2017

Risk Modeling of Variable Probability External Initiating Events

Dempere, Jose; Papakonstantinou, Nikolaos; O'Halloran, Bryan; Van Bossuyt, Douglas L.

Dempere, Jose, et al. "Risk modeling of variable probability external initiating events." Reliability and Maintainability Symposium (RAMS), 2017 Annual. IEEE, 2017.
http://hdl.handle.net/10945/61100

Risk Modeling of Variable Probability External Initiating Events

Jose Dempere, Nikolaos Papakonstantinou, Bryan O'Halloran, Douglas L. Van Bossuyt[1]

Key Words: Risk Analysis, Functional Modeling, Variable Probability, Initiating Event

SUMMARY & CONCLUSIONS

As Components engineering has progressively advanced over the past 20 years to encompass a robust element of reliability, a paradigm shift has occurred in how complex systems fail. While failures used to be dominated by 'component failures,' failures are now governed by other factors such as environmental factors, integration capability, design quality, system complexity, built in testability, etc. Of these factors, environmental factors are difficult to predict and assess. While test regimes typically encompass environmental factors, significant design changes to the system to mitigate any failures found is not likely to occur based on the cost. The early stages of the engineering design process offer significant opportunity to evaluate and mitigate risks due to environmental factors.

Systems that are expected to operate in a dynamic and changing environment have significant challenges for assessing environmental factors. For example, external failure initiating event probabilities will change with respect to time and new types of external initiating events can also be expect with respect to time. While some of the well exercised methods such as Probabilistic Risk Assessment (PRA) [**Error! Reference source not found.**] and Failure Modes and Effects Analysis (FMEA) [**Error! Reference source not found.**] can partially address a time-dependent external initiating event probability, current methods of analyzing system failure risk during conceptual system design cannot. As a result, we present our efforts at developing a Time Based Failure Flow Evaluator (TBFFE). This method builds upon the Function Based Engineering Design (FBED) [**Error! Reference source not found.**] method of functional modeling and the Function Failure Identification and Propagation (FFIP) [**Error! Reference source not found.**] failure analysis method that is compatible with FBED. Through the development of TBFFE, we have found that it can provide significant insights into a design that is to be used in an environment with variable probability external initiating events and unique external initiating events. We present a case study of the conceptual design of a nuclear power plant's spent fuel pool undergoing a variety of external initiating events that vary in probability based upon the time of year. The case study illustrates the capability of TBFFE by identifying how seasonally variable initiating event occurrences can impact the probability of failure on a month timescale that otherwise would not be seen on a yearly timescale. Changing the design helps to reduce the impact that time-varying initiating events have on the monthly risk of system failure.

1 BACKGROUND

There are several methods required to understand TBFFE and its background; one commonality all of those methods have is that they do not easily model failure probability shifts caused by time-based initiating event probabilities. This section aims to cover those methods as well as methods in the literature that demonstrate how this methodology is different from other methods.

1.1 Functional Modeling

Functional modeling, at its most basic, connects a series of inputs, outputs, flows, and functions together that transform the inputs into outputs [**Error! Reference source not found.**]. When functions are networked together, the result is a network of functions that transforms various inputs into a desired output. This tool is useful for modeling systems at a variety of resolutions. A common functional modeling implementation is FBED [**Error! Reference source not found.**]; we use FBED as the basis for our method. Functional modeling's robustness makes it a useful tool for many kinds of systems modeling [**Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.**]. However, functional modeling not useful for the stated goal of this method because on its own it does not even have a concept of failures.

1.2 Function Failure Design Method

The Function Failure Design Method (FFDM) is the groundwork upon which TBFFE is built [**Error! Reference source not found.**]]. Essentially, all functions are given a list of potential failures, and the probability of that failure is then entered for every function in the functional model. Then, the probability of a functional model failing can be calculated in much the same way as a failure is calculated in PRA – via cutset development and calculation. The limitation of this method that TBFFE endeavors to overcome is that FFDM has no way to modify a risk's chance of occurring over time without creating a new functional model.

1.3 Function Failure Identification and Propagation

FFIP is an extension of the functional modeling theory underlying FFDM [**Error! Reference source not found.**]. Instead of utilizing a table to quantify the possible failures, FFIP analysis iterates through failures of possible functions and follows the failure flow until it exits the system as an output.

[1] Corresponding author.

This method allows for a user to see how a failure state transmits across a complex system and whether or not it ultimately poses a major risk to the system. While the addition of flows adds the concept of failure propagation to a system modeled using functional modeling, FFIP fails to live up to the needs of those who want to include time in the failure probabilities because it does not cover failure mechanisms or how they change over time.

1.4 Prognostic System Variable Configuration Comparison

The Prognostic System Variable Configuration Comparison (PSVCC) tool is a failure analysis method that helps to determine how useful sensors may be in particular applications to detect incipient failures when a mitigation action can still be taken to prevent system failure [**Error! Reference source not found.**]. PSVCC is relevant to TBFFE due to its implementation of time-based analysis for sensor placement, based on what operators of the system can do to fix the system after an incipient failure has been detected. However, this method does not account for initiating events that are time-variant, such as seasonal weather patterns.

