# TIME-BASED RISK-INFORMED SAFETY MARGINS: CONCEPTS AND APPLICATION TO HETEROGENEOUS SYSTEMS

A Thesis

by

Jack Matthew Cavaluzzi

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

| | |
|---|---|
| Chair of Committee, | Paul Nelson |
| Committee Members, | Karen Vierow |
| | Martin Wortman |
| Head of Department, | Yassin Hassan |

December 2015

Major Subject: Nuclear Engineering

## ABSTRACT

A model to quantify the temporal failure probability for a nuclear power station's fleet of multiple, redundant, emergency diesel generators (EDGs) is developed and demonstrated in this thesis. The initiating event for this problem is Loss of Offsite Power (LOOP). This model calculates the probability that the load on the system overcomes (LOOP duration) the capacity of the system (time until the EDGs fail), as a means to quantify system safety margin; this concept comes from The United States Department of Energy (DOE), the Idaho National Laboratory (INL) and the Electric Power Research Institute (EPRI) collaboration on the "Risk-Informed Safety Margin Characterization" (RISMC) approach. The ultimate application of this model is to quantify improved safety margin for an originally two-EDG system that has been upgraded with an additional, reinforced, FLEX diesel generator (DG). Some unique features of the Non-Recovery Integral (NRI) (main model of this thesis) are that it can account for dynamic timing of the EDG failures, model both hot and cold standby EDG arrangements, and accept time-dependent hazard function inputs for hot standby cases (when the hazard functions meet certain conditions). Nuclear industry and Standardized Plant Analysis Risk (SPAR) model data are used as inputs to the NRI to create six specific system model cases. The results from these cases are compared to see how different EDG arrangements affect the overall system reliability. The three main conclusions drawn from the various result comparisons are the following: (1) adding a FLEX DG to an originally two-EDG system makes the system three times less likely to fail for LOOP durations of 24 hours (further improvement in system reliability is seen for longer LOOP durations); (2) the specific model of load placed on the system has a major impact on the system failure probability quantification; and (3) the most effective way to increase safety margin (for the most likely LOOP duration scenarios) is to reduce the likelihood of common-cause failure events.

## ACKNOWLEDGEMENTS

First I would like to thank my advisor and graduate committee chair, Dr. Paul Nelson. The opportunity to work under him has made it possible for me to pursue a master's degree and complete my thesis. He has provided me with countless hours of guidance throughout the entire course of this project. The knowledge he has shared with me in nuclear safety, mathematical modeling, and technical writing has been invaluable to me. He is an excellent example of a lifelong learner and has truly been an inspiration to me. I want to express my thanks to my graduate committee members, Dr. Karen Vierow and Dr. Martin Wortman, for their review of my thesis and the useful comments they provided.

I would also like to thank some of the industry professionals that I've had the pleasure of working with over the course of this thesis work. A special thanks to Vera Moiseytseva for her assistance with the Markov models in Sections IV.2.1, IV.3.1, and IV.4.1. Thanks go to Michael Powell from the Nuclear Energy Institute for his insight into the FLEX strategy. Thanks also to John Schroeder from Idaho National Laboratory for answering my questions about some aspects of SPAR modeling methods. Finally I want to note the valuable industry-perspective input of some PRA professionals from South Texas Project Nuclear Operating Company, especially Shawn Rodgers, Ernie Kee, and Fatma Yilmaz.

Thanks also go to my friends and faculty in the nuclear engineering department for making my time at Texas A&M University such a great experience.

Lastly, thanks to my mother and father, Jeannie and George Cavaluzzi, for their continued encouragement and love. I would not have made it this far without them and their support.

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

Page

# CHAPTER I

# INTRODUCTION

This chapter will introduce the thesis model, point towards the application of the model, and describe features of the model that are relevant to the progression of system reliability quantification. The objective of this thesis and a description of how the thesis model can meet these objectives are given in Section 1.1. Motivation for the model from a historical sense is given in Section 1.2; this section also highlights some recent risk assessment challenges as well as a relevant application for the model due to the new FLEX [1] program. A high level problem overview is given in Section I.3; information about redundancy types, emergency diesel generator (EDG) system operation, nuclear industry risk assessment practices, and an overview of the thesis model features are presented there. Section 1.4 provides an outline of the remaining chapters in this thesis.

## I.1 Objective

The objective of this thesis is to develop and demonstrate a model to quantify the temporal failure probability for a fleet of multiple, redundant EDGs, given a Loss of Offsite Power (LOOP) initiating event at a nuclear power station. The general system models are developed in Chapter II and then applied to specific case studies in Chapter IV using data that are introduced in Chapter III. The results from the case studies in Chapter IV will show how an overall system failure probability varies with different EDG arrangements and operation modes. The ultimate model application is to quantify improved safety margin for an originally two-EDG system that has been upgraded with an additional, reinforced, FLEX [1] EDG. (The term FLEX here refers to an initiative created by the Nuclear Energy Institute (NEI) called “Flexible and Diverse Coping Strategies” and is discussed in more detail in Section I.2.3.)

The primary probability model for this thesis is based on a previously developed Non-Recovery Integral (NRI) [2], [3] and has adopted the same name here. The NRI models developed in Chapter II and demonstrated in Chapter IV are the primary models used to accomplish the thesis objective; the Markov models of Chapters II and IV are used to verify the accuracy of the NRI. As with the previous NRIs, the offsite power recovery time distribution is

assumed to be statistically independent from the distribution of EDG system failure time. The probability density functions (PDFs) for these two distributions are multiplied and integrated in order to compute the probability that the load (offsite power recovery time) overcomes the capacity of the system (EDG system failure time), as a way to quantify the failure probability of the system. The concepts of load and capacity are developed in the context of the Risk-Informed Safety Margin Characterization (RISMC) pathway of the U.S. DOE Light-water Reactor Sustainability program [4], [5] in Sections II.1 and II.1.1.

As part of the primary objective, another goal of this thesis is to add new modeling capabilities and reduce over-conservatism in relation to current probabilistic risk assessment (PRA) techniques. This goal is concerned with the development of failure time PDFs for EDG systems; PDFs are generated for different operational modes of both two- and three-EDG systems in Chapter II. The EDG system failure time PDFs for the various NRI cases are created using the generalized hazard rate formulation of Shaked and Shanthikumar [6], as it permits systematic development of the distribution of failure times for the emergency power system. Another advantage of this approach is that it accounts for stochastic ordering of the EDG failure times and does not assume that these random variables (EDG failure times) are statistically independent. The thesis model can account for both component-caused and externally-caused common-cause failures (CCFs), a concept which is explored in Section III.3.3. The thesis NRI can model both hot and cold standby EDG operation under certain conditions; hot and cold standby operation are defined in Section I.3.1 while details for how to modify the NRI to account for cold standby is described in Section II.5.1. The NRI model does not currently account for the repair of failed EDGs. This limitation is discussed more in Section I.3.4 and in the second introductory paragraph of Chapter II. An additional model is introduced in Chapter V that can account for this phenomenon.

**I.2 Motivation**

Motivation for this EDG system model comes from past PRA experiences as well as recent events. Since their early use in the nuclear industry, PRAs have recognized that complete loss of AC power, termed station blackout (SBO), is a large risk contributor to total core damage frequency [7]. The recent nuclear accident at Fukushima Daiichi has brought to light the dire consequences of an extended SBO. This led the Nuclear Energy Institute (NEI) to develop

guidance [1] for the FLEX plan that is expected to add defense in depth (DID) in order to mitigate extended SBO consequences. One of the suggestions offered by the FLEX plan is for plants to add a diesel generator (DG) housed separately from their standard EDG fleet. The main application of the methodology developed in this thesis is to quantify potential improved safety margin against SBO as a function of the reliability of the FLEX DG. The accident also led the Nuclear Regulatory Commission (NRC) to document [8] current PRA technology issues; and the models in this thesis offer improvements for some of these issues.

The motivation and main objective of this thesis are important for understanding potential SBO risk and the effectiveness of the recent improvements thorough FLEX DG, especially considering the fact that nuclear station PRAs were not used as an input to the FLEX strategy development process. The insights and techniques developed in this study could help improve current PRA models to more accurately quantify safety margin at nuclear power plants.

**I.2.1 Historical Background**

Nuclear reactor safety and some of its current principles originated during the Manhattan Project. Chemical engineers from the Du Pont Corporation brought with them chemical plant safety principles, as they led the effort to build nuclear reactors at the Hanford, WA site. The reactor design began by splitting the system into mostly independent subsystems whose design was frozen early such that additional dependent sub-systems could be incorporated later [9]. "This created the notion of functional independence, and later gave rise to the concept of 'defense-in-depth', which promoted layers of independent 'barriers' realizing safety functions to prevent, protect and/or to mitigate release of radioactive substances into the environment" [9]. The use of defense-in-depth (DID) by the Hanford engineers was necessary due to the large safety margin uncertainty.

One of the biggest milestones in PRA occurred in 1975 when the newly developed NRC published its first probabilistic reactor safety study [7]. This controversial WASH-1400 report was eventually embraced and marked some of the first industry acceptance of PRA methodology. This report also recognized that SBO could be a significant contributor to overall risk at a plant [7].

The use of PRA by the NRC continued to grow and in 1988 the NRC issued Generic Letter 88-20 [10]. The overall purpose of this letter was to discuss with the industry what a PRA is and

how to use it in the future. The letter recognized that each plant is different and may be subject to specific vulnerabilities [10]. This letter from the NRC urged each plant to perform individual plant examinations in order to understand their specific risks better [10]. This year was also when the NRC added 10 CFR 50.63, the Station Blackout (SBO) rule, which required each plant to be able to cope and recover from a SBO for a specified duration of time [6]. The time duration was plant specific, but generally only about 4 to 8 hours was required.

The next major move by the NRC occurred in 1995 with their PRA policy statement [11]. The policy statement directed that "the use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data, and in a manner that complements the U.S. Nuclear Regulatory Commission's (NRC's) deterministic approach and supports the NRC's traditional defense-in-depth philosophy" [11]. This policy statement eventually led to the current implementation plan by the NRC, the Risk-Informed and Performance-Based Plan [12].

**I.2.2 Fukushima Daiichi**

The 2011 tsunami in Japan placed the Fukushima Daiichi nuclear power plant in an extended SBO condition which eventually led to partial core melt and radioactive release. The sea wall surrounding the plant would have prevented any damage due to a design-base tsunami; however, this natural disaster was most certainly beyond the design basis of the plant. This event has highlighted some weak points in the safety culture of the nuclear industry. One lessoned learned is that even though a plant can be perfectly protected against its Design Basis Accidents (DBAs), there is always the possibility of low probability, high consequence events that are outside the scope of DBAs [1]. The NRC defines a DBA as "a postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety" [13]. It should also be noted that, in the U.S., DBAs for a specific plant must be spelled out in the license agreement, with proper justifications.

**I.2.3 FLEX**

Due to these events at Fukushima Daiichi, on March 12, 2012 the NRC issued a Mitigation Strategies Order urging all U.S. nuclear power plants to begin implementing strategies that will allow them to cope with extended SBOs [14]. This order is a precursor to the Station Blackout

Mitigating Strategies Final Rule, which is due by the end of 2016. This final rule will place requirements on plants such that if a plant loses power, it should have sufficient procedures, strategies, and equipment to enable "mitigation for an indefinite time period" [14].

One response to this order has been industry collaboration through NEI to develop the "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide". This guidance document outlines a plan to increase DID for Beyond Design Basis Accidents (BDBAs), specifically a simultaneous Extended Loss of AC Power (ELAP) and Loss of Ultimate Heat Sink (LUHS) [1].

FLEX is planned to provide additional equipment for emergency power and cooling situations. The equipment will be portable so that it can be stored in a secure location and then moved into position as needed. Some of the equipment will be stored onsite, but provisions will be made for offsite equipment to be transported to the plant for longer-term scenarios [1].

The FLEX plan is meant to increase DID an unknown amount by extending and improving the SBO coping capability of the plant, as illustrated in Figure 1. It is important to note that current plant PRA model input (which could help better identify the plant vulnerabilities) was not a part of the FLEX plan development. The FLEX plan does not affect plant emergency plans or Severe Accident Management Guidelines (SAMGs).

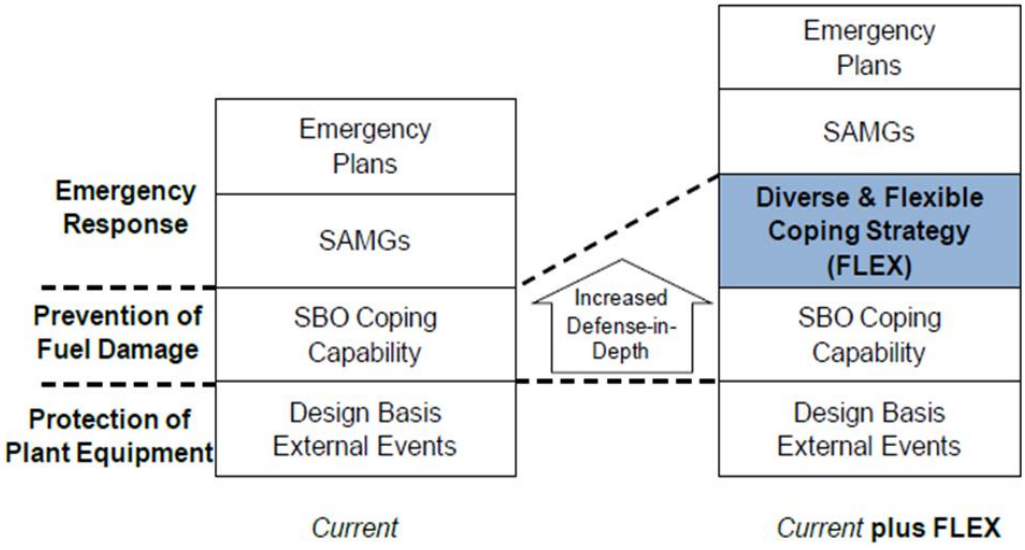


**Figure 1 – FLEX Increases Defense-in-Depth (reprinted with permission from [1]).**

The FLEX guide provides prescriptive coping strategies, but makes no attempt at quantifying their potential risk reduction [1]. However, the NEI is aware that there is a need to quantify the increased safety margin due to FLEX, and there are new efforts to begin looking at FLEX from a probabilistic viewpoint. There is no literature on probabilistic analysis of the FLEX plan that is publicly available at this time. However, contact was made with Mr. Michael Powell, a nuclear industry professional who is very knowledge of the FLEX program. He is the Director of Fukushima Daiichi Initiatives for the Palo Verde Nuclear Generating Station and is responsible for implementation of all the Fukushima Daiichi issues including the FLEX program. He is also a member of the NEI/Industry Core FLEX Team and assisted in the development of NEI 12-06 [1]. Mr. Powell provided the following insight into the status of probabilistic analysis of the FLEX plan [15]:

"The US Utilities are currently focused on implementing the Mitigating Strategies NRC Order and the development of PRA techniques for crediting the use of the FLEX equipment is lagging behind implementation. The Pressurized Water Reactor Owners Group (PWROG) issued a report in March 2015, PWROG-14003 –P (Revision 1), 'Implementation of FLEX Equipment in Plant-Specific PRA Models' which identifies issues with crediting FLEX equipment in a PRA. This guide provides some approaches for resolving issues but not all issues are addressed."

Mr. Powell then went on to list some of the major PRA data and modeling considerations that need to be addressed, as suggested by the above mentioned PWROG report (which is currently proprietary information). It is appropriate to note here that these issues are not stopping plants from crediting FLEX equipment in their PRA; however, these are some important issues to address to obtain more realistic (and less conservative) credit for FLEX. They are listed here as follows:

- Time window for installing the FLEX equipment and getting the equipment operational
- Application specific failure-to-start, failure-to-run
- Booster pump (if needed) – Application specific failure-to-start, failure-to-run

- Suction and Discharge Piping – Application specific failure to deliver flow due to clogging of lines or filters/strainers, air leaks, FLEX piping damage, rupture or excessive leakage
- System unavailability time for refueling of FLEX pumps, cleaning clogs in piping, or cleaning filters/ strainers. These items need to be considered on a site-specific basis due to differences in installed piping, use and redundancy of filters/ strainers, and the source of the alternate water supply.

This thesis makes no attempt at addressing any of the above issues, but recognizes their importance for practical PRA applications. Instead this thesis is focused on a simplified SBO problem and only models the behavior of the power-producing components (the EDGs and FLEX DG). While a detailed PRA analysis for FLEX may become necessary, this thesis aims to use the simplified problem model to gain a possible first-look insight into the effects of an additional FLEX DG. The main phenomenon under consideration is common-cause failure (CCF). The FLEX DG will be housed separately from the EDGs and will have its own separate electrical connections and support systems, thus lowering the frequency of a CCF that fails all onsite power sources. The FLEX DG will also be called into action only after the failure of the standard onsite EDGs, thus the FLEX DG can be modeled as a cold standby component (the difference between hot and cold standby redundancy is discussed in Section II.5). The culminating analysis will be for a backup power system composed of two EDGs and one FLEX DG. The 3-out-of-3 CCF parameter (for the three diesels) will be adjusted to assess how it affects the probability of system failure.

**I.2.4 Probabilistic Risk Assessment (PRA) Challenges**

In addition to motivating the deterministic FLEX strategy, the Fukushima Daiichi accident prompted the industry to examine weak points in current PRA technology. The probability model of this thesis attempts to quantify the benefits of an additional FLEX DG, while trying to advance a few PRA practices. This section briefly highlights some of these current PRA issues and points to how the proposed thesis model could offer enhancement.

The accident at Fukushima Daiichi did more than just highlight the need for additional barriers and mitigation strategies against BDBAs. It also called attention to technical issues with certain PRA methods. The 2013 NRC report [8] says that while the disaster was due to an

extremely rare initiating event, we should not limit “our [Probabilistic Safety Assessment] PSA technology improvement efforts on the assessment of the likelihood of severe natural hazards”, or we might “miss other useful lessons that could lead to improvements in how we assess the risk of future accidents, which, should they occur, may or may not look like the events following the Tōhoku earthquake” [8]. The purpose of the NRC report [8] is to document results from an on-going review of the Fukushima Daiichi accident with a focus on improving PRA technology. The report lists many “potential PSA technology challenges and reminders”, and a few of these are addressed by this thesis.

One of the challenges recognized by the report was to reconsider ‘Game Over’ modeling and intentional conservatism. The term ‘Game Over’ refers to, “modeling [which] relies on conservative simplifying assumptions to terminate PSA accident scenarios early” [8]. The report goes on to give the following example: “typical PSA treatments of scenarios involving complete loss of power lead to predictions of core melt much quicker than the times reported for Fukushima Daiichi Units 2 and 3”. Such treatments, “miss the opportunity to identify and assess potentially effective accident management improvements” [8]. The premise of this example is that well-meaning conservatism in certain PRA areas can potentially skew results so “that truly risk-significant scenarios may be masked” [8]. Another challenging topic recognized by the above mentioned NRC report was treating long duration scenarios. By modeling accident progressions more realistically, simplifying assumptions might be removed thus leading to a long duration scenario. The NRI methodology, as extended in this thesis, can also explicitly credit the possibility of offsite power recovery (given a distribution of the offsite power recovery time), and this allows long duration scenarios to be easily analyzed.

The thesis model (NRI) was conceived with intentions to model, more robustly than traditional PRA means, the failure probability of an EDG system after a LOOP event by accounting for the dynamic timing of successive EDG failures (while differentiating between hot and cold standby EDGs), accepting time-dependent EDG failure rate inputs, and considering both component-caused and externally-caused CCFs (as well as their implications to conditional hazard functions). Throughout the thesis research it became apparent that not all of these model features could be captured accurately with confidence by using the joint failure time distribution developed by Shaked and Shanthikumar. However, this research has provided

greater insight into assumptions, features, and limitations of both the NRI model of this thesis and current nuclear PRA practices; this is discussed in conjunction with a problem overview in the following Section I.3. The possibility of creating a model based on a semi-Markov process (with more feature capabilities) is discussed as future work in Chapter V.

### I.3 Problem Overview

The purpose of this thesis is to develop a temporal probability model for an emergency power system composed of multiple, redundant EDGs. The goal of this model is to calculate the probability that the EDG system fails and offsite power is not restored by some time of interest. The NRI model can account for these redundant EDGs to be operated either in cold or hot standby; Sections II.2 and II.3 develop the NRI for hot standby systems and Section II.5.1 shows how to modify the NRI model to account for cold standby arrangements. The main goal of the case studies presented in Chapter IV is to examine how different numbers of EDGs, and how they are operated, affect the system failure probability.

#### I.3.1 Cold and Hot Standby Redundancy

A cold standby system is defined in [16] (p. 24) as follows: “In the cold standby redundancy arrangement, the redundant components are sequentially used in the system at component failure times. Each redundant component in the cold standby arrangement can operate only when it is switched on. When the component in operation fails, one of the redundant ones [a cold spare] is switched on to continue the operation.” This standby mode is contrasted in [16] with the hot standby mode which is characterized by all the redundant components becoming active at the beginning of the system lifetime. Each of these arrangements has their own advantages. A cold standby system “improves system life more effectively” [16], since the spare components are not receiving unnecessary wear. A hot standby system however has the advantage of decreased downtime due to switching between the failed component and the next hot spare that is put into operation. The appropriate mode of redundancy for a system is based on the specific details of operation. Hot and cold standby as defined above are on opposite ends of the spectrum for all possible redundancy types.

#### I.3.2 EDG System Operation

All U.S. nuclear power plants are required to have redundant onsite emergency AC power sources in case the offsite power source is lost [17]. These onsite redundant power sources

come in the form of EDG trains, which include a diesel engine, generator, cooling system, breaker, and everything else necessary to turn diesel fuel into plant useable AC power. The EDG trains are simply referred to as EDGs for the remainder of this thesis; a more detailed description of the components included in a train can be found in Section III.1. Generally, each EDG is a completely redundant form of onsite AC power. Thus a single EDG can carry the entire plant load for the essential shutdown, safety, and decay heat removal systems; each plant is required to have at least one level of redundancy, one EDG can fail and the emergency power system can still operate. At South Texas Project (STP) Nuclear Operating Company, the standby AC power system is composed of three separate and independent EDG trains, "supplying power to three associated load groups designated Train A, Train B, and Train C" [18]. While each train is independent it "is not totally redundant; two trains are necessary to mitigate the consequences of a design basis accident (DBA)" [18]. These standby EDGs are housed in permanent locations and when a loss of offsite power (LOOP) event occurs the necessary plant load can be quickly picked up by them. When a LOOP event occurs at STP, all three EDGs are started and loaded with some amount of the 4.16KV AC Class 1E Power System load [18]. While STP operates in this manner, many other U.S. nuclear power plants have either two or three EDGs and only require a single EDG to carry the entire plant load; as such, the EDG system models presented in this thesis have either a 1-out-of-2 or a 1-out-of-3 success criterion. It is also believed that most U.S. nuclear plants operate their onsite emergency power system in a hot standby arrangement. The new FLEX program intends to equip plants with a separately housed EDG which is called into action once it is needed; these FLEX DGs are treated as both hot and cold standby components in Sections IV.5.1 and IV.5.2, respectively. This thesis does not claim to actually know or understand the standby operation of either the standard onsite or FLEX DGs; it does however provide models that can account for either of the two extremes, hot or cold standby.

### I.3.3 Current PRA Modeling Practices

#### I.3.3.1 Safety Margin and the RISMC Approach

The concept of safety margins emerged early on in the development of commercial nuclear power "as a part of the defense-in-depth approach to ensuring nuclear safety" [4]. Safety margin is defined as the minimum distance between the 'loading' and 'capacity' of the system.

“Due to limited knowledge, large (i.e., conservatively specified) safety margins are applied to compensate for approximations used in (the phenomenological or deterministic) models and associated computer codes which estimate the “loads” and the “capacity” in the reactor systems that occur during the complex accident sequences that are analyzed” [4].

The United States Department of Energy (DOE), the Idaho National Laboratory (INL) and the Electric Power Research Institute (EPRI) have collaborated to create “a Risk-Informed Safety Margin Characterization (RISMC) approach to evaluate and manage changes in plant safety margins over long time horizons” [4]. In the past framework, “the concept of safety margin is limited to characterizing the ‘load’ as a known quantity with the margin given by the distance from this load to the defined safety limit” [4]. “In this concept, uncertainties only are addressed implicitly, i.e., the assessment of the ‘load’ is conducted using conservative assumptions and analysis methods” [4]. However, as Figure 2 illustrates, load and capacity are not discrete values but instead have distributions. Treating the load and capacity as discrete values has several issues. “First, the current generation of physics-based models are capable of only providing approximate results of the real ‘load’ representing the actual plant condition. Second, the application of conservatisms (in assumptions and modeling) can lead to non-conservative predictions of the load. In the current approach, the use of a safety limit as a surrogate for the ‘capacity’ serves as an additional conservatism; however, because the degree to which the safety limit is conservative is unknown, this approach prescribes significant operational limitations on the plant. The intent of a risk-informed approach to characterization of safety margins is to integrate the information from both deterministic and probabilistic safety analyses to obtain a complete picture” [4].

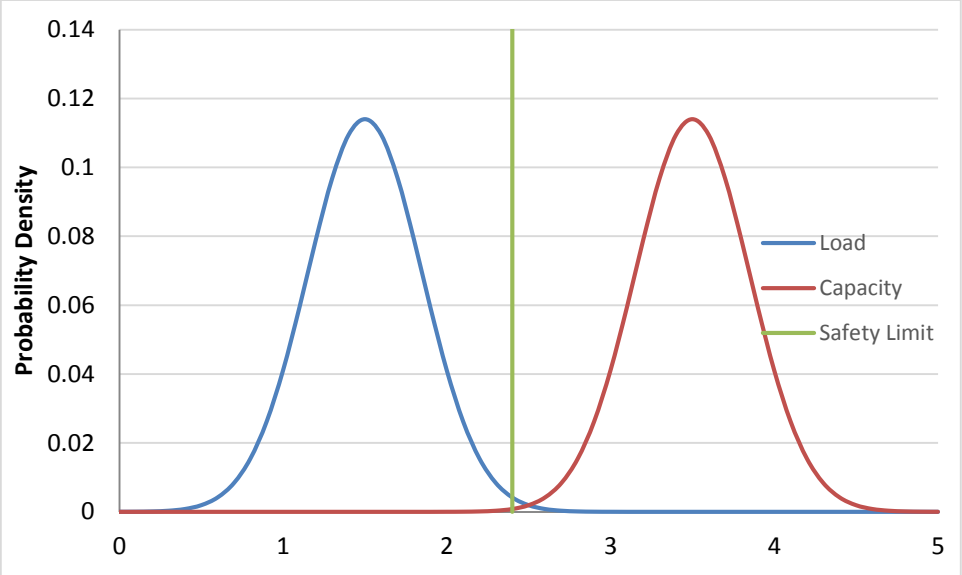


**Figure 2 – Schematic of Safety Margin.**

In this abstract formulation the natures of "capacity" and "load" have been consciously left unspecified, and indeed quite different instances are both possible, and appropriate to different circumstances. For an example from [19], consider an initiating event (for a BWR) to be LOOP plus station blackout, (effectively) employ clad failure temperature as capacity, with randomness introduced by a triangular distribution having mode at the 2200 °F regulatory limit, and fuel temperature calculated from RELAP-5 as load, with random variation induced by treating certain input parameters as stochastic, with assumed known distributions. See also [20] and [21] for additional examples of load and capacity.

**I.3.3.2 SPAR**

In the past, Standardized Plant Analysis Risk (SPAR) models and industry both relied on static fault tree models, which resulted in over-conservative total system failure probabilities due to incorrect timing dependencies. More recently, some industry models began trying to address these simplifications from excessive assumptions through improved modeling techniques. Currently, the accepted industry approach to account for the timing issues (due to consecutive individual EDG failures) is through the use of a convoluted distribution method

[22]. The convoluted distribution technique used in SPAR for LOOP/SBO modeling is for a system of EDGs in hot standby and can only accept constant failure rate inputs [22]. This convoluted distribution method and how it relates to the NRI are explored further in Section II.2.4.

### I.3.4 Thesis Model Features, Limitations, and Insights

Chapter II presents two different ways to model the probability of EDG failure sequences; the primary way is the above-mentioned NRI and a standard Markov state transition model was used to verify the NRI results. The main model (NRI) of this thesis can account for dynamic timing of the EDG failures. The NRI is best suited for hot standby system cases, and can accept time-dependent hazard function inputs for hot standby cases (when the hazard functions meet certain conditions, as described in Section V.3.1). The NRI can be modified for cold standby cases when constant hazard rate inputs are used, and this is verified against a Markov and Convoluted Distribution model in Section II.5. The NRI in this thesis does not account for the possibility of a repair following an EDG failure; while this limitation may add unnecessary over-conservatism to the results in Chapter IV, it does not affect the ultimate application for the model of comparing the improved reliability due to an additional FLEX DG. Previously developed NRI models from [2] and [3] do credit the possibility of EDG repair, but only after all the EDGs have failed.

A well-known Markov state transition model was used to verify the correctness of the NRI. This model can only accept constant failure rates. The Markov model could also easily handle the possibility of constant rate EDG repair, however repair was neglected for all the developed models and case studies in this thesis. The Markov model can be written for either hot or cold standby cases; the Markov models are first developed for hot standby in Section II.4, while Section II.5.2 shows how to set up a Markov model for a simple two-EDG system in cold standby.

Throughout the research required to complete this thesis, it became apparent that a semi-Markov model may be a more appropriate way to capture some of the important processes associated with the LOOP/SBO problem. Chapter V will discuss possible future work by presenting the emergency power system problem in terms of a semi-Markov process. A semi-Markov model can also easily accept time-dependent failure and repair rates, but this limits its

applicability to cold standby systems (as explained in Section V.2). A simple system case is developed in Chapter V and used to compare results between the NRI model and semi-Markov model. This case will use a Weibull hazard function with a shape parameter greater than 1 because this conveniently represents an increasing failure rate.

**I.4 Thesis Outline**

The outline of the thesis is as follows:

Chapter II is devoted to development of the theory and general models necessary to meet the overall thesis objective; specifically, the development of the NRI models for both the two- and three-EDG system cases. In addition to this, an analytical solution to Markov models for the same two- and three-EDG system cases will be developed there.

Chapter III is focused on the specific data used in the case studies of Chapter IV. This will consist of explaining where the model data come from, why these data sources were chosen, and what assumptions have been made for the data. In addition to this some nuclear PRA concepts such as basic failure event types, different types of CCF, and how the alpha factor model works will be discussed there.

In Chapter IV, specific models will be applied within the general two- and three-EDG system models that were developed in Chapter II. Here, the specific model inputs and assumptions for these cases will be discussed in detail. The first few NRI models will be compared against identical Markov model cases in order to verify the results and coding of the NRI models. The culminating case for this chapter is a system of 2 identical EDGs and one non-identical FLEX DG. This case will be used to show how the safety margin of the system changes with respect to the reliability of the FLEX DG.

Potential future work related to this thesis is discussed in Chapter V, with an emphasis on possible advantages of modeling the SBO problem with a semi-Markov process. A simple problem for a two-EDG system with time-dependent failure rates is presented here and then modeled using both a semi-Markov and NRI models.

Finally, a summary and conclusions will be provided in Chapter VI.

# CHAPTER II

# THEORY

In this chapter, underlying theory and the NRI model development is presented. The overall thesis objective of quantifying the failure probability for various EDGs system arrangements is accomplished in Chapter IV using specific data introduced in Chapter III and the general models developed in this chapter. The NRI model can be generalized as calculating the probability that some load overcomes the capacity of the system, as a way to quantify the safety margin of the system. The integrand for this model is formed by multiplying a PDF for time of onsite power system failure by a complementary cumulative distribution function (CCDF) for time of offsite power recovery; the load and capacity of the model are described with this CCDF and PDF, respectively. Section II.1 will expand on the idea of load versus capacity and introduce the offsite power recovery term. Section II.2 will focus on development of the PDF for time of onsite power system failure (for a system of two EDGs). Section II.3 will extend the system failure PDF to a case with three redundant EDGs. Section II.4 will build a connection between the developed system failure model and a Markov model of the same system, as a means of verification. Finally, Section II.5 will show how to modify the EDG system failure time PDF in the NRI so that it can also model cold standby systems; the models developed in Sections II.2, II.3, and II.4 are all for hot standby systems.

The NRIs developed in this thesis makes novel use of the joint distribution functions from [23], [24], and [6]. The joint PDF models stochastic ordering of the individual EDG failure times and thus accounts for dependence among these random variables; this is more general than the commonly used PRA assumption that the individual failure times are statistically independent. The inputs (and in fact building blocks) of this joint PDF are conditional hazard functions. These hazard functions, $\lambda(t)'s$, are instantaneous failure rates about $t+dt$ as $dt$ tends to zero (a generic hazard function is described more fully in Equations (I-1)-(I-2)). Use of hazard functions in the joint PDF is important because they allow component failure propensities to change all the way up to the time of failure. If constant failure rates are used in this joint PDF, the hazard functions will be constant with respect to time, however the values of

the hazard functions are still conditional on which specific components are still operating in the system. For example, in a two-EDG system, the hazard function for an individual failure event of a specific EDG depends on whether the other EDG in the system is still operating.

The joint distribution function from Shaked and Shanthikumar [6] is written such that once one of the components fails it cannot be repaired and returned to operation. This detail introduces unnecessary over-conservatism in the NRIs in this thesis. Current industry PRA LOOP/SBO models already credit the possibility of a failed EDG being repaired before CSBO is reached, which makes the NRI seem inferior in this regard. However, accounting for EDG repair is not an objective of this thesis; instead, the main focus of the overall objective is on developing a more accurate EDG failure time distribution. The application for this thesis model (NRI) is to quantify improved safety margin from adding a FLEX DG and this quantification can be captured without dealing with EDG repair; looking at the relative risk between a system of two EDGs and a similar system with an additional FLEX DG can provide useful insight into system behavior without accounting for EDG repair. It may be possible to modify the NRI formulation or add a correction factor to account for EDG repair, but this work has not yet begun.

The two- and three-EDG system NRI models developed in this chapter are written showing time dependence of the hazard function inputs. The actual case studies performed and presented in the Chapter IV however all use constant failure rates for three reasons; time-dependent EDG failure data are not currently available from the NRC, the Markov model used to verify the NRI has been restricted to constant failure rates (in order to simplify its solution), and use of time-dependent rates limits the applicability of the NRI to hot standby systems.

**II.1 Load and Capacity**

It is worth acknowledging that the viewpoint developed in this section, especially the notion of time to cessation of process demand as “load” and time to failure of safety system to be able to meet that demand as “capacity,” owes much to the notions developed within the Risk-Informed Safety Margin Characterization (RISMC) pathway of the U.S. DOE Light-water Reactor Sustainability program [4], [5].

Much of the following terminology is adapted from Chapter 10 of [25]. Suppose a hazardous system imposes a process demand (i.e., an initiating event occurs) at time $t = 0$, and

that this demand is characterized by a *load* comprising a random time $T_L$ at which this demand ends. Further take the load as distributed according to the cumulative distribution function (CDF) $F_L$, so that

$$\Pr\{T_L \le t_L\} = F_L(t_L). \tag{II-1}$$

It is supposed that $T_L$ is positive with probability 1, so that

$$F_L(0) = F_L(0+) = \lim_{t \to 0+} F_L(t) = 0. \tag{II-2}$$

(And of course $F_L(t_L) = 0$ for $t_L < 0$.)

The system under consideration is designed so that this load is intended to be met by a primary system that is characterized by its *capacity*, defined as the random time $T_C$ after which the primary safety system no longer is capable of meeting the process demand. Let this capacity be distributed as the CDF $F_C$. It is assumed that load and capacity are statistically independent, so that their joint distribution factors as

$$F(t_L, t_C) := \Pr\{T_L \le t_L \text{ and } T_C \le t_C\} = F_L(t_L) F_C(t_C). \tag{II-3}$$

In general terms, the safety system has the capacity to meet the load imposed on it if, and only if, $T_L \le T_C + T_{\text{crit}}$, where $T_{\text{crit}}$ is some deterministically specified time. In terms of the EDG problem, $T_{crit}$ is taken as the (deterministic) amount of time it takes for the primary coolant to boil down to a level lower than the top of the active fuel, with due consideration for the effectiveness of the various coping measures (such as batteries) installed to deal with situations in which the load exceeds the capacity of the primary safety system. The criterion for success, which is to say the safety system having the capacity to successfully meet the load imposed upon it, is therefore $T_L \le T_C + T_{crit}$. The probability of such success is

$$\Pr\{T_L \le T_C + T_{crit}\} = \int_{0-}^{\infty} \int_{0}^{t_C + T_{crit}} dF_L(t_L) dF_C(t_C) = \int_{0-}^{\infty} F_L(t_C + T_{crit}) dF_C(t_C). \tag{II-4}$$

The quantity in Equation (II-5) is termed as the temporal margin of safety. A slightly more convenient measure to work with is the probability that the safety system will fail, in the sense that the load imposed upon it exceeds its capacity. The probability of such failure is

$$\Pr\{T_L > T_C + T_{crit}\} = 1 - \int_0^\infty F_L(t_C + T_{crit}) dF_C(t_C) = \int_0^\infty \bar{F}_L(t_C + T_{crit}) dF_C(t_C), \quad \text{(II-6)}$$

where $\bar{F}$ is the generic notation for 1-*G*, the CCDF associated to the CDF *G*.

The "NRI" on the right-hand side of Equation (II-6) can be evaluated as

$$\text{Probability of Failure} = P_f = \int_{0-}^\infty \bar{F}_L(t_C + T_{crit}) f_C(t_C) dt_C, \quad \text{(II-7)}$$

where $f_C$ is the PDF for the capacity.

**II.1.1 Models of Load**

Any application of Equation (II-7), for the temporal probability of failure, requires some quantitative model of the statistical distribution of the load and capacity associated to the problem under consideration. Sections II.2 and II.3 will develop PDFs for capacity, specifically the failure times for an EDG system. Both the mission-time model of load and a more realistic model of load are presented in this section. These load models are employed in the case studies performed using NRIs (Chapter IV).

A particularly simple and widely used model of load is based on the concept of "mission time". Under such a model the safety subsystem is deemed to perform successfully if it operates for a time $T_C \geq T_M$, where $T_M$ is some designated "mission time." This corresponds to a load that has value $T_M$ with (almost) certainty, and hence CDF

$$F_L(t_L) = \begin{cases} 0, t_L < T_M, \\ 1, t_L \geq T_M \end{cases}. \quad \text{(II-8)}$$

The value $T_M = 24$ hours often is used in probabilistic risk analysis, and indeed is endorsed by the ASME standard for PRA [26].

