Toward a Dedicated Failure Flow Arrestor Function Methodology

Conference Paper · August 2015

DOI: 10.1115/DETC2015-46270

2 authors:

Michael Slater
Colorado School of Mines
1 PUBLICATION **6** CITATIONS
SEE PROFILE

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **936** CITATIONS
SEE PROFILE

Proceedings of the ASME 2015 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference
IDETC/CIE 2015
August 2-5, 2015, Boston, USA

DETC2015-46270

TOWARD A DEDICATED FAILURE FLOW ARRESTOR FUNCTION METHODOLOGY

Michael R.S. Slater
Graduate Research Assistant
Nuclear Science and Engineering Program
Colorado School of Mines
Golden, Colorado 80401
Email: mslater@mines.edu

Douglas L. Van Bossuyt*
Assistant Professor
Nuclear Science and Engineering Program
Department of Mechanical Engineering
Colorado School of Mines
Golden, Colorado 80401
Email: dvanboss@mines.edu

ABSTRACT

Risk analysis in engineering design is of paramount importance when developing complex systems or upgrading existing systems. In many complex systems, new generations of systems are expected to have decreased risk and increased reliability when compared with previous designs. For instance, within the American civilian nuclear power industry, the Nuclear Regulatory Commission (NRC) has progressively increased requirements for reliability and driven down the chance of radiological release beyond the plant site boundary. However, many ongoing complex system design efforts analyze risk after early major architecture decisions have been made. One promising method of bringing risk considerations earlier into the conceptual stages of the complex system design process is functional failure modeling. Function Failure Identification and Propagation (FFIP) and related methods began the push toward assessing risk using the functional modeling taxonomy. This paper advances the Dedicated Failure Flow Arrestor Function (DFFAF) method which incorporates dedicated Arrestor Functions (AFs) whose purpose is to stop failure flows from propagating along uncoupled failure flow pathways, as defined by Uncoupled Failure Flow State Reasoner (UFFSR). By doing this, DFFAF provides a new tool to the functional failure modeling toolbox for complex system engineers. This paper introduces DFFAF and provides an illustrative simplified civilian Pressurized Water Reactor (PWR) nuclear power plant case study.

Acronyms

AF Arrestor Function
DFFAF Dedicated Failure Flow Arrestor Function
ECCS Emergency Core Cooling System
FACE Function-based Analysis of Critical Events
FBED Functional Basis for Engineering Design
FFDM Function Failure Design Method
FFIP Function Failure Identification and Propagation
FMEA Failure Modes and Effects Analysis
FSL Flow State Logic
IAEA International Atomic Energy Agency
NRC Nuclear Regulatory Commission
PRA Probabilistic Risk Assessment
PWR Pressurized Water Reactor
RAMS Risk Assessment Method Statement
RBD Reliability Block Diagram
RCCL Reactor Core Coolant Loop
RPN Risk Priority Number
SIS Safety Injection System
UFFSR Uncoupled Failure Flow State Reasoner

1 INTRODUCTION

Risk is an important part of engineering design, and is an essential consideration when developing highly complex systems. New designs for systems released to the market must be less risky than previous designs. Unfortunately, risk is usually con-

*Address all correspondence to this author.

sidered after the design of a complex system, and is not a major consideration until optimizing a design. Certain industries, such as the civilian nuclear power industry and the aerospace industry, often use risk as a quantitative design parameter in the design process only after the primary design work has been completed. In nuclear systems design, risk analysis is considered extensively, and is legally required by the Nuclear Regulatory Commission (NRC) in the United States of America, and by similar groups in other countries. However, even in nuclear power plant designs, risk is still often analyzed after primary design work has occurred.

Currently, the primary tool used in industry to quantitatively analyze risk is Probabilistic Risk Assessment (PRA), along with other component-based methods, that analyze already-designed systems. PRA determines the failure likelihoods of complex systems based on data collected about each component within the system using Bayesian statistical approaches. PRA methods traditionally are only used after a design is substantially completed. In an effort to incorporate risk as a design parameter, research is ongoing in functional failure modeling methods that allow high level analysis of conceptual designs before large architecture choices have been made. In its current form, functional failure modeling is useful but is unable to completely model the failure information that PRA methods can. Recent research and methodological developments have begun to improve the suitability of functional failure modeling techniques for the early phases of conceptual system design for nuclear power plants with the eventual goal of developing a functional failure modeling design tool.

This paper extends the Uncoupled Failure Flow State Reasoner (UFFSR) method, which extended the Function Failure Identification and Propagation (FFIP) and Flow State Logic (FSL) methods, with a new technique called the Dedicated Failure Flow Arrestor Function (DFFAF) methodology. DFFAF uses FFIP failure models along with UFFSR uncoupled failure flow propagation models to introduce the idea of Arrestor Functions (AFs). These AFs are implemented to arrest uncoupled failure flows and stop the failure flows from propagating to critical components. The DFFAF method increases the utility of functional failure modeling, progressing it towards becoming a conceptual design tool.

1.1 Specific Contributions

DFFAF is a novel extension to the UFFSR method, which analyzes failure flows that cross between nominally uncoupled functions that were previously not directly modeled in the FFIP methodology. DFFAF extends the UFFSR method to determine where to place AFs to mitigate the largest uncoupled failure flow probabilities. After placing AFs and recalculating the failure probabilities, the AFs which should or can be implemented are found by determining which AFs cause the largest overall decrease in failure probability as compared to results from the UFFSR analysis. This is useful for pre-existing systems, where components cannot be moved, and as a tool in design, when space and placement are constraints in the design process. The DFFAF expands efforts to develop a complete function failure analysis tool that can be used in the early phases of complex system design.

The DFFAF method addresses uncoupled failure flows, nominal failure flows, is iterative in nature to improve system design and stability, and specifies how to include AFs. UFFSR focuses on uncoupled failure flows, and FFIP focuses on nominal flows, along material, energy, and information flow paths. DFFAF incorporates and builds upon both FFIP and UFFSR, by providing a new method to improve designs that specifically addresses uncoupled flows found by using the UFFSR analysis. DFFAF is a functionally-based tool that is applicable to the early stages of complex system design, where PRA and other later-stage design methods are not as useful in spite of advanced PRA analysis that can account for some classes of uncoupled failure flow mitigating strategies.

2 BACKGROUND

The complex systems being designed by engineers today are increasingly required to be highly reliable at completing their intended mission, even in partial failure situations. Civilian nuclear power plants have long been designed using defense in depth strategies that develop multiple redundant and diverse subsystems to prevent component and subsystem failures from causing critical system-level failures [1–3]. Critical system-level failures, in the case of nuclear power plants, can lead to radiation release beyond the site boundary of a plant. The very few but high profile cases of radioactive release beyond the site boundary are a testament to the defense in depth strategy yet shows the need to further prepare for highly unlikely failure situations that defense in depth does not always account for.