1.5 Related Functional Model-Based Methods

There are various authors in multiple fields that have attempted to address the subject of applying time-variable risk analysis, but few of have addressed functional modeling. The closest match for a functional model that accounts for time is Hutcheson et. al.'s work in attempting to fit failure modes to functions during prototypes [**Error! Reference source not found.**]. While Hutcheson's method creates a certain amount of flexibility for modeling various stages of a mission when a system may be in different configurations, the method is not meant to encapsulate different rates of change, merely different system configurations that are disconnected by time [**Error! Reference source not found.**]]. Another related method is a semi-functional nonparametric analysis by Aneiros-Perez that attempts to use a series of past values as predictors for later behavior [**Error! Reference source not found.**]]. This method does not match the needs of functional modeling because its nonparametric analysis methods are well beyond the scope of a basic functional model or FFDM methods. TBFFE is not a forecasting method, but rather a method by which previous data is used as a predictor. This means that applying Aneiros-Perez's approach to a functional model would be difficult and not produce desired results. Dynamic risk assessment techniques, such as those described by Siu, are applicable to multiple engineering systems, but they lack a functional framework and focus instead on the use of PRA and similar systems [**Error! Reference source not found.**].

The final related method discussed here was developed by Woltjer et. al. and presents a functional analysis meant to react to shifting airplane conditions [**Error! Reference source not found.**]. However, there are issues with this method because it does not account for multiple potential failure conditions and uses velocity components to resolve a time-based issue so that planes enter in the right order to a flight pattern rather than utilizing time to modify the failure velocity. In essence, their analysis method is, like Hutcheson's, meant to change dynamically with time rather than take into account time from a risk analysis perspective so that probabilistic risk of failure may be determined.

1.6 Probabilistic Risk Assessment

PRA is a method that exists outside of the functional flow modeling that has been discussed so far. This system concerns itself primarily with a component-level, rather than functional-level assessment of an engineering system [**Error! Reference source not found.**]. The focus of the PRA method is to create a series of cutsets based on initiating events to create a series of potential failure flows and their associated probabilities.

PRA's use in nuclear power plants has resulted in its modification to deal with time-dependent issues unique to that specific use case [**Error! Reference source not found.**]. In particular, the exploration of core damage frequency as a surrogate measure to reach particular safety goals is of interest when discussing time-variate risk mitigation methods. This method focuses on whether or not changes to a reactor are allowed by evaluating the frequency of reactor core damage.

1.7 Related Physics-of-Failure and Parametric Analysis Methods

Despite the limitations of previously discussed methods, engineers do have various tools to evaluate time-dependent failure probabilities in a variety of contexts – however, the usefulness of these methods to an engineering team analyzing time-varying external initiating events is debatable. One such discipline is physics-of-failure mathematics. Physics-of-failure mathematics, pioneered by the University of Maryland among other groups, represents the identification and analysis of the physical causes for the failure of a particular component and then modeling the resulting data to develop a probability density function along a system's lifetime [**Error! Reference source not found.**]. Of note is the resulting probability distribution over time that frequently results from such analyses. While this approach is useful for looking at the probabilities of failure that happen within any particular component, the approach does not contain any methodology for design teams to act on the data-- it is primarily a statistical method, not a design method.

Another methodology used to determine risk of failure is parametric analysis which is a statistical technique used when the unknown parameters of a particular component's longevity are populated with random values and a distribution is made of the resultant variables. This approach has many implementations, being integrated both in PRA analysis as well as in time-dependent probabilities of failure [**Error! Reference source not found.**, **Error! Reference source not found.**]. However, there are certain issues with this approach – parametric analyses require the population of a data set to be developed through a tool such as Monte Carlo analysis, which can lead to a high computational expense when the methodology is applied to a more complex functional framework.

2 METHODOLOGY

TBFFE is a risk quantification method used to analyze complex, cyber physical systems during engineering design. This method is focus primarily in early engineering design where systems have opportunity for configuration charges. The goal of this method is to inform the designer on predominate risks that may be realized during the system's life cycle, and thus, the method systematically analyzes all known risks of the system.

The results of TBFFF can be used to enhance a design by reducing its risk of failure. The type of results produced by TBFFF include the systems's functional risk, which combines failure probability with the loss in functional health, tied to an initiating event. The results are presented across time (e.g., per month in the following case study) to represent heightened risk during specific time periods. An example solutions to an unacceptable risk could include a design configuration change where the failure propagation has a behavior to renders the system less susceptible to the specific initiating events being analyzed. Another example could include turning backup systems on to reduce the load carried by primary systems.

A fundamental difference from other known risk methods is that TBFFF uses discrete time-based failure probabilities with a short time scales to more accurately model the reality of environment factors. Typical failure probabilities are modeled on an annual basis, however we analyze failure probabilities either monthly (as in the case study), daily, or even hourly. The discretization depends on the fidelity of the data used to build the probability values. For example, when assessing the risk of failures due to storms, failure probabilities would depend on the occurrence of storms in the local environment. If data is recorded in storms per month, the discretized failure probabilities will be monthly.

TBFFE is a process-oriented methodology that has several well defined steps. These steps are meant to guide a design team from a basic functional model to a complete time-dependent representation of all potential points of failure that can affect a system.