For a mission-time load, Equation (II-7) for the temporal probability of failure simplifies as

$$\text{Probability of Failure} = P_f = \int_{0-}^{T_M - T_{crit}} f_C(t_C) dt_C = F_C(T_M - T_{crit}). \quad \text{(II-9)}$$

A somewhat more realistic model of the distribution of times of recovery of offsite power, following a LOOP event, is the lognormal distribution with mean of the natural logarithm of the recovery time = $\mu = 0.3$ and standard deviation of that quantity = σ = 1.064. This distribution

corresponds to grid-related LOOP events, which were found to occasion slightly over half of all LOOP events occurring in the US from 1986 to 2004; cf. p. v and Table 4.1, pp. 27-28, of Vol. 1 of NUREG/CR-6890 [27]. Data used to fit this distribution are for a LOOP duration of up to 24 hours and therefore is not necessarily valid for longer duration events. LOOP durations do not generally last longer than 24 hours. In fact, the longest LOOP duration category in NUREG/CR-6890 [27] was from "Severe and Extreme" events, and these durations had a mean time of only 14.2 hours. While most actual LOOP duration do not exceed 24 hours, it is the rare long duration LOOP events that have the highest potential for core damage.

While the NRI could easily handle accounting for this lognormal distribution of recovery times, the Markov models used to verify the NRI could not; in order to simplify the development of the Markov models, rate parameters were restricted to constant values only. As such, to account for recovery of offsite power for the "recovery" cases in Chapter IV (Sections IV.2 and IV.4), following a LOOP event, an exponential distribution with a constant recovery rate of $0.04\ \text{hour}^{-1}$.

The realistic (lognormal) model of load is compared in Figure 3 against two exponential distribution models and the mission-time model (with the canonical 24-hour mission time). Use of the mission-time model often is justified on the basis of conservatism. Indeed Figure 3 shows that while the mission-time load takes no credit for recovery of offsite power during the first 24 hours, the realistic load suggests that in fact recovery occurs with 95% probability within about the first 7.5 hours, and has occurred with graphical certainty by 24 hours. Figure 3 also compares these to the exponential CDF with a constant recovery rate of $0.04\ \text{hour}^{-1}$. This constant recovery rate is over-conservative in estimating the probability of CSBO, compared to the more realistic lognormal model of load. Developing the NRI so that it reduces over-conservatism compared to current PRA practices is part of the objective in this thesis; however, using this exponential load distribution for the recovery cases in Chapter IV is completely justifiable. The main purpose of these recovery cases (Sections IV.2 and IV.4) is to see how the system failure probability changes when an EDG is added to the system. A more realistic lognormal distribution of load could be used in future NRI developments, if less conservative results are desired.

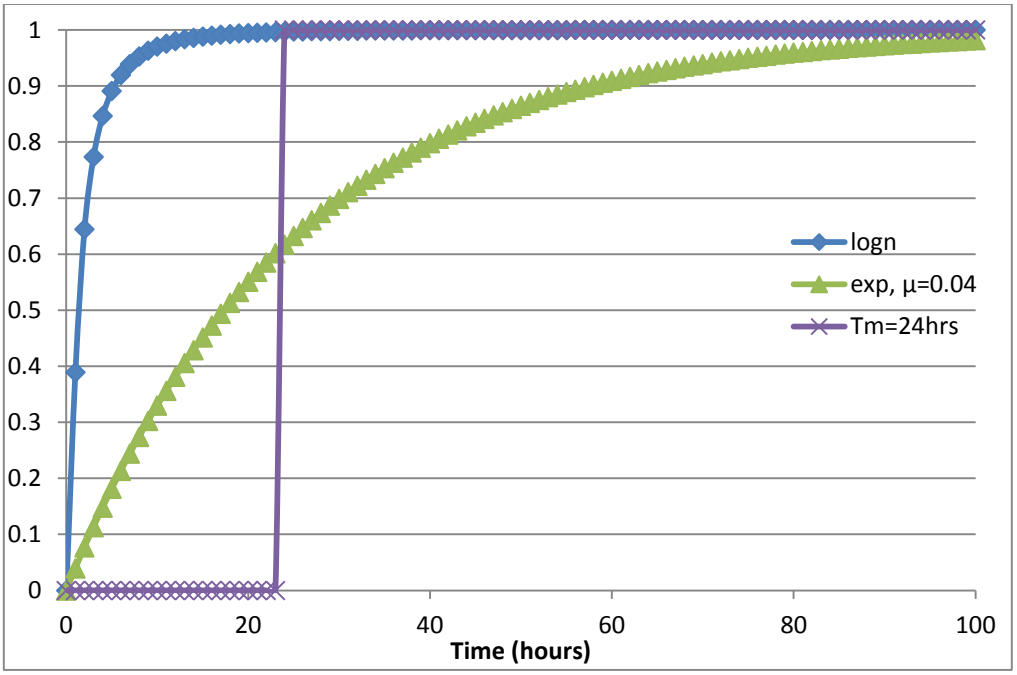


**Figure 3 – Cumulative Distribution Functions for the Deterministic Mission-Time Load (purple) and the Realistic Load (blue).**

For example consider the highly hypothetical case of an emergency power system that is very narrowly tailored to the 24-hour mission time, so that it would always fail at precisely 25 hours. This corresponds to a capacity distribution (where $\delta$ is the Dirac delta function),

$$f_C(t) = \delta(t - 25). \tag{II-10}$$

For $T_{crit} = 0$ and any load distribution, (II-7) then gives

$$P_f = \overline{F_L}(25). \tag{II-11}$$

For the 24-hour mission-time load this would give $P_f = 0,$ so that the emergency power system would perform perfectly, as evaluated by the 24-hour mission-time load, presumably as designed. But the more realistic load would lead to

$$P_f = 1 - F_T(25;.3,1.064) \text{»} .00304, \tag{II-12}$$

which could well be deemed an unacceptably high degree of risk (per initiating event).

Of course one would (and could) never in practice employ such a knife-edge emergency power system. Nonetheless, this simple example does illustrate the potential for conclusions drawn from mission-time models of load to depend sensitively upon the precise choice of mission time.

**II.2 System Failure Model (Two EDGs)**

Consider a safety system composed of two hot standby redundant EDGs, indexed as $i$ = 1, 2, with respective random individual failure times $T_1, T_2$; the EDGs operate in parallel (are redundant) so the system fails when both EDGs are failed. In the current Section II.2, a probability model for the failure time of the EDG system is developed; however, the model can easily be generalized to other types of systems composed of multiple redundant components. The specific model developed here accepts data similar to that of a standard SPAR model for EDG failure. (This is further discussed in Chapter III.) Following the same basic failure event model as prescribed by the NRC, each EDG is subject to demand failures at t=0 (given data are probabilities) or continuous-time failures for t>0 (given data are used as rates); these are termed individual failures because each event affects a single EDG. Thus the random variables for the EDG failure times are both discrete (t=0) and continuous (t>0). The EDGs are also subject to common root-cause failure events (with random failure time $T_{12}$), and probability or rate parameters are used to describe the frequency of single events that fail both EDGs at the same time (here termed a coincident failure). Again, system failure occurs when all (both) EDGs have failed; the corresponding basic event sequences that result in system failure are the following:

1. The first failure occurs while running, then the second failure occurs while running (2 individual, continuous failures)
2. A single coincident failure while running event occurs, thus both EDGs fail simultaneously
3. The first failure occurs at start (on demand), and then the second failure occurs while running
4. The EDGs experience a coincident failure at start (on demand)

Two individual failure to start events is not considered a possibility, thus the above list comprises an exhaustive list of system failure sequences.

The main input parameters and building blocks of the probability model are hazard functions, which are essentially instantaneous rates for their respective failure events and conditions. Although well-known outside this thesis, the concept of a hazard function is defined here since it is used often for the remainder of this chapter. The following definitions are from basic survival analysis probability theory (page 9 and 10 of [24]).

The hazard function is an instantaneous failure rate as $\Delta t$ tends to zero, as defined:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{\Pr\{t \le T < t + \Delta t\}}{\Delta t \cdot \Pr\{T > t\}}. \tag{II-13}$$

This continuous failure rate is related to, $F(t)$, the CDF that describes the probability of the random failure time ( $T$ ) in the interval $0 < T \le t$ ,

$$\Pr\{T \le t\} = F(t), \quad t \ge 0. \tag{II-14}$$

This CDF is the integral of the failure PDF, $f(t)$,

$$F(t) = \int_0^t f(\tau) d\tau, \tag{II-15}$$

and (if $f$ is continuous at $t$ ),

$$f(t) = \frac{d}{dt} F(t). \tag{II-16}$$

In a physical sense, $f(t)dt$ is the probability of $T$ falling within the infinitesimal interval $[t, t+dt]$.

The hazard function can now be defined in terms of the complementary CDF (also called survival function, $S(t)$ ) and PDF as

$$\lambda(t) = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{S(t)}. \tag{II-17}$$

The PDF can now be defined as

$$f(t) = \lambda(t) S(t) = \left\{ \lim_{\Delta t \to 0} \frac{\Pr\{t \le T < t + \Delta t\}}{\Delta t \cdot \Pr\{T > t\}} \right\} \Pr\{T > t\} = \frac{\Pr\{t \le T < t + dt\}}{dt}, \tag{II-18}$$

where $dt$ is an infinitely small number.

The hazard functions used for the system failure models developed in this thesis are conditional on which specific components are still operating versus which ones have failed. These hazard functions and their conditions will be explicitly defined in the following subsections.

In Section II.2.1 the probability model is developed for system failure resulting from subsequent, individual, running failures of each EDG. In Section II.2.2, the probability model for the coincident failure sequence is developed. Finally in Section II.2.3, basic event sequences involving demand failures are addressed. Also, the previously developed models for their respective mutually exclusive system failure sequences are combined to create the complete PDF and CDF for all the random failure times of the EDG system (the system failure time CDF is equivalent to the NRI with a mission-time model of load). The results of Section II.2.1 are taken directly from the multivariate joint distribution function developed by Shaked and Shanthikumar [6]; the results of Sections II.2.2 and II.2.3 are extensions of the results of [6] to accommodate respectively CCFs and failures on demand.

**II.2.1 Continuous Individual Failures**

The model development begins with a simple case of a system composed of two redundant components. Each component is subject to continuous individual failures described by designed and influenced hazard functions as in Equations (II-19) and (II-20), respectively. Here, the subscript numbers 1 and 2 refers to the different components. As first developed in [23], the joint distribution is described in terms of the hazard functions $\lambda_1(\tau)$, $\lambda_2(\tau)$, $\lambda_1(t)$, and $\lambda_2(t)$. These building blocks of the model are described in the following paragraphs. For the two EDG model, $\tau$ is some failure time for an event where one EDG survives, while $t$ is some failure time for an event where no EDGs survive (system failure).

The *designed hazard functions* for the two EDGs are given by Equation (II-19). This function describes the frequency of individual failure events for a specific EDG given neither EDG has failed.

$$\lambda_i(\tau) = \lambda_i(\tau \,|\, T_1, T_2 \geq \tau) = \lim_{\Delta\tau \to 0} \frac{\Pr\{\tau \leq T_i < \tau + \Delta\tau \,|\, T_1, T_2 \geq \tau\}}{\Delta\tau}, i = 1,2 \qquad \text{(II-19)}$$

The *influenced hazard functions* for the two EDGs are given by Equation (II-20). This function describes the frequency of individual failure events for a specific EDG given the other EDG has failed. Note that the absence of coincident failures in this section does not necessarily mean the two failure times are statistically independent. To the contrary, the following definition explicitly contemplates that failure of one of the two subsystems can influence the rate at which the other fails - just not (yet) to the extent that failure of the other occurs immediately. The concept makes more sense in the context of component-caused versus externally-caused CCF, which is explained more in Section III.3.3. The important point here is that the failure of the first EDG influences the hazard function formulation for the second EDG failure which then determines the joint pdf in [28].

$$\lambda_i(t) = \lambda_i(t \,|\, T_{i'} = \tau, T_i \geq t) = \lim_{\Delta t \to 0} \frac{\Pr\{t \leq T_i < t + \Delta t \,|\, T_{i'} = \tau, T_i \geq t\}}{\Delta t},\ i = 1,2,\ 1' = 2,\ \text{and}\ 2' = 1 \qquad \text{(II-20)}$$

The above hazard functions completely specify the joint distribution of $T_1$ and $T_2$, as follows. The bivariate PDF $f(\tau, t)$ is given by Equation (40) of [23], as in Equation (II-21),

$$f(\tau, t) = \lambda_1(\tau)\tilde{\lambda}_2(t)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u) + \lambda_2(u)\right)du - \int_{\tau}^{t}\tilde{\lambda}_2(u)du\right\}, \qquad \text{(II-21)}$$

for $T_2 \geq T_1$, with an analogous expression for $T_1 \geq T_2$. This PDF is expressed in terms of probability in Equation (II-22).

$$f(\tau, t) = \frac{\Pr\{\tau \leq T_1 < \tau + d\tau \bigcap t \leq T_2 < t + dt \,|\, \tau \leq T_1, t \leq T_2, \tau < t\}}{d\tau dt} \qquad \text{(II-22)}$$

The specific system considered is composed of two EDG trains and is subject to the same three failures modes typically considered in SPAR models [29], [30]. These failure modes are treated slightly differently than standard industry practice; the specific sources and assumptions used to obtain the model parameters are discussed later in Chapter III. At this point in the development, consider only the two following failure modes. From time t=0 to t=1 hour an EDG may experience an individual failure to load (FTL), while after time t=1 hour an EDG may experience an individual failure to run (FTR). Thus the given hazard functions are actually piecewise, as expressed in the following equations, which denote the specific hazard time regime with a superscript on $\lambda$ ; L and R stand for FTL and FTR hazards, respectively. There are now three distinct component failure sequences which lead to system failure,

$$\lambda_i(\tau)=\begin{cases}\lambda_i^L(\tau), & \text{if } \tau<1hr\\ \lambda_i^R(\tau), & \text{if } \tau\geq 1hr\end{cases} \quad \text{and} \quad \lambda_i(t)=\begin{cases}\lambda_i^L(t), & \text{if } t<1hr\\ \lambda_i^R(t), & \text{if } t\geq 1hr\end{cases}. \tag{II-23}$$

Equation (II-24) represents the sequence where the first EDG experiences a FTL and then the second EDG experiences a FTL. This equation is easily obtained from Equation (II-21) by simply specifying that the only hazards experienced are FTL. Equation (II-24) accounts for both cases, $T_2 \geq T_1$ and $T_1 \geq T_2$.

$$\begin{aligned} f(\tau<1,t\leq 1)&=\lambda_1^L(\tau)\tilde{\lambda}_2^L(t)\exp\left\{-\int_0^\tau\left(\lambda_1^L(u)+\lambda_2^L(u)\right)du-\int_\tau^t\tilde{\lambda}_2^L(u)du\right\}\\ &+\lambda_2^L(\tau)\tilde{\lambda}_1^L(t)\exp\left\{-\int_0^\tau\left(\lambda_1^L(u)+\lambda_2^L(u)\right)du-\int_\tau^t\tilde{\lambda}_1^L(u)du\right\}\end{aligned} \tag{II-24}$$

Equation (II-25) represents the sequence where the first EDG experiences a FTL and then the second EDG experiences a FTR. The designed hazard function portion of this is identical to Equation (II-24), while $\lambda's$ the outside the exponential are changed to reflect the hazard experienced at the point of failure ($t$) of the second EDG.

$$\begin{aligned} f(\tau\leq 1,t>1)&=\lambda_1^L(\tau)\tilde{\lambda}_2^R(t)\exp\left\{\begin{array}{l}-\int_0^\tau\left(\lambda_1^L(u)+\lambda_2^L(u)\right)du\\ -\left(\int_\tau^1\tilde{\lambda}_2^L(u)du+\int_1^t\tilde{\lambda}_2^R(u)du\right)\end{array}\right\}\\ &+\lambda_2^L(\tau)\tilde{\lambda}_1^R(t)\exp\left\{\begin{array}{l}-\int_0^\tau\left(\lambda_1^L(u)+\lambda_2^L(u)\right)du\\ -\left(\int_\tau^1\tilde{\lambda}_1^L(u)du+\int_1^t\tilde{\lambda}_1^R(u)du\right)\end{array}\right\}\end{aligned} \tag{II-25}$$

The integral limits on the influenced hazard functions are split to account for the change in hazard from FTL to FTR, as follows:

$$\int_\tau^t\tilde{\lambda}_i(u)du=\int_\tau^1\tilde{\lambda}_i^L(u)du+\int_1^t\tilde{\lambda}_i^R(u)du. \tag{II-26}$$

Equation (II-27) represents the sequence where the first EDG experiences a FTR and then the second EDG experiences a FTR. Here, the integral limits on the summed designed hazard functions are split at t=1 hour to account for the change in hazard from FTL to FTR. The rest of this joint density function is similar to Equation (II-21) except the hazard functions are specified as FTR (with superscript $R$'s).

$$f(\tau>1,t>1)=\lambda_1^R(\tau)\tilde{\lambda}_2^R(t)\exp\left\{\begin{array}{l}-\left(\int_0^1\left(\lambda_1^L(u)+\lambda_2^L(u)\right)du+\int_1^\tau\left(\lambda_1^R(u)+\lambda_2^R(u)\right)du\right)\\-\int_\tau^t\tilde{\lambda}_2^R(u)du\end{array}\right\}$$
$$+\lambda_2^R(\tau)\tilde{\lambda}_1^R(t)\exp\left\{\begin{array}{l}-\left(\int_0^1\left(\lambda_1^L(u)+\lambda_2^L(u)\right)du+\int_1^\tau\left(\lambda_1^R(u)+\lambda_2^R(u)\right)du\right)\\-\int_\tau^t\tilde{\lambda}_1^R(u)du\end{array}\right\} \quad \text{(II-27)}$$

With the three variations to the joint PDF shown above in Equations (II-24)-(II-27), the CDF of failure times for this two-EDG system is shown in Equation (II-28).

$$F(T_1,T_2)=\Pr\{T_1<T_m\le T_2\}+\Pr\{T_2<T_m\le T_1\}=\int_0^{T_2}\int_0^t f(\tau,t)d\tau dt+\int_0^{T_1}\int_0^t f(\tau,t)d\tau dt$$

where

$$\int_0^{T_2}\int_0^t f(\tau,t)d\tau dt=\left\{\int_0^1\int_0^t f(\tau<1,t\le1)d\tau dt+\int_1^{T_2}\left(\int_0^t f(\tau,t>1)d\tau\right)dt\right\}$$
$$=\left\{\int_0^1\int_0^t f(\tau<1,t\le1)d\tau dt+\int_1^{T_2}\left(\int_0^1 f(\tau\le1,t>1)d\tau+\int_1^t f(\tau>1,t>1)d\tau\right)dt\right\} \quad \text{(II-28)}$$
$$=\left\{\int_0^1\int_0^t f(\tau<1,t\le1)d\tau dt+\int_1^{T_2}\int_0^1 f(\tau\le1,t>1)d\tau dt+\int_1^{T_2}\int_1^t f(\tau>1,t>1)d\tau dt\right\}$$

and similarly,

$$\int_0^{T_1}\int_0^t f(\tau,t)d\tau dt=\left\{\int_0^1\int_0^t f(\tau<1,t\le1)d\tau dt+\int_1^{T_1}\int_0^1 f(\tau\le1,t>1)d\tau dt+\int_1^{T_1}\int_1^t f(\tau>1,t>1)d\tau dt\right\}$$

**II.2.2 Continuous Coincident Failures**

In Section II.2.1, the system failure CDF was developed using conditional hazard functions for individual EDG failures (FTL or FTR), and the system failed once two successive individual failures occurred. In this section the notion of coincident failure is introduced (also referred to as CCF). This type of failure occurs when a single root cause leads to the failure of both EDGs at the same time.

For this system failure scenario there is only a single coincident failure time random variable and therefore a joint distribution is not required as in the last Section. Let $F$ be the distribution function of the absolutely continuous random lifetime $T$ (single coincident failure time) and let $S(t)=1-F$ and $f=dF/dt$ be respectively the corresponding survival function

and density function of $T$. The coincident hazard rate function $\lambda_{12}$ of $T$ is defined in Equation (II-29). In Section II.2.1, $t$ was defined as the random variable for the time of second EDG failure, which is also the time of system failure. In this section $t$ is defined as the time of coincident failure, which is again the time of system failure.

$$\lambda_{12}(t) = \lambda_{12}(t \mid T_1, T_2, T_{12} \geq t) = \lim_{\Delta t \to 0} \frac{\Pr\{t \leq T_{12} < t + \Delta t \mid T_1, T_2, T_{12} \geq t\}}{\Delta t} \tag{II-29}$$

The inclusion of coincident failures requires a slight redefinition of the designed and influenced hazard functions for individual failures; this is shown in Equations (II-30) and (II-31) respectively.

$$\lambda_i(\tau) = \lambda_i(\tau \mid T_1, T_2, T_{12} \geq \tau) = \lim_{\Delta \tau \to 0} \frac{\Pr\{\tau \leq T_i < \tau + \Delta\tau \mid T_1, T_2, T_{12} \geq \tau\}}{\Delta \tau},\ i = 1,2 \tag{II-30}$$

$$\begin{aligned} \tilde{\lambda}_i(t) &= \lambda_i(t \mid T_{i'} = \tau,\ T_i, T_{12} \geq t) \\ &= \lim_{\Delta t \to 0} \frac{\Pr\{t \leq T_i < t + \Delta t \mid T_{i'} = \tau,\ T_i, T_{12} \geq t\}}{\Delta t},\ i = 1,2,\ 1' = 2, \text{ and } 2' = 1 \end{aligned} \tag{II-31}$$

As in Section II.2.1, the given hazard functions are piecewise, as expressed in Equation (II-32).

$$\lambda_i(\tau) = \begin{cases} \lambda_i^L(\tau), & \text{if } \tau < 1hr \\ \lambda_i^R(\tau), & \text{if } \tau \geq 1hr \end{cases},\ \lambda_i(t) = \begin{cases} \lambda_i^L(t), & \text{if } t < 1hr \\ \lambda_i^R(t), & \text{if } t \geq 1hr \end{cases}, \text{ and } \lambda_{12}(\tau) = \begin{cases} \lambda_{12}^L(t), & \text{if } t < 1hr \\ \lambda_{12}^R(t), & \text{if } t \geq 1hr \end{cases} \tag{II-32}$$

Starting from a non-failed state after time t=0, the system may experience one of three different hazards; EDG 1 could individually fail, EDG 2 could individually fail, or both EDGs could coincidentally fail. Thus the cumulative hazard function $\Lambda$ from t=0 until the time of the first hazard is given as

$$\Lambda(t) = \int_0^t \lambda_{total}(u)du, \tag{II-33}$$

where $\lambda_{total}(u) = \lambda_1(u) + \lambda_2(u) + \lambda_{12}(u)$. It is well known that $S$ and $\lambda$ determine each other via the relation seen in Equation (II-34).

$$\lambda(t) = \frac{f(t)}{S(t)} \quad \text{and} \quad S(t) = \exp\{-\Lambda(t)\} \tag{II-34}$$

Thus, the PDF for time of coincident failure is seen in Equation (II-35).

$$f(t) = \lambda_{12}(t)\exp\left\{-\int_0^t \left(\lambda_{total}(u)\right)du\right\} \quad \text{(II-35)}$$

The above PDF is for the case when neither EDG fails individually, but instead a coincident failure causes system failure $(T_{12} < T_1, T_2)$. This PDF is expressed in terms of probability in (II-36).

$$f(t) = \frac{\Pr\{t \le T_{12} < t + dt \,|\, t \le T_{12}, T_1, T_2\}}{dt} \quad \text{(II-36)}$$

Likewise, the CDF for time of coincident failure is shown in Equation (II-37).

$$F(T_{12}) = \Pr\left\{T_m \le T_{12}\right\} = \int_{-\infty}^{T_{12}} f(t)dt = \int_0^{T_{12}} f(t)dt$$
$$= \int_0^1 f(t \le 1)dt + \int_1^{T_{12}} f(t > 1)dt$$
where (II-37)
$$f(t \le 1) = \lambda_{12}^L(t)\exp\left\{-\int_0^t \left(\lambda_{total}^L(u)\right)du\right\}$$
and
$$f(t > 1) = \lambda_{12}^R(t)\exp\left\{-\int_0^1 \left(\lambda_{total}^L(u)\right)du - \int_1^t \left(\lambda_{total}^R(u)\right)du\right\}$$

**II.2.3 Failures on Demand**

In addition to the designed and influenced individual and coincident continuous hazards, the possibility of an individual or coincident failure on demand is considered. This notion of demand failure is from the standard PRA basic event for EDGs; fail to start (FTS). These demand failures can occur at time $t = 0$, next the system is subject to continuous FTL hazards from $0 < t \le 1hr$, and then finally continuous FTR hazards from $1hr < t \le T_m$. The system can be in one of four states at t=0. The associated probabilities for these demand states are

$P_1(0) =$ probability that EDG "1" individually fails to start,
$P_2(0) =$ probability that EDG "2" individually fails to start,
$P_3(0) =$ probability that both EDGs coincidentally fail to start,
and
$P_0(0) = 1 - P_1(0) - P_2(0) - P_3(0) =$ probability of no failures on demand.

This addition of demand failures introduces some new failure sequences that could cause system failure. The most obvious of these is a coincident failure on demand of both EDGs; the probability of this is obtained from industry data for EDG common-cause FTS events [30], [31].

The other new sequences occur when the first component failure occurs on demand and the second component failure is a continuous, influenced, individual failure. Using the relations shown in Equations (II-33) and (II-34), the PDF for the time of this second component failure is formed as in Equation (II-38).

$$f(t) = \tilde{\lambda}_i(t) \exp\left\{-\int_0^t \left(\tilde{\lambda}_i(u)\right) du\right\} \tag{II-38}$$

This PDF is expressed in terms of probability as follows:

$$f(t) = \frac{\Pr\{t \le T_i < t + dt \,|\, T_{i'} = t_{i'}, T_i \ge t, T_{12} > \mathrm{t}\}}{dt}, \; i = 1,2, \; 1' = 2, \text{ and } 2' = 1. \tag{II-39}$$

Likewise, the CDF for time of the second component failure is shown in Equation (II-40).

$$\begin{aligned} F(T_i) &= \sum_{i=1}^{2} \Pr\{T_m \le T_i\} = \sum_{i=1}^{2} \int_{-\infty}^{T_i} f_i(t \,|\, \tau) dt = \sum_{i=1}^{2} \int_{0}^{T_i} f_i(t \,|\, \tau) dt \\ &= \sum_{i=1}^{2} \left[ \int_0^1 f_i(t \le 1 \,|\, \tau) dt + \int_1^{T_i} f_i(t > 1 \,|\, \tau) dt \right] \end{aligned}$$

where (II-40)

$$f_i(t \le 1 \,|\, \tau) = \tilde{\lambda}_i^L(t) \exp\left\{-\int_0^t \left(\lambda_{total}^L(u)\right) du\right\}$$

and

$$f_i(t > 1 \,|\, \tau) = \tilde{\lambda}_i^R(t) \exp\left\{-\int_0^1 \left(\lambda_{total}^L(u)\right) du - \int_1^t \left(\lambda_{total}^R(u)\right) du\right\}$$

In the past two (and current) sections, PDFs were developed in order to compute the probability for each failure sequence possible, according to this specific model case. In Equation (II-41), these PDFs for the mutually exclusive failure sequences are added to form a PDF for total system failure. From state 0, a single coincident or two successive individual continuous failures will create system failure. From state 1 or 2, a single individual continuous failure will create system failure. State 3 is defined as system failure; the probability that the system is in this state at t=0 is the coincident FTS probability determined from NRC data.

$$f(t) = P_0(0)\left\{ f(t_{12}) + \int_0^t f(\tau, t) d\tau \right\} + P_1(0) f_2(t \,|\, \tau) + P_2(0) f_1(t \,|\, \tau) \tag{II-41}$$

The CDF for time of system failure can be computed as in Equation (II-42).

$$
\begin{aligned}
F(T) &= F(0) + \int_0^T f(t)dt = P_3(0) + \int_0^T \left[ P_0(0)\left\{ f(t_{12}) + \int_0^t f(\tau,t)d\tau \right\} + P_1(0) f_2(t\,|\,\tau) + P_2(0) f_1(t\,|\,\tau) \right] dt \\
&= P_3(0) + P_0(0)\int_0^T \lambda_{12}(t)\exp\left\{ -\int_0^t \lambda_{total}(u)du \right\} dt \\
&+ P_0(0)\int_0^T \tilde{\lambda}_2(t)\left[ \int_0^t \lambda_1(\tau)\exp\left\{ -\int_0^\tau \lambda_{total}(u)du - \int_\tau^t \tilde{\lambda}_2(u)du \right\} d\tau \right] dt \\
&+ P_0(0)\int_0^T \tilde{\lambda}_1(t)\left[ \int_0^t \lambda_2(\tau)\exp\left\{ -\int_0^\tau \lambda_{total}(u)du - \int_\tau^t \tilde{\lambda}_1(u)du \right\} d\tau \right] dt \\
&+ P_1(0)\int_0^T \tilde{\lambda}_2(t)\exp\left\{ -\int_0^t \tilde{\lambda}_2(u)du \right\} dt + P_2(0)\int_0^T \tilde{\lambda}_1(t)\exp\left\{ -\int_0^t \tilde{\lambda}_1(u)du \right\} dt
\end{aligned}
\qquad \text{(II-42)}
$$

*where*

$\lambda_{total}(u) = \lambda_1(u) + \lambda_2(u) + \lambda_{12}(u)$,

$\tau$ is for single component failure, and $t$ is for system failure.

When this is completely written out, with the failure modes (FTL and FTR) specified, Equation (II-43) results:

$$
\begin{aligned}
F(T) &= P_3(0) + P_0(0)\left\{ \begin{array}{l} \int_0^1 \lambda_{12}^L(t)\exp\left\{ -\int_0^t \lambda_{total}^L(u)du \right\} dt \\ + \int_1^T \lambda_{12}^R(t)\exp\left\{ -\int_0^1 \lambda_{total}^L(u)du - \int_1^t \lambda_{total}^R(u)du \right\} dt \end{array} \right\} \\
&+ P_0(0)\sum_{i=1}^{2}\left\{ \begin{array}{l} \int_0^1 \tilde{\lambda}_i^L(t)\left[ \int_0^t \lambda_i^L(\tau)\exp\left\{ -\int_0^\tau \lambda_{total}^L(u)du - \int_\tau^t \tilde{\lambda}_i^L(u)du \right\} d\tau \right] dt \\ + \int_1^T \tilde{\lambda}_i^R(t)\left[ \int_0^1 \lambda_j^L(\tau)\exp\left\{ -\int_0^\tau \lambda_{total}^L(u)du - \int_\tau^1 \tilde{\lambda}_i^L(u)du - \int_1^t \tilde{\lambda}_i^R(u)du \right\} d\tau \right] dt \\ + \int_1^T \tilde{\lambda}_i^R(t)\left[ \int_1^t \lambda_j^R(\tau)\exp\left\{ -\int_0^1 \lambda_{total}^L(u)du - \int_1^\tau \lambda_{total}^R(u)du - \int_\tau^t \tilde{\lambda}_i^R(u)du \right\} d\tau \right] dt \end{array} \right\} \\
&+ \sum_{i=1}^{2} P_i(0)\left\{ \begin{array}{l} \int_0^1 \tilde{\lambda}_j^L(t)\exp\left\{ -\int_0^t \tilde{\lambda}_j^L(u)du \right\} dt \\ + \int_1^T \tilde{\lambda}_j^R(t)\exp\left\{ -\int_0^1 \tilde{\lambda}_j^L(u)du - \int_1^t \tilde{\lambda}_j^R(u)du \right\} dt \end{array} \right\}
\end{aligned}
$$

*for* $i \neq j$ (II-43)

Here we have developed a systematic way to model the distribution of failure times for a system of redundant components which are subject to individual and coincident continuous and demand failures.

### II.2.4 NRI Compared to the SPAR Convoluted Distribution Model

Throughout the work for this thesis, it was discovered that the convoluted distribution method used by the industry SPAR models [22] (to quantify consecutive EDG failure sequences for LOOP/SBO problems) is actually a specialized case of the NRI developed in this thesis. When the NRI is constrained to modeling a hot standby system with constant failure rates, it produces the same result as the SPAR convoluted distribution model; this is shown in the current subsection with a simple two-EDG system example problem. The example problem only looks at the system failure sequence from two consecutive individual failures and is evaluated using a mission-time model of load.

Equation (II-44) shows the general (two-EDG) form of the NRI (for two consecutive individual failures) developed in this thesis.

$$\begin{aligned} &f(\tau_1,t_2)=\lambda_1(\tau)\tilde{\lambda}_2(t)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)\right)du-\int_{\tau}^{t}\tilde{\lambda}_2(u)du\right\},\\ &f(\tau_2,t_1)=\lambda_2(\tau)\tilde{\lambda}_1(t)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)\right)du-\int_{\tau}^{t}\tilde{\lambda}_1(u)du\right\},\\ &\text{and}\\ &F_{sys}(T)=\int_0^T\int_0^T f(\tau_1,t_2)d\tau_1dt_2+\int_0^T\int_0^T f(\tau_2,t_1)d\tau_2dt_1 \end{aligned} \tag{II-45}$$

If we specialize this equation to a system of two identical EDGs with constant failure rates and no CCF (each EDG's single failure rate is just $\lambda$), then Equation (II-46) is formed. The analytic evaluation of the system failure time CDF is shown at the end of Equation (II-47).

$$\begin{aligned} &f(\tau,t)=\lambda\lambda\exp\left\{-\left(\lambda+\lambda\right)\tau-\lambda(t-\tau)\right\}\\ &\text{and}\\ &F_{sys}(T)=2\int_0^T\int_0^T f(\tau,t)d\tau dt=\exp(-2T\lambda)*(\exp(T\lambda)-1)^2 \end{aligned} \tag{II-48}$$

This same problem is modeled using the SPAR convoluted distribution method. The PDF for the failure time of each EDG (1 and 2) is taken from Equation (34) of [22] and shown here in Equation (II-49).

$$f_{d1}(t)=\lambda\exp(-\lambda t)\ \text{and}\ f_{d2}(t)=\lambda\exp(-\lambda t) \tag{II-50}$$

The failure time PDF for each EDG is then convolved and integrated as shown in Equation (II-51), which has been adapted from Equation (33) of [22].

$$\begin{aligned} F_{sys}(T) &= 2\int_0^T f_{d1}(t_1)\int_{t_1}^T f_{d2}(t_2)dt_2dt_1 \\ &= 2\int_0^T \lambda\exp(-\lambda t_1)\int_{t_1}^T \lambda\exp(-\lambda t_2)dt_2dt_1 \\ &= \exp(-2T\lambda)*(\exp(T\lambda)-1)^2 \end{aligned} \quad \text{(II-52)}$$

The analytical evaluation for the system failure time CDF for both models produces the same expression, as seen in the last line of Equations (II-53) and (II-54). This problem was coded and analytically integrated using MATLAB. The code for this test case is shown as follows:

```
clear all
syms r t1 t2 T
%% SPAR
f1s=r.*exp(-r.*t1);f2s=r.*exp(-r.*t2);
Fsys_SPAR=int(f1s.*int(f2s,t2,t1,T),t1,0,T)
%% NRI
f1n=r.*exp(-2.*r.*t1);f2n=r.*exp(-r.*(t2-t1));
Fsys_NRI=int(int(f1n.*f2n,t1,0,t2),t2,0,T)
```

**II.3 Extension to Three-EDG Model**

The three-EDG system failure time probability model development is considered as an extension from the two-EDG case. As before, the system fails once all (three) EDGs have failed. Each EDG is subject to continuous hazards and demand failure events, similar to those from Section II.2; the main differences here are related to coincident events and influenced hazard functions. With a system of 3 EDGs, coincident failures can now come in two varieties; either 2-out-of-3 fail, or all 3-out-of-3 fail. Also, influenced coincident failures can now occur as a 2-out-of-2 failure event. Again, the term "hazard function" ( $\lambda(t)$ ) is used to mean an instantaneous failure rate as $\Delta t$ tends to zero. These hazard functions are conditional on the specific EDG failure times. As before, all the hazard functions are piecewise as illustrated in the following equation:

$$\lambda(\tau) = \begin{cases} \lambda^L(\tau), & \text{if } \tau < 1hr \\ \lambda^R(\tau), & \text{if } \tau \geq 1hr \end{cases}. \quad \text{(II-55)}$$

The *designed hazard functions* describe a frequency for a specific failure event, given that no EDGs have failed previously. The possible failure events are one of two types, either an individual (single EDG fails) or coincident (multiple EDGs fail) failure. The specific EDGs are referenced with a number (1, 2, or 3), and those involved in each failure event are denoted with a subscript number on $\lambda$. The hazard functions for individual failures are $\lambda_1(\tau)$, $\lambda_2(\tau)$ or, $\lambda_3(\tau)$. The hazard functions for 2-out-of-3 coincident failures are $\lambda_{12}(t')$, $\lambda_{23}(t')$ or, $\lambda_{13}(t')$. The hazard function for the coincident failure event where all three EDGs fail is $\lambda_{123}(t)$. This model has three different types of failure time random variables which are denoted as follows; $\tau$ is for a failure event where two EDGs survive; $t'$ is for a failure event where 1 EDG survives, and $t$ is for a failure event where no EDGs survive (system failure). Equation (II-56) defines a generic designed hazard function for this case in terms of probability of failure times.

$$\lambda_x(u) = \lambda_x(u \mid T \geq u) = \lim_{\Delta u \to 0} \frac{\Pr\{u \leq T_x < u + \Delta u \mid T \geq u\}}{\Delta u} \tag{II-56}$$

where

$$(x,u) = \begin{cases} (i,\tau), & \text{for an individual failure} \\ (ij,t'), & \text{for a 2-out-of-3 coincident failure} \\ (123,t), & \text{for a 3-out-of-3 coincident failure} \end{cases}$$

and

$T = T_1, T_2, T_3, T_{12}, T_{13}, T_{23}, \text{and } T_{123}$

The total hazard function for all possible failure events that could occur to the designed system is defined in Equation (II-57).

$$\lambda_{total}(u) = \lambda_1(u) + \lambda_2(u) + \lambda_3(u) + \lambda_{12}(u) + \lambda_{23}(u) + \lambda_{13}(u) + \lambda_{123}(u) \tag{II-57}$$

The *influenced hazard functions* describe a frequency for a specific failure event, given that certain EDGs have failed previously. Again, the possible failure events can be either an individual or coincident failure. The hazard function for the individual failure of the i$^{th}$ EDG given that the j$^{th}$ EDG has already failed is written as $\lambda_{i|j}(t')$. Similarly, the hazard function for a 2-out-of-2 coincident failure (both the i$^{th}$ and j$^{th}$ EDGs fail given that the k$^{th}$ EDG has already failed) is written as $\lambda_{ij|k}(t)$. These two similar hazard functions are defined in Equation (II-58).