Many tools exist and are in common use in industry for the design and analysis of nuclear power plants or have found traction in academia with relation to functional failure modeling. Below, a review of the most common and important tools are presented. The work presented in this paper is based upon the previous important developments reviewed below.

Failure Modes and Effects Analysis (FMEA) is a tool that assesses component failures. A value can be generated for the failure severity, probability of occurrence, and how detectable the problem is before it occurs. These values are multiplied to reveal which failures are the most risky, via a Risk Priority Number (RPN), and in highest need of being addressed [4, 5]. This does not however tell us how likely something is to fail like PRA and functional methodologies do, and thus work is often exerted to fix problems that do not actually significantly impact a systems failure rate.

Another method to assess failure is Reliability Block Diagrams (RBDs). This method illustrates the flow of material or energy through a system, and looks for single-point failures. A block is assigned to each component. Components which definitely fail if other components fail are put in series with each other and components that are redundant are put in parallel. Probabilities can be generated for the failure of the system [6]. RBDs are a very useful tool for determining which functions are highly critical to success, and thus are not redundant, allowing a designer to find and avoid such situations when possible [7]. RBDs lack the capability to show the flow of failures, something which is critical in the design phase of engineering, especially when making large architectural decisions about a design, and figuring out component layout and arrangement.

The Risk Assessment Method Statement (RAMS) is another tool for analyzing reliability and risk to determine a rate of failure, and necessary maintenance steps throughout the life of a system. It utilizes basic probability theory to demonstrate what components are risky, and how a system will fail [8]. The RAMS cycle assesses risk throughout the design process, forcing an assessment and revision of goals and design, based on the outcome at each point through the process and a comparison of the goals to the design and outcome.

In recent decades, efforts in complex system design methodology development and in risk methods development have produced new methods useful for understanding potential failure pathways that the traditional defense in depth strategy may have otherwise missed. Within nuclear power, PRA has been developed over the last five decades to help identify potential complex, multi-component failure modes that can challenge a plant's defenses [9,10]. PRA is built upon fault-tree and event-tree models of system failure scenarios. Probabilistic basic event models are then built upon past component failure data using Bayesian statistical methods to adapt generic failure data to specific plant conditions. The resulting "cut-sets," which show failure pathways to complete system failure have attached failure probabilities that indicate the likelihood over a defined time period of system failure occurring. Many other industries have adopted or are in the process of adopting PRA. More recently, functional and functional failure design and analysis methods have begun to tackle some of the problems that are challenging for PRA to adequately address.

It is important to understand what a cut-set is. A cut set is the minimum viable failure pathway where the failure rate is determined by looking at the probability of that pathway occurring. The failure rate is calculable because each component has probabilities of failure associated with it. PRA, FFIP and other functional methods usually return lists of cut sets, and sum the failure rates of all the cut sets to get an overall system failure rate.

PRA faces several challenges in the methodology [11] and in specific applications including detailed and accurate fire and flood propagation analysis, failures that propagate across functional/system boundaries, and a lack of cross-applicable methodologies from different industries. PRA provides a sound methodology for numerically analyzing fire risk, but is lacking because the data needed to evaluate the risk of a fire require a large quantity of data, rely on the data being available for the area being analyzed, and assume that the data for the item being assessed is the same as the data available [12]. Similar problems exist in flood management and risk analysis [13]. Because most research into risk assessment has been performed for specific fields, specific methodologies and practices have been developed that are difficult to compare across fields and difficult to use together [14]. Another problem that PRA faces is a lack in capability to have errors and faults cross system/functional boundaries without significant manual development of these fault propagation scenarios. These types of failures can be incorporated by adding specific 'components' to a fault tree that simulate this risk but this is more of a work-around of the limitations of PRA rather than a strong method to adequately address faults crossing functional or system boundaries. External boundaries on the system limit the scope of the analysis but can also make it difficult to accurately predict risk [15]. Functional modeling methodologies are a new and different set of tools that hold the promise of addressing some of the shortcomings of PRA especially for the early stages of complex system design.

The Functional Basis for Engineering Design (FBED) modeling methodology developed by Stone and Wood [16], and later further refined [17–19], provides a standardized way of representing system functionality in complex engineered systems. Since the introduction of FBED, several methods and extensions have been developed to model system risk from a functional basis. The first significant development was the Function Failure Design Method (FFDM). FFDM provides function failure probability data based upon component failure databases [20]. This allows designers to make decisions to take mitigating actions in the early phases of design of a new engineered system. System state changes during various phases of a system's mission, such as with multi-stage orbiter/lander/rover robotic exploration missions, are modellable using the Function-based Analysis of Critical Events (FACE) method [21]. The FFDM method is very useful, but only a small part of a much larger set of methods, that is still under development. The FFIP methodology provides a tool to analyze the propagation of failure flows along nominal flow pathways [22] and FSL introduces rigorous quantitative probabilistic analysis tools to FFIP [23, 24].

FFIP utilizes the modeling methodology of FBED. The FFIP methodology first starts by functionally modeling a system, either already in operation or under development, using FBED. These functions are linked together with flow paths to indicate the flow of material, energy, or information between functions and into and out of the system boundaries. Once the functional model is developed, FFIP looks at each functional block and in-

duces a failure. Similar to PRA, these failures are like initiating events [15]. Then a determination is made whether or not a function will emit a failure flow, and the flow is followed to the next function where a probability is determined for whether or not the failure flow from the initially failed function fails another function down the line. This process is continued until the flow is stopped or a failed flow leaves the system. This is repeated with each function that can fail. FFIP also analyzes failures if a failed flow from another system enters the system being analyzed (similar to external initiating events in PRA models). This allows a probability of failure for the system to be determined, and is also useful as a design tool to mitigate potential failures from the outset of design.

In order to address shortcomings in the modeling of cross-functional-boundary flow propagation in FFIP, the UFFSR method was developed to assess likelihood that a failure flow will propagate along flow pathways that are not nominal and thus not modeled in FFIP and related methods [25, 26]. FFIP and FSL are restricted in their design to analyze flows along nominal pathways. In reality, flows can occur that are along unexpected, non-nominal flow pathways. For example, a ruptured pipe likely will spray water, especially in a high pressure system like a nuclear Pressurized Water Reactor (PWR), and this water can lead to electrical shorts in systems in the range of spray. FFIP captures the probability of failure from the loss of water in the system, but ignores the chance that the ruptured pipe could cause a failure in the uncoupled electrical system, or in a system redundant to the ruptured pipes. UFFSR is a methodology that accounts for these types of failures, encouraging the use of physics and geometry to determine the likelihood of a failure propagating to an uncoupled system. With the ruptured pipe example, UFFSR determines the likelihood that the rupture will cause a water spray, and whether or not that water will spray in a direction with sufficient force to reach, and then fail the electrical system.