2.1 Step 1: Functional Model Creation

The first step is the creation of a functional model based on the initial system architecture. The initial system architecture is usually a body of work developed by the design team and ranges across design requirements, sketches, blueprints, flowcharts, reliability block diagrams, as well as piping and instrumentation diagrams. In the absence of such existing work, an experienced design team might instead opt to generate a native FBED [**Error! Reference source not found.**] from scratch based on the desired system inputs and outputs given to the team.

2.2 Step 2: Initiating Event Identification

After creating a functional model, the team must note potential initiating events that may cause a failure. Finding initiating events in TBFFE is similar to the method utilized in PRA. For TBFFE the, designers are encouraged to consider external, internal, and special initiating events. External events are those which originate outside the system, such as weather or debris. After compiling a list of external events, designers then go through the system and identify potential internal initiating events, such as mechanical wear, fire, internal flooding, or an electrical bus failure. Having a comprehensive list of internal and external initiating events, designers can then analyze potential edge cases that might not fit within either category, such as animals finding their way into the system and chewing through wiring. By utilizing these categories, the design team can be thorough in their analysis and capture the greatest number of potential initiating events.

2.3 Step 3: Time-Dependent Initiating Event Identification

After developing a list of initiating events, the design team then classifies each event as time-dependent or independent. Those events which are based on seasonal phenomena, weather events, or events of variable strength such as storms are considered time-dependent.

For each time-dependent initiating event, there must be a particular profile to how risk increases or decreases over the course of a year (or other time increment that is normally analyzed across). With each event, practitioners should consider how the risk of the initiating event occurring increases or decreases. The team can choose to model certain initiating events either through a gradual function or through a discretized, step-wise function. Gradual increases best serve events like storms where there is an identifiable period of peak intensity followed by a drop-off. Typically, a design team is limited in how discretized the available data is. Engineers might have access to thorough meteorological data for their region that covers several days, or they might only know that storms occur more frequently over a particular range of months out of the year. Another important aspect to cover is how a system's probability of failure is affected by long-term or short term forecasts. As an example, the engineering team may know that a seasonally-affected failure is only possible during certain hours of the day (such as the position of the sun affecting certain sensors only certain months of the year). As a rule of thumb, design teams are encouraged to account for short-term forecasts if they represent a change in probability greater than a standard deviation from their given probability of risk. Changes of less than one standard deviation will likely be inconsequential as compared to other factors within the risk analysis during the conceptual design process such as design, model, and data uncertainty. The result of the data acquired by the engineers will be similar to a Bayesian statistical model, but dependent on time.

In the TBFFE method, the design team is presumed to have existing probability of failure (per year or unit of time used for the particular system) as well as more discrete and detailed data for initiating events. The existing probability of failure divided by the unit of time for the overlay data is the baseline probability. If a design team has a yearly probability of failure by storm, and monthly values for frequency of storms in their region, then they would divide their probability by twelve. The data that the design team has should resolve itself into a

function that shows frequency over time. In the case of the storm example, they will be able to chart the per-month frequency of storms over the year. As a verification step, the overlay data can be scaled such that, when combined, its value equals the existing yearly frequency of occurrence of the initiating event.

In the case that the design team does not have access to a dataset time-discretized for an initiating event, but does know that the probability of occurrence will be increased at certain times or decreased in others, they can create data themselves utilizing the standard deviations as local minima and maxima. Ensuring that the integral of the constructed occurrence probability distribution is equal to the yearly averaged occurrence probability is more of an art as the design team has control of the rate of dropoffs and increases.

2.4 Step 4: Analyze Failure Propagation in the System

Once the various initiating events have been given a time-dependent profile, a probability of failure for each function within the model can be constructed. Both time-dependent and time-independent initiating events represent causes of failure that can map to particular functions. The design team can assign various causes of failure to individual functions. A function's probability of failure is the OR probability of any particular event occurring. By calculating the function's probability of failure at each time step, the design team develops a time-dependent failure profile for each function. Doing this for all functions allows the design team to have an FFIP model that they can look through time, allowing them to identify peak risks for particular functions.

2.5 Step 5: Design Iteration or Retrofit the System

By analyzing the various probabilities of failure present at particular time steps, the design team can begin to optimize their design. Starting with functions crucial to the system's operation, the designers can look at local maxima of failure probability for a given function. Those functions that exhibit the highest risk across any period of time can then be marked as at-risk. By identifying the initiating event or events responsible for this heightened state of risk, designers can focus on mitigating the probability of those initiating events happening, potentially by including specific functions or components that are used specifically in times of heightened risk. Starting with the highest risk functions, designers can continue to mitigate risks within the constraints of time, complexity, cost, etc. Once optimizations are complete, they can then iterate through the previous step to compare how their design has improved.