There is no $T_{123}$ mentioned in this definition or in (II-59) because once one EDG has failed, it becomes impossible for a 3-out-of-3 coincident failure to occur.

$$\tilde{\lambda}_{x|i}(u) = \lambda_{x|i}(u \,|\, T_i = \tau,\ T_j, T_k, T_{jk} \geq u) = \lim_{\Delta u \to 0} \frac{\Pr\left\{u \leq T_j < u + \Delta u \,|\, T_i = \tau,\ T_j, T_k, T_{jk} \geq u\right\}}{\Delta u}$$

where (II-58)

$$(x,u) = \begin{cases} (j,t'), & \text{for a 1-out-of-2 individual failure} \\ (jk,t), & \text{for a 2-out-of-2 coincident failure} \end{cases}$$

The hazard function for a 1-out-of-1 individual failure (the i$^{th}$ EDG fails given that the j$^{th}$ and k$^{th}$ EDGs have already failed) is written as $\lambda_{i|jk}(t)$.

$$\tilde{\lambda}_{k|ij}(t) = \lambda_{k|ij}(t \,|\, T_i, T_j, T_{ij} \leq t',\ T_k \geq t) = \lim_{\Delta u \to 0} \frac{\Pr\left\{u \leq T_j < u + \Delta u \,|\, T_i, T_j, T_{ij} \leq t',\ T_k \geq t\right\}}{\Delta t} \quad \text{(II-59)}$$

The total hazard function, defined in Equation (II-60), is for all possible failure events that could occur to a system where one EDG has already failed. The total hazard function for a system where two EDGs have already failed is simply $\tilde{\lambda}_{k|ij}(t)$.

$$\lambda_{total|i}(u) = \lambda_{j|i}(u) + \lambda_{k|i}(u) + \lambda_{jk|i}(u) \quad \text{(II-60)}$$

In addition to these continuous time hazards, the EDGs are subject to demand failures to start. The system can be in one of seven states at t=0, the associated probabilities for these demand states are described as follows:

$P_1(0) =$ probability that EDG "1" individually fails to start
$P_2(0) =$ probability that EDG "2" individually fails to start
$P_3(0) =$ probability that EDG "3" individually fails to start
$P_4(0) =$ probability that EDGs "1" and "2" coincidentally fail to start
$P_5(0) =$ probability that EDGs "2" and "3" coincidentally fail to start
$P_6(0) =$ probability that EDGs "1" and "3" coincidentally fail to start
$P_7(0) =$ probability that EDGs "1", "2", and "3" coincidentally fail to start
$P_0(0) = 1 - P_1(0) - P_2(0) - P_3(0) - P_4(0) - P_5(0) - P_6(0) - P_7(0) =$ probability of no failures on demand

**II.3.1 Failure Sequences**

In Sections II.3.1 through II.3.3, PDFs are developed in order to compute the probability for each possible sequence of events that will fail this three-EDG system. In Equation (II-61), these

PDFs for the mutually exclusive failure sequences are added to form a PDF for total system failure. The subscript numbers on the time variables denote which EDGs fail and correspond to the specific failure event; instances of multiple subscript numbers on a time variable indicate a coincident failure event. When the letters $i, j,$ or $k$ appear on the subscript the conditions $i = 1,2,3,\ j = 1,2,3,\ k = 1,2,3,$ and $i \neq j \neq k$ apply (this is done to account for every combination of failure time orders while only expressing equations for the case $T_i \leq T_j \leq T_k$).

Following no failures to start (state 0), the system will fail from any one of the following event sequences (the corresponding PDF is also shown):

- 3-out-of-3 coincident failure; $f(t_{ijk})$
- 2-out-of-3 coincident failure, then an individual failure; $f(t'_{ij}, t_k)$, $t'_{ij} < t_k$
- Individual failure, then a 2-out-of-2 coincident failure; $f(t'_i, t_{jk})$, $t'_i < t_{jk}$
- Three subsequent individual failures; $f(\tau_i, t'_j, t_k)$, $\tau_i < t'_j < t_k$

Following an individual failure to start (states 1, 2, or 3), the system will fail from either a 2-out-of-2 coincident failure or from two subsequent individual failures (PDFs for these are $f(t_{jk})$ and $f(t'_j, t_k)$, respectively). Following a 2-out-of-3 coincident failure to start (states 4, 5, or 6), the system will fail once the survived EDG individually fails (PDF is $f(t_k)$).

The above listed failure sequences PDFs are developed in the following subsections. These PDFs come in three main varieties; this is due to the fact that each PDF will have three, two, or one random failure time variables. The bivariate and univariate PDF models have already been developed in Section II.2. In Section II.3.1.1, the multivariate joint distribution of Shaked [6] is used to develop the PDF model for sequences with three different failure times. In Equation (II-61), these PDFs are combined to create a PDF for the system failure time due to every possible event sequence. The system failure PDF is written for all combinations of ordered failure times (that is, $T_1 \leq T_2 \leq T_3, T_1 \leq T_3 \leq T_2, T_2 \leq T_1 \leq T_3, T_2 \leq T_3 \leq T_1$, $T_3 \leq T_1 \leq T_2$, and $T_3 \leq T_2 \leq T_1$).

$$
\begin{aligned}
f(t) = P_0(0)\Bigg\{ & f(t_{123}) + \int_0^t f(t'_{12},t)dt' + \int_0^t f(t'_{23},t)dt' + \int_0^t f(t'_{13},t)dt' + \int_0^t f(t',t_{23})dt' + \int_0^t f(t',t_{13})dt' \\
& + \int_0^t f(t',t_{12})dt' + \int_0^t \int_0^{t'} f(\tau_1,t'_2,t_3)d\tau dt' + \int_0^t \int_0^{t'} f(\tau_1,t'_3,t_2)d\tau dt' + \int_0^t \int_0^{t'} f(\tau_2,t'_1,t_3)d\tau dt' \\
& + \int_0^t \int_0^{t'} f(\tau_2,t'_3,t_1)d\tau dt' + \int_0^t \int_0^{t'} f(\tau_3,t'_1,t_2)d\tau dt' + \int_0^t \int_0^{t'} f(\tau_3,t'_2,t_1)d\tau dt' \Bigg\} \\
& + P_1(0)\left\{ f(t_{23}) + \int_0^t f(t'_2,t_3)dt' + \int_0^t f(t'_3,t_2)dt' \right\} + P_2(0)\left\{ f(t_{13}) + \int_0^t f(t'_1,t_3)dt' + \int_0^t f(t'_3,t_1)dt' \right\} \\
& + P_3(0)\left\{ f(t_{12}) + \int_0^t f(t'_1,t_2)dt' + \int_0^t f(t'_2,t_1)dt' \right\} + P_4(0)f(t_3) + P_5(0)f(t_1) + P_6(0)f(t_2)
\end{aligned}
\qquad \text{(II-61)}
$$

### II.3.1.1 Three Continuous Random Failure Times

The model development begins with the system failure event caused by three consecutive continuous time hazards. As a means to account for the combinatorial sequencing of the three random failure times, an extension of the previously used joint PDF by Cox [23] is employed. This extension is given for the case of a general number of components, with ordered failure times $T_1 \le T_2 \le \ldots \le T_n$ [6]. The PDF is composed of both designed and influenced hazard functions as defined in Equations (II-62) and (II-63), respectively.

$$
\lambda_i(t) = \lim_{\Delta t \to 0} \frac{\Pr\{t \le T_i < t + \Delta t \,|\, T_1, T_2, \ldots, T_n \ge t\}}{\Delta t}, \quad \mathrm{i} = 1,2,\ldots,n \qquad \text{(II-62)}
$$

$$
\tilde{\lambda}_i(t_i \,|\, T_{i-1} = t_{i-1}.) = \lim_{\Delta t \to 0} \frac{\Pr\{t \le T_i < t + \Delta t \,|\, T_{i-1} = t_{i-1}; T_i \ge t_i > t_{i-1}\}}{\Delta t}, \quad \mathrm{i} = 2,3,\ldots,n \qquad \text{(II-63)}
$$

The general form of the multivariate joint density $f$ of the vector of random EDG failure times $\boldsymbol{T}$ can be shown in Equation (II-64) for $t_1 \le t_2 \le \ldots t_n$, as from page 152 of Shaked and Shanthikumar [6].

$$
\begin{aligned}
& f(t_1,\ldots,t_n) = \lambda_1(t_1)\exp\left\{ -\int_0^{t_1} \left( \sum_{j=1}^{n} \lambda_j(u) \right) du \right\} \\
& \times \prod_{i=2}^{n} \left[ \lambda_i(t_i \,|\, T_1 = t_1,\ldots,T_{i-1} = t_{i-1},.) \times \exp\left\{ -\int_{t_{i-1}}^{t_i} \left( \sum_{j=i}^{n} \lambda_j(u \,|\, T_1 = t_1,\ldots,T_{i-1} = t_{i-1},.) \right) du \right\} \right]
\end{aligned}
\qquad \text{(II-64)}
$$

The PDF, Equation (II-65), for the three individual EDG failure case (for $T_i < T_j < T_k$) is formed by setting n=3 for the general PDF above.

$$f(\tau_i, t'_j, t_k) = \lambda_i(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}(u)\right)du\right\} \times \lambda_{j|i}(t)\exp\left\{-\int_{\tau}^{t'}\left(\lambda_{total|i}(u)\right)du\right\}$$
$$\times\lambda_{k|ij}(t)\exp\left\{-\int_{t'}^{t}\left(\lambda_{k|ij}(u)\right)du\right\} \quad \text{(II-65)}$$

Equation (II-65) is expressed as a probability statement directly below.

$$f(\tau_i, t'_j, t_k) = \frac{\Pr\left(\tau \le T_i < \tau + d\tau \bigcap t' \le T_j < t' + dt' \bigcap t \le T_k < t + dt \,\middle|\, \begin{matrix}\tau \le T_i, t' \le T_j, t \le T_k, \\ \tau_i < t_j < t_k\end{matrix}\right)}{d\tau dt' dt} \quad \text{(II-66)}$$

Again, the EDGs are subject to two types of continuous-time hazards; from time t=0 to t=1 hour an EDG may experience an individual failure to load (FTL), while after time t=1 hour an EDG may experience an individual failure to run (FTR). The specific time regime for each hazard function is denoted with a superscript letter on $\lambda$; L and R stand for FTL and FTR hazards, respectively. The piecewise hazard functions which compose Equation (II-65) have a jump discontinuity at t=1 hour and each of the three individual failure time variables are associated with a specific hazard function from either side of this discontinuity; thus Equation (II-65) contains four unique cases as in Equations (II-67)-(II-70).

Equation (II-67) is written for the case where all three subsequent individual failures are from failure to load events ($\tau_i < t'_j < t_k \le 1$). The three failure times occur before the one hour mark, so this equation is easily obtained from Equation (II-65) by simply specifying that the only hazards experienced are FTL.

$$f(\tau_i < 1, t'_j < 1, t_k \le 1) = \lambda_i^L(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}^L(u)\right)du\right\}$$
$$\times\lambda_{j|i}^L(t')\exp\left\{-\int_{\tau}^{t'}\left(\lambda_{total|i}^L(u)\right)du\right\} \times \lambda_{k|ij}^L(t)\exp\left\{-\int_{t'}^{t}\left(\lambda_{k|ij}^L(u)\right)du\right\} \quad \text{(II-67)}$$

Equation (II-68) is given for the case where first an EDG fails to load, next an EDG fails to load, and then the last EDG fails to run ($\tau_i < t'_j \le 1 < t_k$). The first two multiplied terms are identical to Equation (II-67), while the $\lambda_{k|ij}$ outside the exponential is changed to reflect the hazard experienced at the point of failure ($t$) for the third EDG. The integral limits on the last term are split to account for the change in hazard from FTL to FTR, as shown here $\int_{t'}^{t}\lambda_{k|ij}(u)du = \int_{t'}^{1}\lambda_{k|ij}^L(u)du + \int_1^t \lambda_{k|ij}^R(u)du$.

$$f(\tau_i<1,t_j'\le 1,t_k>1)=\lambda_i^L(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}^L(u)\right)du\right\}$$
$$\times\lambda_{j|i}^L(t')\exp\left\{-\int_{\tau}^{t'}\left(\lambda_{total|i}^L(u)\right)du\right\}\times\lambda_{k|ij}^R(t)\exp\left\{-\left(\int_{t'}^{1}\lambda_{k|ij}^L(u)du+\int_1^t\lambda_{k|ij}^R(u)du\right)\right\} \quad \text{(II-68)}$$

Equation (II-69) is given for the case where first an EDG fails to load, next an EDG fails to run, and then the last EDG fails to run ( $\tau_i\le 1<t_j'<t_k$ ). The first multiplied term is identical to the pervious case, and the influenced hazard functions, $\lambda's$, outside the exponential are both specified as FTR hazards. The integral limits on the middle term are split to account for the change in hazard from FTL to FTR, as shown here $\int_{\tau}^{t'}\lambda_{total|i}(u)du=\int_{\tau}^{1}\lambda_{total|i}^L(u)du+\int_1^{t'}\lambda_{total|i}^R(u)du$.

$$f(\tau_i\le 1,t_j'>1,t_k>1)=\lambda_i^L(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}^L(u)\right)du\right\}$$
$$\times\lambda_{j|i}^R(t')\exp\left\{-\left(\int_{\tau}^{1}\lambda_{total|i}^L(u)du+\int_1^{t'}\lambda_{total|i}^R(u)du\right)\right\}\times\lambda_{k|ij}^R(t)\exp\left\{-\int_{t'}^{t}\lambda_{k|ij}^R(u)du\right\} \quad \text{(II-69)}$$

Equation (II-70) is written for the case where all three EDGs loaded and successfully made it through time t=1 hour, and then each subsequently failed to run ( $1<\tau_i<t_j'<t_k$ ). The integral limits on the first exponential are split at t=1 hour to account for the change in hazard from FTL to FTR, as shown here $\int_0^{\tau}\lambda_{total}(u)du=\int_0^1\lambda_{total}^L(u)du+\int_1^{\tau}\lambda_{total}^R(u)du$. The rest of this joint density function is similar to Equation (II-65) except the hazard functions are specified as FTR (with superscript *R* 's).

$$f(\tau_i>1,t_j'>1,t_k>1)=\lambda_i^R(\tau)\exp\left\{-\left(\int_0^1\lambda_{total}^L(u)du+\int_1^{\tau}\lambda_{total}^R(u)du\right)\right\}$$
$$\times\lambda_{j|i}^R(t')\exp\left\{-\int_{\tau}^{t'}\lambda_{total|i}^R(u)du\right\}\times\lambda_{k|ij}^R(t)\exp\left\{-\int_{t'}^{t}\lambda_{k|ij}^R(u)du\right\} \quad \text{(II-70)}$$

**II.3.1.2 Two Continuous Random Failure Times**

The model for the joint distribution of two continuous failure times for components subject to both FTL and FTR hazards has already been developed in Equations (II-19)-(II-21) of Section II.2. Again, this model is based on the result from [23].

For the system of 3 EDGs introduced in Section II.3, the bivariate PDF can be used to describe the following system event sequences:

- Individual FTS and then two subsequent individual failures; $f(t_j',t_k)$

- 2-out-of-3 coincident failure, then an individual failure; $f(t'_{ij}, t_k)$
- Individual failure, then a 2-out-of-2 coincident failure; $f(\tau_i, t_{jk})$

Using the basic form of Equation (II-21), and the hazard functions defined at the beginning of this section, the expressions for these specific cases of the bivariate PDF are explicitly stated in Equations (II-71)-(II-73). The first line of these equations is expressed using hazard functions while the second line expresses them as a probability.

$$\begin{aligned} f(t'_j, t_k) &= \lambda_{j|i}(t')\lambda_{k|ij}(t)\exp\left\{-\int_0^{t'}\lambda_{total|i}(u)du - \int_{t'}^{t}\lambda_{k|ij}(u)du\right\} \\ &= \frac{\Pr\{t' \le T_j < t' + dt' \cap t \le T_k < t + dt \,|\, T_i = 0, t' \le T_j, t \le T_k\}}{dt'_j dt_k} \end{aligned} \tag{II-71}$$

$$\begin{aligned} f(t'_{ij}, t_k) &= \lambda_{ij}(t')\lambda_{k|ij}(t)\exp\left\{-\int_0^{t'}\lambda_{total}(u)du - \int_{t'}^{t}\lambda_{k|ij}(u)du\right\} \\ &= \frac{\Pr\{t' \le T_{ij} < t' + dt' \cap t \le T_k < t + dt \,|\, t' \le T_{ij}, t \le T_k\}}{dt'_{ij} dt_k} \end{aligned} \tag{II-72}$$

$$\begin{aligned} f(\tau_i, t_{jk}) &= \lambda_i(\tau)\lambda_{jk|i}(t)\exp\left\{-\int_0^{\tau}\lambda_{total}(u)du - \int_{\tau}^{t}\lambda_{total|i}(u)du\right\} \\ &= \frac{\Pr\{\tau \le T_i < \tau + d\tau \cap t \le T_{jk} < t + dt \,|\, \tau \le T_i, t \le T_{jk}\}}{d\tau_i dt_{jk}} \end{aligned} \tag{II-73}$$

All hazard functions are piecewise with a discontinuity at t=1 hour, as explained in Equation (II-55). Equation (II-74) shows how to write the bivariate PDF for ordered pairs of failure times due to the following respective hazard pairs; (FTL,FTL), (FTL,FTR), (FTR,FTR). Equation (II-74) expresses (II-71) for the three different bivariate PDF cases for this section; this formalism similarly applies to Equations (II-72) and (II-73).

$$\begin{aligned} f(t'_j < 1, t_k \le 1) &= \lambda^L_{j|i}(t')\lambda^L_{k|ij}(t)\exp\left\{-\int_0^{t'}\lambda^L_{total|i}(u)du - \int_{t'}^{t}\lambda^L_{k|ij}(u)du\right\} \\ f(t'_j \le 1, t_k > 1) &= \lambda^L_{j|i}(t')\lambda^R_{k|ij}(t)\exp\left\{-\int_0^{t'}\lambda^L_{total|i}(u)du - \left(\int_{t'}^{1}\lambda^L_{k|ij}(u)du + \int_1^{t}\lambda^R_{k|ij}(u)du\right)\right\} \\ f(t'_j > 1, t_k > 1) &= \lambda^R_{j|i}(t')\lambda^R_{k|ij}(t)\exp\left\{-\left(\int_0^{1}\lambda^L_{total|i}(u)du + \int_1^{t'}\lambda^R_{total|i}(u)du\right) - \int_{t'}^{t}\widetilde{\lambda^R_{k|ij}}(u)du\right\} \end{aligned} \tag{II-74}$$

#### II.3.1.3 One Continuous Random Failure Time

A model for the PDF of a single continuous random failure time has already been developed in Section II.2 and is used again here.

For the system of 3 EDGs introduced in Section II.3, this univariate PDF can be used to describe the following system event sequences:

- 2-out-of-3 coincident FTS, then an individual failures; $f(t_k)$
- Individual FTS, then a 2-out-of-2 coincident failure; $f(t_{jk})$
- 3-out-of-3 coincident failure; $f(t_{123})$

Using Equations (II-33)-(II-35), but with the hazard functions defined at the beginning of this section, the expressions for these specific cases of the univariate PDF are explicitly stated in Equations (II-75)-(II-77). The second line of these equations express the PDF in terms of probability.

$$\begin{aligned} f(t_{123}) &= \lambda_{123}(t)\exp\left\{-\int_0^t\left(\lambda_{total}(u)\right)du\right\} \\ &= \frac{\Pr\{t \le T_{123} < t+dt \,|\, t < T_i, T_{ij}\}}{dt_{123}} \end{aligned} \tag{II-75}$$

$$\begin{aligned} f(t_k) &= \lambda_{k|ij}(t)\exp\left\{-\int_0^t \lambda_{k|ij}(u)du\right\} \\ &= \frac{\Pr\{t \le T_k < t+dt \,|\, \tau = T_i \cup t' = T_{ij}, t \le T_k\}}{dt_k} \end{aligned} \tag{II-76}$$

$$\begin{aligned} f(t_{jk}) &= \lambda_{jk|i}(t)\exp\left\{-\int_0^t \lambda_{total|i}(u)du\right\} \\ &= \frac{\Pr\{t \le T_{jk} < t+dt \,|\, \tau = T_i, t \le T_{jk}\}}{dt_{jk}} \end{aligned} \tag{II-77}$$

The single random failure time is due to either a FTL or FTR hazard. Equation (II-78) expresses Equation (II-75) for these two different cases of the univariate PDFs in this section; this formalism also applies to Equations (II-76) and (II-77).

$$\begin{aligned} f(t_{ijk} \le 1) &= \lambda^L_{ijk}(t)\exp\left\{-\int_0^t\left(\lambda^L_{total}(u)\right)du\right\} \\ f(t_{ijk} > 1) &= \lambda^R_{ijk}(t)\exp\left\{-\int_0^1\left(\lambda^L_{total}(u)\right)du - \int_1^t\left(\lambda^R_{total}(u)\right)du\right\} \end{aligned} \tag{II-78}$$

### II.4 Connection to Markov Model

This section introduces a Markov model of the same two- and three-EDG systems from Sections II.2 and II.3, respectively. The only difference is that the NRI models (from Sections II.2 and II.3) can accept time varying hazard functions (under certain conditions), while the Markov models in Section II.4 can only accept constant failure rates. Markov models are well known and understood for survival analysis problems, hence they were chosen as means to verify the system failure time CDFs from Sections II.2 and II.3. Section II.4.1 and II.4.2 develop the general two- and three-EDG Markov models, respectively. Chapter IV, "Results and Benchmarking", will compare specific case results between the NRI and Markov models as a means to verify the results and coding of the NRI.

#### II.4.1 Markov Model for Two Identical EDGs

The state transition diagram for the two-EDG Markov model can be seen in Figure 4.The system states are described as follows: 0, no EDGs are failed; 1, EDG "1" is failed; 2, EDG "2" is failed; 3, both EDG are failed (thus system failure). The hazard functions ($\lambda_{12}, \lambda_i$, and $\tilde{\lambda}_i$, for i=1,2) in Figure 4 correspond to those defined in Equations (II-29)-(II-31), respectively. The initial state probabilities ($P_0^{(0)}, P_1^{(1)}, P_2^{(1)}, P_3^{(2)}$) are the same used in the model from Section II.2.3. Both two-EDG models have the same logic, assumptions, and inputs; thus the CDF for system failure times from Section II.2 (Equation (II-43)) should be identical to the temporal probability results (for state 3 of the Markov model) developed in this section. These results should be equal, while the specific process used to obtain them and the details they reveal are different. Section II.2 modeled the temporal probability for every possible event sequence that lead to system failure separately, and then summed these mutually exclusive results to obtain the complete PDF and CDF for the system failure times. The Markov model developed here computes the probability that the system is in each of its four possible states, as a function of time.

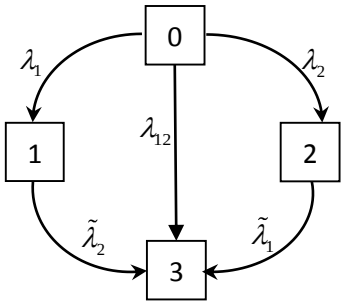


**Figure 4 – State-Transition Diagram for the Two-EDG Markov Model.**

The state-transition differential equations for the system described above can be written as follows:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\lambda_{total} P_0(t) \\ \dfrac{dP_1(t)}{dt} = \lambda_1 P_0(t) - \tilde{\lambda}_2 P_1(t) \\ \dfrac{dP_2(t)}{dt} = \lambda_2 P_0(t) - \tilde{\lambda}_1 P_2(t) \\ \dfrac{dP_3(t)}{dt} = \lambda_{12} P_0(t) + \tilde{\lambda}_2 P_1(t) + \tilde{\lambda}_1 P_2(t) \end{cases} \quad \text{(II-79)}$$

where $\lambda_{total} = \lambda_1 + \lambda_2 + \lambda_{12}$

And the corresponding initial conditions are:

$$\begin{cases} P_0\left(t=0\right) = \tilde{P}_0 = 1 - \tilde{P}_1^{(1)} - \tilde{P}_2^{(1)} - \tilde{P}_3^{(2)} \\ P_1\left(t=0\right) = \tilde{P}_1^{(1)} \\ P_2\left(t=0\right) = \tilde{P}_2^{(1)} \\ P_3\left(t=0\right) = \tilde{P}_3^{(2)} \end{cases} \quad \text{(II-80)}$$

The first three of the transition Equations in (II-79) will be solved using a standard method of solving linear first-order differential equations. Assuming the following generic initial value problem,

$$\frac{dy}{dx} + p(x)y = f(x) \qquad \text{with} \quad y(x_0) = y_0, \quad \text{(II-81)}$$

its solution is given as

$$y(x)=\frac{1}{\mu(x)}\left[y_0+\int_{x_0}^{x}\mu(u)f(u)du\right] \quad \text{with} \quad \mu(x)=\exp\left(\int_{x_0}^{x}p(u)du\right). \tag{II-82}$$

Written in the same form as the generic initial value problem, the transition equation for state 0 becomes

$$\frac{dP_0(t)}{dt}+\lambda_{total}P_0(t)=0, \tag{II-83}$$

and its solution is

$$P_0(t)=\frac{1}{\mu(t)}\left[\tilde{P}_0+\int_0^t\mu(u)(0)du\right]=\tilde{P}_0\exp\left\{-\int_0^t\lambda_{total}du\right\}. \tag{II-84}$$

Likewise, the transition equation and solution for state 1 is

$$\begin{aligned}
&\frac{dP_1(t)}{dt}+\tilde{\lambda}_2P_1(t)=\lambda_1P_0(t)\\
&\qquad P_1(t)=\frac{1}{\mu(t)}\left[\tilde{P}_1^{(1)}+\int_0^t\mu(\tau)\lambda_1P_0(\tau)d\tau\right]\\
&\qquad\quad=\exp\left\{-\int_0^t\tilde{\lambda}_2du\right\}\left[\tilde{P}_1^{(1)}+\int_0^t\lambda_1P_0(\tau)\exp\left\{\int_0^\tau\tilde{\lambda}_2du\right\}d\tau\right]\\
&\qquad\quad=\exp\left\{-\int_0^t\tilde{\lambda}_2du\right\}\tilde{P}_1^{(1)}+\int_0^t\lambda_1P_0(\tau)\exp\left\{-\int_\tau^t\tilde{\lambda}_2du\right\}d\tau\\
&\qquad\quad=\tilde{P}_1^{(1)}\exp\left\{-\int_0^t\tilde{\lambda}_2du\right\}+\tilde{P}_0\int_0^t\left(\lambda_1\exp\left\{-\int_0^\tau\lambda_{total}du-\int_\tau^t\tilde{\lambda}_2du\right\}\right)d\tau.
\end{aligned} \tag{II-85}$$

It should be noted here that Equation (II-85) above uses the following relation to arrive at its line 4,

$$\exp\left\{-\int_\tau^t\tilde{\lambda}_2du\right\}=\exp\left\{\int_0^\tau\tilde{\lambda}_2du-\int_0^t\tilde{\lambda}_2du\right\}. \tag{II-86}$$

The state 2 transition equation and solution are similar to those of state 1; these can be shown in Equations (II-87) and (II-88), respectively.

$$\frac{dP_2(t)}{dt}+\tilde{\lambda}_1P_2(t)=\lambda_2P_0(t) \tag{II-87}$$

$$P_2(t)=\tilde{P}_2^{(1)}\exp\left\{-\int_0^t\tilde{\lambda}_1du\right\}+\tilde{P}_0\int_0^t\left(\lambda_2\exp\left\{-\int_0^\tau\lambda_{total}du-\int_\tau^t\tilde{\lambda}_1du\right\}\right)d\tau \tag{II-88}$$

The state 3 transition equation is shown as follows,

$$\frac{dP_3(t)}{dt} = \lambda_{12}P_0(t) + \tilde{\lambda}_2 P_1(t) + \tilde{\lambda}_3 P_2(t). \tag{II-89}$$

It is worth noting here that Equation (II-89) and (II-41) are similar functions which were developed using two different methods. Integration of either of these two functions, however, produces the exact same result.

$$\frac{dP_3(t)}{dt} \sim f(t) = P_0(0)\left\{ f(t_{12}) + \int_0^t f(\tau, t)d\tau \right\} + P_1(0)f_2(t\,|\,\tau) + P_2(0)f_1(t\,|\,\tau) + P_3(0) \tag{II-90}$$

Because the right-hand side of (II-89) does not depend on $P_3(t)$, the state 3 equation can be obtained by simply integrating, as shown here:

$$P_3(T) = \int_0^T dP_3(t) = \tilde{P}_3^{(2)} + \int_0^T \left( \lambda_{12}P_0(t) + \tilde{\lambda}_2 P_1(t) + \tilde{\lambda}_3 P_2(t) \right) dt. \tag{II-91}$$

This gives the probability that the system is in state 3 at or before time T (both EDGs failed, system failure).

After some algebraic manipulations, Equation (II-91) in terms of the basic parameters of the model is shown in Equation (II-92). This equation is identical to the system failure time CDF shown in Equation (II-42).

$$\begin{aligned} P_f(T) = \tilde{P}_3^{(2)} + \tilde{P}_0 & \left[ \begin{array}{l} \int_0^T \lambda_{12} \exp\left\{ -\int_0^t \lambda_{total} du \right\} dt \\ + \int_0^T \tilde{\lambda}_2 \int_0^t \left( \lambda_1 \exp\left\{ -\int_0^\tau \lambda_{total} du - \int_\tau^t \tilde{\lambda}_2 du \right\} \right) d\tau dt \\ + \int_0^T \tilde{\lambda}_1 \int_0^t \left( \lambda_2 \exp\left\{ -\int_0^\tau \lambda_{total} du - \int_\tau^t \tilde{\lambda}_1 du \right\} \right) d\tau dt \end{array} \right] \\ + \tilde{P}_1^{(1)} \int_0^T \tilde{\lambda}_2 \exp\left\{ -\int_0^t \tilde{\lambda}_2 du \right\} dt & + \tilde{P}_2^{(1)} \int_0^T \tilde{\lambda}_1 \exp\left\{ -\int_0^t \tilde{\lambda}_1 du \right\} dt \end{aligned} \tag{II-92}$$

As in Sections II.2 and II.3, each hazard function comes in two varieties, FTL or FTR. The piecewise nature of the hazard functions are shown in Equation (II-93).

$$\lambda_i = \begin{cases} \lambda_i^L, & \text{if } t < 1hr \\ \lambda_i^R, & \text{if } t \geq 1hr \end{cases}, \lambda_i = \begin{cases} \lambda_i^L, & \text{if } t < 1hr \\ \lambda_i^R, & \text{if } t \geq 1hr \end{cases}, \text{and } \lambda_{12} = \begin{cases} \lambda_{12}^L, & \text{if } t < 1hr \\ \lambda_{12}^R, & \text{if } t \geq 1hr \end{cases} \tag{II-93}$$

When this is completely written out, with the failure modes (FTL and FTR) specified, Equation (II-94) is formed. Equation (II-94) is the state 3 transition equation solution which computes the probability of system failure by some time input, $T$ . This equation is identical to the system failure time CDF shown in Equation (II-43) (except the failure rates are time-dependent in (II-43)). While these final results are identical, the process used to arrive at these two results is very different. Equation (II-94) was obtained by solving a system of differential Markov state equations, while (II-43) is actually the sum of every possible (and mutually exclusive) system failure event sequence CDFs.

$$
\begin{aligned}
P_f(T) = \tilde{P}_3^{(2)} + \tilde{P}_0 & \left\{ \begin{array}{l} \int_0^1 \lambda_{12}^L \exp\left\{ -\int_0^t \lambda_{total}^L du \right\} dt \\ + \int_1^T \lambda_{12}^R \exp\left\{ -\int_0^1 \lambda_{total}^L du - \int_1^t \lambda_{total}^R du \right\} dt \end{array} \right\} \\
+ \tilde{P}_0 \sum_{i=1}^{2} & \left\{ \begin{array}{l} \int_0^1 \tilde{\lambda}_i^L \left[ \int_0^t \lambda_i^L \exp\left\{ -\int_0^\tau \lambda_{total}^L du - \int_\tau^t \tilde{\lambda}_i^L du \right\} d\tau \right] dt \\ + \int_1^T \tilde{\lambda}_i^R \left[ \int_0^1 \lambda_j^L \exp\left\{ -\int_0^\tau \lambda_{total}^L du - \int_\tau^1 \tilde{\lambda}_i^L du - \int_1^t \tilde{\lambda}_i^R du \right\} d\tau \right] dt \\ + \int_1^T \tilde{\lambda}_i^R \left[ \int_1^t \lambda_j^R \exp\left\{ -\int_0^1 \lambda_{total}^L du - \int_1^\tau \lambda_{total}^R du - \int_\tau^t \tilde{\lambda}_i^R du \right\} d\tau \right] dt \end{array} \right\} \\
+ \sum_{i=1}^{2} \tilde{P}_i^{(1)} & \left\{ \begin{array}{l} \int_0^1 \tilde{\lambda}_j^L \exp\left\{ -\int_0^t \tilde{\lambda}_j^L du \right\} dt \\ + \int_1^T \tilde{\lambda}_j^R \exp\left\{ -\int_0^1 \tilde{\lambda}_j^L du - \int_1^t \tilde{\lambda}_j^R du \right\} dt \end{array} \right\} \\
& \text{for } i \neq j
\end{aligned}
\qquad \text{(II-94)}
$$

### II.4.2 Markov Model for Three Identical EDGs

The system states are described as follows: 0, no EDGs are failed; 1, EDG “1” is failed; 2, EDG “2” is failed; 3, EDG “3” is failed; 4, EDGs “1” and “2” are failed; 5, EDGs “2” and “3” are failed; 6, EDGs “1” and “3” are failed; 7, all three EDGs are failed (thus system failure). The EDGs in this system are subject to the same failure events as the three-EDG model introduced in Section II.3. The hazard functions for these events are defined in Equations (II-56), (II-58), and (II-59) From state 0 they are subject to designed failure events; either a single EDG, two EDGs, or all three EDGs can fail during a single failure event. From states 1, 2, and 3, the EDGs are

subject to the same influenced failure events; either one EDG can fail, or both remaining EDGs can fail. From states 4, 5, and 6, the only remaining EDG is subject to a single influenced failure event. The only major difference is that the previous three-EDG model was developed to handle hazard rates as a function of time while this Markov model only accepts constant failure rates.

The initial state probabilities are the same used in the three-EDG model from Section II.3. Both three-EDG models have the same logic and assumptions (the same initial conditions and failure rate inputs are used to verify results); thus the CDF for system failure times in Section II.3 should be identical to the temporal probability results (for state 7 of the Markov model) developed in this section. These results should be equal, while the specific process used to obtain them and the details they reveal are different. Section II.3 modeled the temporal probability for every possible event sequence that lead to system failure separately, and then summed these mutually exclusive results to obtain the complete PDF and CDF for the system failure times. The Markov model of this section computes the probability that the system is in each of its eight possible states, as a function of time.