3 METHODOLOGY

Developing a tool to conduct functional failure analysis in the early stages of design that encompasses all areas currently analyzed by PRA methodologies has been an ongoing goal of several research efforts. Already UFFSR, FFIP, and others have made strides to this end. The next critical development that is presented in this paper is DFFAF where an analysis of how adding AFs to the functional model will impact system failure probabilities. An AF is a function specifically meant to stop the propagation of failures across physical distances. These functions are typically added after the initial functional failure analysis to try to limit the failures caused by flows that propagate from one uncoupled system to another, which are found by utilizing UFFSR.

Once the location and placement of AFs within the functional model is complete then analysis is performed to determine which AF decreased the failure probabilities the most, and determine which AFs are the most effective to implement in the physical system. To truly determine the best outcome, multiple AFs of different designs are analyzed and added to the functional model. When an AF is added, it still needs to allow for graceful failure propagation in case the AF itself fails. Essentially AFs can be thought of as probability reducers for uncoupled function failure flows reaching from one function to another. Physically, AFs can be thought of as, for instance, spray guards placed around potential failure spray sources to reduce the probability of water reaching unprotected electronics.

In order to perform the DFFAF method, several steps must be performed. Initial steps use existing methodologies in the literature. Later steps implement AFs and the core DFFAF methodology. The steps to perform DFFAF analysis are as follows, and can be viewed as a process flow in Figure 1.

1. Model system of interest using FBED.
2. Determine critical export flows.
3. Develop a FFIP model of the system using FSL.
4. Perform UFFSR analysis of the system to determine uncoupled failure flow paths.
5. Determine highest probability failure flow propagation paths along uncoupled failure flow paths (from UFFSR). Determine if these flows can be arrested. If not, move on to lower frequency failures. If the failure frequency caused by uncoupled flows is lower than the failure rate due to failures found with FFIP, attention should first be paid to these failures, as they are of higher importance.
6. Insert DFFAF functions at appropriate locations to mitigate the highest probability failure flow propagation paths, as determined by UFFSR. This is performed in a manner that allows for determination of which AFs decreased the failure likelihood the most (performed in the next step). AFs are chosen by determining what function could stop as many failure flows as possible from reaching uncoupled components. (IE: One barrier wall could stop critical uncoupled failure flows from reaching several functions.)
7. Rerun UFFSR with new DFFAF functions in place. Note that new DFFAF functions are analyzed for failure flow propagation along nominal flow paths, uncoupled failure flow paths, and designated failure flow paths. Recognize that certain implementations of AFs can lead to new failure scenarios that will need to be analyzed. For example, if hit with a projectile hard enough, a concrete wall could break and send shrapnel to damage another function, or the concrete wall could crumble by itself and break the function it is supposed to protect.
8. Repeat step 4 through 7 as needed, adding and removing AFs, until an ideal configuration is found.

The practitioner should note that addressing failures found with UFFSR should be done before addressing FFIP failures

when the UFFSR failures have higher probability than those found from FFIP. If the FFIP failures are more probable, then they should be addressed first. Following this order of analysis operations increases the overall system reliability the most effectively.

The DFFAF methodology is an iterative process. It uses a FBED-modeled system along with FFIP and FSL to model standard, nominal failure flows. It then implements UFFSR to determine which failures create flows that cross functional boundaries, and which failure flows are of the highest importance. DFFAF then determines how to place AFs by iteratively choosing the best placement. Using many AFs is a potentially attractive way to limit cross-boundary failure rate but strategic placement of AFs will limit the cost of physical implementation while retaining the benefits of reduced system failure probability.

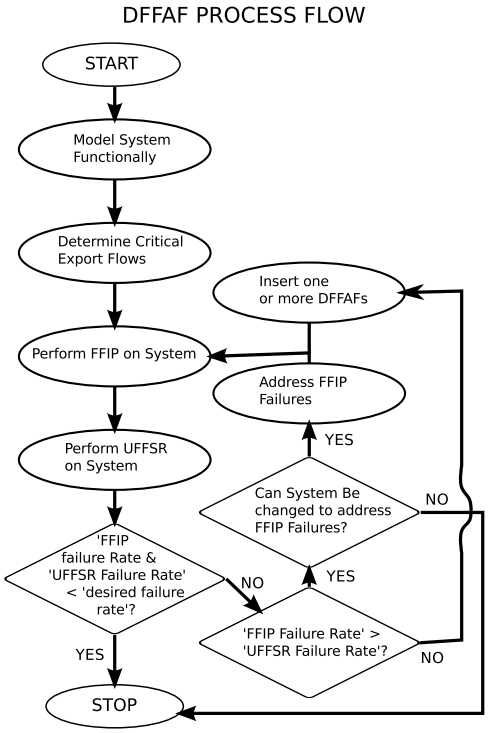

FIGURE 1. PROCESS FLOW DIAGRAM FOR THE DFFAF METHOD

4 CASE STUDY

In order to illustrate DFFAF, a case study is presented in this section based upon a portion of the Emergency Core Cooling System (ECCS) found in a generic large commercial PWR nuclear power plant. Of specific interest to this case study within the ECCS is the Safety Injection System (SIS) that provides cold water injection into the primary Reactor Core Coolant Loop (RCCL). The SIS has two redundant subsystems (known as "trains" in the nuclear engineering field) each with two motor valves, pumps, check valves, and heat exchangers. Figure 2 shows the component layout in a room within the generic PWR. The system boundary for this case study was set to correspond with the room geometry for ease of understanding. In this system, import and export flows include liquid material, thermal energy, electrical energy, and control signals that correspond to hot water, cold water, electricity, and command data at the component level. Certain flows, such as thermal energy along the liquid material flow path, have been omitted for brevity and clarity although their omission does not adversely impact the analysis presented here. The case study follows the UFFSR methodology in the following subsections.

The DFFAF method works equally well with much larger functional models than are presented here. The DFFAF method is being developed to address complex and large systems, such as nuclear power plants. Highly complex systems can become computationally intensive and require a large capacity for data storage and processing. This is because each function can potentially interact and create its own set of cut-sets that can effect the system failure rate. For very large functional models, the author advocates using truncations methods to limit computational resource requirements.