3 CASE STUDY

In this section, we present a case study that demonstrates TBFFE and its capabilities; a representative example was created of the potential applications in a nuclear power context. Note that we have intentionally fictionalized probability data and plant design, and explicitly do not recommend using the results of this case study in a real-world application. The case study is demonstrative of the method and is intentionally not directly applicable to a specific nuclear power plant. In this example, a new nuclear power plant somewhere on the East coast of the United States is being designed. The engineers are working on designing a spent fuel pool, where they will store spent fuel rods until the rods are cool enough for disposal. Consequently, the fuel pool's main purpose is to cycle hot water through to a system of heat exchangers to continuously maintain the temperature of the water at acceptable levels. The region the plant is being constructed in is prone to stormy weather, as well as seasonal algae blooms. The plant is planned to have one internal loop of water exchanging heat to the ocean. The design team decides to utilize TBFFE to anticipate and mitigate time-variant risks due to these unique conditions.

3.1 Step 1: Functional Model Creation

As a first step, the group creates a functional model (see Figure 1). This functional model represents their desired design prior to any iteration. At this stage, the design team already decided that they wanted to include multiply redundant systems; three sets of motors power three sets of pumps that move the water in the primary pool, and three different heat exchangers are available. The pumps are designed to begin operation one after the other, in the event of failure, while the heat exchangers are designed such that one of them can transfer heat efficiently enough to keep the system nominal. These kinds of design decisions are acceptable at this stage of TBFFE.

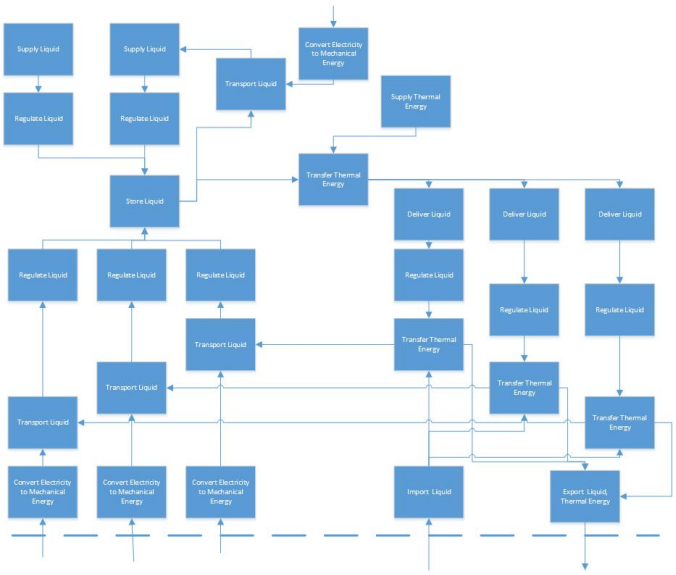


Figure 1: Functional model of a spent fuel pool.

3.2 Step 2: Initiating Event Identification

Once the functional model was complete, the group considered potential initiating events and began research into the probabilities associated with each failure probability until they had a list of initiating events they felt was complete (see Table 1). They first identified external failures like electrical storms shorting out motors or algae blooms clogging up the intake to the heat exchangers, and then went on to internal failures such as mechanical wear within the machines. Going through each function, they were able to compile a list of

initiating events they believed could fail the system.

3.3 Step 3: Time-Dependent Initiating Event Identification

Once the design team has a list of potential initiating events, they can go through each initiating event and classify it as time-variant or time-invariant. The team quickly recognized that algae blooms, electrical failures due to storms affecting the pumps, and heat exchanger failures due to storms affecting the intake of secondary water as significant initiating events that have a time-varying probability of occurrence. The reason for this is simple: both algae blooms and storms are events that occur seasonally, with significant change in event frequency occurring depending on the month.

Table 1: List of initiating events for spent fuel pool used in case study. Note that items that are italicized are time variant in their probabilities, which is discussed further in the next section. They are presented here as an averaged yearly probability statistic. See Tables 2 and 3 for further details on these two events.

Initiating Event	Prob/year
IE_MechanicalFailureCondenser	0.003
IE_Algae	0.004
IE_MechanicalFailureValve	0.001
IE_MechanicalFailurePump	0.005
IE_MechanicalFailureMotor	0.002
IE_Storm1	0.003
IE_MechanicalFailureValve	0.001
IE_MechanicalFailurePipe	0.003
IE_Storm2	0.002
IE_MechanicalFailureTank	0.0005

Having identified which risks were time-dependent, the design team moved on to determine how well they could characterize those risks over time. By now, the team had finished their research on their initiating events and were able to work using yearly probabilities of occurrence for all of the initiating events, as well as on-demand failure probabilities for all components. To acquire more detailed information on the behavior of their system, the team realized they needed a monthly time step for their external event analysis. For storms, they determined the monthly number of storms that occurred in their area, which they found to be sufficient. On the other hand, when researching the propagation of the algae they knew to be problematic, they were restricted to data from marine biologists that forecast them to be most prevalent from the months of July to October and otherwise not present in the area. Knowing this, the design team created a set of Boolean values corresponding to each month. Knowing the yearly probability of failure for the heat exchangers being installed for the spent fuel cooling pool due to storms and algae (as well as pumps due to storms), the team was able to create Tables 2 and 3 to calculate the monthly probability. Specifically, the annual failure rate for algae was evenly distributed across the months of May-Oct. Similarly, the annual failure rate for storms was proportionately distributed across the year based on the number of storms in each month (Storm1 for January: 0.03 * 10/526 = 5.7E-05 fails /month).