The state-transition differential equations for the system described above can be written as follows:

$$
\begin{cases}
\dfrac{dP_0(t)}{dt} = -\lambda_{total} P_0(t) \\
\dfrac{dP_1(t)}{dt} = \lambda_1 P_0(t) - \left(\tilde{\lambda}_{2|1} + \tilde{\lambda}_{3|1} + \tilde{\lambda}_{23|1}\right) P_1(t) \\
\dfrac{dP_2(t)}{dt} = \lambda_2 P_0(t) - \left(\tilde{\lambda}_{1|2} + \tilde{\lambda}_{3|2} + \tilde{\lambda}_{13|2}\right) P_2(t) \\
\dfrac{dP_3(t)}{dt} = \lambda_3 P_0(t) - \left(\tilde{\lambda}_{2|3} + \tilde{\lambda}_{1|3} + \tilde{\lambda}_{12|3}\right) P_3(t) \\
\dfrac{dP_4(t)}{dt} = \lambda_{12} P_0(t) + \tilde{\lambda}_{2|1} P_1(t) + \tilde{\lambda}_{1|2} P_2(t) - \tilde{\lambda}_{3|12} P_4(t) \\
\dfrac{dP_5(t)}{dt} = \lambda_{23} P_0(t) + \tilde{\lambda}_{2|3} P_3(t) + \tilde{\lambda}_{3|2} P_2(t) - \tilde{\lambda}_{1|23} P_5(t) \\
\dfrac{dP_6(t)}{dt} = \lambda_{13} P_0(t) + \tilde{\lambda}_{1|3} P_3(t) + \tilde{\lambda}_{3|1} P_1(t) - \tilde{\lambda}_{2|13} P_6(t) \\
\dfrac{dP_7(t)}{dt} = \begin{cases} \lambda_{123} P_0(t) + \tilde{\lambda}_{23|1} P_1(t) + \tilde{\lambda}_{13|2} P_2(t) + \\ \tilde{\lambda}_{12|3} P_3(t) + \tilde{\lambda}_{3|12} P_4(t) + \tilde{\lambda}_{1|23} P_5(t) + \tilde{\lambda}_{2|13} P_6(t) \end{cases}
\end{cases}
$$

where $\lambda_{total} = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_{12} + \lambda_{23} + \lambda_{13} + \lambda_{123}$. (II-95)

It is assumed that the three EDGs are identical and subject to the exact same failure events, thus states 1 through 3 are identical and states 4 through 6 are identical as well. Thus the state equations for 1 through 3 and 3 through 4 have been collapsed to states $i$ and $ij$, respectively (as in Equation (II-96)).

$$
\begin{cases}
\dfrac{dP_0(t)}{dt} = -\lambda_{total} P_0(t) \\
\dfrac{dP_i(t)}{dt} = \lambda_i P_0(t) - \left(2\tilde{\lambda}_{j|i} + \tilde{\lambda}_{jk|i}\right) P_i(t) \\
\dfrac{dP_{ij}(t)}{dt} = \lambda_{ij} P_0(t) + 2\tilde{\lambda}_{j|i} P_i(t) - \tilde{\lambda}_{k|ij} P_{ij}(t) \\
\dfrac{dP_7(t)}{dt} = \lambda_{123} P_0(t) + 3\tilde{\lambda}_{jk|i} P_i(t) + 3\tilde{\lambda}_{k|ij} P_{ij}(t)
\end{cases}
$$

where $\lambda_{total} = 3\lambda_i + 3\lambda_{ij} + \lambda_{123}$ (II-96)

The first three of the transition equations in (II-96) are solved using a standard method of solving linear first-order differential equations. Assuming the following generic initial value problem,

$$
\frac{dy}{dx} + p(x)y = f(x) \qquad \text{with} \quad y(x_0) = y_0, \tag{II-97}
$$

its solution is given as

$$y(x)=\frac{1}{\mu(x)}\left[y_0+\int_{x_0}^{x}\mu(u)f(u)du\right] \quad \text{with} \quad \mu(x)=\exp\left(\int_{x_0}^{x}p(u)du\right). \tag{II-98}$$

Written in the same form as the generic initial value problem, the transition equation for state 0 becomes (II-99),

$$\frac{dP_0(t)}{dt}+\lambda_{total}P_0(t)=0, \tag{II-99}$$

and its solution is given as

$$P_0(t)=\frac{1}{\mu(t)}\left[\tilde{P}_0+\int_0^t\mu(u)(0)du\right]=\tilde{P}_0\exp\left\{-\int_0^t\lambda_{total}du\right\}. \tag{II-100}$$

Likewise, state $i$'s transition equation and solution can be shown in Equation (II-101).

$$\begin{aligned}
&\frac{dP_i(t)}{dt}+\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)P_i(t)=\lambda_iP_0(t)\\
&P_i(t)=\frac{1}{\mu(t)}\left[\tilde{P}_i^{(1)}+\int_0^t\mu(\tau)\lambda_iP_0(\tau)d\tau\right]\\
&=\exp\left\{-\int_0^t\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}\left[\tilde{P}_i^{(1)}+\int_0^t\lambda_iP_0(\tau)\exp\left\{\int_0^\tau\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}d\tau\right]\\
&=\exp\left\{-\int_0^t\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}\tilde{P}_i^{(1)}+\int_0^t\lambda_iP_0(\tau)\exp\left\{-\int_\tau^t\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}d\tau\\
&=\tilde{P}_i^{(1)}\exp\left\{-\int_0^t\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}+\tilde{P}_0\int_0^t\left(\lambda_i\exp\left\{-\int_0^\tau\lambda_{total}du-\int_\tau^t\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}\right)d\tau
\end{aligned} \tag{II-101}$$

It should be noted here that Equation (II-101) above uses the following relation to arrive at its line 4

$$\exp\left\{-\int_\tau^t\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}=\exp\left\{\int_0^\tau\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du-\int_0^t\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}. \tag{II-102}$$

State $ij$'s transition equation is written in the same form as the generic initial value problem, and solved for in a similar manner, as in Equation (II-103).

$$
\begin{aligned}
&\frac{dP_{ij}(t)}{dt}+\tilde{\lambda}_{k|ij}P_{ij}(t)=\lambda_{ij}P_0(t)+2\tilde{\lambda}_{j|i}P_i(t)\\
&P_{ij}(t)=\frac{1}{\mu(t)}\left[\tilde{P}_{ij}^{(2)}+\int_0^t\mu(\tau)\left(\lambda_{ij}P_0(\tau)+2\tilde{\lambda}_{j|i}P_i(\tau)\right)d\tau\right]\\
&=\exp\left\{-\int_0^t\tilde{\lambda}_{k|ij}du\right\}\left[\tilde{P}_{ij}^{(2)}+\int_0^t\left(\lambda_{ij}P_0(\tau)+2\tilde{\lambda}_{j|i}P_i(\tau)\right)\exp\left\{\int_0^\tau\tilde{\lambda}_{k|ij}du\right\}d\tau\right]\\
&=\exp\left\{-\int_0^t\tilde{\lambda}_{k|ij}du\right\}\tilde{P}_{ij}^{(2)}+\int_0^t\left(\lambda_{ij}P_0(\tau)+2\tilde{\lambda}_{j|i}P_i(\tau)\right)\exp\left\{-\int_\tau^t\tilde{\lambda}_{k|ij}du\right\}d\tau\\
&=\tilde{P}_{ij}^{(2)}\exp\left\{-\int_0^t\tilde{\lambda}_{k|ij}du\right\}+\int_0^t\left(\lambda_{ij}P_0(\tau)+2\tilde{\lambda}_{j|i}P_i(\tau)\right)\exp\left\{-\int_\tau^t\tilde{\lambda}_{k|ij}du\right\}d\tau\\
&=\tilde{P}_{ij}^{(2)}\exp\left\{-\int_0^t\tilde{\lambda}_{k|ij}du\right\}\\
&+\int_0^t\left(\begin{array}{l}\lambda_{ij}\tilde{P}_0\exp\left\{-\int_0^\tau\lambda_{total}du\right\}\\ +2\tilde{\lambda}_{j|i}\left[\begin{array}{l}\tilde{P}_i^{(1)}\exp\left\{-\int_0^\tau\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}\\ +\tilde{P}_0\int_0^\tau\left(\lambda_i\exp\left\{-\int_0^{\tau'}\lambda_{total}du-\int_{\tau'}^\tau\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du\right\}\right)d\tau'\end{array}\right]\end{array}\right)\exp\left\{-\int_\tau^t\tilde{\lambda}_{k|ij}du\right\}d\tau\\
&P_{ij}(t)=\tilde{P}_{ij}^{(2)}\exp\left\{-\int_0^t\tilde{\lambda}_{k|ij}du\right\}+\int_0^t\left(\lambda_{ij}\tilde{P}_0\exp\left\{-\int_0^\tau\lambda_{total}du-\int_\tau^t\tilde{\lambda}_{k|ij}du\right\}\right)d\tau\\
&+2\tilde{P}_i^{(1)}\int_0^t\left(\tilde{\lambda}_{j|i}\exp\left\{-\int_0^\tau\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du-\int_\tau^t\tilde{\lambda}_{k|ij}du\right\}\right)d\tau\\
&+2\tilde{P}_0\int_0^t\left(\tilde{\lambda}_{j|i}\int_0^\tau\left(\lambda_i\exp\left\{-\int_0^{\tau'}\lambda_{total}du-\int_{\tau'}^\tau\left(2\tilde{\lambda}_{j|i}+\tilde{\lambda}_{jk|i}\right)du-\int_\tau^t\tilde{\lambda}_{k|ij}du\right\}\right)d\tau'\right)d\tau
\end{aligned}
\qquad \text{(II-103)}
$$

The last state (7) equation can be put in the same form as the generic initial value problem and solved in a similar way. However there is no $\mu(t)$ term (because there are no transition rates leaving state 7) so this simplifies the calculation to an initial condition plus an integral over the possible state transitions that lead to state 7 (as seen in the last line of Equation (II-104)).

$$
\begin{aligned}
&\frac{dP_7(t)}{dt}=\lambda_{123}P_0(t)+3\tilde{\lambda}_{jk|i}P_i(t)+3\tilde{\lambda}_{k|ij}P_{ij}(t)\\
&P_7(T)=\frac{1}{\mu(T)}\left[\tilde{P}_7^{(3)}+\int_0^T\mu(t)\left(\lambda_{123}P_0(t)+3\tilde{\lambda}_{jk|i}P_i(t)+3\tilde{\lambda}_{k|ij}P_{ij}(t)\right)dt\right]\\
&=\tilde{P}_7^{(3)}+\int_0^T\left(\lambda_{123}P_0(t)+3\tilde{\lambda}_{jk|i}P_i(t)+3\tilde{\lambda}_{k|ij}P_{ij}(t)\right)dt
\end{aligned}
\qquad \text{(II-104)}
$$

When the state equation solutions (for states 0, $i$, and $ij$ shown in (II-100), (II-101), and (II-103), respectively) are inserted and FTL vs. FTR failure modes are specified, Equation (II-104) is identical to Equation (II-61) from Section II.3 (once the specific PDF equations are input to (II-61) and integrated).

**II.5 Hot Standby versus Cold Standby**

Sections II.2 through II.4 have shown how to develop both the NRI and Markov models for a hot standby system of EDGs; however, this section is for an EDG system in a cold standby arrangement. A simple example problem is presented in the following paragraph and modeled three different ways in Sections II.5.1 through II.5.3. The NRI and Markov models are modified to fit a cold standby system of EDGs in Sections II.5.1 and II.5.2, respectively. The (cold standby) convoluted distribution model for the example problem is presented in Section II.5.3. Finally, the results for all three models are compared in Section II.5.4.

The example problem is for a system composed of two EDGs that are operated in cold standby. Each EDG is subject to an individual running failure rate of 0.01 failures per hour, $\lambda_1$ and $\lambda_2$. There is no possibility of a CCF of both the EDGs. The first EDG is started with certainty (no demand failure) and run until failure, at which point the second EDG is started with certainty and run until failure.

**II.5.1 Non-Recovery Integral**

The models from Sections II.2 through II.4 have been developed for the case of a hot standby emergency AC power system, but the NRI can be modified to the cold standby case by simply replacing a couple of hazard function inputs and time variables in a system failure sequence PDF. When the component is subject to different failure types in certain time ranges (specifically failure to load and run (FTLR) for the first hour, and failure to run (FTR) after the first hour, as discussed in Chapter III), the cold-modified NRI provides a close approximation to the probability of system failure. The distinction between these two standby cases are shown below using the simple case of the general bivariate joint pdf, as first introduced in Equation (II-21) (each EDG is subject to a single failure but no CCF).

$$f(\tau,t)=\lambda_1(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)\right)du\right\}\tilde{\lambda}_2(t)\exp\left\{-\int_{\tau}^{t}\tilde{\lambda}_2(u)du\right\} \qquad \text{(II-105)}$$

Equation (II-105) is written for two EDGs (that both begin operating at time zero (when the LOOP first occurs); the EDGs fail sequentially and the first failure time variable is $\tau$ and the second is $t$. The probability that neither EDG fails from 0 to $\tau$ is captured by the factor $\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)\right)du\right\}$. A simple way to think about this is that the hazard functions in the exponential term describe the various failure options which could occur in the time period between the limits of integration. The hot standby system described by Equation (II-105) has both EDGs operating between time 0 and $\tau$, and either of these EDGs could potentially fail. For a cold standby system, the redundant EDG cannot fail while running until it is called upon after the first EDG failure and the above-mentioned factor should be switched to $\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)\right)du\right\}$ to reflect that.

The probability that the second failure occurs around some infinitesimal time $dt$ is $\tilde{\lambda}_2(t)dt$ and this is integrated from 0 to the hypothesized system failure time, $T$. When a time-dependent hazard function is used as this model input, it is important to correct for the fact that the EDG does not experience any wear out from 0 to $\tau$. This is done by changing the time variable for the second failure hazard function, as shown in $\tilde{\lambda}_2(t-\tau)$. Please note that $\tilde{\lambda}_2=\lambda_2$, since this example case does not consider CCF. The bivariate joint PDF for the case of a cold standby system is

$$f(\tau,t)=\lambda_1(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)\right)du\right\}\tilde{\lambda}_2(t-\tau)\exp\left\{-\int_{\tau}^{t}\tilde{\lambda}_2(u)du\right\}. \qquad \text{(II-106)}$$

Equation (II-106) is integrated as in Equation (II-107) to give the results presented in Section II.5.4.

$$F(T)=\int_0^T\int_0^t f(\tau,t)d\tau dt \qquad \text{(II-107)}$$

Both of the above bivariate joint PDFs are shown for cases which do not consider CCFs. For a hot standby system or a cold standby system with externally-caused CCFs, a CCF hazard function should be added to the first exponential term. For a cold standby system with component-caused CCF (assuming each EDG contributes one half to the probability of CCF), one

half of the CCF hazard function should be added to the first exponential term. These distinctions can be noted in the following three equations, respectively.

$$
\begin{aligned}
f(\tau,t) &= \lambda_1(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)+\lambda_{CCF}(u)\right)du\right\}\tilde{\lambda}_2(t)\exp\left\{-\int_{\tau}^{t}\tilde{\lambda}_2(u)du\right\} \\
f(\tau,t) &= \lambda_1(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_{CCF}(u)\right)du\right\}\tilde{\lambda}_2(t-\tau)\exp\left\{-\int_{\tau}^{t}\tilde{\lambda}_2(u)du\right\} \\
f(\tau,t) &= \lambda_1(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\tfrac{1}{2}\lambda_{CCF}(u)\right)du\right\}\tilde{\lambda}_2(t-\tau)\exp\left\{-\int_{\tau}^{t}\tilde{\lambda}_2(u)du\right\}
\end{aligned}
\qquad \text{(II-108)}
$$

A detailed description of both externally-caused and component-caused CCF can be found in Section III.3.3.

**II.5.1.1 Mixed (Hot and Cold) Standby Case Example**

Modeling a mixed case standby system (some EDGs are hot while others are cold standby) is explored in this section. Consider a system of three EDGs. Each EDG is subject to single running failures and no CCFs (the only way the system fails is from three consecutive single failures). The single failure rates are expressed as $\lambda's$ with subscript numbers to denote the specific EDG. The EDGs fail sequentially and the first failure time variable is $\tau$, the second is $t'$, and the third is $t$. The joint PDFs in this section are shown for the failure sequence where EDG "1" fails first, followed by EDG "2", and then finally EDG "3" fails. The multivariate joint PDF for the case of a purely hot standby arrangement is shown below in Equation (II-109).

$$
\begin{aligned}
f(\tau,t',t) = \lambda_1(\tau)&\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)+\lambda_3(u)\right)du\right\} \\
&\times\lambda_2(t')\exp\left\{-\int_{\tau}^{t'}\left(\lambda_2(u)+\lambda_3(u)\right)du\right\}\times\lambda_3(t)\exp\left\{-\int_{t'}^{t}\lambda_3(u)du\right\}
\end{aligned}
\qquad \text{(II-109)}
$$

Using the same concepts developed in Section II.5.1, Equation (II-109) is modified to fit two different cold standby cases for this EDG system. The first modified case is for EDGs "1" and "2" in hot standby while EDG "3" is in cold standby. The multivariate joint PDF for this case is shown below, in Equation (II-110).

$$
\begin{aligned}
f(\tau,t',t) = \lambda_1(\tau)&\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)\right)du\right\} \\
&\times\lambda_2(t')\exp\left\{-\int_{\tau}^{t'}\lambda_2(u)du\right\}\times\lambda_3(t-t')\exp\left\{-\int_{t'}^{t}\lambda_3(u)du\right\}
\end{aligned}
\qquad \text{(II-110)}
$$

The second modified case is for EDG "1" in hot standby while EDGs "2" and "3" are in cold standby. The multivariate joint PDF for this case is shown below in Equation (II-111).

$$f(\tau,t',t)=\lambda_1(\tau)\exp\left\{-\int_0^{\tau}\lambda_1(u)du\right\}\times\lambda_2(t'-\tau)\exp\left\{-\int_{\tau}^{t'}\lambda_2(u)du\right\}$$
$$\times\lambda_3(t-t')\exp\left\{-\int_{t'}^{t}\lambda_3(u)du\right\} \quad \text{(II-111)}$$

**II.5.2 Markov**

The state transition equations for the (cold standby system) Markov model is shown in Equation (II-112)

$$\begin{cases}\dfrac{dP_0(t)}{dt}=-\lambda_1P_0(t)\\ \dfrac{dP_1(t)}{dt}=\lambda_1P_0(t)-\lambda_2P_1(t)\\ \dfrac{dP_2(t)}{dt}=\lambda_2P_1(t)\end{cases} \quad \text{(II-112)}$$

At time equals zero, the system starts in state 0 with certainty. In state 0, EDG 1 runs while EDG 2 is in cold standby. EDG 1 can fail which brings the system into state 1 where EDG 2 begins running. When EDG 2 fails, the system transitions to the absorbing state 2. The probability of system failure is the solution to $P_2(t)$ and these results are presented in Section II.5.4. These results were obtained by solving the system of equations seen in (II-112) using the ode45 function in MATLAB [32] (based on an explicit Runge-Kutta (4,5) formula, the Dormand-Prince pair).

**II.5.3 Convoluted Distribution**

Part of the SPAR model has a technique called the convoluted distribution method which is for components in hot standby. The convoluted distribution model that is adapted here is for a cold standby system, is taken from [33], and is quoted as follows:

"The failure probability density for the $i$th and all prior units, $f_{12\ldots i}(t)$, may be expressed in terms of that for the $(i-1)$th unit and all prior units, as the convolution of two failure probability densities:

$$f_{12\ldots i}(t)=\int_0^t f_i(t-t')f_{12\ldots(i-1)}(t')\,\mathrm{dt'''} \quad \text{(II-113)}$$

In this equation, the failure probability density for the $i$th unit, $f_i(t-t')$, accounts for the system failure probability density for the time $(t-t')$ during which the $i$th unit is in operation,

while the $f_{12\ldots(i-1)}(t')\mathrm{d}t'$ accounts for the failure probability of the $(i-1)$th unit in $dt'$ about time $t'$ after all other units $j, j<(i-1)$, have failed. The integration over the time of failure $t'$ of the $(i-1)$th unit ranges from 0 to $t$ because the actual time of the $i$th failure can occur any time between 0 and $t$.

Equation (II-113) can be written in the form of nested integrals by recursively applying the equation. The result is

$$f_{12\ldots\mathrm{i}}(t)=\int_0^t dt_{i-1}f_i(t-t_{i-1})\int_0^{t_{i-1}}dt_{i-2}f_{i-1}(t_{i-1}-t_{i-2})\ldots \\ \times\int_0^{t_2}dt_1f_2(t_2-t_1)f_1(t_1). \tag{II-114}$$

The system failure probability density function is obtained from the general equation for a system of *n* components as in Equation (31) of [22]. For the specific example system consisting of two EDGs, the system failure PDF is shown in Equation (II-115)

$$f_{12}(t)=\int_0^t f_2(t-t')f_1(t')\mathrm{d}t' \tag{II-115}$$

The EDGs have identical and constant failure rates. The failure time PDFs for the EDGs are equal and can be seen in Equation (II-116) (as from Equation (34) of [22]).

$$f_1(t)=f_2(t)=\lambda\exp(-\lambda t) \tag{II-116}$$

The individual failure time PDFs of Equation (II-116) are input to the system failure time PDF of Equation (II-115) and this is integrated to obtain the results shown in Section II.5.4.

$$F_{12}(T)=\int_0^T\int_0^t\lambda_2\exp(-\lambda_2(t-t'))\lambda_1\exp(-\lambda_1t')\mathrm{d}t'\,dt \tag{II-117}$$

**II.5.4 Results Comparison**

The results for the models developed in Sections II.5.1 through II.5.3 are presented in Table 1. This result comparison is meant to confirm that the modified NRI (Equation (II-107)) and the convolution method are both modeling a cold standby system. The results for these two models are compared against the results for the well-known Markov model.

**Table 1 – Results for Simple Cold Standby System.**

| T (hrs) | NRI | Markov | Convolution |
|---|---|---|---|
| 0 | 0.000E+00 | 0.000E+00 | 0.000E+00 |
| 50 | 9.020E-02 | 9.020E-02 | 9.020E-02 |
| 100 | 2.642E-01 | 2.642E-01 | 2.642E-01 |
| 200 | 5.940E-01 | 5.940E-01 | 5.940E-01 |

Table 1 shows that the results agree relatively well. Table 2 shows the difference between the results. There is no difference between the results of the NRI and convolution method. The small amount of difference between these results (NRI and convolution method) and the results of the Markov model is likely due to numerical approximations of the ode45 function in MATLAB (which was used to evaluate Equation (II-112)).

**Table 2 – Difference between Results.**

| T (hrs) | NRI-Convolution | NRI-Markov |
|---|---|---|
| 0 | 0.000E+00 | 0.000E+00 |
| 50 | 0.000E+00 | -1.185E-10 |
| 100 | 0.000E+00 | -4.582E-09 |
| 200 | 0.000E+00 | -1.006E-07 |

# CHAPTER III

# DATA

In this chapter, data are introduced that will later be used as inputs to the case study models of Chapter IV. These model input parameters are intended to represent an industry averaged EDG probability or rate of failure with distinctions between failure mode and possible CCF groups. The Risk Assessment of Operational Events (RASP) Handbook was used to aid in parameter development [29]. This handbook was created with the main objective to "document methods and guidance that NRC staff could use to achieve more consistent results when performing risk assessments of operational events", and a secondary objective "to provide analysts and SPAR model developers with additional guidance to ensure that the SPAR models used in the risk analysis of operational events represent the as-build, as-operated plant to the extent needed to support the analyses". The RASP Handbook references [34], which provides the basic event classification scheme as well as the alpha factor model used to estimate these basic event frequencies. The two types of inputs to the alpha factor model are a total unreliability estimate for a single component ($Q_t$) and the alpha factors ($\alpha_k^m$) (where *k* and *m* denote the number of components failed and the total number in the common-cause group; this is explained further in Section III.3).

As prescribed by the RASP Handbook, component unreliability estimates were obtained from [30], and complimentary alpha factor estimates were obtained from [31]. Both of these sources have parameter estimates for the same three failure modes; failure to start (FTS), failure to load and run (FTLR), and failure to run (FTR). It is this division of failure modes that drives some of the model development in Chapter. For the models presented in this thesis, an EDG is subject to three different basic event types. First, the EDG may experience a demand based (probability data) FTS at time t=0. If instead the component successfully starts, it may experience a time based (rate data) FTLR from 0<t<1 hour or a FTR for times greater than 1 hour. The use of data for FTLR events is slightly different than presented in [30]; this difference is explained in Section III.2.2.

The component unreliability estimates used represent the total frequency (include both individual and coincident hazard contributions) of the specified failure mode as averaged throughout the industry, and are not tailored to any one specific EDG group size. The alpha factor estimates however do depend on group size and thus provide a means to distinguish between single and coincident failures.

It is worth noting that the model parameters developed using NRC guidance and data sources for continuous (or running) failures are constant rates. The models developed in Sections II.2 and II.3, however, can handle time-dependent hazard functions (under certain conditions), although this type of component failure data are not used or available for nuclear PRA applications at this time.

**III.1 EDG Component Boundary**

The component boundary encompasses the set of piece parts that are considered to form the component. The definition of this boundary dictates which failure event data are used to estimate parameters. The EDG boundary definition found in [30] is slightly different from the one used in [31]. One would think these component boundaries should be the same since the RASP Handbook recommends using these two data sources to obtain the basic event frequency estimates. These slight differences in boundary are noted here, but no data correction is employed.

The following excerpt from [30] describes what is included inside the EDG boundary:

"The EDG boundary includes the diesel engine with all components in the exhaust path, electrical generator, generator exciter, output breaker, combustion air, lube oil systems, fuel oil system, and starting compressed air system, and local instrumentation and control circuitry. However, the sequencer is not included. For the service water system providing cooling to the EDGs, only the devices providing control of cooling flow to the EDG heat exchangers are included. Room heating and ventilating is not included. [30]"

The following list from [34] is valid for the parameter estimates presented in [31]; it describes the sub-components that make up the EDG component, as well as the smaller parts that make up each sub-component:

- Battery
- Breaker

- Logic circuit, relay, switch

- Cooling
  - Miscellaneous, valve, heat exchanger, pump, piping
- Engine
  - Piping, valve, turbocharger, shaft, piston, miscellaneous, governor, fuel rack, fuel nozzles, bearing, sensors
- Exhaust
  - valve
- Fuel oil
  - Fuel rack, strainer, tank, valve, pump, miscellaneous, piping
- Generator
  - Casing, generator excitation, load sequencer, logic circuit, power resistor, relay, rotor, voltage regulator
- Instrumentation & control
  - Instrumentation, fuse, governor, load sequencer, miscellaneous, piping, relay, sensors, valve, voltage regulator, generator excitation
- Lube oil
  - Tank, check valve, heat exchanger
- Starting
  - Valve, strainer, miscellaneous, motor

The main difference between these boundaries is that [34] includes the sequencer and room HVAC in the EDG piece-parts, while [30] does not.

**III.2 Component Unreliability Data**

Component unreliability estimates were obtained from [30]. This type of estimate can be viewed as a representative-averaged total probability of failure for a single component. These estimates are independent of group size and do not make distinctions for common-cause events; instead they are concerned with capturing all failure events for a given component type and failure mode in order to reduce statistical uncertainty. In fact, the most basic maximum likelihood estimate (MLE) used to estimate these component reliabilities from data are simply

the ratio of total number of failures (for a specific component type and failure mode) to the total number of demands (or run time) for the same type and mode. The parameter estimates in [30] were obtained by applying the standard estimation methods as documented in [35].

The unreliability estimates used in this thesis are the industry averaged median point value for each failure mode, as shown in Table 3 (Table A.2.17-6 of [30]). The unreliability estimates for FTS and FTLR are both failure on demand probabilities, while the estimate for the FTR event is a failure rate.

**Table 3 – Industry Average Unreliability Estimates (reprinted with permission from [30]).**

| Failure Mode | Source | 5% | Median | Mean | 95% | Distribution | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Type | α | β |
| FTS | EB/PL/KS | 2.77E-04 | 3.24E-03 | 4.53E-03 | 1.32E-02 | Beta | 1.075 | 2.363E+02 |
| FTLR | EB/PL/KS | 3.07E-04 | 2.25E-03 | 2.90E-03 | 7.69E-03 | Beta | 1.411 | 4.856E+02 |
| FTR | EB/PL/KS | 1.52E-04 | 7.12E-04 | 8.48E-04 | 2.01E-03 | Gamma | 2.010 | 2.371E+03 |

These distributions were obtained from data pooled at the plant level. This means the adjusted EPIX data for all the EDGs at each plant were combined to get representative EDG data for each individual plant; EPIX data are discussed further in Section III.2.1. Next, MLEs were computed at the plant level for the three failure modes. An estimate for this FTS mode was computed by dividing all the EDG FTS events for a specific plant by all the EDG start demands at that same plant. The MLE for the FTLR probability was computed in the same way, while the MLE for the FTR rate was computed similarly but with runtime hours in the numerator instead of demands. Once MLEs were computed for each plant, this data were fit to a distribution. Empirical Bayes analyses with a Kass-Steffey adjustment were used to characterize the distributions; the details for this adjustment can be found on page 8-6 of [35]. For the entirety of [30], demand failures are fit to a Beta distribution, while running failures are fit to a Gamma distribution. This is due partly to the data fitting well, and partly because Bayesian updating is very straightforward when using these distributions [35].

### III.2.1 Raw Data Collection and Review

The raw data used to estimate the EDG failure parameters come from the EPIX database, as processed using the Reliability and Availability Data System (RADS) analysis tool (as explained in Section 4.1.3.3 of [35]). The data come from events that occurred from 1998-2002, and involves 225 EDGs from 95 plants. The EPIX database provides failure data at the component level, so this needs to be appropriately pooled to obtain industry average parameter estimates. A routine in RADS was used to search through reportable events logged in EPIX in order to obtain and group the FTS and FTR failure modes [35].

A process was used in [30] to subdivide the FTR mode from EPIX into FTLR≤1 hour and FTR>1 hour failure modes. This was done because the journal article, "Historical perspective on failure rates for US commercial reactor components" [36], indicates that there is approximately a factor of 15 difference between failure rates for these two subdivisions. The process used to make this subdivision is approximate because failure records in EPIX often fail to include the operating time of a component before it had a FTR event. The process used, taken directly from page 27 of [30], is the following:

1. Sort the components by run hours/demand, from lowest to highest.
2. Add cumulative columns to the sorted component list indicating the total component demands and total component hours (up through the component being considered).
3. Identify within this sorted list the component where the cumulative run hours divided by cumulative demands equals 1.0. The subset of components up through this component has an average of one hour of run time per demand.
4. Calculate the FTR≤1H rate from the subset of components identified, using their run hours and FTR events.
5. Use the remaining components to calculate FTR>1H. However, the FTR event total from these other components is reduced by the expected number of FTR≤1H events. (The expected number of FTR≤1H events is just the number of demands for this group times the FTR≤1H rate.) Also, the run hours in this group are reduced by the number of demands. In cases where the modified FTR>1H event total was negative, it was assumed that there were no FTR>1H events.

At this point, raw data from EPIX have been processed so that each of the 225 total EDGs has a count of FTS, FTLR, and FTR events, as well as the associated demands and failures [30]. Next, data were grouped at the plant level (data from multiple EDGs at a plant are combined to give representative EDG data for that plant) and reviewed in order to spot any anomalies [30]. This review indicated that several plants had unreasonably low start and/or load and run demands. In order for an EDG to attempt to load, it must have successfully started. However, when an EDG fails to start, it experiences a start demand but not a load demand. Thus the EDGs start demands must be greater than the load demands. Likewise, the same thinking applies for run events, where load demands must be greater than run demands. Because this review indicated some plants had too high load and run demands, the following data processing routine from [30] was used to find and modify this illogical data. If the load and run demands were greater than the start demands, then they were set equal to each other. However, if the load and run demands were less than 75% of the start demands, then they were changed to 75% of the start demands.

**III.2.2 Modified Use of FTLR Data**

Reference [30] presents the FTLR data as a failure on demand at one hour. The way these data were obtained, however, does not indicate that a FTLR is actually a failure on demand. As described in the numbered process in Section III.2.1, the FTLR event data were obtained as the lowest run hour grouping of FTR events that had an average duration of 1 hour. This means the FTLR events occurred after a successful start on demand and after running for an average of 1 hour. At the 1 hour mark, the FTLR events did not suddenly occur on demand as the presented FTLR demand failure probabilities suggest. In the Chapter IV models, the FTLR data are used as rates for a failure event that can occur after a successful start and before time equals 1 hour. Using the FTLR data as a demand probability at 1 hour versus a failure rate from 0 to 1 hour has the largest difference of results for mission times between 0 and 1 hour. All of the model cases presented in Chapter IV are concerned with much larger mission times, and this slight misuse of data from how [30] originally intended does not have a large impact on the model results.

**III.3 CCF Data and the Alpha Factor Model**

This thesis uses the alpha factor method as a convenient way to compute individual and coincident failure parameters using component, total-unreliability data obtained from [30].

Alpha factors from [31] provide a means to estimate how CCF groups occur. An alpha factor ($\alpha_k^m$) is defined as the fraction of total failure events that involve *k* component failures, for a common-cause component group (CCCG) of *m* identical components [34]. For example, $\alpha_2^3$ is defined as the ratio of total number of CCF events involving two components in a CCCG of size three, to the total number of all failure events for the same group.

With Equation (III-1) from the alpha factor method (as presented in [34]), both single and coincident event parameters can be computed for each failure mode. More specifically, Equation (III-1) computes the probability (or rate) of a basic event involving *k* specific components out of a group sized *m*.

$$Q_k^{(m)} = \frac{m}{\binom{m}{k}} \frac{\alpha_k^{(m)}}{\alpha_t} Q_t \qquad \text{(III-1)}$$

Here,

$Q_t$ = The total failure frequency of each component (includes single and coincident failures),

$\alpha_k^m$ = The fraction of the total frequency of failure events that occur in the system involving the failure of *k* components in a system of *m* identical components, and

$\alpha_t = \sum_{k=1}^{m} k\alpha_k^{(m)}$.

The following section will use an example to further define alpha factors and show how they are related to basic event frequencies.

**III.3.1 Basic Failure Events**

The model inputs are the demand failure probabilities and hazard functions for the EDGs. These inputs are determined from a common-cause probability model, specifically the alpha factor model (as explained on page 70 of [34]). The following example should explain the logic of the model and illustrate how a single EDG can be subject to various basic failure events. This example borrows heavily from concepts developed in Section 3.3 of [37].

Consider a system of three components called A, B, and C. All the basic failure events for component A are defined as one of the following types:

$A_I$ = Independent failure of A ; $C_{AB}$ = coincident failure of both A and B

$C_{AC}$ = coincident failure of both A and B ; $C_{ABC}$ = coincident failure of A, B, and C

These failure events partition the failure space of component A based on the impact the event had to other components in the group. Thus these events are mutually exclusive.

The components are assumed to be identical so that probabilities of similar basic events are equal as follows:

$$\begin{aligned} P(A_I) = P(B_I) = P(C_I) &= Q_1^{(3)}, \\ P(C_{AB}) = P(C_{BC}) = P(C_{AC}) &= Q_2^{(3)}, \\ P(C_{ABC}) &= Q_3^{(3)}. \end{aligned} \tag{III-2}$$

Therefore a basic event probability is defined in general as:

$Q_k^{(m)}$ = probability of a basic event involving *k* specific components, out of a group of *m* identical components.

The total failure probability (or rate) of A in this group of three similar components is the sum of every basic event probability (or rate) which involves component A. This is shown in Equation (III-3).

$$P(A_{total}) = P(A_I) + P(C_{AB}) + P(C_{AC}) + P(C_{ABC}) = Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)} \tag{III-3}$$

Because the group of components is assumed to be similar, this can be expressed in general as,

$$P(A_{total}) = Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)}, \tag{III-4}$$

where $Q_t$ is the total failure frequency and its estimate is obtained from [30]. The binomial coefficient in Equation (III-4) represents the number of specific failure event types that will fail component A; only one independent or 3-out-of-3 CCF event will fail component A, while two different 2-out-of-3 CCF events will also fail component A. Alpha factors are defined in terms of basic event frequencies as,

$$\alpha_k^{(m)} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)}}, \qquad \text{(III-5)}$$

where

$\binom{m}{k} Q_k^{(m)}$ = the total frequency of events involving any k component failures, in a group of m components.

The denominator of Equation (III-5) is the sum of these frequencies, and includes every basic event that may occur in the group as a whole for the specific failure mode in question. Going back to the three component sized group example, Equation (III-6) defines $\alpha_2^{(3)}$ in terms of basic event frequencies

$$\alpha_2^{(3)} = \frac{3Q_2^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}} = \frac{P(C_{AB}) + P(C_{AC}) + P(C_{BC})}{P(A_I) + P(B_I) + P(C_I) + P(C_{AB}) + P(C_{AC}) + P(C_{BC}) + P(C_{ABC})} \qquad \text{(III-6)}$$

The above shows how alpha factors are defined, but this formulation is somewhat the reverse of how they are actually used. However, alpha factor parameters are estimated in a similar manner. Reference [34] uses the ratio of the total number or CCF events to the total number of failure events to create MLEs (which its parameter estimate distributions are based on).

**III.3.2 Alpha Factor Estimation**

Distributions of alpha factors are estimated using impact vectors. Impact vectors are numerical quantifications of sometimes ambiguous event report data, and they facilitate the statistical analysis used to estimate alpha factors. Some details for how event reports are translated to impact vectors via data analysis are explained in the following paragraphs. For more detail, please refer to Section 7 of [34].

Impact vectors are a convenient way to classify a CCF event using numerals. For a group of *m* components, the impact vector is a *m*+1 dimensional vector. The *i*th component in this vector corresponds to how the number of components (*i*-1) affected in an event; 0 represents no failure and 1 represents failure. Their meaning is explained well by this example from [34]:

"Consider a component group of size 2. Possible impact vectors are the following:

- [1, 0, 0] No components failed.
- [0, 1, 0] One and only one component failed.
- [0, 0, 1] Two components failed due to a shared cause."

Sometimes uncertainty lies in the exact cause of a failure or an event report provides insufficient detail. If two or more possible impact vector classifications of an event could exist, the data analyst may compute a weighted average impact vector to classify the event. This is shown in Figure 5.

| | |
|---|---|
| Event Description: | Main Yankee, August 1977. Plant at power. Two diesel generators failed to run due to plugged radiators. The third unit radiator was also plugged. |
| Failure Mode: | Fail to Run |
| Common-cause Component Group Size: | 3 |

| Hypothesis | Probability | Elements of Impact Vector | | | |
|---|---|---|---|---|---|
| | | $F_0$ | $F_1$ | $F_2$ | $F_3$ |
| Two of three components fail | 0.9 | 0 | 0 | 1 | 0 |
| All three components fail | 0.1 | 0 | 0 | 0 | 1 |
| Average Impact Vector ( $\bar{I}$ ) | | $\overline{F_0}$ | $\overline{F_1}$ | $\overline{F_2}$ | $\overline{F_3}$ |
| | | 0 | 0 | 0.9 | 0.1 |

**Figure 5 – Example for Average Impact Vector Estimation (reprinted with permission from [34]).**

Some events are even more ambiguous and require additional techniques to compute their impact vector. They generally fall into three categories, as follows (taken directly from page 59 of [34]):

1. Events involving degraded component states

2. Events involving multiple component failures closely related in time but not simultaneously
3. Events involving multiple failures for which the presence of a shared cause cannot be established with certainty.

These techniques are explained fully in Section 7.2, "Generic Impact Vector Assessment," of [34].

CCF event frequenies can be estimated from impact vectors, as in Equation (III-7),

$$n_k = \sum_{i=1}^{m} \overline{F}_k(i), \tag{III-7}$$

where,

$n_k$ = total number of basic events involving failure of k similar components,
$m$ = number of elements in the CCCG,
$\overline{F}_k(i)$ = the $k^{th}$ element of the average impact vector for event I.

Finally, the maximum likelihood estimator for the alpha factor parameters can be seen in Equation (III-8).

$$\hat{\alpha}_k = \frac{n_k}{\sum_{j=1}^{m} n_j} \tag{III-8}$$

Reference [34] acknowledges that its CCF parameter estimation techniques were first developed in more detail in Volumes I and II of NUREG/CR-4780, reference [37] and [38] respectively. For more detail on how alpha factor parameter distributions are obtained please refer to Appendix E in [38].

**III.3.3 Types of CCF**

Reference [34] dictates and explains the CCF parameter estimation efforts by the NRC. On page 5, this reference acknowledges that "the definition of a CCF is closely tied to an understanding of the nature and significance of dependent events" [34]. It then goes on to classify types of dependencies; "In this classification, dependencies are first categorized based on whether they stem from intended intrinsic functional and physical characteristics of the system or are caused by external factors and unintended characteristics. Therefore, the dependence is either intrinsic or extrinsic to the system" [34]. The main classification

distinction made here is that “an intrinsic dependency refers to cases where the functional status of one component is affected by the functional status of another component”, while “extrinsic dependency refers to cases where the dependency or coupling is not inherent or intended in the functional characteristics of the system. The source and mechanism of such dependencies are often external to the system” [34]. Reference [34] acknowledges that intrinsic dependencies should be “modeled explicitly in the logic model (e.g., fault tree) of the system”. It also says that while many extrinsic dependencies should be modeled this way, “there are a large number of extrinsic mechanisms that are unpredictable (or misunderstood) and cannot be modeled” [34]. In these cases or when the mechanisms are understood but it is not cost effective to model explicitly, “the combined probabilistic effect of dependencies is treated parametrically. This means that these types of events are treated together as one group known as CCFs” [34]. Reference [34] provides the guidelines for parameter estimation that are used in the CCF Parameter Estimations updates (currently [31]), thus this definition for CCFs was applied when evaluating event data and estimating the alpha factors that are presented in [31].