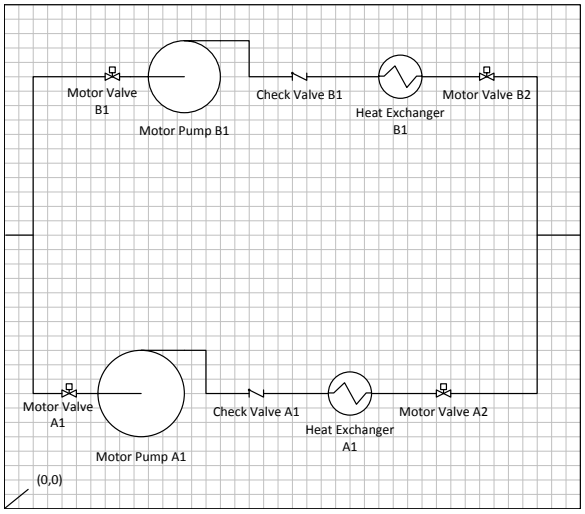

FIGURE 2. COMPONENT LAYOUT OF ECCS-SIS TWO TRAIN SUBSYSTEM. EACH SQUARE IS ONE METER BY ONE METER

4.1 Model System Using FBED

Figure 3 shows the functional model of the portion of the SIS being analyzed in this case study. Table 1 provides component location information and corresponding function names. The FBED has turned the system layout into a functional based system.

TABLE 1. FUNCTION TO COMPONENT MAP AND COMPONENT LOCATION

Component Name	Function Name	Location (x,y) (m)
Motor Valve A1/B1	Regulate Liquid A1/B1	(4.5,8)/(7.5,30)
Check Valve A1/B1	Regulate Liquid A2/B2	(17.5,8)/(20.5,30)
Motor Valve A2/B2	Regulate Liquid A3/B3	(30.5,8)/(33.5,30)
Motor Pump A1/B1	Transfer Liquid A1/B1	(9.5,8)/(12.5,30)
Heat Exchanger A1/B1	Transfer Thermal A1/B1	(24,8)/(27,30)

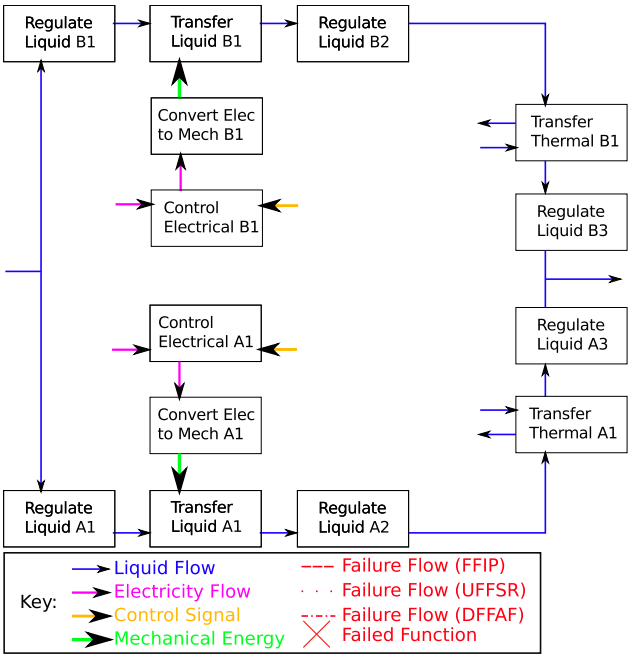

FIGURE 3. FUNCTIONAL MODEL OF PORTION OF ECCS TRAIN

4.2 Critical Flows

The critical export flow from this system is a liquid flow at the nominal operating temperature. Hence, it is assumed that each train has sufficient capability to regulate the flow and temperature, and only if both trains fail is the export flow failed.

4.3 Develop FFIP model using FSL

To model the failure probabilities for this system, representative realistic values were developed. They are not based upon actual data, but are of the representative range of failure likelihood. Data-driven values that engineers can use in practice are available from several sources including the NRC [27] and the International Atomic Energy Agency (IAEA) [28,29] among others.

To calculate failures, probabilities of each component failure and the probabilities to transfer the failures to functions along nominal flow paths are multiplied together using boolean algebra. When forcing the secondary train to also fail, the linear failure values along the individual trains are the same for both trains A and B, and are multiplied together to get the probability of both trains failing.

A representative FFIP example with the Transfer Liquid A1 function failing is shown in Figure 4. This example does not fail the system because only one of the two trains has failed.

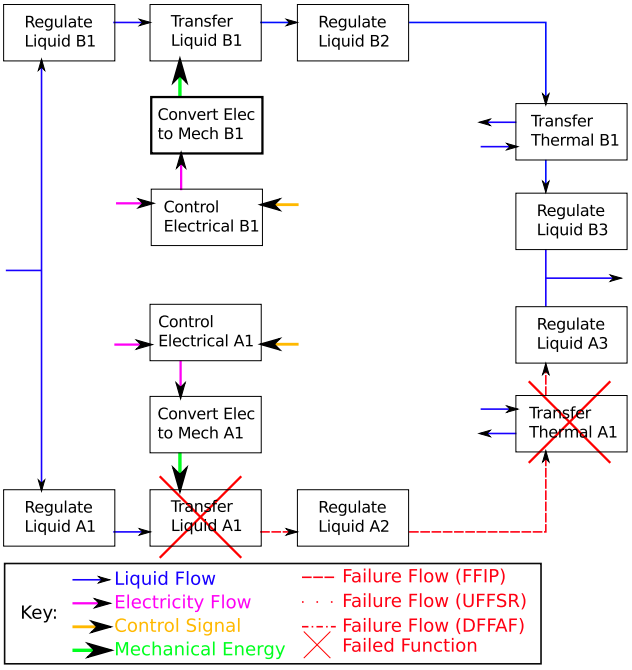

FIGURE 4. FFIP EXAMPLE FAILURE FLOW. FAILED TRANSFER LIQUID DOES NOT FAIL THE SYSTEM.