3.4 Step 4: Analyze Failure Propagation in the System

The team then generated cutsets based on the functional model of what possible failures could occur based on the propagation of certain components breaking. Table 4 shows the yearly probabilities of failure for ten generated example cutsets. Of those ten cutsets, four of them involved time-variant initiating events. Table 5 was consequently generated to track the monthly probabilities of failure. These were generated based on the probability of the failures required to cause the system to completely fail.

Table 2: Monthly frequency values for storms as well as yes/no values for algae presence in the oceans. This data is utilized by the engineering team to produced scaled monthly probabilities, shown in Table 3.

Available Monthly Frequencies		
Month	Storm	Algae
1	10	0
2	5	0
3	7	0
4	12	0
5	22	1
6	35	1
7	77	1
8	110	1
9	96	1
10	80	1
11	50	0
12	22	0

Table 3: Monthly Initiating Event Probabilities of Occurrence

Monthly Probabilities (prob of failure per month)		
Month	Storm	Algae
1	5.7E-05	0
2	2.85E-05	0
3	3.99E-05	0
4	6.84E-05	0
5	0.000125	0.000667
6	0.0002	0.000667
7	0.000439	0.000667
8	0.000627	0.000667
9	0.000548	0.000667
10	0.000456	0.000667
11	0.000285	0
12	0.000125	0
Total:	0.003	0.004

Table 4: Cutsets for yearly failure probabilities.

Cutset Number	Prob(freq)/year	Cutset
1	4.00E-03	IE_Algae, Import Liquid, Transfer Thermal Energy, Transfer Thermal Energy, Transfer Thermal Energy, Export Liquid/Thermal Energy
2	3.00E-09	IE_Storm1, Transfer Thermal Energy Transfer Thermal Energy, Transfer Thermal Energy, Export Liquid/Thermal Energy
3	1.80E-08	IE_Storm2, Convert Mechanical Energy to Electrical Energy, Transport Liquid, Regulate Liquid, Transport Liquid, Regulate Liquid, Transport Liquid, Regulate Liquid, Store Liquid, Transfer Thermal Energy
4	3.20E-08	IE_MechanicalFailureMotor, Convert Mechanical Energy to Electricity, Convert Mechanical Energy to Electricity, Convert Mechanical Energy to Electricity, Transport Liquid, Transport Liquid, Transport Liquid, Store Liquid, Transfer Thermal Energy
5	6.00E-08	IE_MechanicalFailurePump, Transport Liquid, Regulate Liquid, Convert Mechanical Energy to Electricity, Transport Liquid, Regulate Liquid, Transport Liquid, Regulate Liquid, Store Liquid, Transfer Thermal Energy
6	1.60E-08	IE_MechanicalFailureValve, Regulate Liquid, Convert Mechanical Energy to Electricity, Transport Liquid, Regulate Liquid, Convert Mechanical Energy to Electricity, Transport Liquid, Regulate Liquid, Store Liquid, Transfer Thermal Energy
7	1.00E-09	IE_MechanicalFailureValve, Regulate Liquid, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy, Transfer Thermal Energy
8	3.00E-09	IE_MechanicalFailurePipe, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy
9	6.00E-09	IE_MechanicalFailureExchangers, Transfer Thermal Energy, Regulate Liquid, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy
10	6.00E-09	IE_Storm1, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy, Regulate Liquid, Deliver Liquid, Transfer Thermal Energy

Table 5: Monthly probability of algae bloom creating a failure event as described in Cutset 1.

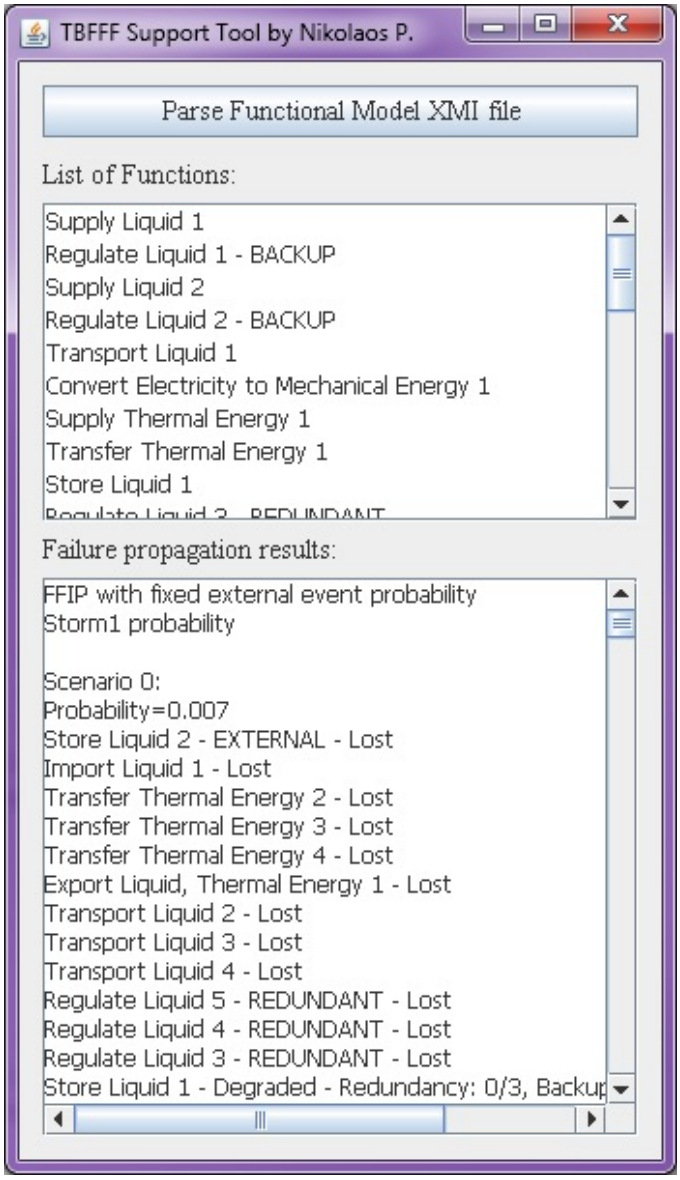
Cutset 1: Yearly Probability	4.00E-03
Month:	Monthly Probability
1	0
2	0
3	0
4	0
5	6.67E-04
6	6.67E-04
7	6.67E-04
8	6.67E-04
9	6.67E-04
10	6.67E-04
11	0
12	0
Total:	4.00E-03