However, this definition for the types of CCF events that should be modeled with CCF parameters does not mesh well with the model objectives in this thesis. The models presented here do not attempt to model CCF dependencies of the EDGs explicitly in the logic model, but instead acknowledges the randomness of these events and treats them parametrically; these models also acknowledge that the EDGs are not only subject to extrinsic dependencies. The ultimate application of this thesis is to determine the level of improved safety margin from adding a hardened EDG to a location separate from the other normal onsite EDGs. This additional EDG would still be subject to some extrinsic dependencies, but the fact that it is in a hardened structure at a high elevation would reduce the likelihood of it taking damage from an external flooding event, for example (see Section I.2.3 for more details). The additional hardened EDG would be physically separated from the other EDGs and would not share any connections, thus the possibility of an intrinsic dependency event affecting all EDGs is eliminated. For example, if some root cause affects a single EDG in such a way that it fails explosively, this explosion could in turn fail another EDG that is housed nearby. This type of event would be very difficult to model explicitly, so parametric treatment of this possible CCF is

needed. However, the additional EDG, its location, and support systems have all been designed against these types of intrinsic dependencies. As such, a slightly different classification of CCF events are adopted here and used to modify some of the CCF parameters. This scheme was adopted from reference [39]. This scheme divides CCFs into two classes, externally-caused and component-caused CCFs; the following Section III.3.3.1 will explain the differences between these two types of CCF events in more detail.

**III.3.3.1 Externally-Caused and Component-Caused CCF**

Vaurio [39] makes the distinction between extrinsic and intrinsic dependencies and asserts that CCF parameters should only be used to model the extrinsic dependencies that cannot be modeled explicitly. The focus of [39], however, "is on CCFs that occur at random times and are properly modeled by general multi-failure rates (GMFR) $\lambda_{k/n}$, i.e. frequencies of events failing specific *k* out of *n* components" [39]. It should be noted here that the term $\lambda_{k/n}$ is equivalent to $Q_k^{(m)}$ in Equation (III-1). Vaurio argues that certain types of intrinsic dependencies (specifically cascading component failures) should be modeled using CCF parameters, and it provides some of the logic to do this using available data. The focus of this article is the problem of how to combine failure data from dissimilar plants, as expressed in the following quote:

"One general problem is that failure events observed at one or few plants are not generally sufficient to estimate the basic parameters. Assimilating experience from other plants is essential. It is complicated by the fact that other plants (source plants) may have different numbers $n=n'$ of redundant components compared to the target plant of interest which has the common-cause component group (CCCG) size $n=n_0$. Lay-out, design and component separation principles are often different in families of plants with different degrees of redundancy. When $k'$ components failed at a plant with CCCG size $n'$, it is not clear at all how relevant that event is to another plant with CCCG size $n'$. A safe way is to use data only from source plants that have the same degree of redundancy, $n_0$. However, if one wants to use data from plants with different values of $n$, one has to make assessments about how likely the cause event would occur at the target plant, and conclude how many would have failed if the plant had $n$ equal to $n_0$ instead of $n'$, and had separation principles similar to the target plant."

The article makes the distinction between the two different sets of CCF mechanisms and assumptions, as expressed in the following paragraph (taken directly from [39]).

"The first set of mapping-down rules can be obtained assuming externally-caused CCFs, and assuming that the plants with $n-1$ trains are similar to the plants with $n$ trains, with one component removed. 'Similarity' here means that all cause events occur with the same frequency and have equal consequences, i.e. the cause events fail existing components equally likely at both families of plants."…"The second set of mapping-down rules has been developed for cascading failures or component-caused CCFs, meaning that a single component failure causes other components to fail with certain probabilities. Furthermore, it is assumed that plants with $n-1$ trains have the same single failure rates and the same failure propagation probabilities as the plant with $n$ trains."

It should be noted here that these rules are intended for combining failure data from plants with different numbers of CCCGs and that "both sets of rules assume identical design, separation, operations and maintenance principles in plants with different CCCG sizes $n$" [39]. This thesis uses these rules to compute its "influenced" failure rates, a concept that is explored at the end of this chapter. These "influenced" rates are essentially an adjusted failure event rate considering that some component(s) has already failed.

The mapping-down rules from [39] for CCF rates are used here. The general mapping-down equation for externally-caused CCF rates can be seen in Equation (III-9). The examples given for this type of event are "shocks like lightning or maintenance actions to hit subgroups of components" [39]. Essentially, the CCF cause comes from something external to the CCCG.

$$\lambda_{k/n-1} = \lambda_{k/n} + \lambda_{k+1/n}, \quad \text{for } k = 1,2,...,n-1 \tag{III-9}$$

Figure 6 illustrates how to map down from a system of $n=2$ to $n=1$ by obtaining the effective rate $\lambda_{1/1} = \lambda_{1/2} + \lambda_{2/2}$.

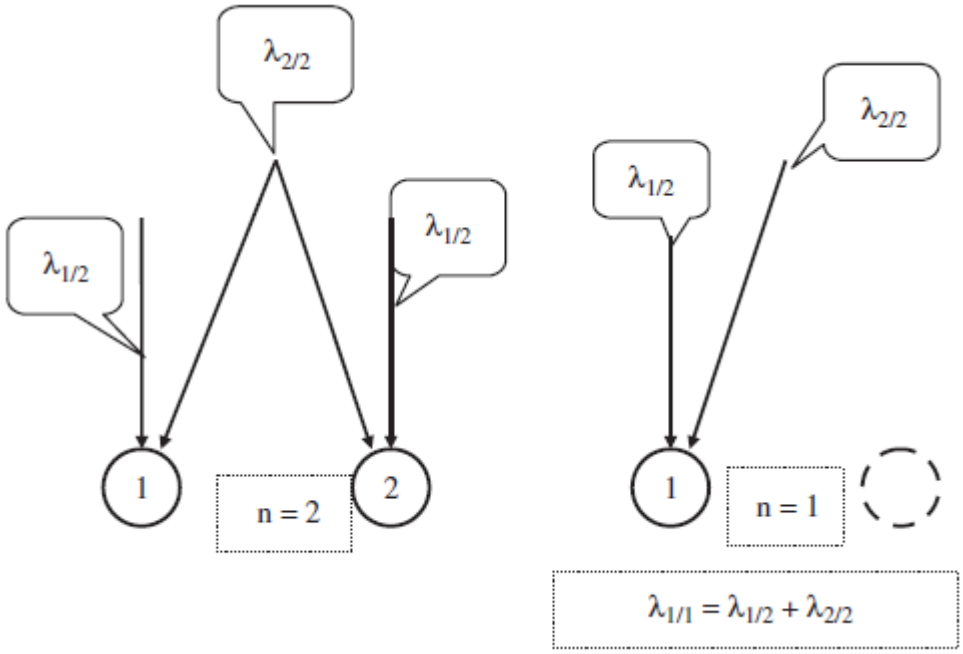


**Figure 6 – Mapping-Down from a Two- to One-EDG System, for Externally-Caused CCF (reprinted with permission from [39]).**

The general mapping-down equation for component-caused CCF rates can be seen in Equation (III-10). This rule is "based on the assumption that all $k/n$-events initiate as a failure of one of the components, and the failure can propagate to one or more other components, with some probabilities" [39]. For this type of event, the CCF cause initiates from a single component failure and then cascades to other components inside the CCCG.

$$\lambda_{k/n-1} = \lambda_{k/n} + \frac{k}{k+1}\lambda_{k+1/n}, \quad \text{for } k = 1,2,\ldots,n-1 \qquad \text{(III-10)}$$

Figure 7 illustrates how to map down from a system of $n=2$ to $n=1$ by obtaining the effective rate $\lambda_{1/1} = \lambda_{1/2} + \frac{1}{2}\lambda_{2/2}$.

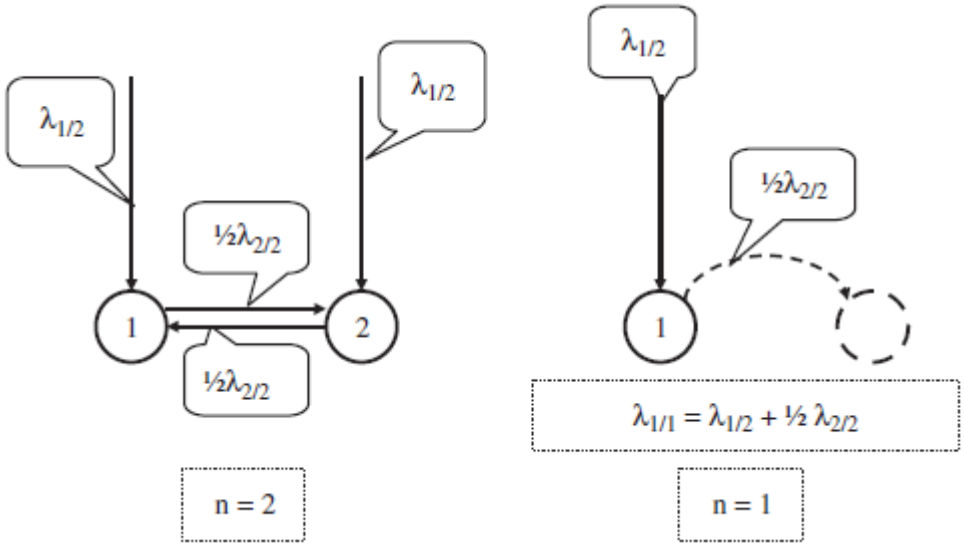


**Figure 7 – Mapping-Down from a Two- to One-EDG System, for Component-Caused CCF (reprinted with permission from [39]).**

### III.3.3.2 Alpha Factor Test

It is important to understand if the alpha factor estimates provided in [31] are given for externally-caused, component-caused, or both types of CCF events. Unfortunately [31] does not explicitly state this assumption, but Vaurio [39] states that "mapping rules of externally-caused CCF were applied already when the alpha-values were estimated in NUGEG/CR-5497 [40]". Reference [40] was the first "Common-Cause Failure Parameter Estimations" report issued by the NRC in 1998. The current update to this report is "CCF Parameter Estimations, 2012 Update" [31] and it is assumed that these alpha factors are also estimated using externally-caused CCF event rules. This assumption can be verified by using Equations (III-9) and (III-10), as shown in the mathematical check below.

Reference [30] does not mention group size when it reports the total unreliability estimates for single components ($Q_t$'$s$) so we assume these estimates are independent of group size (this alone hints at the externally-caused nature of alpha factor method). Because $Q_t$ is independent of group size, as the CCCG size increases it does not affect the value of $Q_t$, and this implies that additional components do not affect the frequency at which a single component in the group

fails. This notion is proved mathematically in Equations (III-11)-(III-15). First, by using Equation (III-1) $Q_k^{(m)}$'s (for $m=3$) are computed in terms of alpha factors and $Q_t$, as in Equation (III-11).

$$Q_1^3 = \frac{\alpha_1^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3},\ Q_2^3 = \frac{\alpha_2^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3},\ Q_3^3 = \frac{3\alpha_3^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3}. \quad \text{(III-11)}$$

Next, the $Q_k^{(m)}$'s for a CCCG of m=3 are mapped down to m=2 by using the externally- and component-caused mapping-down rules as seen in (III-9) and (III-10), respectively. The component-caused mapping-down can be seen in (III-12) while the externally-caused mapping-down can be seen in (III-13).

$$Q_1^2 = Q_1^3 + \tfrac{1}{2}Q_2^3 \text{ and } Q_2^2 = Q_2^3 + \tfrac{2}{3}Q_3^3 \quad \text{(III-12)}$$

$$Q_1^2 = Q_1^3 + Q_2^3 \text{ and } Q_2^2 = Q_2^3 + Q_3^3 \quad \text{(III-13)}$$

Now the validity of these assumptions are checked for the component-caused event case. By using (III-4), $Q_t$ can be computed in terms of the mapped down, two component group $Q_k^{(m)}$'s, as seen in (III-14). The right hand side of the first line in (III-14) substitutes the results from (III-12) to put this in terms of the m=3. The second and third lines of (III-14) write these $Q_k^{(m)}$'s in terms of alpha factors, by substituting the definitions in Equation (III-11). The fact that this equation for $Q_t$ does not simplify back to $Q_t$ after these substitutions are made indicates that either Equation (III-1) is not intended for component-caused events, and/or that $Q_t$ is intended to vary with CCCG size for component-caused events.

$$Q_t = Q_1^2 + Q_2^2 = Q_1^3 + \tfrac{3}{2}Q_2^3 + \tfrac{2}{3}Q_3^3,$$

thus,

$$Q_t = \frac{\alpha_1^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} + \frac{3}{2}\frac{\alpha_2^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} + \frac{2}{3}\frac{3\alpha_3^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} \quad \text{(III-14)}$$

$$= \frac{\alpha_1^3 Q_t + \tfrac{3}{2}\alpha_2^3 Q_t + \tfrac{2}{3}3\alpha_3^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} = \frac{Q_t\left(\alpha_1^3 + \tfrac{3}{2}\alpha_2^3 + 2\alpha_3^3\right)}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} \neq Q_t$$

Lastly, the validity of these assumptions are checked for the externally-caused event case. The same process that was followed above for the component-caused case is repeated here in Equation (III-15). The fact that this equation for $Q_t$ does simplify back to $Q_t$ after these substitutions are made indicates that the rules in [34] are intended for externally-caused events

and thus the alpha factor parameters found in [31] have been estimated for these same CCF event types.

$$Q_t = Q_1^2 + Q_2^2 = Q_1^3 + 2Q_2^3 + Q_3^3,$$

thus,

$$Q_t = \frac{\alpha_1^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} + 2\frac{\alpha_2^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} + \frac{3\alpha_3^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} \qquad \text{(III-15)}$$

$$= \frac{\alpha_1^3 Q_t + 2\alpha_2^3 Q_t + 3\alpha_3^3 Q_t}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} = \frac{Q_t\left(\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3\right)}{\alpha_1^3 + 2\alpha_2^3 + 3\alpha_3^3} = Q_t$$

# CHAPTER IV

# RESULTS AND VERIFICATION

This chapter presents specific EDG case studies and their results, using the NRI model developed in Chapter II and the data introduced in Chapter III. The presented NRI results provide a means to quantify how system reliability changes for various EDG arrangements; a comparison of results for different arrangements is provided in Section IV.6.

All (but the last) of the cases presented here are given for hot standby systems because it seems standard onsite EDG systems are actually operated in hot standby, as discussed in Section I.3.2. These first four hot standby cases (Sections IV.1-IV.4) are for systems composed of two and three identical EDGs. These four cases will be examined using both a mission-time model of load and an offsite-recovery model of load (as discussed in Section II.1.1); results will be evaluated for a wide range of LOOP durations, many of which far exceed the standard PRA 24 hour mission time cutoff. The numerical results from these first four cases are also verified using results from the analytical solutions to standard Markov model state transition equations. The NRI equations for these system cases were coded and evaluated using MATLAB [32]; the code for Sections IV.1 and IV.2 is displayed in Appendix A while the code for Sections IV.3 and IV.4 is displayed in Appendix B. The comparison between the NRI and Markov model results serve to verify that the NRI coding and numerical integration performed in MATLAB are correct and accurate.

The last two cases presented in this chapter will be for an emergency power system composed of two standard EDGs in either hot or cold standby (one case for each option) and one FLEX DG in cold standby; these cases will employ a mission-time model of load. These two cases will only be modeled using the NRI; no equivalent Markov models will be developed for these cases. The NRI equations for these two cases were coded and evaluated using MATLAB [32]; the code for Section IV.5.1 is displayed in Appendix C while the code for Section IV.5.2 is displayed in Appendix D. The failure rate inputs for the FLEX DG will be varied in order to explore the extent to which the entire system failure probability is a function of the reliability of the FLEX DG, either independently or as part of a common-cause group.

**IV.1 Two Identical EDGs with Mission-Time Load**

The NRI model inputs and results for the system case of 2 identical emergency diesel generators (iEDGs) with a mission-time model of load are presented in this section. Results from a Markov model of the same system will also be presented as a means to verify the NRI results and numerical integration.

The alpha factor data used here are from pages 240, 241, and 243 of "CCF Parameter Estimates, 2012 Update"; specifically the median point value for a CCCG of two EDGs for each of the three failure modes [31]. Only the $\alpha_1$ value was so obtained, while the second alpha factor is computed as $\alpha_2 = 1 - \alpha_1$. The component unreliability estimates ($Q_t's$) were obtained from Table A.2.17-6 of [30] (the median point value for the EB/PL/KS analysis type). These data can be seen in Table 4.

**Table 4 – α-Factor Parameters for Two-iEDG Model.**

| | $\alpha_1$ | $\alpha_2$ | $Q_t$ | |
|---|---|---|---|---|
| FTS (Failure To Start) | 0.990656 | 9.3440E-03 | 3.24E-03 | unitless |
| FTL (Failure To Load) | 0.997015 | 2.9850E-03 | 2.25E-03 | 1/hr |
| FTR (Failure To Run) | 0.984593 | 1.5407E-02 | 7.12E-04 | 1/hr |

By using the above FTS data and the alpha factor method (Equation (III-1)), the initial conditions for the problem can be computed, as shown in Table 5. Here $P_1(0)$ and $P_2(0)$ are the failure on demand probabilities for EDG "1" and "2", respectively, $P_3(0)$ is the probability of CCF on demand, and $P_0(0)$ is the probability of no failures on demand, computed as $P_0(0) = 1 - P_1(0) - P_2(0) - P_3(0)$.

**Table 5 – Initial Conditions for Two-iEDG Model.**

| | |
|---|---|
| $P_1(0)$ | 3.18001141335362E-03 |
| $P_2(0)$ | 3.18001141335362E-03 |
| $P_3(0)$ | 5.99885866463764E-05 |
| $P_0(0)$ | 9.93579988586646E-01 |

The definitions and notations for hazard functions developed in Chapter II are used again here. The "designed" failure rates can be computed using the FTL and FTR data of Table 5 in Equation (III-1); these are shown in Table 6.

**Table 6 – Designed Failure Rates for Two-iEDG Model.**

| | | FTL | FTR |
|---|---|---|---|
| single failure rate for EDG "1" | $\lambda_1$ | 2.2366E-03 | 6.9039E-04 |
| single failure rate for EDG "2" | $\lambda_2$ | 2.2366E-03 | 6.9039E-04 |
| 2-out-of-2 CCF rate | $\lambda_{12}$ | 1.3392E-05 | 2.1606E-05 |

The influenced failure rates for each EDG are computed assuming that all CCF events are due to only component causes, not external causes. The designed failure rates and Equation (III-10) are used to compute the influenced failure rates, as in Equation (IV-1). The specific values for the influenced failure rates are shown in Table 7.

$$\tilde{\lambda}_i = \lambda_{1/1} = \lambda_i + \tfrac{1}{2}\lambda_{12}, \quad \text{for } i = 1,2 \qquad \text{(IV-1)}$$

**Table 7 – Influenced Failure Rate for Two-iEDG Model.**

| | FTL | FTR |
|---|---|---|
| $\tilde{\lambda}_i$ | 2.2433E-03 | 7.0119E-04 |

When constant failure rates are applied to Equation (II-43) it simplifies to Equation (IV-2) (this was coded in MATLAB [32]). Numerical integration was performed using the MATLAB functions integral and integral2. The absolute and relative error tolerances for these integration routines were adjusted; it will be shown that as the error tolerances are lowered, the results approach the analytical solution of the Markov model.

$$
\begin{aligned}
F(T) = P_3(0) + P_0(0) & \left\{ \begin{array}{l} \int_0^1 \lambda_{12}^L \exp\left\{-\lambda_{total}^L t\right\} dt + \\ \int_1^T \lambda_{12}^R \exp\left\{-\lambda_{total}^L - \lambda_{total}^R (t-1)\right\} dt \end{array} \right\} \\
+P_0(0) \sum_{i=1}^{2} & \left\{ \begin{array}{l} \int_0^1 \tilde{\lambda}_i^L \left[ \int_0^t \lambda_i^L \exp\left\{-\lambda_{total}^L \tau - \tilde{\lambda}_i^L (t-\tau)\right\} d\tau \right] dt + \\ \int_1^T \tilde{\lambda}_i^R \left[ \int_0^1 \lambda_j^L \exp\left\{-\lambda_{total}^L \tau - \tilde{\lambda}_i^L (1-\tau) - \tilde{\lambda}_i^R (t-1)\right\} d\tau \right] dt \\ + \int_1^T \tilde{\lambda}_i^R \left[ \int_1^t \lambda_j^R \exp\left\{-\lambda_{total}^L - \lambda_{total}^R (\tau-1) - \tilde{\lambda}_i^R (t-\tau)\right\} d\tau \right] dt \end{array} \right\} \\
+\sum_{i=1}^{2} P_i(0) & \left\{ \begin{array}{l} \int_0^1 \tilde{\lambda}_j^L \exp\left\{-\tilde{\lambda}_j^L t\right\} dt + \\ \int_1^T \tilde{\lambda}_j^R \exp\left\{-\tilde{\lambda}_j^L - \tilde{\lambda}_j^R (t-1)\right\} dt \end{array} \right\} \\
& \text{for } i \neq j = 1,2
\end{aligned}
\tag{IV-2}
$$

When the integrals in Equation (II-94) (for the Markov model) are evaluated explicitly, for constant failure rates, Equation (IV-3) is formed. This equation was coded in Excel [41] and evaluated for various values of time, $T$ .

$$F(T) = P_3(0) + P_0(0)\left\{\begin{array}{l}\frac{\lambda_{12}^L}{\lambda_{total}^L}\left(1-\exp\left\{-\lambda_{total}^L\right\}\right)+\\ \frac{\lambda_{12}^R}{\lambda_{total}^R}\exp\left\{-\lambda_{total}^L\right\}\left(1-\exp\left\{-\lambda_{total}^R(T-1)\right\}\right)\end{array}\right\}+$$

$$P_0(0)\sum_{i=1}^{2}\left\{\begin{array}{l}\frac{\lambda_i^L}{\lambda_{total}^L(\lambda_{total}^L-\tilde{\lambda}_i^L)}\left(\lambda_{total}^L\left(-\exp\left\{-\tilde{\lambda}_i^L\right\}\right)+\left(\exp\left\{-\lambda_{total}^L\right\}-1\right)\tilde{\lambda}_i^L+\lambda_{total}^L\right)\\ \frac{\lambda_j^L}{\tilde{\lambda}_i^L-\lambda_{total}^L}\left(\left(\exp\left\{\lambda_{total}^L\right\}-\exp\left\{\tilde{\lambda}_i^L\right\}\right)\left(\exp\left\{\tilde{\lambda}_i^R\right\}-\exp\left\{\tilde{\lambda}_i^R T\right\}\right)\exp\left\{-\lambda_{total}^L-\tilde{\lambda}_i^L-\tilde{\lambda}_i^R T\right\}\right)+\\ \frac{\lambda_j^R}{\lambda_{total}^R(\lambda_{total}^R-\tilde{\lambda}_i^R)}\exp\left\{-\lambda_{total}^L\right\}\left(-\lambda_{total}^R\exp\left\{\tilde{\lambda}_i^R-\tilde{\lambda}_i^R T\right\}+\tilde{\lambda}_i^R\left(\exp\left\{\lambda_{total}^R-\lambda_{total}^R T\right\}-1\right)+\lambda_{total}^R\right)\end{array}\right\} \quad \text{(IV-3)}$$

$$+\sum_{i=1}^{2}P_i(0)\left\{\begin{array}{l}\left(1-\exp\left\{-\tilde{\lambda}_j^L\right\}\right)+\\ \exp\left\{-\tilde{\lambda}_j^L\right\}\left(1-\exp\left\{\tilde{\lambda}_j^R-\tilde{\lambda}_j^R T\right\}\right)\end{array}\right\}$$

*for* $i \neq j = 1,2$

The analytical results from the Markov model are compared against the NRI results in Table 8 below. This NRI was evaluated in MATLAB [32] using three different sets of numerical integration error tolerances (high, default, and low tolerances corresponding to smaller, intermediated, and higher accuracies). The default tolerance setting has an absolute tolerance of 1e-10 while the relative tolerance is 1e-6. The high tolerance setting has an absolute tolerance of 1e-6 and a relative tolerance of 1e-2. The low tolerance setting has an absolute tolerance of 1e-16 and a relative tolerance of 1e-12. See Table 8 for the results.

**Table 8 – Results; Two iEDGs with Mission-Time Load.**

| | | Non-Recovery Integral | | |
|---|---|---|---|---|
| T (hrs) | Markov Analytical | high tol. | default tol. | low tol. |
| 0 | 6.00E-05 | 6.00E-05 | 6.00E-05 | 6.00E-05 |
| 1 | 9.25E-05 | 9.25E-05 | 9.25E-05 | 9.25E-05 |
| 6 | 2.49E-04 | 2.49E-04 | 2.49E-04 | 2.49E-04 |
| 12 | 4.66E-04 | 4.66E-04 | 4.66E-04 | 4.66E-04 |
| 24 | 9.98E-04 | 9.98E-04 | 9.98E-04 | 9.98E-04 |
| 48 | 2.44E-03 | 2.44E-03 | 2.44E-03 | 2.44E-03 |
| 96 | 6.73E-03 | 6.73E-03 | 6.73E-03 | 6.73E-03 |
| 192 | 2.03E-02 | 2.03E-02 | 2.03E-02 | 2.03E-02 |
| 384 | 6.30E-02 | 6.30E-02 | 6.30E-02 | 6.30E-02 |
| 768 | 1.83E-01 | 1.83E-01 | 1.83E-01 | 1.83E-01 |
| 1000 | 2.64E-01 | 2.64E-01 | 2.64E-01 | 2.64E-01 |
| 2000 | 5.76E-01 | 5.76E-01 | 5.76E-01 | 5.76E-01 |

Most of the results agree for ten or more digits, much more than the three digits shown in Table 8; thus, an easier way to compare them is to look at their difference. Table 9 below shows three columns where the high, default and low tolerance cases are each subtracted from the analytical results for the Markov model. As the numerical integration error tolerance is lowered, the Markov model analytical and NRI results agree more closely. The difference for each case changes from positive to negative at least once which indicates the difference is likely due to numerical integration approximations. For very long times, the low tolerance case and Analytical results agree to 15 digits of accuracy.

**Table 9 – Difference between Results; Two iEDGs with Mission-Time Load.**

| T (hrs) | Analytical-high | Analytical-default | Analytical-low |
|---|---|---|---|
| 0 | 9.49E-20 | 9.49E-20 | 9.49E-20 |
| 1 | 2.42E-16 | 1.65E-16 | 1.65E-16 |
| 6 | 5.40E-16 | 2.59E-16 | 2.59E-16 |
| 12 | 1.50E-15 | 1.27E-16 | 1.27E-16 |
| 24 | 8.23E-15 | -1.79E-16 | -1.80E-16 |
| 48 | 2.61E-14 | 1.40E-16 | 1.40E-16 |
| 96 | 2.49E-13 | 0.00E+00 | 0.00E+00 |
| 192 | 1.78E-12 | 3.02E-16 | 3.02E-16 |
| 384 | 5.93E-12 | 3.90E-15 | -4.11E-15 |
| 768 | -2.80E-10 | 7.60E-14 | 0.00E+00 |
| 1000 | -1.08E-09 | 2.58E-13 | 0.00E+00 |
| 2000 | -1.08E-08 | 7.26E-12 | 0.00E+00 |

### IV.2 Two Identical EDGs with Exponential Offsite-Recovery Load

The NRI model results for the system case of 2 identical EDGs with an offsite power recovery model of load are presented in this section. Results from a Markov model of the same system will also be presented as a means to verify the NRI results and numerical integration. The logic, state equations, and analytical solutions for the Markov model will be developed in Section IV.2.1.

As explained in Section II.1, the NRI model assumes that the random variables for system failure time and offsite power recovery time are statistically independent. Therefore the system failure PDF ( $f_C$ ) is identical to the "no recovery" case (Section IV.4), and is multiplied by a CCDF for offsite power recovery time ( $\overline{F}_L$ ), as illustrated in Equation (IV-4). For this specific model case, $T_{crit} = 0$, and the power recovery rate is a constant 0.04 hour$^{-1}$, therefore $\overline{F}_L(t_C) = \exp(-0.04 t_C)$.

$$\text{Probability of Failure} = P_f = \int_{0-}^{\infty} \overline{F}_L(t_C + T_{crit}) f_C(t_C) dt_C \qquad \text{(IV-4)}$$

The initial conditions and failure rates used for this case are identical to the data in Section IV.1 (as seen in Table 5, Table 6, and Table 7). The state equations and analytical solutions for

the Markov model are presented in Section IV.2 and the state transition diagram is illustrated in Figure 8.

The analytical results from the Markov model are compared against the NRI results in Table 10 below. The NRI was numerically integrated in MATLAB [32] using the functions integral and integral2 and two different sets of error tolerances. The default tolerance setting has an absolute tolerance of 1e-10 while the relative tolerance is 1e-6. The low tolerance setting has an absolute tolerance of 1e-16 and the relative tolerance is 1e-12. It can be seen below that as the error tolerances are lowered, the results approach the analytical solution of the Markov model.

**Table 10 – Results; Two iEDGs with Offsite-Recovery Load.**

| | Markov Model | Non-Recovery Integral | |
|---|---|---|---|
| T (hrs) | Analytical Solution | default tolerance | low tolerance |
| 0 | 5.99885866463764E-05 | 5.99885866463763E-05 | 5.99885866463763E-05 |
| 1 | 9.18171727364025E-05 | 9.18171727364094E-05 | 9.18171727364094E-05 |
| 6 | 2.27440793074019E-04 | 2.27440793074024E-04 | 2.27440793074024E-04 |
| 12 | 3.79056468279794E-04 | 3.79056468279792E-04 | 3.79056468279794E-04 |
| 24 | 6.37885838466108E-04 | 6.37885838466027E-04 | 6.37885838466103E-04 |
| 48 | 9.82656398295802E-04 | 9.82656398293078E-04 | 9.82656398295802E-04 |
| 96 | 1.24454317648595E-03 | 1.24454317643100E-03 | 1.24454317648600E-03 |
| 192 | 1.31000490458345E-03 | 1.31000490623800E-03 | 1.31000490458300E-03 |
| 384 | 1.31216133238182E-03 | 1.31216133089200E-03 | 1.31216133238200E-03 |
| 768 | 1.31216278738664E-03 | 1.31216279650700E-03 | 1.31216278738700E-03 |
| 2000 | 1.31216278738703E-03 | 1.31216278818500E-03 | 1.31216278738700E-03 |

Because the results agree for many digits, an easier way to compare them is to look at their difference. Table 11 below shows two columns where the default and low tolerance cases are each subtracted from the analytical results for the Markov model. As time increases, the difference for each case changes from positive to negative which indicates the difference is likely due to numerical integration approximations.

**Table 11 – Difference between Results; Two iEDGs with Offsite-Recovery Load.**

| T (hrs) | Analytical-default | Analytical-low |
|---|---|---|
| 0 | 8.13151629364E-20 | 8.13151629364E-20 |
| 1 | -6.85757874097E-18 | -6.85757874097E-18 |
| 6 | -4.79759461325E-18 | -4.79759461325E-18 |
| 12 | 1.51788304148E-18 | -4.87890977618E-19 |
| 24 | 8.12067427192E-17 | 5.20417042793E-18 |
| 48 | 2.72438321902E-15 | 0.00000000000E+00 |
| 96 | 5.49530039529E-14 | -4.68375338514E-17 |
| 192 | -1.65454629164E-12 | 4.53847029402E-16 |
| 384 | 1.48982020297E-12 | -1.79760720198E-16 |
| 768 | -9.12035984929E-12 | -3.59738280831E-16 |
| 2000 | -7.97970196864E-13 | 2.99239799606E-17 |

### IV.2.1 Markov Model Analytical Solution

The analytical solution of the Markov model is derived here. The solution derivation for this problem has been provided by Vera Moiseytseva. Both EDGs have identical failure parameters, thus to simplify the notation used only two failure rates are used (the single failure event and CCF event rates, as defined directly below)

$$\lambda = \lambda_1 = \lambda_2 \quad \text{and} \quad \lambda_{cc} = \lambda_{12}$$

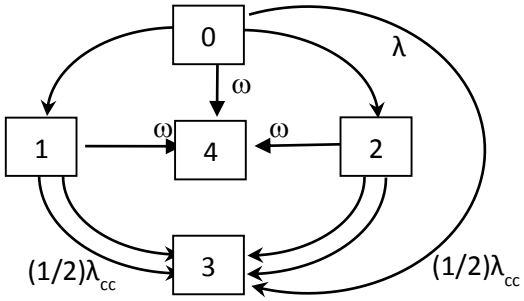


**Figure 8 - Markov Diagram for Two iEDGs with Offsite Power Recovery.**

The state-transition differential equations for the system shown in Figure 8 can be written as:

$$\begin{cases} \frac{dP_0(t)}{dt} = -2\lambda P_0(t) - \omega P_0(t) - \lambda_{cc} P_0(t) \\ \frac{dP_1(t)}{dt} = \lambda P_0(t) - \lambda P_1(t) - \frac{1}{2}\lambda_{cc} P_1(t) - \omega P_1(t) \\ \frac{dP_2(t)}{dt} = \lambda P_0(t) - \lambda P_2(t) - \frac{1}{2}\lambda_{cc} P_2(t) - \omega P_2(t) \\ \frac{dP_3(t)}{dt} = \lambda_{cc} P_0(t) + \lambda P_1(t) + \frac{1}{2}\lambda_{cc} P_1(t) + \lambda P_2(t) + \frac{1}{2}\lambda_{cc} P_2(t) \\ \frac{dP_4(t)}{dt} = \omega P_0(t) + \omega P_1(t) + \omega P_2(t) \end{cases}$$

The corresponding initial conditions are:

$$\begin{cases} P_0(t=0) = \tilde{P}_0 = 1 - \tilde{P}_1^{(1)} - \tilde{P}_2^{(1)} - \tilde{P}_3^{(1)} \\ P_1(t=0) = \tilde{P}_1^{(1)} \\ P_2(t=0) = \tilde{P}_2^{(1)} \\ P_3(t=0) = \tilde{P}_3^{(2)} \\ P_4(t=0) = \tilde{P}_4 = 0 \end{cases}$$

Similar to the state transition equations shown in Section II.4.1, this system is composed of first-order linear differential equations. As in Chapter II, these equations are solved using an integrating factor to obtain the general solution. Differently from before, the integrals are indefinite and evaluated analytically as they appear; next the integration constant is solved for using the initial conditions. The state "0" equation solution is straightforward and can be seen in the equation below.

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t) - \omega P_0(t) - \lambda_{cc} P_0(t) = -(2\lambda + \omega + \lambda_{cc}) P_0(t)$$
$$\Rightarrow P_0(t) = \tilde{P}_0 e^{-(2\lambda+\omega+\lambda_{cc})t}$$

The state "1" equation is rewritten below to make the general form of the ODE.

$$\frac{dP_1(t)}{dt} = \lambda P_0(t) - \lambda P_1(t) - \frac{1}{2}\lambda_{cc} P_1(t) - \omega P_1(t)$$

$$\frac{dP_1(t)}{dt} + \left(\lambda + \omega + \frac{1}{2}\lambda_{cc}\right) P_1(t) = \lambda P_0(t)$$

The state "1" equation general solution is derived below.

$$\Rightarrow P_1(t) = e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t}\left\{\lambda\int P_0(t')e^{\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t'}dt'\right\} = e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t}\left\{\lambda\tilde{P}_0\int e^{-(2\lambda+\omega+\lambda_{cc})t'}e^{\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t'}dt'\right\}$$

$$= e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t}\left\{\lambda\tilde{P}_0\int e^{-\left(\lambda+\frac{1}{2}\lambda_{cc}\right)t'}dt'\right\} = e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t}\left\{\lambda\tilde{P}_0\frac{-1}{\lambda+\frac{1}{2}\lambda_{cc}}e^{-\left(\lambda+\frac{1}{2}\lambda_{cc}\right)t} + Const\right\}$$

$$= -\lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}e^{-(2\lambda+\omega+\lambda_{cc})t} + Const\, e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t}$$

Next, the state "1" initial condition is used to solve for the integration constant, and the exact solution is shown below.

$$P_1(t=0) = \tilde{P}_1^{(1)} = -\lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}} + Const \Rightarrow Const = \tilde{P}_1^{(1)} + \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}$$

$$P_1(t) = \left(\tilde{P}_1^{(1)} + \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}\right)e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t} - \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}e^{-(2\lambda+\omega+\lambda_{cc})t}$$

Because both EDGs are identical, the state "1" and "2" equations are similar as shown in the equation below.

$$P_2(t) = \left(\tilde{P}_2^{(1)} + \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}\right)e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t} - \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}e^{-(2\lambda+\omega+\lambda_{cc})t}$$

Since $P_1(t) = P_2(t)$, the state "3" equation reduces to the one shown below.

$$\frac{dP_3(t)}{dt} = \lambda_{cc}P_0(t) + (2\lambda + \lambda_{cc})P_1(t)$$

And now the state "3" equation solution can be obtained by simply integrating the state "0" and "1" equation solutions, as shown in the equation below.

$$P_3(t) = \tilde{P}_3^{(2)} + \lambda_{cc}\int_0^t P_0(t')dt' + (2\lambda + \lambda_{cc})\int_0^t P_1(t')dt'$$

$$\int_0^t P_0(t')dt' = \tilde{P}_0\int_0^t e^{-(2\lambda+\omega+\lambda_{cc})t'}dt' = \tilde{P}_0\frac{1}{2\lambda+\omega+\lambda_{cc}}\left(1 - e^{-(2\lambda+\omega+\lambda_{cc})t}\right)$$

$$\int_0^t P_1(t')dt' = \left(\tilde{P}_1^{(1)} + \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}\right)\int_0^t e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t'}dt' - \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}\int_0^t e^{-(2\lambda+\omega+\lambda_{cc})t'}dt'$$

$$= \left(\tilde{P}_1^{(1)} + \lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}\right)\frac{1}{\lambda+\omega+\frac{1}{2}\lambda_{cc}}\left(1 - e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t}\right)$$

$$-\lambda\tilde{P}_0\frac{1}{\lambda+\frac{1}{2}\lambda_{cc}}\frac{1}{2\lambda+\omega+\lambda_{cc}}\left(1 - e^{-(2\lambda+\omega+\lambda_{cc})t}\right)$$

Now that these integrals are computed, they are input back to the state "3" equation solution, and the analytical solution is obtained as seen below.

$$P_3(t) = \tilde{P}_3^{(2)} + \lambda_{cc}\left\{\tilde{P}_0\frac{1}{2\lambda+\omega+\lambda_{cc}}\left(1 - e^{-(2\lambda+\omega+\lambda_{cc})t}\right)\right\}$$

$$+2\left\{\left(\tilde{P}_1^{(1)}\left(\lambda+\frac{1}{2}\lambda_{cc}\right) + \lambda\tilde{P}_0\right)\frac{1}{\lambda+\omega+\frac{1}{2}\lambda_{cc}}\left(1 - e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t}\right)\right.$$

$$\left.-\lambda\tilde{P}_0\frac{1}{2\lambda+\omega+\lambda_{cc}}\left(1 - e^{-(2\lambda+\omega+\lambda_{cc})t}\right)\right\}$$

The state "4" equation is in a form very similar to the state "3" equation; thus their solutions are obtained in a similar manner, as seen in the equations below.

$$\frac{dP_4(t)}{dt} = \omega P_0(t) + \omega P_1(t) + \omega P_2(t) = \omega P_0(t) + 2\omega P_1(t)$$

$$\Rightarrow P_4(t) = \tilde{P}_4 + \omega\int_0^t P_0(t')dt' + 2\omega\int_0^t P_1(t')dt'$$

$$P_4(t) = \tilde{P}_4 + \tilde{P}_0 \frac{\omega}{2\lambda + \omega + \lambda_{cc}} \left(1 - e^{-(2\lambda+\omega+\lambda_{cc})t}\right)$$

$$+2\omega \left\{ \left( \tilde{P}_1^{(1)} + \lambda \tilde{P}_0 \frac{1}{\lambda + \frac{1}{2}\lambda_{cc}} \right) \frac{1}{\lambda + \omega + \frac{1}{2}\lambda_{cc}} \left( 1 - e^{-\left(\lambda+\omega+\frac{1}{2}\lambda_{cc}\right)t} \right) \right.$$

$$\left. -\lambda \tilde{P}_0 \frac{1}{\lambda + \frac{1}{2}\lambda_{cc}} \frac{1}{2\lambda + \omega + \lambda_{cc}} \left(1 - e^{-(2\lambda+\omega+\lambda_{cc})t}\right) \right\}$$

It should be noted here that the above derivation does not explicitly differentiate between FTL and FTR failure rates, but this poses no problem because constant failure rates are used and the model is "memoryless". As explained in Chapter 2, FTL rates are valid for time ≤ 1 hour while FTR rates are valid for time > 1 hour. Thus the state equation solutions for time equal to or less than one hour use the given initial conditions and FTL rates as illustrated in Equation (IV-5) for the state 0 solution.

$$P_0(t=1) = \tilde{P}_0(1) = \tilde{P}_0 e^{-\left(2\lambda^L + \omega + \lambda_{cc}^L\right)(t=1)} \tag{IV-5}$$

For times greater than 1 hour, the initial conditions are replaced with the state solution for t=1 hour, FLR rates are used, and t is replaced with t-1, as in Equation (IV-6) below.

$$P_0(t > 1hr) = \tilde{P}_0(1) e^{-\left(2\lambda^R + \omega + \lambda_{cc}^R\right)(t-1)} \tag{IV-6}$$

This same logic applies to the Markov model solutions developed in Sections IV.3 and IV.4.