4.4 UFFSR Analysis

To perform a UFFSR analysis, it is assumed that certain functions can fail and propagate a failure flow to a functionally uncoupled system. This case study is limited, for clarity, to only analyzing a non-nominal liquid fail spray from the Transfer Liq-

uid or Transfer Thermal functions and impacting the Transfer Liquid function of the other train. An illustrative example flow is shown in Figure 5. Probabilities for acceptance into uncoupled components are geometrically determined. To determine if a flow sprays in the proper direction thus becomes an uncoupled failure flow, it is assumed that there is an equal probability of the transfer liquid or transfer heat function undergoing something like a rupture and creating a liquid failure flow (water jet) in any direction (spherically). If better data about how a system will fail and cause an uncoupled failure flow is available, a specific and statistically accurate model can be created for that system. As designs are refined from the early conceptual stage to the final stages of design before a plant is constructed, refinement of the failure propagation directions and distances can occur. The spherical probability of spraying in a direction that could induce failure in the pump of the other train of the system is given by equation 1:

$$P_{correctDirection} = \frac{A_{sa}}{4\pi r_{ab}^2} \quad (1)$$

A_{sa} is the surface area of the receptor component exposed to the water. Each component is considered to be a rectangular prism and is assumed that twice the area of the largest face is an acceptable area that can be affected. r_{ab} is the shortest distance from the failed and spraying function to the accepting function. The shortest distance between components is used to get a conservative probability failure chance.

Probabilities of accepting the failed spray are selected based on normal shielding or electrical panel casing keeping the water away from electronics. For the purposes of this analysis, the chance that the failed liquid spray hits electrical components is weighted at 12.5% probability while 87.5% of the time the water will hit the pump or other related components in the pump assembly. This probability can change based upon the design of the pump and electrical controls, the orientation of the pump and electrical controls to spray source, or a variety of other potential failure propagation mitigators or aggravators.

4.5 Highest Probability Failure Flows From UFFSR

It was determined that the highest probability flows from the UFFSR analysis were caused by the transfer liquid function rupturing in either train followed by a failed liquid spray being accepted by the redundant trains Convert Electrical to Mechanical function, followed by the same accepting function, but the Transfer Thermal Function failing. Detailed cut-sets are provided in Table 3.

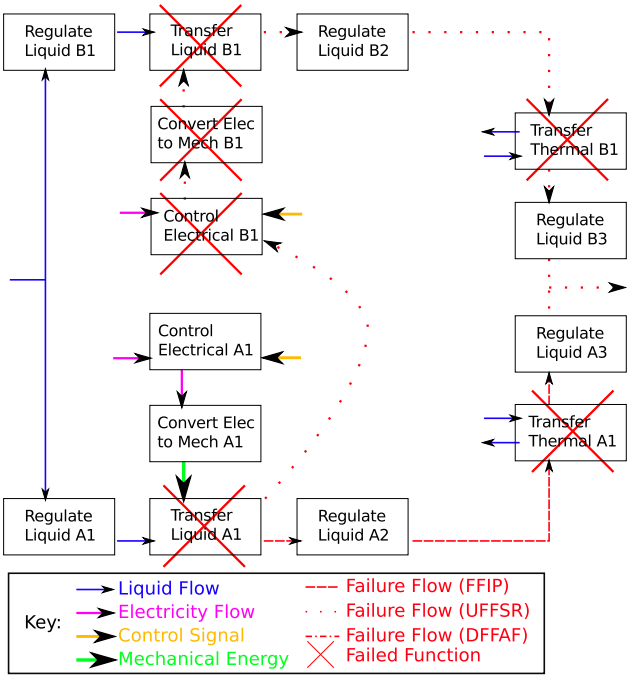

FIGURE 5. UFFSR EXAMPLE FAILURE FLOW. TRANSFER LIQUID FAILS UNCOUPLED CONTROL ELECTRICAL LEADING TO SYSTEM FAILURE.

4.6 Insert DFFAF Functions

Based on the top cut sets in Table 3, it was determined that the Transfer Liquid Function or its sub-functions (Convert Electrical to Mechanical and Control Electrical) have the highest probabilities of failure, these were the functions focused on when inserting AFs. An illustrative failure with an AF is shown in Figure 6. Two Contain Liquid functions were inserted, one for train A and one for train B. These functions will limit the impact of failed liquid sprays to or from the functions. It was determined that at minimum, two are needed. One Contain Liquid function stops failure flows from that transfer function, or going to it from the other Transfer Liquid or Transfer Thermal functions, but then the other Transfer Liquid function would have no protection from a failure flow from the primary train's Transfer Thermal fail flow. Thus, two AFs were deemed the appropriate number to start reducing risk.

4.7 Re-Run UFFSR

When determining the probability that the new AF worked, it was assumed to be something solid, that physically would block the path of the water spray. Physical examples of the AF include a metal casing surrounding the source of the failure flow or a concrete wall next to the source of the failure flow to block the flow from propagating across functional boundaries. As will be seen below, the Transfer Liquid functions have a much higher

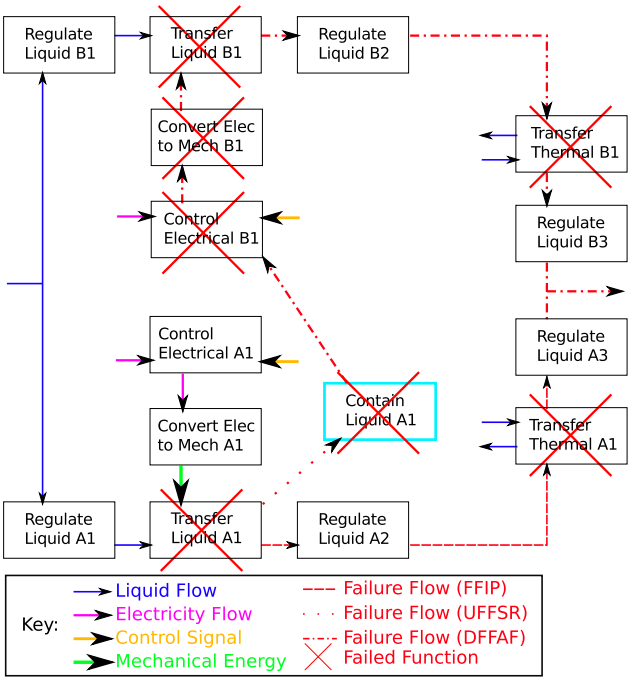

FIGURE 6. DFFAF EXAMPLE FAILURE FLOW INCLUDING FAILURE PROPAGATION PATHS. NON-NOMINAL FLOW HAS BEEN STOPPED BY AF BUT MAY STILL PROPAGATE TO OTHER FUNCTIONS WITH A SIGNIFICANTLY REDUCED LIKELIHOOD.

chance of damaging each other than the Transfer Thermal functions do. Thus, an AF has been added next to each of the pumps to block the failure flows and failure probabilities are then recalculated. Note that each AF works to isolate each train from the other train so that the AF stops the failure flow from either being accepted by or emitted from the function. Thus a failure flow from Transfer Liquid A must propagate through two AFs specifically designed to prevent failure propagation before the failure flow can reach the Transfer Liquid B function.