3.5 Step 5: Design Iteration or Retrofit the System

Based on analyzing the existing data, the design team noticed some statistically significant spikes in the probability of failure. For example, they discovered from their cutsets that the probability of heat exchanger failure due to storms was highest in August, as was the probability of an electrical failure. Consequently, the team realized that they could redesign their system to mitigate the risk of failure during those months. For example, the team decided that from July to October, the team could utilize a cooling pond rather than directly using the ocean to prevent both algae blooms and flotsam created by storms from clogging up the heat exchangers. Similarly, they realized that they could run backup generators during those months to dampen the risk of an outage caused by electrical storms. Beyond these specific seasonal improvements, the team also noticed that they could implement an emergency cooling water pipe going from the water tanks to the secondary loop to ensure that heat exchange could continue in the case of an inlet clog. From there, the team is able to create new, lowered monthly probability profiles and iterate further through their design.

4 RESULTS AND DISCUSSION

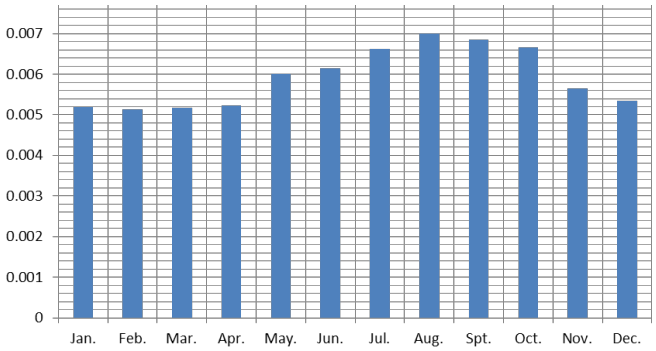
To better demonstrate the full capabilities of our method when applied to iterative design, our group developed a tool based on a Universal Modeling Language (UML) [**Error! Reference source not found.**] backend that does the work of generating cutsets automatically based on the functional model and using the TBFFE method. By implementing functional modeling in UML, defining critical functions that cannot be



interrupted, and providing a per-month list of the probability of initiating events, the tool runs through all cutsets which result in the failure of the system and then calculate the overall risk of failure applied on the given timescale. This tool enables designers to use TBFFE even in scenarios that involve rapid iteration. In our fuel pool example, the critical function was defined as the transfer of heat to the water of the fuel pool. Figure 2 shows the resultant UML functional model, and Figure 3 shows the results of the overall risk analysis.

Figure 2: TBFFE Tool Implementation.

From these results, it is possible to see how the resolution



afforded by creating monthly probabilities is useful to design teams. The step of mathematical characterization showcased how risk profiles can spike dependent on the month; however, sometimes yearly probabilities are all that is available to an engineering team in databases for nuclear power plant failure events, and seasonal occurrences like storms or algae blooms are often unique to a region. The design team is best served by fitting local data to yearly probabilities that might be otherwise useful to their facility.

Figure 3: Probability of System Failure per Month

By utilizing the UML-based tool, we were able to perform iterative design as described in the previous section. We used the idea of a fuel pool as a starting point for iterative design. We ran cutsets on a modified functional model from the months of July to October that uses a cooling pond as a cooling water intake. Based on this model, the peak of risk was reduced significantly-- the probability of a failure was reduced by 10% in August, and consistent decreases along similar months. Figure 4 displays the new set of probabilities--the new risk profile is significantly flatter, and showcases potential avenues that the design team can take to improve the risk profile of their fuel pool.

