely  $p = \text{Uniform}$ .

In the **event lifetime simulation** approach, we focus on the determination of *times* until a transition. Examples of these times are the duration a pump operates, the time until a pressure transducer sends a spurious signal, the time until an inoperable component is repaired, or the time until an initiating event occurs. If we assume that one of these states follow an exponential process, then the time to a state transition is a random variable and can be represented probabilistically by:

$$p(T < t) = 1 - e^{-\lambda t}$$

where

- $\lambda$  = the rate of transitions,
- $T$  = the time until the occurrence of a state transition,
- $t$  = the operational time.

Using the probability integral transformation theorem, the parameter  $t$  can be simulated by solving for  $t$ :

$$t = \frac{1}{-\lambda} \ln[1 - P(T < t)]$$

However,  $1 - P(T < t)$  is a uniform distribution from 0 to 1, so:

$$t = \frac{1}{-\lambda} \ln[\text{Uniform}]$$

### A.1.2 Simulation Examples

As an example, we will use Excel to simulate an initiating event. Assume that a facility resides on a river that sees moderate floods once every 10 years on average. Thus, the initiating event for “moderate floods” is 0.1/yr. The simulation will be performed with both event thinning and event lifetime approaches. A total of 10,000 iterations, where we simulate one year of operation of the facility, will be calculated.

The spreadsheet setup is shown in Figure A-1. The initiating event rate is stored in Cell B2. The simulations are performed in column B (using thinning event simulation) and column C (using event lifetime simulation). We check the results (cells E2 and E3) for each simulation type by counting how many “events” we see (for example, we saw an initiating event in iteration 4 for the event lifetime count approach) and divide the total by 10,000.

	A	B	C	D	E	F
1				Check Results (should = IE Rate)		
2	IE Rate	0.1 per year		Thinning =	0.099 per year	
3				Lifetime =	0.097 per year	
4						
		Thinning Event	Event Lifetime			
5	Iteration	Count	Count			
6	1	0	0			
7	2	0	0			
8	3	0	0			
9	4	0	1			
10	5	1	0			
11	6	0	0			

**Fig. A-1 Simulation example structure in Excel.**

The Excel formula used for the thinning event simulation is:

$$=IF((RAND()/1)<\$B\$2,1,0)$$

Note that the value for  $\lambda$  is stored in cell  $\$B\$2$  and a Uniform distribution is called by using the  $RAND()$  function. When the transition criteria is met (i.e.,  $Uniform/\Delta t < \lambda$ ), then the Excel IF function produces a value of 1 (indicating we saw an initiating event in the one-year timeframe), otherwise it produces a 0.

The Excel formula for the event lifetime simulation is:

$$=IF((-1/\$B\$2)*LN(RAND())<1,1,0)$$

Note that the value for  $\lambda$  is stored in cell \$B\$2. When the transition criteria is met (i.e.,

$$\frac{\ln(\text{Uniform})}{-\lambda} < 1)$$

then the Excel IF function produces a value of 1 (indicating we saw an initiating event in the one-year timeframe), otherwise it produces a 0.

### A.1.2 Flow Rate Calculations

The flow rate into penetration points was calculated using a standard discharge rate formula. Pressure from wave impact force was not considered in these calculations. Additions to the simulation code to accurately measure flow and pressure on openings or areas is currently being added.

Flow Formula

$$Q = C_d A \sqrt{2gh}$$

Q is the water discharge flow rate into the room.

$C_d$  is the discharge coefficient. (.65 was used for Venting, .75 for failed doors)

A is the orifice area.

g is gravity 9.80655 m/s<sup>2</sup>.

h is the hydrostatic head.