4.8 Repeat Steps

After re-running UFFSR, the probabilities of failure dropped to be in the same range as the probabilities from FFIP. Thus rearranging and re-optimizing the DFFAF functions was deemed unnecessary.

5 RESULTS AND DISCUSSION

In this section, results of the DFFAF method are presented, discussed, and compared with the existing FFIP and UFFSR methodologies. It can be seen through the results presented here that DFFAF presents new and useful information that was not otherwise available to the engineer in FFIP and UFFSR. The case study results, while limited to a small portion of a much larger system and limited to one failure mode, are informative and reveal the usefulness of DFFAF. Failure of the system analyzed in this paper is defined as both trains of the system failing. Each train is a redundant system to the other train.

5.1 FFIP Results

In this case study, several failures using FFIP logic were calculated. The top eight cut-sets for this are shown in Table 2. This indicates that the highest failure likelihood arose from the Transfer Liquid function in each train spontaneously rupturing, and the two redundant failures accounted for 40% of the failure likelihood. The highest frequency of failure by double Transfer Liquid failure was on the order of 10^{-11}/yr, and the overall failure frequency was on the order of 10^{-10}/yr. The other high-probability failures were electrical failures in the pump, or ruptures of the heat exchanger. Using only FFIP results, it appears necessary to make the pumps more reliable as the best method of improving system reliability.

5.2 UFFSR Results

When performing the UFFSR analysis, only the failed Transfer Liquid and Transfer Thermal failures from the FFIP were carried forward into the UFFSR analysis. This is for simplicity of the case study and because the uncoupled failure that is most likely to occurr in this system is a water spray (liquid failure flow) from a ruptured component. The top eight cut-sets for the UFFSR are presented in Table 3. These cut-sets show that the highest likelihood event to fail the system is a transfer liquid failure followed by an uncoupled liquid failure flow from the failed function to the functions of the other train. These failures happen at a rate of about 10^{-8}/yr, which is two orders of magnitude higher than the overall system failure likelihood calculated using FFIP. Analysis conducted using UFFSR shows that the best improvement would be to somehow stop the uncoupled failure flow (a water spray in the instance of the case study) from the transfer liquid function or transfer thermal function from reaching the transfer liquid function on the other train. Thus, fixing the problems determined by UFFSR should be of a higher priority than fixing the problems determined by using the FFIP methodology.

5.3 DFFAF Results

The DFFAF analysis cut-sets, shown in Table 4, were generated by placing an AF on each transfer liquid function (physically this is equivalent to putting a shield around each pump). By including the contain liquid AFs, the system failure rate dropped from about 10^{-8}/yr to 10^{-9}/yr (a significant improvement) using AFs that are relatively simple to implement in the physical world. However, even with using DFFAF to mitigate uncoupled failure flow paths identified by UFFSR, the system failure probability compared to FFIP is still higher by an order of magnitude. This

TABLE 2. FFIP ANALYSIS TOP CUT SETS

Prob/Freq per year	Total Prob.	Top 8 FFIP Cut Sets
3.20E-10	1.000	
6.40E-11	0.200	Trans_Liq_A1-Rupture, Trans_Therm_A1-Fail, Trans_Liq_B1-Rupture, Trans_Therm_B1-Fail, Export_Liq_Fail
6.40E-11	0.200	Trans_Liq_B1-Rupture, Trans_Therm_B1-Fail, Trans_Liq_A1-Rupture, Trans_Therm_A1-Fail, Export_Liq_Fail
4.00E-11	0.125	Cont_Elec_A1_ElecLoss, Conv_ElecToMech_A1-fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Trans_Liq_B1-Rupture, Trans_Therm_B1-Fail, Export_Liq_Fail
4.00E-11	0.125	Cont_Elec_B1_ElecLoss, Conv_ElecToMech_B1-fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Trans_Liq_A1-Rupture, Trans_Therm_A1-Fail, Export_Liq_Fail
3.20E-11	0.100	Trans_Therm_A1-Rupture, Trans_Liq_B1-Rupture, Trans_Therm_B1-Fail, Export_Liq_Fail
3.20E-11	0.100	Trans_Therm_B1-Rupture, Trans_Liq_A1-Rupture, Trans_Therm_A1-Fail, Export_Liq_Fail
2.40E-11	0.075	Conv_ElecToMech_A1-MotorFail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Trans_Liq_B1-Rupture, Trans_Therm_B1-Fail, Export_Liq_Fail
2.40E-11	0.075	Conv_ElecToMech_A1-MotorFail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Trans_Liq_B1-Rupture, Trans_Therm_B1-Fail, Export_Liq_Fail

TABLE 3. UFFSR ANALYSIS TOP CUT SETS

Prob/Freq per year	Total Prob	Top 8 UFFSR Cut Sets
3.90E-08	1.000	
1.31E-08	0.336	Trans_Liq_A1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_A1-Fail, Conv_ElecToMech_B1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
1.31E-08	0.336	Trans_Liq_B1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_B1-Fail, Conv_ElecToMech_A1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Export_Liq_Fail
2.97E-09	0.076	Trans_Therm_A1-Rupture & Export_Liq_Fail_Spray Conv_ElecToMech_B1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
2.97E-09	0.076	Trans_Therm_B1-Rupture & Export_Liq_Fail_Spray Conv_ElecToMech_A1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Export_Liq_Fail
2.81E-09	0.072	Trans_Liq_A1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_A1-Fail, Cont_Elec_B1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_B1-Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
2.81E-09	0.072	Trans_Liq_B1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_B1-Fail, Cont_Elec_A1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_A1-Fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Export_Liq_Fail
6.36E-10	0.016	Trans_Therm_A1-Rupture & Export_Liq_Fail_Spray, Cont_Elec_ B1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_B1-Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
6.36E-10	0.016	Trans_Therm_B1-Rupture & Export_Liq_Fail_Spray, Cont_Elec_A1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_A1-Fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Export_Liq_Fail

is as a result of the AF failure probability. The AF is assumed to have a probability of not being successful in arresting the uncoupled failure flow. Were the AF perfect at its intended function, the FFIP and DFFAF results would show the same system failure probability. Thus, DFFAF produces a more accurate system failure probability and more accurate cut-sets than either FFIP or UFFSR generate.