**IV.3 Three Identical EDGs with Mission-Time Load**

The NRI model inputs and results for the system case of 3 identical EDGs with a mission-time model of load are presented in this section. Results from a Markov model of the same system will also be presented as a means to verify the NRI results and numerical integration. The logic, state equations, and analytical solutions for the Markov model will be developed in Section IV.3.1.

The alpha factor data used here are from pages 240, 241, and 243 of "CCF Parameter Estimates, 2012 Update" [31]; specifically the mean point value for a CCCG of 3 EDGs for each of the three failure modes. The $\alpha_1$ and $\alpha_3$ values were obtained from this reference, while the

second alpha factor is computed as $\alpha_2 = 1 - \alpha_1 - \alpha_3$. The component unreliability estimates ( $Q_t's$ ) were obtained from Table A.2.17-5 of [30] (the median point value for the EB/PL/KS analysis type). These data are shown in Table 12.

**Table 12 – α-Factor Parameters for Three-iEDG Model.**

| Parameters for α-factor model | | | | | |
|---|---|---|---|---|---|
| | $\alpha_1$ | $\alpha_2$ | $\alpha_3$ | $Q_t$ | |
| FTS (Failure To Start) | 0.990496 | 6.16E-03 | 3.34E-03 | 3.24E-03 | unitless |
| FTL (Failure To Load) | 0.991208 | 7.42E-03 | 1.37E-03 | 2.25E-03 | 1/hr |
| FTR (Failure To Run) | 0.985501 | 8.86E-03 | 5.64E-03 | 7.12E-04 | 1/hr |

By using the above FTS data and the alpha factor method (Equation (III-1)), the initial conditions for the problem can be computed as shown in Table 13. $P_1(0)$, $P_2(0)$, and $P_3(0)$ are the failure on demand probabilities for EDG "1","2", and "3", respectively. $P_4(0)$, $P_5(0)$, and $P_6(0)$ are the failure on demand probabilities for the 2-out-of-3 CCF (for the failures of "1"&"2", "2"&"3", and "1"&"3", respectively). The probability of no failures on demand, $P_0(0)$, is computed as in Equation (IV-7).

$$P_0(0) = 1 - P_1(0) - P_2(0) - P_3(0) - P_4(0) - P_5(0) - P_6(0) - P_7(0) \qquad \text{(IV-7)}$$

**Table 13 – Initial Conditions for Three-iEDG Model.**

| Initial Conditions | |
|---|---|
| $P_1(0)$ | 3.16851068871416E-03 |
| $P_2(0)$ | 3.16851068871416E-03 |
| $P_3(0)$ | 3.16851068871416E-03 |
| $P_4(0)$ | 1.97181007144238E-05 |
| $P_5(0)$ | 1.97181007144238E-05 |
| $P_6(0)$ | 1.97181007144238E-05 |
| $P_7(0)$ | 3.20531098569967E-05 |
| $P_0(0)$ | 9.90403260521857E-01 |

The definitions and notations for hazard functions developed in Chapter II are used here for the constant failure rates. The "designed" failure rates can be computed using the FTL and FTR data above input to Equation (III-1); these are shown in Table 14.

**Table 14 – Designed Failure Rates for Three-iEDG Model.**

| | | FTL | FTR |
|---|---|---|---|
| single failure rate | $\lambda_i$ | 2.20778251409180E-03 | 6.87824612136189E-04 |
| 2-out-of-3 CCF rate | $\lambda_{ij}$ | 1.65315068276178E-05 | 6.18308681463999E-06 |
| 3-out-of-3 CCF rate | $\lambda_{123}$ | 9.15447225296537E-06 | 1.18092142345308E-05 |

The influenced failure rates for each EDG are computed assuming that all CCF events are due to only component-causes, not external-causes. The designed failure rates and Equation (III-10) are used to compute the influenced failure rates, as in Equations (IV-8)-(IV-10). The specific values for the influenced failure rates are shown in Table 15.

$$\tilde{\lambda}_{j|i} = \lambda_j + \tfrac{1}{2}\lambda_{ij} \qquad \text{(IV-8)}$$

$$\tilde{\lambda}_{jk|i} = \lambda_{jk} + \tfrac{2}{3}\lambda_{123} \qquad \text{(IV-9)}$$

$$\tilde{\lambda}_{k|ij} = \lambda_k + \tfrac{1}{2}\lambda_{ik} + \tfrac{1}{2}\lambda_{jk} + \tfrac{1}{3}\lambda_{123} \quad \text{(IV-10)}$$

**Table 15 – Influenced Failure Rates for Three-iEDG Model.**

| | FTL | FTR |
|---|---|---|
| $\tilde{\lambda}_{j\|i}$ | 2.21604826750561E-03 | 6.90916155543509E-04 |
| $\tilde{\lambda}_{jk\|i}$ | 2.26344883295947E-05 | 1.40558963043272E-05 |
| $\tilde{\lambda}_{k\|ij}$ | 2.22736551167041E-03 | 6.97944103695673E-04 |

The NRI model is based up the PDFs developed in Section II.3. The NRI model CDF for the system failure time of this case is shown in Equation (IV-11). This equation was formed by integrating and combining the previously developed failure sequence PDFs. The three EDGs are identical, thus the failure sequences involving 3 and 2 failure events are multiplied by 6 and 3, respectively (in order to account for each unique combination of the failure ordering for EDGs. Equation (IV-11) was coded and evaluated using MATLAB [32]. Numerical integration was performed using the MATLAB functions integral, integral2, and integral3. The absolute and relative error tolerances for these integration routines were adjusted; it will be shown that as the error tolerances are lowered, the results approach the analytical solution of the Markov model.

$$F(T) = 6 * P_0(0)\left( \int_0^1 \int_0^{t_k} \int_0^{t_j'} f(\tau_i < 1, t_j' < 1, t_k \le 1)\, \mathrm{d}\tau_i dt_j' dt_k + \int_1^T \int_0^1 \int_0^{t_j'} f(\tau_i < 1, t_j' \le 1, t_k > 1)\, \mathrm{d}\tau_i dt_j' dt_k \right.$$

$$\left. + \int_1^T \int_1^{t_k} \int_0^1 f(\tau_i \le 1, t_j' > 1, t_k > 1)\, \mathrm{d}\tau_i dt_j' dt_k + \int_1^T \int_1^{t_k} \int_1^{t_j'} f(\tau_i > 1, t_j' > 1, t_k > 1)\, \mathrm{d}\tau_i dt_j' dt_k \right)$$

$$+6 * P_i(0)\left( \int_0^1 \int_0^{t_k} f(t_j' < 1, t_k \le 1) dt_j' dt_k + \int_1^T \int_0^1 f(t_j' \le 1, t_k > 1) dt_j' dt_k + \int_1^T \int_1^{t_k} f(t_j' > 1, t_k > 1) dt_j' dt_k \right)$$

$$+3 * P_0(0)\left( \int_0^1 \int_0^{t_k} f(t_{ij}' < 1, t_k \le 1) dt_{ij}' dt_k + \int_1^T \int_0^1 f(t_{ij}' \le 1, t_k > 1) dt_{ij}' dt_k + \int_1^T \int_1^{t_k} f(t_{ij}' > 1, t_k > 1) dt_{ij}' dt_k \right)$$

$$+3 * P_0(0)\left( \int_0^1 \int_0^{t_{jk}} f(\tau_i < 1, t_{jk} \le 1) d\tau_i dt_{jk} + \int_1^T \int_0^1 f(\tau_i \le 1, t_{jk} > 1) d\tau_i dt_{jk} + \int_1^T \int_1^{t_{jk}} f(\tau_i > 1, t_{jk} > 1) d\tau_i dt_{jk} \right)$$

$$+3 * P_{ij}(0)\left( \int_0^1 f(t_k \le 1) dt_k + \int_1^T f(t_k > 1) dt_k \right) + 3 * P_i(0)\left( \int_0^1 f(t_{jk} \le 1) dt_{jk} + \int_1^T f(t_{jk} > 1) dt_{jk} \right)$$

$$+P_0(0)\left( \int_0^1 f(t_{jik} \le 1) dt_{jk} + \int_1^T f(t_{jik} > 1) dt_{jk} \right) + P_7(0)$$

where

$P_i(0) = P_1(0) = P_2(0) = P_3(0)$

$P_{ij}(0) = P_4(0) = P_5(0) = P_6(0)$

(IV-11)

The analytical results for the Markov model are compared against the NRI results in Table 16. The NRI was evaluated in MATLAB [32] using two different sets of numerical integration error tolerances. The default tolerance setting has an absolute tolerance of 1e-10 while the relative tolerance is 1e-6. The low tolerance setting has an absolute tolerance of 1e-16 while the relative tolerance is 1e-12.

**Table 16 – Results; Three iEDGs with Mission-Time Load.**

| | | Non-Recovery Integral | |
|---|---|---|---|
| T (hrs) | Markov Analytical | default tolerance | low tolerance |
| 0 | 3.20531098569967E-05 | 3.205310985700E-05 | 3.205310985700E-05 |
| 1 | 4.16218657460282E-05 | 4.162186574608E-05 | 4.162186574608E-05 |
| 6 | 1.01846796296793E-04 | 1.018467962969E-04 | 1.018467962969E-04 |
| 12 | 1.75491531461444E-04 | 1.754915314614E-04 | 1.754915314614E-04 |
| 24 | 3.28742683653675E-04 | 3.287426836535E-04 | 3.287426836536E-04 |
| 48 | 6.69238288596580E-04 | 6.692382885964E-04 | 6.692382885965E-04 |
| 96 | 1.55963329808756E-03 | 1.559633298088E-03 | 1.559633298088E-03 |
| 192 | 4.65447114911682E-03 | 4.654471149117E-03 | 4.654471149117E-03 |
| 384 | 1.84875326784657E-02 | 1.848753267844E-02 | 1.848753267847E-02 |
| 768 | 8.13086371675060E-02 | 8.130863716749E-02 | 8.130863716751E-02 |

Because the results agree for many digits, an easier way to compare them is to look at their difference. Table 17 shows two columns where the default and low tolerance cases are each subtracted from the analytical results for the Markov model. The difference for each case changes from positive to negative at least once which indicates the difference is likely due to numerical integration approximations. For very long times, the low tolerance case and Analytical results agree to 15 digits of accuracy.

**Table 17 – Difference between Results; Three iEDGs with Mission-Time Load.**

| T (hrs) | Analytical-default | Analytical-low |
|---|---|---|
| 0 | 0.0000000000E+00 | 0.0000000000E+00 |
| 1 | -5.1316644076E-17 | -5.4413396532E-17 |
| 6 | -6.3683325106E-17 | -7.9688859678E-17 |
| 12 | 6.1149002528E-17 | 3.9139698427E-17 |
| 24 | 1.6127507316E-16 | 8.3266726847E-17 |
| 48 | 1.4571677198E-16 | 7.2749965774E-17 |
| 96 | -4.4061976290E-16 | -4.4061976290E-16 |
| 192 | -1.7694179455E-16 | -1.7694179455E-16 |
| 384 | 2.3699792129E-14 | -2.9837243787E-16 |
| 768 | 1.4030443474E-14 | 0.0000000000E+00 |

### IV.3.1 Markov Model Analytical Solution

The analytical solution of the Markov model is derived here. The solution derivation for this problem has been provided by Vera Moiseytseva. All three EDGs have identical failure parameters, thus to simplify the notation only three designed failure rates are used, as follows:

$\lambda = \lambda_1 = \lambda_2 = \lambda_3$,
$\lambda_{cc,2} = \lambda_{12} = \lambda_{23} = \lambda_{13}$,
and $\lambda_{cc,3} = \lambda_{123}$.

This system is composed of first-order linear differential equations. These equations are solved using an integrating factor to obtain the general solution. The indefinite integrals are solved analytically right away as they appear; next the integration constant is solved for using the initial conditions.

The initial value problem (IVP) for state "0" is as follows:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\left(3\lambda + 3\lambda_{cc,2} + \lambda_{cc,3}\right)P_0(t) \\ P_0(t=0) = \tilde{P}_0 \end{cases}.$$

The state "0" equation solution is straightforward and can be seen in the following equation:

$$P_0(t) = \tilde{P}_0\, e^{-\left(3\lambda + 3\lambda_{cc,2} + \lambda_{cc,3}\right)t}.$$

The initial value problem (IVP) for state "0" is as follows:

$$\begin{cases} \dfrac{dP_1(t)}{dt} = \lambda P_0(t) - \left(2\lambda + 2\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right)P_1(t) \\ P_1(t=0) = \tilde{P}_1 \end{cases}.$$

The state "1" equation general solution is derived in the following equation.

$$P_1(t) = e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}\left(\lambda\int P_0(t')e^{\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t'}dt'\right)$$

$$= e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}\left(\lambda\tilde{P}_0\int e^{-\left(3\lambda+3\lambda_{cc,2}+\lambda_{cc,3}\right)t'}e^{\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t'}dt'\right)$$

$$= e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}\left(\lambda\tilde{P}_0\int e^{-\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t'}dt'\right)$$

$$= e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}\left(\lambda\tilde{P}_0\left(\frac{-e^{-\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t'}}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}+Const\right)\right)$$

$$= -\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}e^{-\left(3\lambda+3\lambda_{cc,2}+\lambda_{cc,3}\right)t'}+Const'e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}$$

Next, the state "1" initial condition is used to solve for the integration constant, and the exact solution is shown below.

$$P_1(t=0)=\tilde{P}_1=-\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}+Const' \Rightarrow Const'=\tilde{P}_1+\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}$$

$$\Rightarrow P_1(t)=\left(\tilde{P}_1+\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\right)e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}-\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}e^{-\left(3\lambda+3\lambda_{cc,2}+\lambda_{cc,3}\right)t'}$$

Since the three EDGs are assumed to be identical for this case, the state "2" and "3" equation solutions are very similar to the state "1" solution. This similarity can be noted in the following two equations.

$$P_2(t)=\left(\tilde{P}_2+\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\right)e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}-\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}e^{-\left(3\lambda+3\lambda_{cc,2}+\lambda_{cc,3}\right)t'}$$

$$P_3(t)=\left(\tilde{P}_3+\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\right)e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}-\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}e^{-\left(3\lambda+3\lambda_{cc,2}+\lambda_{cc,3}\right)t'}$$

The state "4" equation and solution derivation can be seen in the equations below.

$$\begin{cases} \dfrac{dP_4(t)}{dt} = \lambda_{cc,2}P_0(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_1(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_2(t) - \left(\lambda + \lambda_{cc,2} + \dfrac{1}{3}\lambda_{cc,3}\right)P_4(t) \\ P_4(t=0) = \tilde{P}_4 \end{cases}$$

$$P_4(t) = e^{-\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t}\left\{\begin{array}{l} \lambda_{cc,2}\int P_0(t')e^{\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t'}dt' + \left(\lambda+\dfrac{1}{2}\lambda_{cc,2}\right)\int P_1(t')e^{\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t'}dt' \\ +\left(\lambda+\dfrac{1}{2}\lambda_{cc,2}\right)\int P_2(t')e^{\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t'}dt' \end{array}\right\}$$

$$= e^{-\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t}\left\{\begin{array}{l} -\dfrac{\lambda_{cc,2}\tilde{P}_0}{2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}}e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t} + \left(\lambda+\dfrac{1}{2}\lambda_{cc,2}\right) \\ \bullet\left[\left(\tilde{P}_1 - \dfrac{\lambda\tilde{P}_0}{\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)^2}\right)e^{-\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t}\ldots\right. \\ \left. -\dfrac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\bullet\left(-\dfrac{e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}}{2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}}\right)+Const\right] \end{array}\right\}$$

Again, the integration constant (*Const*) can be found from the initial condition for $P_4(t)$.

Finally (taking into account that the EDGs are identical), the state "4"equation solution simplifies as

$$P_4(t)=\left[-\frac{\lambda_{cc,2}\tilde{P}_0}{2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}}+2\left(\lambda+\frac{1}{2}\lambda_{cc,2}\right)\frac{1}{2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}}\bullet\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\right]e^{-\left(3\lambda+3\lambda_{cc,2}+\lambda_{cc,3}\right)t}$$

$$+\left[\frac{-\left(\lambda+\frac{1}{2}\lambda_{cc,2}\right)}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\left(\tilde{P}_1+\tilde{P}_2+\frac{2\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\right)\right]e^{-\left(2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}\right)t}$$

$$+\left[\tilde{P}_4+\frac{\lambda_{cc,2}\tilde{P}_0}{2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}}-\left(\lambda+\frac{1}{2}\lambda_{cc,2}\right)\right.$$

$$\left.\bullet\left(-\frac{1}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\left(\tilde{P}_1+\tilde{P}_2+\frac{2\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\right)+\frac{2}{2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}}\bullet\frac{\lambda\tilde{P}_0}{\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}}\right)\right]e^{-\left(\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}\right)t}.$$

The state "5" and "6" equation solutions are similar to the state "4" solution shown above. In order to simplify the state "7" equation derivation, the following coefficients are introduced:

Let

$$\lambda_1=\lambda+\lambda_{cc,2}+\frac{1}{3}\lambda_{cc,3}$$

$$\lambda_2=2\lambda+2\lambda_{cc,2}+\frac{2}{3}\lambda_{cc,3}=2\lambda_1$$

$$\lambda_{tot}=3\lambda+3\lambda_{cc,2}+\lambda_{cc,3}=\lambda_1+\lambda_2=3\lambda_1$$

$$A=\frac{\lambda}{\lambda_1}\tilde{P}_0$$

$$B=\frac{1}{\lambda_1}\left[2A\left(\lambda+\frac{1}{2}\lambda_{cc,2}\right)-\lambda_{cc,2}\tilde{P}_0\right]$$

$$C=-\frac{2}{\lambda_1}\left(\lambda+\frac{1}{2}\lambda_{cc,2}\right)\left(\tilde{P}_1+A\right)$$

$$D=\tilde{P}_4+\frac{1}{\lambda_2}\left(\lambda_{cc,2}\tilde{P}_0-2A\left(\lambda+\frac{1}{2}\lambda_{cc,2}\right)\right)-C$$

With these coefficients the solutions derived above could be rewritten as follows:

$$P_0(t) = \tilde{P}_0 e^{-\lambda_{tot} t}$$
$$P_1(t) = P_2(t) = P_3(t) = \left(\tilde{P}_0 + A\right) e^{-\lambda_2 t} - A e^{-\lambda_{tot} t}$$
$$P_4(t) = P_5(t) = P_6(t) = B e^{-\lambda_{tot} t} + C e^{-\lambda_2 t} + D e^{-\lambda_1 t}$$

$$\begin{cases} \dfrac{dP_7(t)}{dt} = \lambda_{cc,3} P_0(t) + \left(\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right) + \left(\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right)\left(P_1(t) + P_2(t) + P_3(t)\right) \ldots \\ \qquad + \left(\lambda + \lambda_{cc,2} + \dfrac{1}{3}\lambda_{cc,3}\right)\left(P_4(t) + P_5(t) + P_6(t)\right) \\ \qquad = \lambda_{cc,3} P_0(t) + \left(\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right) + \left(\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right)\left(3P_1(t)\right) + \left(\lambda + \lambda_{cc,2} + \dfrac{1}{3}\lambda_{cc,3}\right)\left(3P_4(t)\right) \\ P_7(t=0) = \tilde{P}_7 \end{cases}$$

Straightforward integration and using the coefficients introduced above will give:

$$P_7(t) = \frac{\lambda_{cc,3}\tilde{P}_0 - 3A\left(\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right) + 3B\lambda_1}{\lambda_{tot}}\left(1 - e^{-\lambda_{tot} t}\right)$$
$$+3\frac{\left(\tilde{P}_1 + A\right)\left(\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right) + C\lambda_1}{\lambda_2}\left(1 - e^{-\lambda_2 t}\right) + 3D\left(1 - e^{-\lambda_1 t}\right) + \tilde{P}_7$$

**IV.4 Three Identical EDGs with Exponential Offsite-Recovery Load**

The NRI model results for the system case of 3 identical EDGs with a mission-time model of load are presented in this section. Results from a Markov model of the same system will also be presented as a means to verify the NRI results and numerical integration. The logic, state equations, and analytical solutions for the Markov model are developed in Section IV.3.1. The initial conditions and failure rates used for this case are identical to the data from Section IV.3, as seen in Table 13, Table 14, and Table 15.

As explained in Section II.1, the NRI model assumes that the random variables for system failure time and offsite power recovery time are statistically independent. Therefore the system failure PDF ( $f_C$ ) is identical to the "no recovery" case, and is multiplied by a CCDF for offsite power recovery time ( $\bar{F}_L$ ), as illustrated in the following equation. For this specific model case, $T_{crit} = 0$ , and the power recovery rate is a constant 0.04 hour$^{-1}$, therefore $\bar{F}_L(t_C) = \exp(-0.04 t_C)$ .

$$\text{Probability of Failure} = P_f = \int_{0-}^{\infty} \overline{F}_L(t_C + T_{crit}) f_C(t_C) dt_C$$

The analytical results for the Markov model are compared against the NRI results in Table 18. The NRI was evaluated in MATLAB [32] using two different sets of numerical integration error tolerances. The default tolerance setting has an absolute tolerance of 1e-10 while the relative tolerance is 1e-6. The low tolerance setting has an absolute tolerance of 1e-16 while the relative tolerance is 1e-12. It can be seen in Table 18 that as the error tolerances are lowered, the results approach the analytical solution of the Markov model.

**Table 18 – Results; Three iEDGs with Offsite-Recovery Load.**

| | Markov Model | Non-Recovery Integral | |
|---|---|---|---|
| T (hrs) | Analytical Solution | default tolerance | low tolerance |
| 0 | 3.2053109857E-05 | 3.2053109857E-05 | 3.2053109857E-05 |
| 1 | 4.1431969197E-05 | 4.1431969197E-05 | 4.1431969197E-05 |
| 6 | 9.3863074078E-05 | 9.3863074078E-05 | 9.3863074078E-05 |
| 12 | 1.4534332021E-04 | 1.4534332021E-04 | 1.4534332021E-04 |
| 24 | 2.2048210762E-04 | 2.2048210762E-04 | 2.2048210762E-04 |
| 48 | 3.0327157306E-04 | 3.0327157313E-04 | 3.0327157306E-04 |
| 96 | 3.5807973281E-04 | 3.5807973281E-04 | 3.5807973281E-04 |
| 192 | 3.7214653605E-04 | 3.7214653618E-04 | 3.7214653605E-04 |
| 384 | 3.7273037183E-04 | 3.7273037152E-04 | 3.7273037183E-04 |
| 768 | 3.7273096305E-04 | 3.7273096621E-04 | 3.7273096305E-04 |
| 2000 | 3.2053109857E-05 | 3.2053109857E-05 | 3.2053109857E-05 |

Because the results agree for many digits, an easier way to compare them is to look at their difference. Table 19 shows two columns where the default and low tolerance cases are each subtracted from the analytical results for the Markov model. As time increases, the difference for each case changes from positive to negative which indicates the difference is likely due to numerical integration approximations.

**Table 19 – Difference between Results; Three iEDGs with Offsite-Recovery Load.**

| T (hrs) | Analytical-default | Analytical-low |
|---|---|---|
| 0 | 0.0000000000E+00 | 0.0000000000E+00 |
| 1 | 1.8838012747E-18 | -2.3174821437E-18 |
| 6 | 5.2841303382E-17 | 1.6398557859E-18 |
| 12 | 1.2834243217E-16 | 1.0327025693E-17 |
| 24 | -1.1595542235E-16 | 7.0473141212E-18 |
| 48 | -6.8935525691E-14 | 4.3368086899E-19 |
| 96 | 3.0037279088E-15 | 9.7578195524E-18 |
| 192 | -1.2899669397E-13 | 8.2941466195E-18 |
| 384 | 3.0767565145E-13 | 1.8648277367E-17 |
| 768 | -3.1608169315E-12 | -5.3939058081E-17 |
| 2000 | 0.0000000000E+00 | 0.0000000000E+00 |

### IV.4.1 Markov Model Analytical Solution

The analytical solution of the Markov model is derived here. The solution derivation for this problem has been provided by Vera Moiseytseva. All three EDGs have identical failure parameters, thus to simplify the notation only three designed failure rates are used as shown in the following equations:

$\lambda = \lambda_1 = \lambda_2 = \lambda_3$,
$\lambda_{cc,2} = \lambda_{12} = \lambda_{23} = \lambda_{13}$,
and $\lambda_{cc,3} = \lambda_{123}$.

Similar to the state transition equations in Sections IV.2.1 and IV.3.1, this system is composed of first-order linear differential equations. These equations are solved using an integrating factor to obtain the general solution. The indefinite integrals are solved analytically right away as they appear; next the integration constant is solved for using the initial conditions.

This system of ODEs is similar to the one in Section IV.3.1 (3 identical EDGs with no recovery) but now the Offsite Recovery state “8” is added. Offsite power can be recovered via a transition from states “0” through “6” and power cannot be lost once it reaches state “8”. Offsite power recovery is not possible once the EDG system has failed (state “7”). The offsite

power recovery rate is $\omega$=0.04 hr$^{-1}$. The system of ODEs for this Markov model is shown in the following equations.

$$
\begin{cases}
\dfrac{dP_0(t)}{dt} = -\left(3\lambda + 3\lambda_{cc,2} + \lambda_{cc,3} + \omega\right)P_0(t) \\
\dfrac{dP_1(t)}{dt} = \lambda P_0(t) - \left(2\lambda + 2\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3} + \omega\right)P_1(t) \\
\dfrac{dP_2(t)}{dt} = \lambda P_0(t) - \left(2\lambda + 2\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3} + \omega\right)P_2(t) \\
\dfrac{dP_3(t)}{dt} = \lambda P_0(t) - \left(2\lambda + 2\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3} + \omega\right)P_3(t) \\
\dfrac{dP_4(t)}{dt} = \lambda_{cc,2}P_0(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_1(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_2(t) - \left(\lambda + \lambda_{cc,2} + \dfrac{1}{3}\lambda_{cc,3} + \omega\right)P_4(t) \\
\dfrac{dP_5(t)}{dt} = \lambda_{cc,2}P_0(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_1(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_2(t) - \left(\lambda + \lambda_{cc,2} + \dfrac{1}{3}\lambda_{cc,3} + \omega\right)P_5(t) \\
\dfrac{dP_6(t)}{dt} = \lambda_{cc,2}P_0(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_1(t) + \left(\lambda + \dfrac{1}{2}\lambda_{cc,2}\right)P_2(t) - \left(\lambda + \lambda_{cc,2} + \dfrac{1}{3}\lambda_{cc,3} + \omega\right)P_6(t) \\
\dfrac{dP_7(t)}{dt} = \lambda_{cc,3}P_0(t) + \left(\lambda_{cc,2} + \dfrac{2}{3}\lambda_{cc,3}\right)\left(P_1(t) + P_2(t) + P_3(t)\right) + \left(\lambda + \lambda_{cc,2} + \dfrac{1}{3}\lambda_{cc,3}\right)\left(P_4(t) + P_5(t) + P_6(t)\right) \\
\dfrac{dP_8(t)}{dt} = \omega\sum_{i=0}^{6} P_i(t)
\end{cases}
$$

And the corresponding initial conditions (ICs) are the same as given in Table 13 with the additional $P_8(t=0)=0$ for state 8. The following notation for ICs is also used: $P_i(t=0)=\tilde{P}_i$, for $i=0,1,2,3,4,5,6,7,8$.

The analytical solutions for the equation above will look pretty similar to the ones derived in Case 2A, the only difference is in the presence of the power recovery rate, $\omega$. The introduction of the following three new coefficients will take care of this.

$$\lambda_1' = \lambda_1 + \omega$$
$$\lambda_2' = \lambda_2 + \omega$$
$$\lambda_{tot}' = \lambda_{tot} + \omega$$

Then the solutions can be written as (using the coefficients from Case 2A and the ones just introduced above):

$$P_0(t) = \tilde{P}_0 e^{-\lambda'_{tot} t}$$

$$P_1(t) = P_2(t) = P_3(t) = \left(\tilde{P}_1 + A\right) e^{-\lambda'_2 t} - A e^{-\lambda'_{tot} t}$$

$$P_4(t) = P_5(t) = P_6(t) = B e^{-\lambda'_{tot} t} + C e^{-\lambda'_2 t} + D e^{-\lambda'_1 t}$$

$$P_7(t) = \frac{\lambda_{cc,3}\tilde{P}_0 - 3A\left(\lambda_{cc,2} + \frac{2}{3}\lambda_{cc,3}\right) + 3B\lambda_1}{\lambda'_{tot}}\left(1 - e^{-\lambda'_{tot} t}\right) +$$

$$+3\frac{\left(\tilde{P}_1 + A\right)\left(\lambda_{cc,2} + \frac{2}{3}\lambda_{cc,3}\right) + C\lambda_1}{\lambda'_2}\left(1 - e^{-\lambda'_2 t}\right) + 3\frac{\lambda_1}{\lambda'_1} D\left(1 - e^{-\lambda'_1 t}\right) + \tilde{P}_7$$

$$P_8(t) = \omega\left\{\tilde{P}_0 \frac{1}{\lambda'_{tot}}\left(1 - e^{-\lambda'_{tot} t}\right) + 3\left[\left(\tilde{P}_1 + A\right)\frac{1}{\lambda'_2}\left(1 - e^{-\lambda'_2 t}\right) - A\frac{1}{\lambda'_{tot}}\left(1 - e^{-\lambda'_{tot} t}\right)\right] +\right.$$

$$\left. +3\left[B\frac{1}{\lambda'_{tot}}\left(1 - e^{-\lambda'_{tot} t}\right) + C\frac{1}{\lambda'_2}\left(1 - e^{-\lambda'_2 t}\right) + D\frac{1}{\lambda'_1}\left(1 - e^{-\lambda'_1 t}\right)\right]\right\}$$

**IV.5 FLEX Model with Mission-Time Load**

In this section we will analyze a backup emergency power system comprised of two standard identical EDGs (iEDGs) and one non-identical FLEX DG. The FLEX DG is comprised of more robust and redundant piece parts, thus it is less susceptible to individual and CCF events. The FLEX DG is in a separate hardened structure far above potential flood zones; thus it does not contribute to nor is it subject to, any component-caused failure events and any externally-caused CCF events are less likely to fail it. While there may be a 2-out-of-2 CCF event for the two identical EDGs, there is no possibility of a CCF event that fails one standard iEDG and the FLEX DG but not the other iEDG. It is assumed that any externally-caused CCF event strong enough to fail one standard iEDG and the FLEX DG would also fail the other iEDG with certainty. The purpose of this model is to quantify how the failure probability (inverse measure of safety margin) of the system changes as a function of the FLEX DG robustness. In order to accomplish this, the single failure rate of the FLEX DG and the 3-out-of-3 CCF rate are varied as fractions of the corresponding baseline failure rates for three iEDGs.

The *designed hazard functions* (here a piecewise constant rate) describe a frequency for a specific failure event, given that no EDGs have failed previously. This follows the definition first

presented in Chapter II, and expressed mathematically in Equation (II-56). The designed failure rates are given for three types of events; a single failure event, a 2-out-of-3 CCF event, and a 3-out-of-3 CCF event. The specific EDGs failed are denoted with a subscript on $\lambda$; for the two iEDGs the subscripts are "1" and "2", while the FLEX DG is denoted with "F". The 2-out-of-3 CCF event can be due to external or component causes, and this is denoted with a superscript "E" or "C", respectively. Only the two iEDGs can experience a 2-out-of-3 CCF; any CCF event which failed an iEDG and the FLEX DG would also fail the other iEDG. The 3-out-of-3 CCF event is only due to external causes. The notation for these events is shown as follows.

single failure event: $\lambda_1$, $\lambda_2$, $\lambda_F$
2-out-of-3 CCF: $\lambda_{12} = \lambda_{12}^E + \lambda_{12}^C$
3-out-of-3 CCF: $\lambda_{12F}$

This EDG system is different from most EDG systems analyzed, hence to obtain all the model parameters some modifications to the standard estimation techniques are made, as described here. The component total unreliability estimates were obtained from the median values listed in Table A.2.17-6 of NUREG/CR-6928 [30]. The alpha factors were obtained from the median value of Section 1.13.1 of "CCF Parameter Estimates, 2012 Update" [31]. Data for a CCF group (CCFG) of 2 were chosen since the two iEDGs are practically in a CCCG by themselves. The data used can be seen in Table 20.

**Table 20 – α-Factor Parameters for FLEX Model.**

| | $\alpha_1$ | $\alpha_2$ | $Q_t$ |
|---|---|---|---|
| FTS (Failure To Start) | 0.990656 | 9.3440E-03 | 3.24E-03 |
| FTL (Failure To Load) | 0.997015 | 2.9850E-03 | 2.25E-03 |
| FTR (Failure To Run) | 0.984593 | 1.5407E-02 | 7.12E-04 |

The single failure (for EDG "1" and "2") and 2-out-of-3 CCF (external cause) event parameters are estimated using the above data and Equation (III-1), assuming a system of two components; the 2-out-of-3 CCF (external cause) event rate is actually estimated as a 2-out-of-2

CCF event. The 2-out-of-3 CCF component-cause event parameter is estimated to be one half of the 2-out-of-3 CCF external-cause event parameter. The rates for the single failure of the FLEX DG, and the 3-out-of-3 CCF event are varied thus creating results for different cases of the FLEX DG robustness. The baseline rates for the single failure of the FLEX DG and the 3-out-of-3 CCF event are one-half of the rates for (EDGs "1" and "2") the single failure and 2-out-of-3 CCF (external cause) rates. These baseline rate values are divided by "robustness factors" (2, 4, 8, and 16) in order to create four different cases of increasing FLEX DG reliability. The designed failure rates can be seen in Table 21; the FLEX rates are given at their baseline value.

**Table 21 – Designed Failure Rates for the FLEX Model.**

| | FTL | FTR |
|---|---|---|
| $\lambda_1$ | 2.23660747668210E-03 | 6.90393326025919E-04 |
| $\lambda_2$ | 2.23660747668210E-03 | 6.90393326025919E-04 |
| $\lambda_F$ | 1.11830373834105E-03 | 3.45196663012959E-04 |
| $\lambda_{12}^E$ | 1.33925233178961E-05 | 2.16066739740813E-05 |
| $\lambda_{12}^C$ | 6.69626165894807E-06 | 1.08033369870406E-05 |
| $\lambda_{12F}$ | 6.69626165894807E-06 | 1.08033369870406E-05 |

The *influenced failure rates* for this system are computed a little differently than in Sections IV.1 through IV.4. The mapping rules from Vaurio [39], as in Equations and (III-10), are again used to estimate these failure rates once one or two EDGs have failed. However, some modification to how these equations are used is needed. The rate for a single failure event of one iEDG, given the other iEDG is failed (and the FLEX DG is operating) can be seen in Equation (IV-12). EDG "1" and "2" can have a CCF from either an external or component cause,

$$\tilde{\lambda}_{1|2} = \lambda_1 + \lambda_{12}^E + \tfrac{1}{2}\lambda_{12}^C, \quad \text{and} \quad \tilde{\lambda}_{1|2} = \tilde{\lambda}_{2|1}. \tag{IV-12}$$

The rate for a single failure event of one iEDG, given the FLEX DG is failed (and the other iEDG is operating), can be seen in Equation (IV-13). There is no possibility of any 2-out-of-3 CCF

between an iEDG and FLEX DG, thus this designed failure rate only includes the single failure rate portion.

$$\tilde{\lambda}_{1|F} = \lambda_1, \text{ and } \tilde{\lambda}_{1|F} = \tilde{\lambda}_{2|F} \quad \text{(IV-13)}$$

The same logic applies to the designed rate for a single failure event of the FLEX DG, given one iEDG has failed (and the other iEDG is operating),

$$\tilde{\lambda}_{F|1} = \lambda_F, \text{ and } \tilde{\lambda}_{F|1} = \tilde{\lambda}_{F|2}. \quad \text{(IV-14)}$$

The rate for a CCF failure event of both iEDGs (given the FLEX DG is failed) is given in Equation (IV-15). The 3-out-of-3 CCF contribution ($\lambda_{12F}$) is due to an external cause, as previously stated.

$$\tilde{\lambda}_{12|F} = \lambda_{12}^{E} + \lambda_{12}^{C} + \lambda_{12F} \quad \text{(IV-15)}$$

The rate for a CCF failure event of an iEDG and the FLEX DG (given an iEDG is failed) can be seen in Equation (IV-16).

$$\tilde{\lambda}_{1F|2} = \lambda_{12F} \quad \text{(IV-16)}$$

The rate for a single failure event of an iEDG (given the other two EDGs have failed) can be seen in Equation (IV-17). An externally-caused 2-out-of-3 CCF event between both iEDGs would appear as a single failure if one of the iEDGs was already failed, thus this failure rate term is found in Equation (IV-17). The same is true for the $\lambda_{12}^{C}$ term, except each iEDG contributes half of this rate. When any two EDGs are failed, the externally-caused 3-out-of-3 failure event would appear as a single failure, which is illustrated with the $\lambda_{12F}$ term included in Equations (IV-17) and (IV-18).

$$\tilde{\lambda}_{1|2F} = \lambda_1 + \lambda_{12}^{E} + \tfrac{1}{2}\lambda_{12}^{C} + \lambda_{12F}, \text{ and } \tilde{\lambda}_{1|2F} = \tilde{\lambda}_{2|1F} \quad \text{(IV-17)}$$

The rate for a failure event of the FLEX DG (given both iEDGs have failed) can be seen in Equation (IV-18).

$$\tilde{\lambda}_{F|12} = \lambda_F + \lambda_{12F} \quad \text{(IV-18)}$$

The baseline influenced failure rates can be seen in Table 22. The single (designed) failure rate for the FLEX DG and the 3-out-of-3 CCF rate are adjusted from their baseline values as discussed in the preceding paragraphs, which in turn affect these rates.