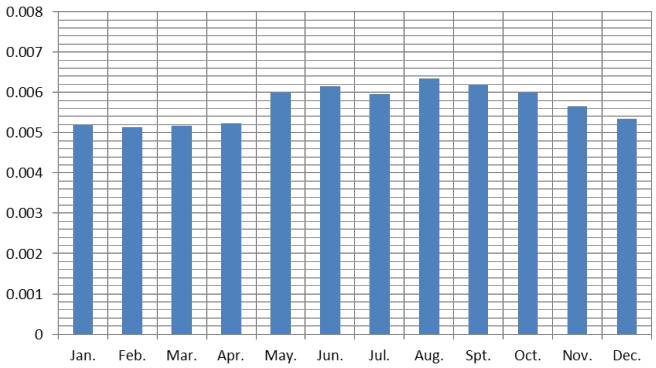


Figure 4: Probability of System Failure per Month After Iterative Design Using Insights Gained from TBFFE

From here, the design team can note new avenues of development-- a surge in risk occurs in May consistent with the heightened risk of failure caused by storms. The design team

could then focus on mitigating that form of system failure by creating redundancies in the power supply such as waterproofing the motor system as well as possibly looking into redundant backup generators. The team could also run TBFFE once more and generate a new risk assessment based on these improvements, aiming to create the smoothest risk profile throughout the year possible. The iterative design potential is the main draw of TBFFE, permitting teams to rapidly identify and mitigate areas of concern for their systems that would go unnoticed without access to time-based failure evaluation methods.

The main benefit of time-dependent analysis of risk is that increased granularity of failure probabilities with respect to time over which the probabilities are analyzed allows engineers to mitigate risk in a more optimal way, thereby focusing on spending resources in times of heightened risk. TBFFE allows practitioners to bring together risk data that operates on non-uniform timescales to create overall profiles of risk that provide insight which otherwise would be obscured by the commonly used yearly timescales of PRA and other risk analysis techniques.

One of the major limitations of the TBFFE method as it exists presently is the need for more granular initiating event data as an input. TBFFE is called for when the design team already knows that their system is going to be affected by time-variant initiating events – in the example of the fuel pool, the designers already knew that algae and storms had been problems in previous nuclear reactors and were able to account for this within their method. TBFFE is a method best suited to characterizing known information with greater granularity – unknowns are harder for the system to deal with and frequently can be as opaque to the design team as they would be had they simply stopped at utilizing a method like FFIP or PRA. A logical extension of this limitation is that TBFFE requires the design team to bring in data beyond what they might get from existing engineering databases to create distinct probability of occurrence data for initiating events. Depending on the initiating event, this might require assumptions on the part of the design team that might not be borne out by reality.

By understanding these weaknesses, it becomes clear that TBFFE is best suited to those scenarios where designers wish to integrate data that is specific to their use case into a larger framework of existing probabilities in their field. Examples that come most readily to mind are specific scenarios such as nuclear reactors or spacecraft, where there is a plurality of information available to an engineering team but where the details born of location or purpose are unique to their particular project.

REFERENCES

1. German Aneiros-Perez and Philippe Vieu. Nonparametric time series prediction: A semi functional partial linear modeling. Journal of Multivariate Analysis, 99(5):834{857, 2008.
2. Corwin L Atwood. Parametric estimation of time-dependent failure rates for probabilistic risk assessment. Reliability engineering & system safety, 37(3):181{194, 1992.
3. US Nuclear Regulatory Commission et al. Regulatory Guide 1.174: An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-specific Changes to the Licensing Basis. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2002.
4. Warren Gilchrist. Modelling failure modes and effects analysis. International Journal of Quality & Reliability Management, 10(5), 1993.
5. PL Hall and JE Strutt. Probabilistic physics-of-failure models for component reliabilities using Monte carol simulation and weibull analysis: a parametric study. Reliability Engineering & System Safety, 80(3):233{242, 2003.
6. Julie Hirtz, Robert B Stone, Daniel A McAdams, Simon Szykman, and Kristin L Wood. A functional basis for engineering design: reconciling and evolving previous efforts. Research in engineering Design, 13(2):65{82, 2002.
7. Ryan S Hutcheson, Daniel A McAdams, Robert B Stone, and Irem Y Tumer. A function-based methodology for analyzing critical events. In ASME 2006 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, pages 1193{1204. American Society of Mechanical Engineers, 2006.
8. K Kimseng, M Hoit, N Tiwari, and M Pecht. Physics-of-failure assessment of a cruise control module. Microelectronics Reliability, 39(10):1423{1444, 1999.
9. Tolga Kurtoglu and Irem Y Tumer. FFIP: A framework for early assessment of functional failures in complex systems. In The International Conference on Engineering Design, ICED, volume 7, 2007.
10. Craig Larman and UML Applying. Patterns: An introduction to object-oriented analysis and design and iterative development. 2004.
11. Nuclear Regulatory Commission et al. Severe accident risks: an assessment for five us nuclear power plants. Technical report, Nuclear Regulatory Commission, 1991.
12. Bryan M O'Halloran, Nikolaos Papakonstantinou, and Douglas L Van Bossuyt. Modeling of function failure propagation across uncoupled systems. In 2015 Annual Reliability and Maintainability Symposium (RAMS), pages 1{6. IEEE, 2015.
13. Bryan M O'Halloran, Nikolaos Papakonstantinou, and Douglas L Van Bossuyt. Cable routing modeling in early system design to prevent cable failure propagation events. In 2016 Annual Reliability and Maintainability Symposium (RAMS), pages 1{6. IEEE, 2016.
14. Nikolaos Papakonstantinou, Markus Porthin, M O'Halloran, and L Van Bossuyt. A model-driven approach for incorporating human reliability analysis in early emergency operating procedure development. In 2016 Annual Reliability and Maintainability Symposium (RAMS), pages 1{6. IEEE, 2016.
15. N Siu. Risk assessment for dynamic systems: an overview. Reliability Engineering & System Safety,