5.4 Discussion of the DFFAF Method in Relation to FFIP and UFFSR

DFFAF is an improvement of existing functional failure modeling techniques. DFFAF has added a method that analyzes the best course of action to take to prevent failure flows from propagating beyond functional boundaries. Functional failure modeling now has a tool to include functions that are specifically inserted into a design for the purpose of capturing uncoupled failure flows and diverting the failure flows from other important system functions. The DFFAF method allows for the analysis

TABLE 4. DFFAF TOP 8 CUT SETS

Prob/Freq per year	Total Prob	Top 8 DFFAF Cut Sets
2.71E-09	1.000	
5.93E-10	0.219	Trans_Therm_A1-Rupture & Export_Liq_Fail_Spray, AF_B1-Fail, Conv_ElecToMech_B1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
5.93E-10	0.219	Trans_Therm_B1-Rupture & Export_Liq_Fail_Spray, AF_A1-Fail, Conv_ElecToMech_A1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Export_Liq_Fail
5.24E-10	0.193	Trans_Liq_A1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_A1-Fail, AF_A1-Fail, AF_B1-Fail, Conv_ElecToMech_B1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
5.24E-10	0.193	Trans_Liq_B1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_B1-Fail, AF_B1-Fail, AF_A1-Fail, Conv_ElecToMech_A1 Accept_Liq_Fail_Spray & Fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Export_Liq_Fail
1.27E-10	0.047	Trans_Therm_A1-Fail & Export_Liq_Fail_Spray, AF_B1-Fail, Cont_Elec_B1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_B1-Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
1.27E-10	0.047	Trans_Therm_B1-Fail & Export_Liq_Fail_Spray, AF_A1-Fail, Cont_Elec_A1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_A1-Fail, Trans_Liq_A1-Fail, Trans_Therm_A1-Fail, Export_Liq_Fail
1.12E-10	0.041	Trans_Liq_A1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_A1-Fail, AF_A1-Fail, AF_B1-Fail, ACont_Elec_B1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_B1-Fail, Trans_Liq_B1-Fail, Trans_Therm_B1-Fail, Export_Liq_Fail
1.12E-10	0.041	Trans_Liq_B1-Rupture & Export_Liq_Fail_Spray, Trans_Therm_B1-Fail, AF_B1-Fail, AF_A1-Fail, Cont_Elec_A1-Accept_Liq_Fail_Spray & Fail, Conv_ElecToMech_A1-Fail, Trans_Liq_A1-Fail, Trans_ThermAB1-Fail, Export_Liq_Fail

and addition of AFs in functional models when designing a system in the early phases of conceptual design. As the design matures, the AFs will be developed into components or subsystems which fulfill the uncoupled failure flow mitigation role that the AFs represent. The addition of DFFAF to the expanding toolbox of functional failure modeling techniques allows designers to analyze functional models for locations where AFs can be inserted to mitigate uncoupled failure flows from impacting uncoupled functions which in turn reduces the overall likelihood of system failure. DFFAF has expanded the applicability of function failure modeling, bringing it one step closer to having the same capabilities for analyzing and improving current systems such as PRA. The DFFAF method is also a useful tool in the design process, allowing for the inclusion of more types of functions.

6 CONCLUSION AND FUTURE WORK

DFFAF is a novel functional failure modeling-based design tool that allows placement and analysis of AFs that are specifically meant to stop failure flows from propagating across uncoupled failure flow paths previously identified in the UFFSR method, itself a method to address uncoupled failure flows not previously modeled in the FFIP method. The DFFAF provides a basis for determining where to place AFs in a system to develop more reliable systems and uncover potential failure pathways that would otherwise have not been identified in existing techniques. Previous developments in functional failure modeling only analyzed failures and suggested methods of redesign of the system to mitigate failures within the exigent functions. DFFAF places new functions (AFs) into the functional model whose soul purpose is mitigation of uncoupled failure flows. Thus functional modeling methods used in complex system design can now more fully consider uncoupled failure flow propagation mitigation strategies and will be able to create more reliable system designs.

Future work will expand the DFFAF specifically to rigorously account for an AF failing and causing a failure flow to be emitted from the AF. In the event of an AF failure, several scenarios could unfold including: 1) propagation of the failure flow without mitigation along its original uncoupled failure flow path, 2) propagation of the failure flow without mitigation along a different uncoupled failure flow path, and 3) propagation of a new failure flow that is either less bad or worse to the overall system state from the failed AF, among other possibilities. Potentially UFFSR can be applied to analyze AF failures, but significant future work beyond the scope of this paper is required to determine appropriate models for AF failure. The end goal is to have a family of functional-based methods that are as or more robust than PRA, and can be used in the early phases of conceptual design, rather than post-conceptual-design like PRA currently is used. These functional methods are envisioned to be used in the conceptual stage of design to help with risk-informed decision-making [30], as a model can be adjusted to include and exclude functions and the component solutions to functions during an optimization process. Rigorous and verified software packages, similar to those available for PRA analysis, will be developed in the future to further the use of functional based design and analysis.

ACKNOWLEDGMENT

This research was partially supported by United States Nuclear Regulatory Commission Grant Number NRC-HQ-84-14-G-0047. Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.

REFERENCES

[1] Fleming, K. N., and Silady, F. A., 2002. "A risk informed defense-in-depth framework for existing and advanced reactors". *Reliability Engineering & System Safety,* ***78***, July, pp. 205–225.

[2] Bakolas, E., and Saleh, J. H., 2011. "Augmenting defense-in-depth with the concepts of observability and diagnosability from control theory and discrete event systems". *Reliability Engineering & System Safety,* ***96***(1), pp. 184–193.

[3] Zio, E., 2009. "Reliability engineering: Old problems and new challenges". *Reliability Engineering & System Safety,* ***94***(2), pp. 125 – 141.

[4] Stamanis, D. H., 2003. *Failure Modes and Effects Analysis: FMEA from Theory to Execution*, 2nd ed. ASQ Quality Press, Milwaukee, WI.

[5] Ben-Daya, M., 2009. "Failure mode and effect analysis". In *Handbook of Maintenance Management and Engineering*, M. Ben-Daya, S. O. Duffuaa, A. Raouf, J. Knezevic, and D. Ait-Kadi, eds. Springer London, pp. 75–90.

[6] Robidoux, R., Xu, H., Xing, L., and Zhou, M., 2010. "Automated modeling of dynamic reliability block diagrams using colored petri nets". *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on,* ***40***(2), March, pp. 337–351.

[7] Hamada, M. S., Wilson, A. G., Reese, C. S., and Martz, H. F., 2008. *Bayesian Reliability*. Springer.

[8] Smith, D., 2011. *Reliability, Maintainability and Risk 8e: Practical Methods for Engineers including Reliability Centred Maintenance and Safety-Related Systems*. Elsevier Science.

[9] Modarres, M., Kaminskiy, M., and Krivtsov, V., 1999. *Reliability engineering and risk analysis: a practical guide*. CRC press.

[10] Keller, W., and Modarres, M., 2005. "A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor norman carl rasmussen". *Reliability Engineering & System Safety,* ***89***(3), pp. 271 – 285.