**Table 22 – Baseline Influenced Failure Rates for the FLEX Case.**

| | FTL | FTR |
|---|---|---|
| $\tilde{\lambda}_{1\|2}, \tilde{\lambda}_{2\|1}$ | 2.25334813082947E-03 | 7.17401668493520E-04 |
| $\tilde{\lambda}_{1\|F}, \tilde{\lambda}_{2\|F}$ | 2.23660747668210E-03 | 6.90393326025919E-04 |
| $\tilde{\lambda}_{F\|1}, \tilde{\lambda}_{F\|2}$ | 1.11830373834105E-03 | 3.45196663012959E-04 |
| $\tilde{\lambda}_{12\|F}$ | 2.67850466357923E-05 | 4.32133479481625E-05 |
| $\tilde{\lambda}_{1F\|2}$ | 6.69626165894807E-06 | 1.08033369870406E-05 |
| $\tilde{\lambda}_{1\|2F}, \tilde{\lambda}_{2\|1F}$ | 2.26004439248842E-03 | 7.28205005480561E-04 |
| $\tilde{\lambda}_{F\|12}$ | 1.12500000000000E-03 | 3.56000000000000E-04 |

Neither of the FLEX cases (Sections IV.5.1 and IV.5.2) account for the possibility of offsite power recovery and instead follow a mission-time model of load. But this detail is secondary to the principal purpose of these cases, which is to see how the overall reliability of the system changes as a function of the reliability of the FLEX DG, and to examine the differences in results when the FLEX DG is operated in hot versus cold standby.

**IV.5.1 Hot FLEX Case**

In this case we assume the FLEX DG is operated in hot standby along with the other two iEDGs. Thus, all three EDGs are started and run together at the same time. The results for this case are presented in Section IV.6.3. The MATLAB code used to obtain these results is in Appendix C.

The possible failure sequences considered for this case are described in the bullet points following this paragraph; failures to load and failures to run will not be differentiated. They will

each simply be described as running failures (if a failure is not described as a failure to start, it should be assumed a running failure).

- All three EDGs start successfully followed by...
    - three subsequent individual running failures
    - a CCF of both iEDGs, then a single failure of the FLEX DG
    - a single failure of the FLEX DG, then a CCF of both iEDGs
    - a single failure of an iEDG, then a CCF of an iEDG and the FLEX DG
    - a CCF of all three EDGs
- A single iEDG fails to start followed by…
    - a single failure of an iEDG, then a single failure of a FLEX DG
    - a single failure of a FLEX DG, then a single failure of an iEDG
    - a CCF of an iEDG and the FLEX DG
- The FLEX DG fails to start followed by…
    - two subsequent single failures of both iEDGs
    - a CCF of both iEDGs
- Both iEDGs have a CCF to start followed by a single running failure of the FLEX DG
- All three EDGs experience an externally-caused CCF to start

The initial conditions of the system (failure on demand probabilities) can be seen in Table 23. The probability for states 1 (also 2) and 4 were computed using the alpha factor model parameters from Table 20 (as the probability of a 1-out-of-2 and 2-out-of-2 failure, respectively. This model does not consider the common-cause FTS of an iEDG and the FLEX DG to be a possibility.

**Table 23 – Initial Conditions for the FLEX Model (Hot).**

| | |
|---|---|
| $P_1$ (0); EDG "1" FTS | 3.18001141335362E-03 |
| $P_2$ (0); EDG "2" FTS | 3.18001141335362E-03 |
| $P_3$ (0); FLEX DG FTS | 1.59000570667681E-03 |
| $P_4$ (0); EDG "1","2" CCFTS | 5.99885866463764E-05 |
| $P_5$ (0); EDG "1",FLEX CCFTS | 0.00000000000000E+00 |
| $P_6$ (0); EDG "2",FLEX CCFTS | 0.00000000000000E+00 |
| $P_7$ (0); 3-out-of-3 CCFTS | 2.99942933231882E-05 |
| $P_0$ (0); no EDGs FTS | 9.91959988586646E-01 |

The equation development for this case follows the same principles as the hot standby, 3-EDG system from Section II.3. The MATLAB code for this hot FLEX case is presented in Appendix D.

**IV.5.2 Cold FLEX Case**

In this case we assume the FLEX DG is operated in cold standby while the two iEDGs are operated in hot standby. Thus, the two iEDGs are started and run together at the same time; once they both have failed the FLEX DG is started and run until failure. However, this case does consider the possibility of a 3-out-of-3 externally-caused CCF, even before the FLEX DG has started. The capacity (joint PDF) for the system failure sequence where two hot standby components individually fail followed by a cold standby component individually failing is developed in Section II.5.1.1. The results for this case are first presented in Section IV.6.3 and then compared with the results from Section IV.1 in Section IV.6.4 in order to see how an additional FLEX DG improves the safety margin for an originally two-EDG system. The MATLAB code used to obtain these results is in Appendix D.

The possible failure sequences considered for this case are described in the bullet points following this paragraph; again, failures to load and failures to run will not be differentiated. They will each simply be described as running failures (if a failure is not described as a failure to start, it should be assumed a running failure).

- Both iEDGs start successfully followed by...

    - two subsequent individual running failures of the iEDGs, a successful start of the FLEX DG, and a running failure of the FLEX DG
    - two subsequent individual running failures of the iEDGs, and a failure to start of the FLEX DG
    - a single individual running failure of an iEDG, and a CCF of the iEDG and FLEX DG (due to the 3-way external cause)
    - a two-way CCF of the iEDGs, a successful start of the FLEX DG, and a running failure of the FLEX DG
    - a two-way CCF of the iEDGs, and a failure to start of the FLEX DG
    - a CCF of all three EDGs
- A single iEDG fails to start followed by…
    - an iEDG running failure, a successful start of the FLEX DG, and a running failure of the FLEX DG
    - an iEDG running failure, and a failure to start of the FLEX DG
    - a CCF of an iEDG and FLEX DG (due to the 3-way external cause)
- Both iEDGs have a CCF to start followed by…
    - A failure to start of the FLEX DG
    - a single running failure of the FLEX DG
- An externally-caused CCF fails all three EDGs at the beginning of the LOOP event; a 3-way CCF to start.

The initial conditions of the system (failure on demand probabilities) can be seen in Table 23. The probability for states 1 (also 2) and 4 were computed using the alpha factor model parameters from Table 20 (as the probability of a 1-out-of-2 and 2-out-of-2 failure, respectively. This model does not consider the common-cause FTS of an iEDG and the FLEX DG to be a possibility.

**Table 24 – Initial Conditions for the FLEX Model (Cold).**

| | |
|---|---|
| $P_1$ (0); EDG "1" FTS | 3.18001141335362E-03 |
| $P_2$ (0); EDG "2" FTS | 3.18001141335362E-03 |
| $P_3$ (0); FLEX DG FTS | 0.00000000000000E+00 |
| $P_4$ (0); EDG "1","2" CCFTS | 5.99885866463764E-05 |
| $P_5$ (0); EDG "1",FLEX CCFTS | 0.00000000000000E+00 |
| $P_6$ (0); EDG "2",FLEX CCFTS | 0.00000000000000E+00 |
| $P_7$ (0); 3-out-of-3 CCFTS | 2.99942933231882E-05 |
| $P_0$ (0); no EDGs FTS | 9.93549994293323E-01 |

The cold standby case has an additional set of initial conditions which occur after both iEDGs have failed. $P_3$(*) denotes the probability that the FLEX DG fails to start while $P_0$(*) denotes the probability that the FLEX DG successfully starts.

**Table 25 – Conditions after First Failure for the FLEX Model (Cold).**

| | |
|---|---|
| P3 (*); FLEX DG FTS | 1.59000570667681E-03 |
| P0 (*); FLEX DG successfully starts | 9.98409994293323E-01 |

The complete equation development is not presented for this case. The equations for the failure sequences consisting of three individual running failures are developed here and the complete MATLAB code is presented in Appendix D.

This equation development begins with Equation (IV-19) which is written for three consecutive, generic, running failures for a system composed of two hot standby EDGs and one cold standby EDG. Equation (IV-20) shows Equation (IV-21) written using the failure rate notation introduced in Section IV.5.

$$
\begin{aligned}
&f(\tau_1,t_2',t_F)=\lambda_1(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_1(u)+\lambda_2(u)+\lambda_{12}(u)+\lambda_{12F}(u)\right)du\right\}\times\\
&\tilde{\lambda}_{2|1}(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{2|1}(u)+\lambda_{12F}(u)\right)du\right\}\times\tilde{\lambda}_{F|12}(t-t')\exp\left\{-\int_{t'}^{t}\tilde{\lambda}_{F|12}(u)du\right\}\\
&=\lambda_1(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}(u)\right)du\right\}\\
&\times\tilde{\lambda}_{2|1}(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{total|1}(u)\right)du\right\}\times\tilde{\lambda}_{F|12}(t-t')\exp\left\{-\int_{t'}^{t}\tilde{\lambda}_{F|12}(u)du\right\}
\end{aligned}
\qquad \text{(IV-22)}
$$

In Equations (IV-23) through (IV-24), superscripts L and R are used to denote FTLR versus FTR running failure modes. The first equality in these equations take the generic running failure joint PDF, $f$, in Equation (IV-25) and spell out each specific failure sequence; the second equality in these equations integrates these PDFs over the correct limits to produce the specified CDF, $P$. These failure sequences are written such that EDG "1" always fails first followed by EDG "2" failing at which point the cold EDG "F" begins running until failure. In the argument for the joint PDF, $f$, for each of these equations the specific running failure mode is specified; 1 here refers to one hour of operation which is the separation point between FTLR and FTR modes.

$$
\begin{aligned}
&f(\tau_1<1,t_2'\le 1,t_F\le t_2'+1)=\lambda_1^L(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}^L(u)\right)du\right\}\\
&\times\tilde{\lambda}_{2|1}^L(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{total|1}^L(u)\right)du\right\}\times\tilde{\lambda}_{F|12}^L(t-t')\exp\left\{-\int_{t'}^{t}\left(\tilde{\lambda}_{F|12}^L(u)\right)du\right\}\\
&\text{and}\\
&P(FTLR1,FTLR2,FTLRF)=\int_0^1\int_0^{t_F}\int_0^{t'}f(\tau_1<1,t_2'\le 1,t_F\le t_2'+1)d\tau_1dt_2'dt_F
\end{aligned}
\qquad \text{(IV-26)}
$$

$$
\begin{aligned}
&f(\tau_1<1,t_2'\le 1,t_F>t_2'+1)=\lambda_1^L(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}^L(u)\right)du\right\}\\
&\times\tilde{\lambda}_{2|1}^L(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{total|1}^L(u)\right)du\right\}\\
&\times\tilde{\lambda}_{F|12}^R(t-t')\exp\left\{-\int_{t'}^{t'+1}\left(\tilde{\lambda}_{F|12}^L(u)\right)du-\int_{t'+1}^{t}\left(\tilde{\lambda}_{F|12}^R(u)\right)du\right\}\\
&\text{and}\\
&P(FTLR1,FTLR2,FTRF)=\int_1^T\int_0^1\int_0^{t'}f(\tau_1<1,t_2'\le 1,t_F>t_2'+1)d\tau_1dt_2'dt_F
\end{aligned}
\qquad \text{(IV-27)}
$$

$$f(\tau_1 \le 1, t_2' > 1, t_F \le t_2' + 1) = \lambda_1^L(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}^L(u)\right)du\right\}$$
$$\times\tilde{\lambda}_{2|1}^R(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{total|1}^R(u)\right)du\right\}\times\tilde{\lambda}_{F|12}^L(t-t')\exp\left\{-\int_{t'}^{t}\left(\tilde{\lambda}_{F|12}^L(u)\right)du\right\} \quad \text{(IV-28)}$$

and

$$P(FTLR1, FTR2, FTLRF) = \int_{T-1}^{T}\int_{1}^{t_F}\int_{0}^{1} f(\tau_1 \le 1, t_2' > 1, t_F \le t_2' + 1)d\tau_1 dt_2' dt_F$$

$$f(\tau_1 \le 1, t_2' > 1, t_F > t_2' + 1) = \lambda_1^L(\tau)\exp\left\{-\int_0^{\tau}\left(\lambda_{total}^L(u)\right)du\right\}$$
$$\times\tilde{\lambda}_{2|1}^R(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{total|1}^R(u)\right)du\right\}$$
$$\times\tilde{\lambda}_{F|12}^R(t-t')\exp\left\{-\int_{t'}^{t'+1}\left(\tilde{\lambda}_{F|12}^L(u)\right)du-\int_{t'+1}^{t}\left(\tilde{\lambda}_{F|12}^R(u)\right)du\right\} \quad \text{(IV-29)}$$

and

$$P(FTLR1, FTR2, FTRF) = \int_{1}^{T}\int_{1}^{t_F}\int_{0}^{1} f(\tau_1 \le 1, t_2' > 1, t_F > t_2' + 1)d\tau_1 dt_2' dt_F$$

$$f(\tau_1 > 1, t_2' > 1, t_F \le t_2' + 1) = \lambda_1^R(\tau)\exp\left\{-\int_0^{1}\left(\lambda_{total}^L(u)\right)du-\int_1^{\tau}\left(\lambda_{total}^R(u)\right)du\right\}$$
$$\times\tilde{\lambda}_{2|1}^R(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{total|1}^R(u)\right)du\right\}\times\tilde{\lambda}_{F|12}^L(t-t')\exp\left\{-\int_{t'}^{t}\left(\tilde{\lambda}_{F|12}^L(u)\right)du\right\} \quad \text{(IV-30)}$$

and

$$P(FTR1, FTR2, FTLRF) = \int_{T-1}^{T}\int_{1}^{t_F}\int_{1}^{t'} f(\tau_1 > 1, t_2' > 1, t_F \le t_2' + 1)d\tau_1 dt_2' dt_F$$

$$f(\tau_1 > 1, t_2' > 1, t_F > t_2' + 1) = \lambda_1^R(\tau)\exp\left\{-\int_0^{1}\left(\lambda_{total}^L(u)\right)du-\int_1^{\tau}\left(\lambda_{total}^R(u)\right)du\right\}$$
$$\times\tilde{\lambda}_{2|1}^R(t')\exp\left\{-\int_{\tau}^{t'}\left(\tilde{\lambda}_{total|1}^R(u)\right)du\right\}$$
$$\times\tilde{\lambda}_{F|12}^R(t-t')\exp\left\{-\int_{t'}^{t'+1}\left(\tilde{\lambda}_{F|12}^L(u)\right)du-\int_{t'+1}^{t}\left(\tilde{\lambda}_{F|12}^R(u)\right)du\right\} \quad \text{(IV-31)}$$

and

$$P(FTR1, FTR2, FTRF) = \int_{1}^{T}\int_{1}^{t_F}\int_{1}^{t'} f(\tau_1 > 1, t_2' > 1, t_F > t_2' + 1)d\tau_1 dt_2' dt_F$$

**IV.6 Results Comparison and Discussion**

The results from the specific system cases in Chapter IV are compared and discussed in the following subsections. These results are presented graphically as plots of system failure probability versus time in hours (unless otherwise specified). The system failure probability

results are the CDFs for system failure time computed using a NRI with either a mission-time or offsite-power recovery model of load; these NRIs were evaluated using default error tolerance for numerical integration in MATLAB [32]. Ratios of system failure probabilities are used in the following subsections as relative risk measures to compare how much safer one system arrangement is over another.

**IV.6.1 Different Models of Load for the System of Two Identical EDGs**

As explained in Section II.1.1, both mission-time and offsite-recovery (exponential) models of load were applied to the cases in Section IV.1 through IV.4. The type of load has a large impact on the overall system failure probability, especially for long duration scenarios. The mission-time model of load produces the most conservative results (for times before the mission time) because it assumes there is no possibility that offsite power is recovered for times before the mission time; for times after the mission time, this model of load assumes that offsite power has been recovered with absolute certainty. The offsite-recovery model of load assigns a high probability of recovery past a certain LOOP duration; for the constant recovery rate used in this chapter (0.04 hour$^{-1}$) there is over a 98% probability of offsite power recovery 100 hours after the LOOP event.

This section shows system failure probability results for a mission-time model of load and two different offsite-recovery models of load; one is an exponential distribution of recovery times (constant recovery rate of 0.04 hour$^{-1}$) while the other is a lognormal distribution with mean of the natural logarithm of the recovery time = $\mu = 0.3$ and standard deviation of that quantity = $\sigma = 1.064$. As explained in Section II.1.1, the lognormal recovery time distribution is more accurate for the first 24 hours and comes from industry data presented in [27]. The case of a two identical EDG system was used to compare system failure probability results for the mission-time, exponential recovery, and lognormal recovery load models. This comparison is shown for the first 24 and 96 hours in Figure 9 and Figure 10, respectively.

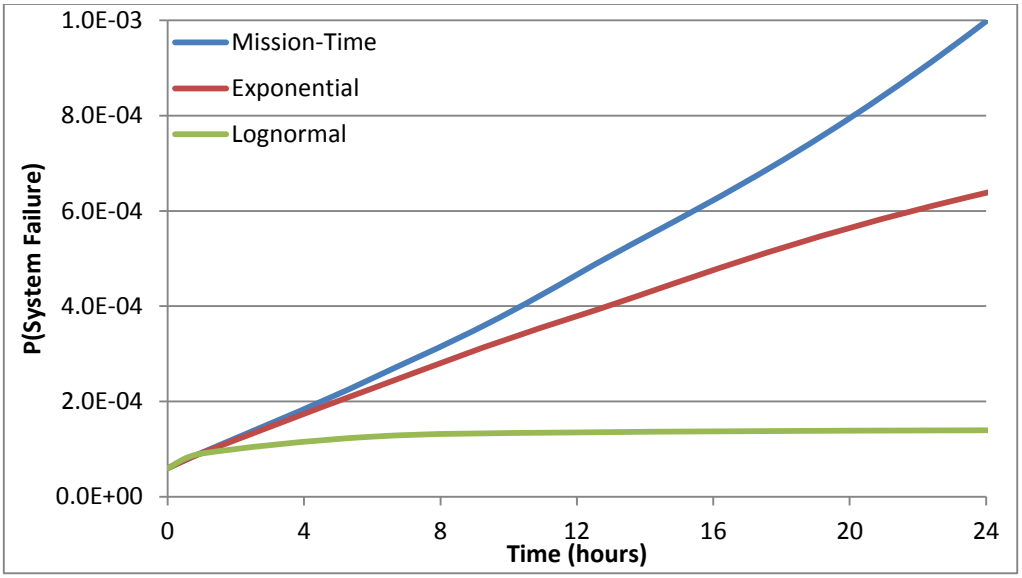


**Figure 9 – Load Comparison for the First 24 Hours of the Two Identical EDGs Case.**

For the lognormal model of load, the system failure probability reaches a plateau around 6 hours and does not increase much after this.

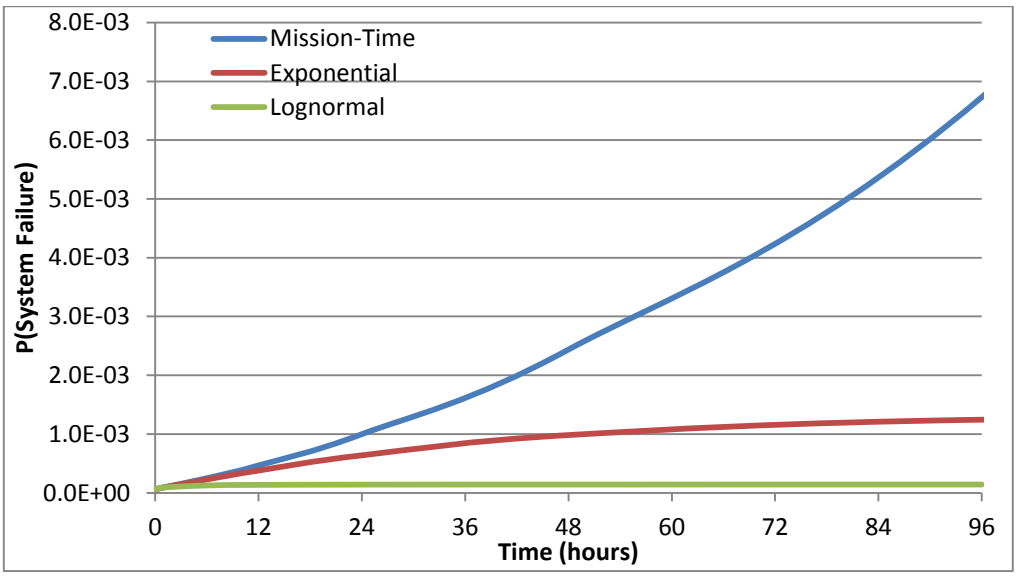


**Figure 10 – Load Comparison for the First 96 Hours of the Two Identical EDGs Case**

For the exponential model of load, the cumulative probability of system failure reaches a plateau around 96 hours and the system failure probability does not increase much after this. While both of the offsite power recovery models of load dramatically decrease the estimated system failure probability compared to the mission-time model, they may be masking interesting results, especially for long-duration scenarios.

**IV.6.2 Two and Three Identical EDG Systems**

A comparison of the results between the two and three identical EDG systems (Section IV.1 through IV.4) is presented in this section for both the mission-time and offsite-recovery (exponential) models of load. We also look at percent contributions from different failure sequences to the total system failure probability at the end of Section IV.6.2.

The comparison is made using a ratio of the two-EDG system failure probability results to the three-EDG system failure probability results, as in Equation (IV-32) . This ratio expresses a multiplication factor for how many times more likely the two-EDG system is to fail, by a given LOOP duration, compared to the three-EDG system; likewise, this ratio expresses a multiplication factor for safety margin of the three-EDG system compared to the two-EDG system. A plot of this ratio versus time is presented in Figure 11; the plot shows results for mission times of 0, 1, 6, 12, 24, 48, 96, 192, 384, and 768 hours.

$$\text{ratio} = P(\text{2EDG system fails}) \Big/ P(\text{3EDG system fails}) \qquad \text{(IV-32)}$$

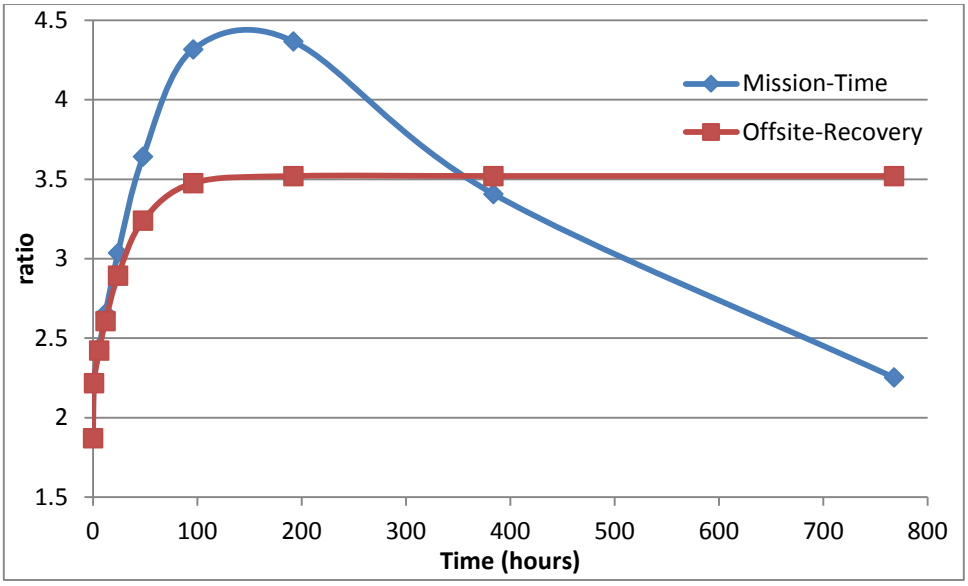


**Figure 11 – The Two- and Three-EDG System Comparison for Mission-Time and Offsite-Recovery Models of Load.**

Both the mission-time and offsite-recovery models of load reach a maximum failure probability ratio (ratio of two-EDG system to three-EDG system) around 196 hours. The ratio for the mission-time load model begins decreasing after that while the offsite-recovery load model ratio plateaus around 3.5.

Some relative contributions to the total system failure probability (for the three-iEDG system) are shown in Table 26. The percent contribution due to 3-out-of-3 FTS, three consecutive individual running failures, and 3-out-of-3 running failure events are shown for various mission times in Table 26.

**Table 26 – Relative Contributions to the Total System Failure Probability.**

| | Demand Failure | Running Failure | |
|---|---|---|---|
| T (hours) | 3-out-of-3 FTS | 3 Single Failures | 3-out-of-3 CCF |
| 1 | 77.0% | 0.03% | 21.7% |
| 6 | 31.5% | 0.18% | 65.6% |
| 24 | 9.75% | 1.75% | 82.1% |
| 96 | 2.06% | 18.0% | 64.8% |
| 192 | 0.69% | 42.3% | 39.5% |
| 768 | 0.04% | 85.4% | 5.47% |

The results in this table indicate that for the first couple hours, the 3-out-of-3 FTS events dominate the contribution to total system failure. As time increases, both the running failure event contributions begin increasing. The 3-out-of-3 CCF contribution increases more quickly and hits a maximum around 24 hours before it begins to decrease. The consecutive individual running failure events contribution increases steadily all the way 768 hours; the individual failure contribution begins to dominate over the CCF contribution around 192 hours.

**IV.6.3 FLEX DG System Case Comparison**

The system failure probability results for both the hot and cold FLEX cases (as described in Sections IV.5.1 and IV.5.2) are presented and compared here. Both of these cases use a mission-time model of load. The results were evaluated for a mission time of 0 to 768 hours, in increments of one hour. The result comparisons in this section are meant to quantify improved safety margin due to the following three factors: operating the FLEX DG in cold standby, increasing the FLEX DG reliability, and decreasing the rate of 3-out-of-3 CCF events. As explained in Section IV.5, the single failure rate for the FLEX DG and the 3-out-of-3 CCF rate were each varied in order to see these combined effects on the overall system reliability. Both of these rates have a base case and they each have cases where “robustness factors” are divided the base case failure rates (thereby lowering the failure rate and increasing the reliability of the FLEX DG). For every case, the same “robustness factor” is divided by the base case rates for both the single failure and 3-out-of-3 CCF events. The last two comparison plots

in this section decompose the “robustness factors” so that separate effects of single FLEX DG failure and 3-out-of-3 CCF events can be examined.

A comparison between the hot and cold standby FLEX arrangements for the base case is shown in Figure 12. The intuitive notion that a system is more reliable when operated in cold standby versus hot standby is confirmed with these results; again, both of these cases have the two iEDGs in hot standby while the FLEX DG arrangement is varied. The difference in reliability between the hot and cold standby cases becomes noticeable about halfway through the 768 hour mission-time, and becomes much more pronounced towards the end of the mission time; however, before a mission time of 200 hours, this difference is miniscule. The small difference for the first 192 hours is because the 3-out-of-3 CCF contribution dominates here (as seen in Table 26) and it is the same for both the hot and cold FLEX arrangements; after 192 hours, the effects from the FLEX DG being in cold standby can be seen since the consecutive single failure contribution begins to dominate (as seen in Table 26).

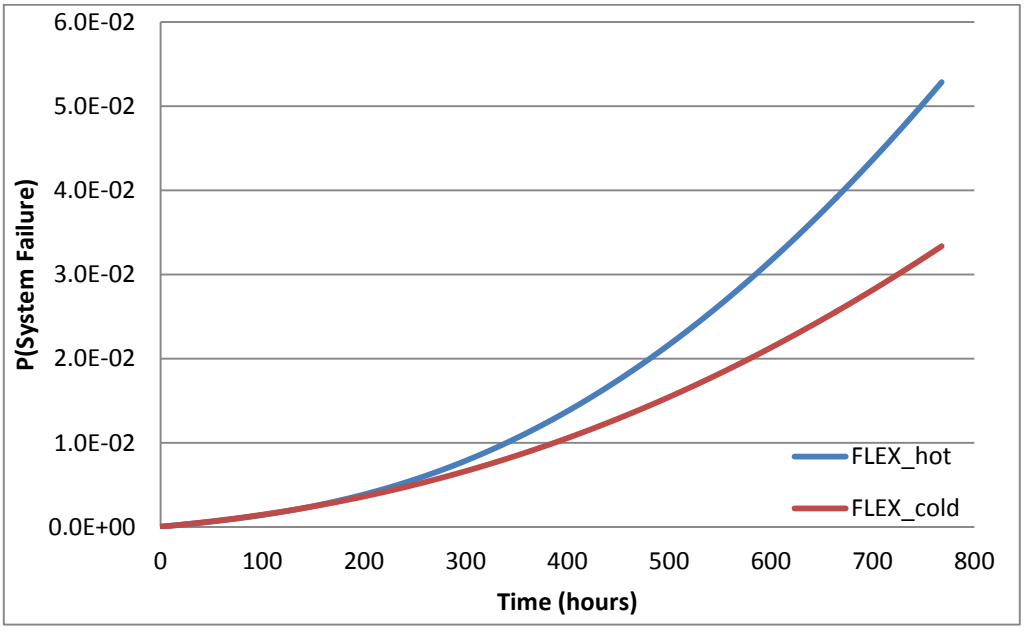


**Figure 12 – Hot and Cold Standby Results for the Base Case.**

Figure 13 is shown in order to compare the base FLEX DG reliability to each of the "robustness factors" for the system of two iEDGs in hot standby and the FLEX DG in cold standby.

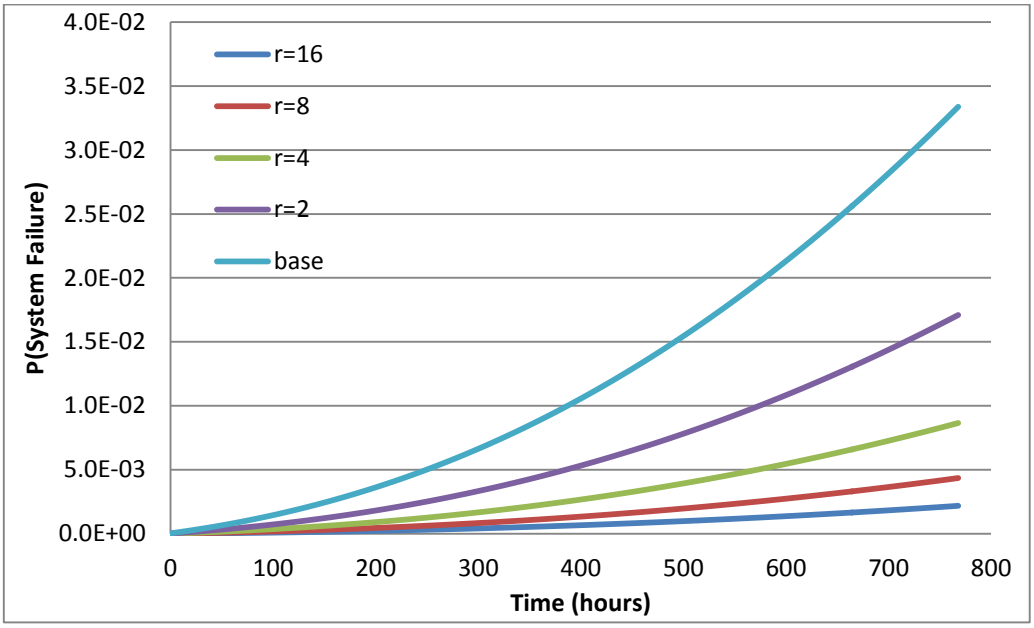


**Figure 13 – All "Robustness Factor" Cases for the Cold FLEX System.**

The results in Figure 13 indicate that the "robustness factor" has a large impact on the overall system failure probability, much more so than whether the FLEX DG is operated in hot or cold standby. These "robustness factors" were applied to both the FLEX DG single failure and 3-out-of-3 CCF rates; next we will examine the impact to safety margin of the FLEX system separately due to the FLEX DG single failure rate and 3-out-of-3 CCF rate in Figure 14 and Figure 15, respectfully.

In order to gain a better understanding of how the FLEX DG reliability impacts the overall system failure probability, we consider another comparison. As explained earlier, the FLEX DG reliability was adjusted using "robustness factors"; these are simply fractions applied to the FLEX DG single failure and 3-out-of-3 CCF rates. In every other section, the same "robustness

factor" was applied to both the FLEX DG single failure and 3-out-of-3 CCF rates. For the results shown in Figure 14, "robustness factors" are only applied to the FLEX DG single failure rate while in Figure 15 they are only applied to the 3-out-of-3 CCF rates. Figure 14 and Figure 15 both show three curves for results at three different mission times (24, 192, and 768 hours). The x-axis for these plots is the "robustness factor", thus as the x-axis increases, the rate decreases for the specific failure event under consideration (single FLEX DG failure or 3-out-of-3 CCF). The y-axis for these plots is the ratio of the base case ("robustness"=1) to the current case (corresponding to the x-axis value for the "robustness factor"). This ratio expresses a multiplication factor for how many times more likely the base case system is to fail, by a given LOOP duration, compared to the system with the specific "robustness factor' applied. This ratio on the y-axis is directly related to the safety margin of the system.

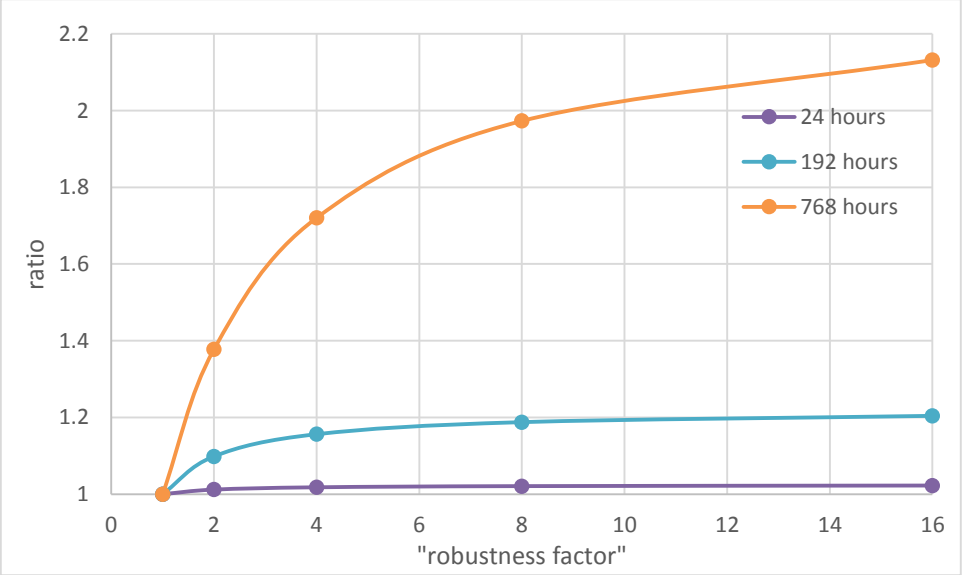


**Figure 14 – Single FLEX DG Failure Impact on Safety Margin.**

Figure 14 clearly shows that decreasing the FLEX DG single failure rate increases safety margin more dramatically for long mission times. In fact, for mission times of 192 hours and

less, decreasing the FLEX DG single failure rate does very little for the safety margin. For mission times of 768 hours, the peak ratio value in Figure 14 suggests that a reduction in single failure rate of 16 times only produces an increase in safety margin of 2.1 times.

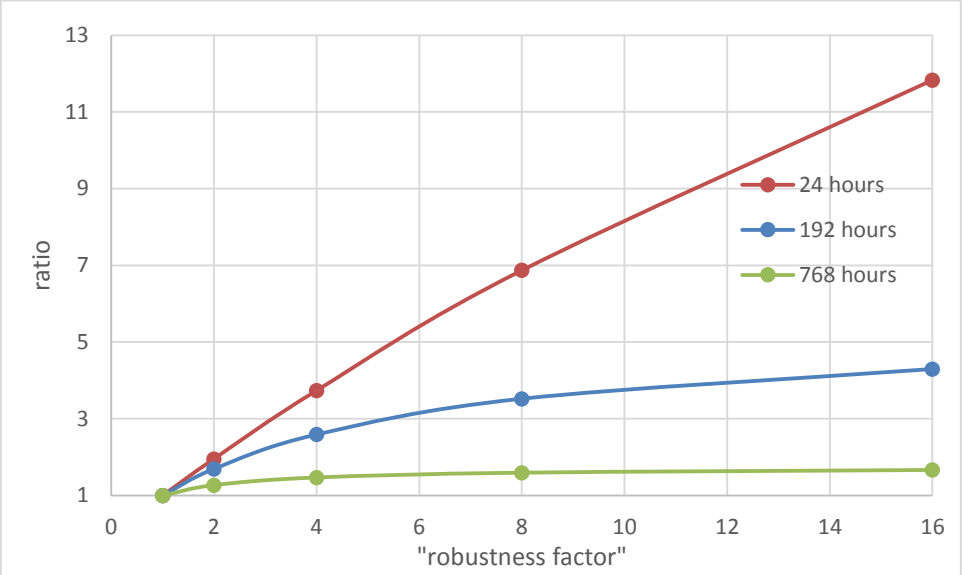


**Figure 15 – CCF (3-out-of-3) Impact on Safety Margin.**

The ratios in Figure 15 are much higher compared to the ratios in Figure 14 (except for the "768 hours" curves in both plots). Figure 15 shows that decreasing the 3-out-of-3 CCF rate increases safety margin more dramatically for shorter mission times. The results in Table 26 can shed some light on what is going on here (even though those results are for a system of three iEDGs, the basic behavior should be the same for the FLEX system). The results in Table 26 suggest that the 3-out-of-3 CCF contribution increases for the first 24 hours (with a maximum around 82% of the total system failure probability), and then begins to decrease. Thus the largest impact that the 3-out-of-3 CCF rate has on the safety margin is for mission times around 24 hours, and this notion is reflected in the "24 hours" curve of Figure 15.