43(1):43{73, 1994.
16. Caitlin Stack and Douglas L Van Bossuyt. Toward a functional failure modeling method of representing prognostic systems during the early phases of design. In ASME 2015 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, pages V02AT03A051{V02AT03A051. American Society of Mechanical Engineers, 2015.
17. Michael Stamatelatos. Probabilistic risk assessment: What is it and why is it worth performing it? NASA Office of Safety and Mission Assurance, 4(05):00, 2000.
18. R.B. Stone, I.Y. Tumer, and M. Van Wie. The function-failure design method. Journal of Mechanical Design, 127(3):397{407, 2005.
19. Robert B Stone and Kristin L Wood. Development of a functional basis for design. Journal of Mechanical design, 122(4):359{370, 2000.
20. Rogier Woltjer and Erik Hollnagel. Functional modeling for risk assessment of automation in a changing air traffic management environment. In Proceedings of the 4th International Conference Working on Safety, volume 30, 2008.

BIOGRAPHIES

Jose Dempere
Colorado School of Mines
1500 Illinois Street, Golden, CO 80401, USA
e-mail: jdempere@mymail.mines.edu

Jose Dempere is a graduate research assistant at the Colorado School of Mines in the Van Bossuyt Research Group housed in the Department of Mechanical Engineering. His research focuses on system failure modeling using functional modeling techniques and risk analysis methods. Systems of interest include rockets and space missions, nuclear power plants, and energy systems. He holds a Bachelor of Science in Petroleum Engineering from the Colorado School of Mines.

Nikolaos Papakonstantinou, PhD
VTT Technical Research Centre of Finland
P.O. Box 1000, FI-02044 VTT, Finland
e-mail: nikolaos.papakonstantinou@vtt.fi

Dr. Nikolaos Papakonstantinou has a diploma in Electrical & Computer Engineering from the University of Patras (Greece) and a doctorate degree in Information Technology in Automation from Aalto University (Finland). Currently he works as a senior scientist at VTT Technical Research Centre of Finland in the area of system modeling and simulations. He focuses on simulation, model and data driven approaches to system design, operation and safety assessment. Even before moving to VTT, as a post-doctoral researcher at Aalto University, he focused on simulation based safety assessment of complex systems using case studies from the nuclear power production industry. He managed the IFAPROBE project, part of the Finnish Research Programme on Nuclear Power Plant Safety and was the responsible teacher for the "Managing the product life cycle" master level course. His earlier research was in the area of automation software design, mainly targeting IEC61131 and IEC61499 based controllers, with applications on machine, batch and continuous process automation control.

Bryan O'Halloran, PhD
Naval Postgraduate School
833 Dyer Road, Bullard Hall 218, Monterey, CA 93943, USA
e-mail: bmohallo@nps.edu

Dr. Bryan O'Halloran is currently an Assistant Professor in the Systems Engineering (SE) department at the Naval Postgraduate School (NPS). Prior to joining NPS, he was a Senior Reliability and Systems Safety Engineer at Raytheon Missile Systems and the Lead Reliability and Safety Engineer for hypersonic missile programs. He holds a Bachelor of Science degree in Engineering Physics and a Master of Science and Doctorate of Philosophy in Mechanical Engineering from Oregon State University. His current research interests include risk, reliability, safety, and failure modeling in the early design of Complex, Cyber-Physical Systems (CCPSs). He is a member of the American Society of Mechanical Engineers (ASME) and the Institute of Electrical and Electronics Engineers (IEEE) and regularly attends the International Design Engineering Technical Conference (IDETC), the International Mechanical Engineering Congress and Exposition (IMECE), and the Reliability and Maintainability Symposium (RAMS).

Douglas L. Van Bossuyt, PhD
Colorado School of Mines
1500 Illinois Street, Golden, CO 80401, USA
e-mail: dvanboss@mines.edu

Dr. Douglas L. Van Bossuyt is currently an Assistant Professor in the Department of Mechanical Engineering, and the Nuclear Science and Engineering program at the Colorado School of Mines where he co-directs the Alliance for the Development of Additive Processing Technologies (ADAPT) Center. He holds a PhD in Mechanical Engineering, a Master's of Science in Mechanical Engineering, an Honors Bachelors of Science in Mechanical Engineering, and an Honors Bachelors of Arts in International Studies from Oregon State University. His research interests lay at the intersection of risk and failure analysis, system design, manufacturing, and operation of complex systems such as defense systems, nuclear reactors, and aerospace systems. Dr. Van Bossuyt is a member of the American Society of Mechanical Engineers (ASME) and the Prognostics and Health Management Society (PHM Society), and regularly attends the International Design Engineering Technical Conference (IDETC), the PHM Society Conference, and the Reliability and Maintainability Symposium (RAMS).