[11] Distefano, S., and Puliafito, A., 2009. "Dependability evaluation with dynamic reliability block diagrams and dynamic fault trees". *Dependable and Secure Computing, IEEE Transactions on,* ***6***(1), Jan, pp. 4–17.

[12] Ramachandran, G., and Charters, D., 2011. *QUANT RISK ASSESS FIRE SAFETY*. Taylor & Francis.

[13] Samuels, P., Huntington, S., Allsop, W., and Harrop, J., 2008. *Flood Risk Management: Research and Practice: Extended Abstracts Volume (332 pages) + full paper CD-ROM (1772 pages)*. Taylor & Francis.

[14] Soares, C., 2010. *Safety and Reliability of Industrial Products, Systems and Structures*. A Balkema Book. Taylor & Francis.

[15] Bedford, T., and Cooke, R., 2001. *Probabilistic Risk Assessment: Foundations and Methods*. Cambridge University Press.

[16] Stone, R. B., and Wood, K. L., 2000. "Development of a functional basis for design". *Journal of Mechanical Design,* ***122***(4), pp. 359–370.

[17] Stone, R. B., Wood, K. L., and Crawford, R. H., 2000. "Using quantitative functional models to develop product architectures". *Design Studies,* ***21***(3), pp. 239–260.

[18] Hirtz, J. M., Stone, R. B., Szykman, S., McAdams, D., and Wood, K. L., 2001. "Evolving a functional basis for engineering design". In Proceedings of the ASME Design Engineering Technical Conference: DETC2001, Pittsburgh, PA.

[19] Hirtz, J., Stone, R. B., McAdams, D. A., Szykman, S., and Wood, K. L., 2002. "A functional basis for engineering design: reconciling and evolving previous efforts". *Research in engineering Design,* ***13***(2), pp. 65–82.

[20] Stone, R. B., Tumer, I. Y., and Stock, M. E., 2005. "Linking product functionality to historic failures to improve failure analysis in design". *Research in Engineering Design,* ***16***(1-2), pp. 96–108.

[21] Hutcheson, R. S., McAdams, D. A., Stone, R. B., and Tumer, I. Y., 2006. "A function-based methodology for analyzing critical events". In Proceedings of the IDETC/CIE.

[22] Kurtoglu, T., and Tumer, I. Y., 2008. "A graph-based fault identification and propagation framework for functional design of complex systems". *Journal of Mechanical Design,* ***130***(5), p. 051401.

[23] Jensen, D., Tumer, I. Y., and Kurtoglu, T., 2009. "Flow state logic (fsl) for analysis of failure propagation in early design". In ASME 2009 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, American Society of Mechanical Engineers, pp. 1033–1043.

[24] Kurtoglu, T., Tumer, I. Y., and Jensen, D. C., 2010. "A functional failure reasoning methodology for evaluation of conceptual system architectures". *Research in Engineering Design,* ***21***(4), pp. 209–234.

[25] Ramp, I. J., and Van Bossuyt, D. L., 2014. "Toward an automated model-based geometric method of representing function failure propagation across uncoupled systems". In Proceedings of the ASME 2014 International Mechanical Engineering Congress and Exposition IMECE2010, ASME.

[26] O'Halloran, B., Papakonstantinou, N., and Van Bossuyt, D. L., 2015. "Modeling of function failure propagation

across uncoupled systems". In Proceedings of the Reliability and Maintainability Symposium.

[27] , 2007. Industry-average performance for components and initiating events at u.s. commercial nuclear power plants. Technical Report NUREG/CR-6928 and INL/EXT-06-11119, Idaho National Laboratory, Washington, DC, February.

[28] , 1988. Component reliability data for use in probabilistic safety assessment. Technical Report IAEA-TECDOC-478, International Atomic Energy Agency, Vienna, Austria.

[29] , 1993. Defining initiating events for purposes of probabilistic safety assessment. Technical Report IAEA-TECDOC-719, International Atomic Energy Agency, Vienna, Austria.

[30] Van Bossuyt, D., Hoyle, C., Tumer, I. Y., and Dong, A., 2012. "Risk attitudes in risk-based design: Considering risk attitude risk attitudes in risk-based design: Considering risk attitude using utility theory in risk-based design". *Artificial Intelligence for Engineering Design, Analysis and Manufacturing,* ***26***, pp. 393–406.

Appendix A: Probability Information Used to Calculate Cut-Sets

TABLE 5. PROBABILITIES USED FOR CUT SET GENERATION. FUNCTION FAILURE RATES ARE IN UNITS OF $(YEAR^{-1})$. OTHER VALUES ARE PROBABILITIES OF THAT EVENT OCCURRING.

Failures	Probability
Transfer Liq A Fail	8.000E-06
Transfer Liq B Fail	8.000E-06
Convert Elec to Mech A Fail	3.000E-06
Convert Elec to Mech B Fail	3.000E-06
Control Elec A Fail	5.000E-06
Control Elec B Fail	5.000E-06
Transfer Thermal A Fail	4.000E-06
Transfer Thermal B Fail	4.000E-06
Transfer Liq A Fails by Spraying	5.000E-01
Spray goes far enough TransLiq A to B	6.000E-01
Sprays towards Trans Liq B from Trans Liq A	3.466E-02
Spray Hits Control Elec B	1.250E-01
Control Elec B accepts Failure Spray	3.000E-01
Control Elec B Fails from Failure Spray	9.000E-01
Transfer Liq B Fails by Spraying	5.000E-01
Spray goes far enough TransLiq B to A	6.000E-01
Sprays towards Trans Liq A from Trans Liq B	3.466E-02
Spray Hits Control Elec A	1.250E-01
Control Elec A accepts Failure Spray	3.000E-01
Control Elec A Fails from Failure Spray	9.000E-01
Spray Hits Conv Elec to Mech A from Trans Liq B	8.750E-01
Conv Elec to Mech A accepts failure spray from Trans Liq B	2.000E-01
Spray Hits Conv Elec to Mech B from Trans Liq A	8.750E-01
Conv Elec to Mech B accepts failure spray from Trans Liq A	2.000E-01
Transfer Thermal A Fails by Spraying	4.000E-01
Spray goes far enough Trans Therm A to Trans Liq B	4.000E-01
Sprays towards Trans Liq B from Trans Therm A	2.943E-02
Transfer Thermal B Fails by Spraying	4.000E-01
Spray goes far enough Trans Therm B to Trans Liq A	4.000E-01
Sprays towards Trans Liq A from Trans Therm B	2.943E-02
Transfer Liq A Arrestor Function Fails	2.000E-01
Transfer Liq B Arrestor Function Fails	2.000E-01