### IV.6.4 Improved Safety Margin Due to FLEX DG

The failure probability results for the two identical EDGs with a mission-time load (Section IV.1) are compared to the cold FLEX system (base case of Section IV.5.2) in this subsection. The ratio of the two-EDG system failure probability to the FLEX system failure probability is plotted versus time in Figure 16 (with data legend "FLEX"). This ratio provides a measure of relative risk as a means to show improved safety margin to a two-EDG system that is upgraded with an additional FLEX DG. The ratio of the two-EDG system failure probability results to the three-EDG system failure probability results (with mission-time loads) are also plotted in Figure 16 (with data legend "3 EDGs") as a way to compare improvement (to a originally two-EDG system) from adding an EDG versus a FLEX DG.

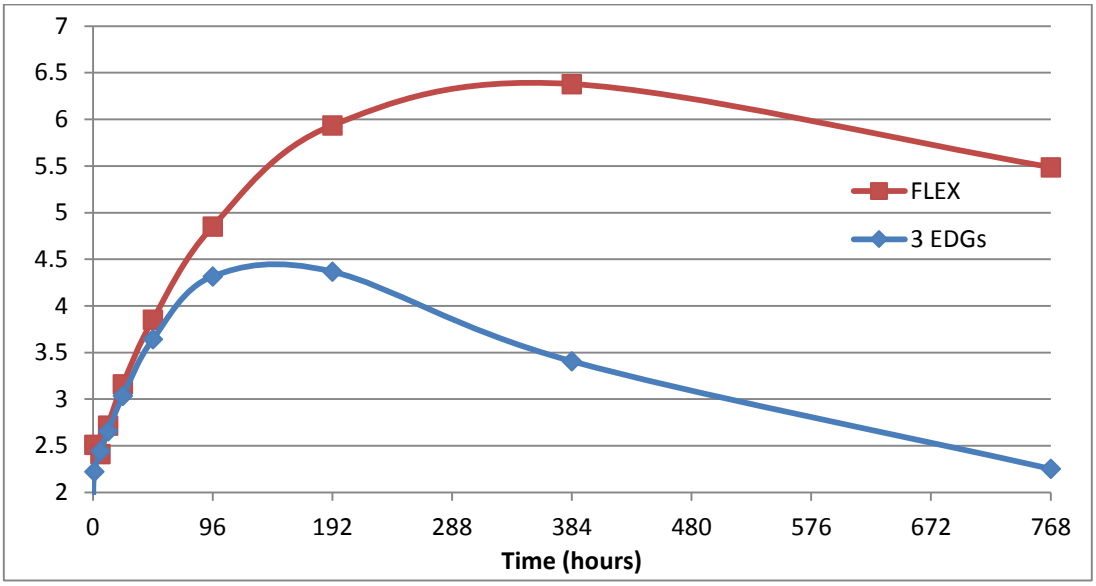


**Figure 16 – Additional FLEX DG Impact on Safety Margin.**

The ratio for the "FLEX" curve in Figure 16 is 2 at the beginning of the LOOP event, increases to nearly 6.5 around a LOOP duration of 300 hours, and then decreases to a ratio of about 5.5 after a 768 hour LOOP duration. This ratio provides a measure for improved safety

margin from adding a FLEX DG to two-EDG system. When compared to the results ratio of the two-EDG to three-EDG systems, it can be easily seen that the FLEX system has a higher safety margin for LOOP durations of around 96 hours and longer.

# CHAPTER V

# FUTURE WORK

Two model features that this thesis did not expand on and could be explored as future work are using time-dependent failure rates and accounting for EDG repair. The NRI can accept time-dependent failure rates (under certain conditions, as discussed in Section V.3.1), but none of the cases in Chapter IV applied this capability. Throughout the research required to complete this thesis, it became apparent that a semi-Markov model may be a more appropriate way to capture the important processes associated with the LOOP/SBO problem (especially when modeling a system containing cold standby components). Modeling the LOOP/SBO problem with a semi-Markov process is explored in this chapter.

A simple two-EDG system case with time-dependent failure rates is presented in Section V.1. Next, a brief semi-Markov model development is reproduced from [42] in Section V.2. The simple two-EDG system problem is solved using the developed semi-Markov model in Section V.2 and the NRI in Section V.3. The results for these two different models are compared in Section V.4.

The problem in this chapter does not include the possibility of EDG repair; a semi-Markov model could account for this repair but the NRI developed in this thesis could not. The main goal of this chapter is to point toward potential features of creating a model based on a semi-Markov process and suggest further development of this idea as an extension of the work in this thesis.

## V.1 Time-Dependent Problem

The system is composed of two EDGs, each subject to individual failures and externally-caused CCFs. The possible failure events are characterized by Weibull distributions of failure times. This problem assumes that there are no failure-on-demand events (both EDGs always start), only failures while running. This system will be modeled in both cold and hot standby redundancy. The NRI in this thesis is only valid for hot standby systems (when constant failure rates are used) while the semi-Markov model is suited for cold standby systems; however each

of these models will be modified so that results for both hot and cold standby systems can be compared between the two models.

There are three different possible failure events; either the first EDG can fail while the other EDG is in standby (hot or cold), both EDGs can fail due to a CCF (while one EDG is in standby), or the second EDG can fail after the first EDG has already failed. The state transition diagrams for the cold and hot standby system cases can be seen in Figure 17 and Figure 18, respectively. Both of these systems start in state 0 at time equals zero with absolute certainty. For the cold standby system only one EDG starts in state 0 while for the hot standby case both EDGs start. For the hot standby case, states 1 and 2 represent either combination of the event when the active EDG fails and the standby EDG becomes active.

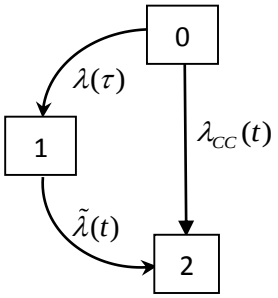


**Figure 17 – Cold Standby System Case.**

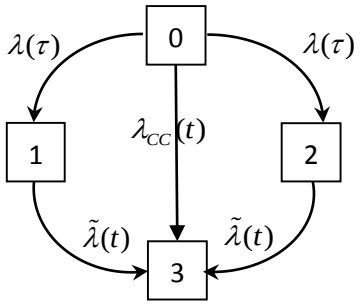


**Figure 18 – Hot Standby System Case.**

Each of the state transition events above are described by a Weibull distribution of failure times. The shape parameter, $\beta$, for each of these events is 1.3 to represent an increasing failure rate. The scale parameters for the failure rates $\lambda(t)$, $\tilde{\lambda}(t)$, and $\lambda_{CC}(t)$ are 0.1, 0.11, and 0.01 failures per hour, respectively. The hazard function, PDF, and CCDF for a transition from state i to j can be found in Equations (V-1)-(V-3), respectively.

$$\lambda_{ij}(t) = \lambda_{ij}^{\beta_{ij}} \beta_{ij} t^{\beta_{ij}-1} \tag{V-1}$$

$$f_{ij}(t) = \lambda_{ij}^{\beta_{ij}} \beta_{ij} t^{\beta_{ij}-1} \exp\left\{-(\lambda_{ij}t)^{\beta_{ij}}\right\} \tag{V-2}$$

$$\bar{F}_{ij}(t) = 1 - \int_0^t f_{ij}(t)dt = \exp\left\{-(\lambda_{ij}t)^{\beta_{ij}}\right\} \tag{V-3}$$

**V.2 Semi-Markov**

A semi-Markov model is suited to analyze cold standby systems because this type of process tracks the sojourn time (the waiting time between transition events); after each transition to a new state, sojourn time resets to zero. This sojourn time is contrasted with what will be referred to as clock time, which is the time the system as a whole has been operating since the initiating event. For a semi-Markov process (only tracks sojourn time), restarting at time zero after each transition means that any time-dependent hazard functions are also reset to zero which lends itself to a new component coming into operation. When the semi-Markov model is applied to the hot standby case (seen in

Figure 18), there is a slight issue with states 1 and 2. The standby EDG has been running since time 0 but comes into action after this, once the system is in state 1 or 2. The standby EDG should have experienced wear since the beginning of state 0, but the transition to state 1 or 2 resets the time-dependent failure rate to a "brand-new" condition. Thus this case is referred to as "warm" standby. The term "warm" standby is used elsewhere in reliability engineering literature to refer to refer to a component which obtains some amount of wear while in standby but not the full amount of wear that it would obtain if it was not in standby, but instead fully operating and loaded; the use of "warm" standby in this chapter should not be confused with the definition typically used in reliability engineering. A generalized semi-Markov tracks both the clock time and sojourn time [43], but its mathematical formulation is beyond the scope of this thesis.

The model developed here was adapted from [42] and the interested reader should refer to this document for further details. The basics of the model development are supplied here. The probability that the system is in state j at time t, given that it entered state i at time zero, is solved for in Equation (4) of [42], and this is shown in Equation (V-4),

$$\phi_{ij}(t) = \delta_{ij} W_i(t) + \sum_k \int_0^t h_{ik}(\tau)\phi_{kj}(t-\tau), \tag{V-4}$$

where,

$t \geq 0$ , $\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$ , and $W_i(t) = 1 - \int_0^t w_i(t)$.

The other two parameters needed for this model are defined in terms of the PDF and CCDF for the Weibull transition events. The holding time probability is defined in Equation (V-5) and the unconditional waiting time density is defined in Equation (V-6).

$$h_{ij}(t) = f_{ij}(t) \prod_{k \neq j} \bar{F}_{ij}(t) \tag{V-5}$$

$$w_i(t) = \sum_j h_{ij}(t) \tag{V-6}$$

Two algorithms to solve Equation (V-4) are derived in Appendix A of [42]. The algorithm based on the trapezoidal rule was used to solve both the hot and cold system cases from Section V.1. These algorithms were coded in MATLAB and can be seen in Appendix E; Section E.1 contains the code for the cold standby case while Section E.2 contains the code for the "warm" standby case.

**V.3 NRI**

The NRI is primarily used to analyze hot standby systems, but it can be modified for cold standby, as explained in Section II.5.1. The general two-EDG NRI model developed in Section II.2 was used for the hot standby case of the time-dependent problem in Section V.1. The cold standby modification developed in Section II.5.1 was used for the cold case of this time-dependent problem. The MATLAB code used to produce the NRI results in Section V.4 is in Section E.3 and E.4 of Appendix E (for the cold and hot standby case, respectively).

### V.3.1 Conditions for Time-Dependent Hazard Functions

The bivariate and multivariate failure time joint PDFs presented by Shaked and Shanthikumar are only proper PDFs when the conditional hazard functions satisfy certain conditions; the following quote from [28] explains these conditions for the two-component (bivariate) case and the mathematical conditions are given in Equation (V-7). For "the multivariate conditional hazard rate functions determine the joint distribution to be a proper bivariate density function, it is necessary that the $\lambda-$ functions are nonnegative and that they satisfy" the following:

$$\begin{aligned} &\int_0^\infty [\lambda_1(u)+\lambda_2(u)]du=\infty, \\ &\int_{t_1}^\infty \tilde{\lambda}_2(u|t_1)du=\infty \text{ for all } t_1>0, \text{ and} \\ &\int_{t_2}^\infty \tilde{\lambda}_1(u|t_2)du=\infty \text{ for all } t_2>0. \end{aligned} \tag{V-8}$$

The hazard function notation above was slightly modified to fit the bivariate joint PDF presented in Equation (II-21). More details about the conditions on the construction of hazard functions for the multivariate case can be found on pages 290-291 of [28].

### V.4 Results

A plot of the results (system failure probability versus time) can be seen in Figure 19.

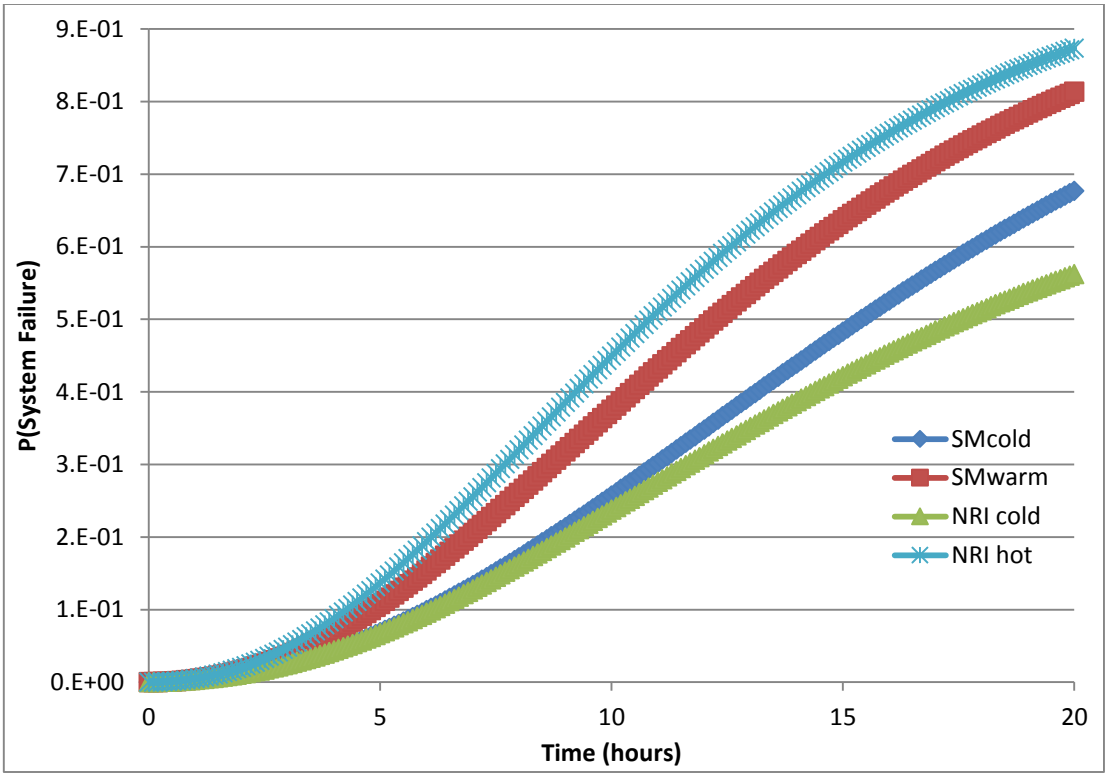


**Figure 19 – Results for the Time-Dependent System Cases.**

It makes sense that the hot standby case results give a higher failure probability for the NRI than the semi-Markov model. This is because in the semi-Markov model the standby EDG does not experience the full amount of wear from when it originally starts in state 0, since time resets to zero when the system moves to another state (specifically states 1 or 2).

It is still unclear why the NRI and semi-Markov model do not agree for the cold standby case. It is known that semi-Markov processes are more suitable for modeling cold standby systems, so we assume that semi-Markov model is more accurate. The NRI is intended for hot standby systems; the modification to cold standby definitely works with constant failure rate inputs (as shown in Section II.5.1 and II.5.4), but it is still unclear how accurate it is with time-dependent failure rate inputs.

# CHAPTER VI

# SUMMARY AND CONCLUSIONS

In this thesis a system failure time PDF for an onsite emergency AC power system (composed of 2 or 3 EDGs) was developed in Chapter II based on a joint PDF developed by Shaked and Shanthikumar [6]. This system failure PDF accounts for the timing dependencies of individual EDG failures, can accept time-dependent failure rates (for a hot standby system only), and can be modified to model a cold standby or mixed case system (this modification is discussed in Section II.5.1). This PDF can be integrated alone or multiplied with an offsite power recovery time distribution to create the NRI model with a mission-time or offsite-recovery loads (discussed in Section II.1.1). A standard Markov model was also developed in order to verify the accuracy of the NRI model results.

Nuclear industry and SPAR model data were used as inputs to the NRI to create the 6 different model cases in Chapter IV. First, a system of two identical EDGs (in hot standby) was modeled with both a mission-time or offsite-recovery load. Next, a system of three identical EDGs (hot standby) was modeled with both a mission-time or offsite-recovery load. Finally, the thesis objective case for a system composed of two identical EDGs and one FLEX DG was modeled with a mission-time load in Section IV.5. This system had two model cases, one where the FLEX DG was operating in hot standby while the other case had it operating in cold standby. As expected, an additional EDG improves system reliability (result shown in Section IV.6.2) while a FLEX DG improves it further (result in Section IV.6.4). In Section IV.6.4, improved safety margin due to an additional FLEX DG is quantified by looking at the ratio of system failure probabilities for a two-EDG system compared to the FLEX DG system. It can be seen that the FLEX DG system is half as likely to fail for the entire range of LOOP durations that were examined (0 to 768 hours); the failure probability ratio (for the FLEX system compared to the two-EDG system) drops to one third by 24 hours and decreases even further for longer LOOP durations.

Some conclusions about EDG system behavior and modeling technique effects can be drawn from the results comparison in Section IV.6. As discussed in Section IV.6.1, Figure 9 and

Figure 10 suggest that an offsite power recovery model of load could mask interesting results for long duration LOOP events when compared to mission-time models of load. The choice of load is very important when making risk-informed decisions based on system failure probability models; a range of different load models should be tested and considered so that a more complete picture of offsite power recovery can be captured. This notion of load choice potentially masking some system behavior appears again when examining the results in Figure 11. The peak ratio (this ratio is a measure of safety margin, as explained in Section IV.6.2) in the mission-time load model curve of this figure shows that the difference in safety margin for the three-EDG system over the two-EDG system occurs around 192 hours and for longer times this difference begins to decrease. The ratio for offsite-power recovery model of load in Figure 11 does not show this peak but instead plateaus around 192 hours; this masks some behavior of the two systems for times longer than 192 hours. The curve peak for the mission-time model in Figure 11 suggest that adding a third EDG to the system has the largest increase in safety margin for the first 192 hours. The results in Table 26 show that the 3-out-of-3 CCF contribution to the total system failure probability dominates over the single failure contribution for the first 100 hours. The results in Figure 11 and Table 26 indicate that reducing 3-out-of-3 CCF is crucial to effectively increase safety margin for the first 100 hours of a LOOP.

Results from the FLEX DG system cases are compared in Section IV.6.3 and some conclusions can be drawn about these results. The results in Figure 12 and Figure 13 show that the "robustness factor" (applied to lower both the FLEX DG single failure rate and 3-out-of-3 CCF rate) has a much larger impact on safety margin than whether or not the FLEX DG is operated in hot or cold standby. In order to examine the impact to safety margin of the FLEX system separately due to the FLEX DG single failure rate and 3-out-of-3 CCF rate, Figure 14 and Figure 15 were created. For the results shown in Figure 14, "robustness factors" are only applied to the FLEX DG single failure rate while in Figure 15 they are only applied to the 3-out-of-3 CCF rates. The ratios (measure of safety margin) in Figure 15 are much higher compared to the ratios in Figure 14 (except for the "768 hours" curves in both plots). Figure 15 shows that decreasing the 3-out-of-3 CCF rate increases safety margin very dramatically for "short" mission times (short here refers to mission times around 24 hours and actual plant data [27] suggests that LOOP events longer than 24 hours are extremely rare). Thus the most effective way to

increase safety margin (for the most likely LOOP duration scenarios) is to reduce the likelihood of 3-out-of-3 CCFs.

## REFERENCES


[1] Nuclear Energy Institute (NEI), "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide, NEI 12-06 [Rev. 0]," Washington, D.C., 2012.

[2] E. J. Kee, S. S. Rodgers, F. Yilmaz, P. Nelson, P. J. Rodi, V. Moiseytseva and C. Gilmore, "Probability of Critical Station Blackout via Computational Evaluation of Nonrecovery Integrals," in ICONE20POWER2012, Anaheim, 2012.

[3] S. Rodgers, C. Betancourt, E. Kee and P. Nelson, "Toward Quantification of the Uncertainty in Estimating Frequency of Critical Station Blackout," in International Conference on Mathematics and Computational Methods Applied to Nuclear Science and Engineering, Rio de Janeiro, 2011.

[4] S. M. Hess, N. Dinh, J. P. Gaertner and R. Szilard, "Risk-informed Safety Margin Characterization," in 17th International Conference on Nuclear Engineering, Brussels, 2008.

[5] S. M. Hess, R. Youngblood and D. Vasseur, "Recent Trends in Risk-Informed Safety Margin Characterization," in ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis, 2011.

[6] J. G. Shanthikumar and M. Shaked, "Multivariate Conditional Hazard Rates and the MIFRA and MIFR Properties," Journal of Applied Probability, vol. 25, no. 1, pp. 150-168, 1988.

[7] U.S. Nuclear Regulatory Commission, "WASH-1400: Reactor Safety Study; NUREG-75/014," Washington DC, 1975.

[8] Nathan Siu, et al., "PSA Technology Challenges Revealed by the Great East Japan Earthquake," in PSAM Topical Conference in Light of the Fukushima Dai-Ichi Accident, Tokyo, 2013.

[9] Modarres and Mohammad, "Technology-Neutral Nuclear Power Plant Regulation: Implications of a Safety Goals-Driven Performance-Based Regulation," Nuclear Engineering and Technology, vol. 37, no. 3, pp. 221-230, 2005.

[10] U.S. Nuclear Regulatory Commission, "Individual Plant Examination for Severe Accident Vulnerabilities; 10 CFR 50.54(f), Generic Letter 88-20," Washington, D.C., 1988.

[11] U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," 1995.

[12] U.S. Nuclear Regulatory Commission, "Risk-Informed and Performance-Based Plan," 2006.

[13] U.S. Nuclear Regulatory Commission, "Glossary: Design-basis accident," 2015. [Online]. Available: http://www.nrc.gov/reading-rm/basic-ref/glossary/design-basis-accident.html. [Accessed 16th May 2015].

[14] U.S. Nuclear Regulatory Commission, "NRC Order Number EA-12-049, Order To Modify Licenses With Regard To Requirements For Mitigation Strategies For Beyond-Design-Basis External Events," Washington, D.C., 2012.

[15] M. Powell, Interviewee, email communication about the FLEX plan. [Interview]. June 2015.

[16] W. Kuo, V. R. Prasad, F. A. Tillman and C.-L. Hwang, "Cold standby redundancy in a single-component system," in Optimal Reliability Design: Fundamentals and Applications, New York, Cambridge University press, 2001, pp. 23-25.

[17] U.S. Nuclear Regulatory Commission, 10 CFR, Appendix A to Part 50, Criterion 17—Electric power systems, Washington, D.C..

[18] South Texas Project, "South Texas Project Electrical Generating Station PRA: 4.16KV Electric Power System Notebook," 2012.

[19] D. Mandelli, C. Smith, T. Riley, J. Schroeder, C. Rabiti, A. Alfonsi, J. Nielsen, Maljovec, Dan, Wang, Bei and Pascucci, Valero, "Risk Informed Safety Margin Characterization (RISMC): BWR Station Blackout Demonstration Case Study," Idaho National Laboratory, Idaho Falls, Idaho, 2013.

[20] Smith, Curtis, D. Schwieder, C. Phelan, A. Bui and P. Bayless, "Risk Informed Safety Margin Characterization (RISMC): Advanced Test Reactor Demonstration Study," Idaho National Laboratory, Idaho Falls, 2012.

[21] C. Smith and D. Mandelli, "A risk-informed approach to safety margins analysis," Nuclear Engineering International, vol. 58, no. 707, pp. 38-40, 2013.

[22] J. A. Schroeder, W. Galyean, "Resolution of SPAR Model Technical Issues," Idaho National Lab, Idaho Falls, 2010.

[23] D. R. Cox, "Regression Models and Life-Tables," Journal of the Royal Statistical Society, vol. 34, no. 2, pp. 187-202, 1972.

[24] J. F. Lawless, "Multivariate Models: Hazard Function Formulations," in Statistical Models and Methods for Lifetime Data, New York, Wiley, 1982, pp. 480-482.

[25] Høyland, M. Rausand and Arnljot, "Reliability of Safety Systems," in System Reliability Theory: Models, Statistical Methods, and Applications, Wiley, 2003.

[26] American Society of Mechanical Engineers, Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME, 2009.

[27] S. A. Eide, C. D. Gentillon, T. E. Wierman and D. M. Rasmuson, "Reevaluation of Station Blackout Risk at Nuclear Power Plants," US Nuclear Regulatory Commission, 2005.

[28] M. Shaked and J. G. Shanthikumar, "Multivariate conditional hazard functions - an overview," Applied Stochastic Models in Business and Industry, vol. 31, pp. 285-296, 2014.

[29] U.S. Nuclear Regulatory Commission, "Risk Assessment of Operational Events: Volume 3 - SPAR Model Reviews," 2010.

[30] S. A. Eide, T. E. Wierman, C. D. Gentillon, D. M. Rasmuson and C. L. Atwood, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, D.C., 2007.

[31] U.S. Nuclear Regulatory Commission, "CCF Parameter Estimations, 2012 Update," 2013.

[32] MATLAB R2014a, Natick, MA: The MathWorks Inc., 2014.

[33] N. J. McCormick, "Convoluted Distribution Models," in Reliability and Risk Analysis: Methods and Nuclear Power Applications, Seattle, Academic Press, 1981, p. 49.

[34] T. E. Wierman, D. M. Rasmuson and A. Mosleh, "Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding," U.S. Nuclear Regulatory Commission, Washington DC, 2007.

[35] C. L. C.L. Atwood, J. L. LaChance, H. F. Martz, D. L. Anderson, M. Englehardt, D. Whitehead and T. Wheeler, "Handbook of Parameter Estimation for Probabilistic Risk Assessment," U.S. NRC, Washington DC, 2003.

[36] S. Eide, "Historical Perspective on Failure Rates for US Commercial Reactor Components," Reliability Engineering and System Safety, p. 80:123–132, 2003.

[37] A. Mosleh, K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge and D. M. Rasmuson, "Procedures for Treating Common-cause Failures in Safety and Reliability Studies, Volume 1," U.S. Nuclear Regulatory Commission, Washington DC, 1988.

[38] A. Mosleh, K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge and D. M. Rasmuson, "Procedures for Treating Common-cause Failures in Safety and Reliability Studies, Volume 2," 1989.

[39] J. K. Vaurio, "Consistent mapping of common cause failure rates and alpha factors," Reliability Engineering and System Safety, vol. 92, no. 5, pp. 628-645, 2007.

[40] F. M. Marshall, D. M. Rasmuson and A. Mosleh, "Common-Cause Failure Parameter Estimations," US Nuclear Regulatory Commission, Washington, DC, 1998.

[41] Microsoft Excel 2010, Microsoft Corporation , 2010.

[42] W. R. Nunn and A. M. Desiderio, "Semi-Markov Processes: An Introduction," Defense Technical Information Center, Arlington, Virginia, 1977.

[43] P. W. Glynn, "A GSMP Formalism for Discrete-Event Systems," Department of Operations Research, Stanford University, Stanford, California, 1988.

## APPENDIX A

## TWO IDENTICAL EDG SYSTEM MATLAB MODELS

This appendix contains the MATLAB code for the system of two iEDGs (Sections IV.1 and IV.2). This code contains both the mission-time and offsite recovery models of load; different values for the variable "H" can be toggled on and off to obtain the specific load cases. This code also contains both the default and low error tolerances for numerical integration.

```
%% Begin input
clear all
T=2000; % mission time in hours
H=@(x) 1;  % toggle for norecovery case
% H=@(x)exp(-.4.*x); % exp CCDF in time (hours) for recovery of offsite
power
% H=@(x)exp(-.04.*x); % exp CCDF in time (hours) for recovery of
offsite power
% H=@(x)(1-logncdf(x,.3,1.064)); % "realistic" lognormal CCDF model of
load
%% failure data
% Failure to start data; failure-on-demand probabilities
QFTS=3.24E-03;alpha1FTS=0.990656;alpha2FTS=1-
alpha1FTS;alphatFTS=alpha1FTS+2*alpha2FTS;
% Initial Conditions; failure on demand probabilities
P1=alpha1FTS*QFTS/alphatFTS; % EDG "0"
P2=P1;            % EDG "1" ; 0 and 1 are identical and have the same
prob/rates
P3=2*alpha2FTS*QFTS/alphatFTS;
P0=1-P1-P2-P3;
% Failure to load-and-run data
QFTLR=2.25E-03;alpha1FTLR=0.997015;alpha2FTLR=1-
alpha1FTLR;alphatFTLR=alpha1FTLR+2*alpha2FTLR;
% Failure to run data; constant failure rates
QFTR=7.12E-04; alpha1FTR=0.984593;alpha2FTR=1-
alpha1FTR;alphatFTR=alpha1FTR+2*alpha2FTR;
%% failure rates
r1_2a=alpha1FTLR*QFTLR/alphatFTLR; r1_2b=alpha1FTR*QFTR/alphatFTR;
r2_2a=2*alpha2FTLR*QFTLR/alphatFTLR; r2_2b=2*alpha2FTR*QFTR/alphatFTR;
r1_1a=r1_2a+.5*r2_2a; r1_1b=r1_2b+.5*r2_2b;
total_a=2*r1_2a+r2_2a; total_b=2*r1_2b+r2_2b;
%%
ymax = @(z) z;
%% First contribution from two independent failures
%% Computation of nonrecovery integral
% 2 Independent FTLR/FTR events
% t0<t1
```

```
FTS_FTLR=@(z)(P1.*(r1_1a.*exp(-r1_1a.*z)).*H(z));
FTS_FTR=@(z)(P1.*(r1_1b.*exp(-r1_1a).*exp(-(r1_1b.*(z-1)))).*H(z));
FTLR_FTLR=@(z,y)(P0.*(r1_2a.*exp(-total_a.*y)).*(r1_1a.*exp(-r1_1a.*(z-
y))).*H(z));
FTLR_FTR=@(z,y)(P0.*(r1_2a.*exp(-total_a.*(y))).*(r1_1b.*exp(-
r1_1a.*(1-y)).*exp(-(r1_1b.*(z-1)))).*H(z));
FTR_FTR=@(z,y)(P0.*(r1_2b.*exp(-total_a).*exp(-total_b.*(y-
1))).*(r1_1b.*exp(-(r1_1b.*(z-y)))).*H(z));
%% 2-way common-cause failure
CCFTLR = @(z)(P0.*(r2_2a.*exp(-total_a.*z)).*H(z));
CCFTR = @(z)(P0.*(r2_2b.*exp(-total_a).*exp(-(total_b.*(z-1)))).*H(z));
%% Numerical Integration   toggle for default and low tolerances
% % probabilities
% P_FTS_FTLR=2.*integral(FTS_FTLR,0,1);
% P_FTS_FTR=2.*integral(FTS_FTR,1,T);
% P_FTLR_FTLR=2.*integral2(FTLR_FTLR,0,1,0,ymax);
% P_FTLR_FTR=2.*integral2(FTLR_FTR,1,T,0,1);
% P_FTR_FTR=2.*integral2(FTR_FTR,1,T,1,ymax);
% % probabilities
% FTS_CCF = P3;
% FTLR_CCF = integral(CCFTLR,0,1);
% FTR_CCF = integral(CCFTR,1,T);
%
% % probabilities
P_FTS_FTLR=2.*integral(FTS_FTLR,0,1,'AbsTol',1e-6,'RelTol',1e-2);
P_FTS_FTR=2.*integral(FTS_FTR,1,T,'AbsTol',1e-6,'RelTol',1e-2);
P_FTLR_FTLR=2.*integral2(FTLR_FTLR,0,1,0,ymax,'AbsTol',1e-
6,'RelTol',1e-2);
P_FTLR_FTR=2.*integral2(FTLR_FTR,1,T,0,1,'AbsTol',1e-6,'RelTol',1e-2);
P_FTR_FTR=2.*integral2(FTR_FTR,1,T,1,ymax,'AbsTol',1e-6,'RelTol',1e-2);
% probabilities
FTS_CCF = P3;
FTLR_CCF = integral(CCFTLR,0,1,'AbsTol',1e-6,'RelTol',1e-2);
FTR_CCF = integral(CCFTR,1,T,'AbsTol',1e-6,'RelTol',1e-2);
% %
%% Total
if T==0
  PCSBO=FTS_CCF;
elseif T<=1
  PCSBO=FTS_CCF+P_FTS_FTLR+P_FTLR_FTLR+FTLR_CCF;       %may be
incorrect for times between 0 and 1 hour
elseif T>1

PCSBO=FTS_CCF+FTLR_CCF+FTR_CCF+P_FTS_FTLR+P_FTLR_FTLR+P_FTR_FTR+P_FTS_F
TR+P_FTLR_FTR;
end
```

## APPENDIX B

## THREE IDENTICAL EDG SYSTEM MATLAB MODELS

This appendix contains the MATLAB code for the system of three iEDGs (Sections IV.3 and IV.4). This code contains both the mission-time and offsite recovery models of load; different values for the variable "H" can be toggled on and off to obtain the specific load cases. This code also contains both the default and low error tolerances for numerical integration.

```
%% Begin Input
clear all
%
T=768;
% H=@(x)1; % uncomment for norecovery case
H=@(x)exp(-.04.*x); % exp CCDF in time (hours) for recovery of offsite
power
%% Input data
% Failure to start data
QFTS=3.24E-03;alpha1FTS=0.990496;alpha3FTS=3.34E-03;alpha2FTS=1-
alpha1FTS-alpha3FTS;alphatFTS=alpha1FTS+2*alpha2FTS+3*alpha3FTS;
% Failure to load-and-run data
QFTLR=2.25E-03;alpha1FTLR=0.991208;alpha3FTLR=1.37E-03;alpha2FTLR=1-
alpha1FTLR-alpha3FTLR;alphatFTLR=alpha1FTLR+2*alpha2FTLR+3*alpha3FTLR;
% Failure to run data
QFTR=7.12E-04;alpha1FTR=0.985501;alpha3FTR=5.64E-03;alpha2FTR=1-
alpha1FTR-alpha3FTR;alphatFTR=alpha1FTR+2*alpha2FTR+3*alpha3FTR;
%
%% Input data for three-way common-cause failures
FTS3way=3*alpha3FTS*QFTS/alphatFTS;FTLR3way =
3*alpha3FTLR*QFTLR/alphatFTLR;FTR3way = 3*alpha3FTR*QFTR/alphatFTR;
%
%% Input data for independent failures
FTS_I=alpha1FTS*QFTS/alphatFTS;FTLR_I=alpha1FTLR*QFTLR/alphatFTLR;FTR_I
=alpha1FTR*QFTR/alphatFTR;
%
%% Input data for two-way common-cause failures
FTS2way=alpha2FTS*QFTS/alphatFTS;FTLR2way=alpha2FTLR*QFTLR/alphatFTLR;F
TR2way=alpha2FTR*QFTR/alphatFTR;
%% 'Basic Event' rates ; the following data assumes 3 identical EDGs
% Designed Hazard Functions a=FTLR and b=FTR
% rates for single failures of EDGs 1,2,and 3
r1_3a=FTLR_I;r1_3b=FTR_I;
% rates for 2 out of 3 CCFs
r2_3a=FTLR2way;r2_3b=FTR2way;
% rate for 3-way CCF
r3_3a=FTLR3way;r3_3b=FTR3way;
```

```
%% Influenced Hazard Functions
% 1-out-of-2; rate for single failure of 2 given 1 has already failed
and 3 has not (EDGs subject to component-caused CCF, not external)
r1_2a=r1_3a+(.5).*r2_3a; r1_2b=r1_3b+(.5).*r2_3b;
% 2-out-of-2; rate for CCF of 2&3 given 1 has already failed(EDGs
subject to component-caused CCF, not external)
r2_2a=r2_3a+(2/3).*r3_3a; r2_2b=r2_3b+(2/3).*r3_3b;
% 1-out-of-1; single failure rate for EDG3 given only EDG3 operating
r1_1a=r1_3a+r2_3a+(1/3).*r3_3a; r1_1b=r1_3b+r2_3b+(1/3).*r3_3b;
%% other rates (combinations of basic event rates); _a=FTLR, _b=FTR
r_total_a=3*r1_3a+3*r2_3a+r3_3a; % total rate of any basic event given
all EDGs operating
r_total_b=3*r1_3b+3*r2_3b+r3_3b;
r_total_2a=2*r1_3a+2*r2_3a+(2/3)*r3_3a; % total rate of any basic event
given two EDGs operating
r_total_2b=2*r1_3b+2*r2_3b+(2/3)*r3_3b;
%% state probabilities; Initial Conditions
%% t=0hr
P1=FTS_I ;P2=P1 ;P3=P1 ;P4=FTS2way ;P5=P4 ;P6=P4 ;P7=FTS3way ;
P0=1-3*P1-3*P4-P7;% no failures
%% three consecutive 'single' failures; written as 1 fails followed by
2 and 3
% define anonymous function for integrand
% (z,y,x)=(t,t',tau)
FTLR_FTLR_FTLR=@(z,y,x)(P0.*(r1_3a.*exp(-r_total_a.*x)).*(r1_2a.*exp(-
r_total_2a.*(y-x))).*(r1_1a.*exp(-r1_1a.*(z-y))).*H(z));
FTLR_FTLR_FTR=@(z,y,x)(P0.*(r1_3a.*exp(-r_total_a.*x)).*(r1_2a.*exp(-
r_total_2a.*(y-x))).*(r1_1b.*exp(-r1_1a.*(1-y)).*exp(-(r1_1b.*(z-
1)))).*H(z));
FTLR_FTR_FTR=@(z,y,x)(P0.*(r1_3a.*exp(-r_total_a.*x)).*(r1_2b.*exp(-
r_total_2a.*(1-x)).*exp(-r_total_2b.*(y-1))).*(r1_1b.*exp(-(r1_1b.*(z-
y)))).*H(z));
FTR_FTR_FTR=@(z,y,x)(P0.*(r1_3b.*exp(-r_total_a).*exp(-r_total_b.*(x-
1))).*(r1_2b.*exp(-r_total_2b.*(y-x))).*(r1_1b.*exp(-(r1_1b.*(z-
y)))).*H(z));
%% 2 random variable integrands
%
FTLR_FTLR=@(z,y)(P1.*(r1_2a.*exp(-r_total_2a.*y)).*(r1_1a.*exp(-
r1_1a.*(z-y))).*H(z));
FTLR_FTR=@(z,y)(P1.*(r1_2a.*exp(-r_total_2a.*(y))).*(r1_1b.*exp(-
r1_1a.*(1-y)).*exp(-(r1_1b.*(z-1)))).*H(z));
FTR_FTR=@(z,y)(P1.*(r1_2b.*exp(-r_total_2a).*exp(-r_total_2b.*(y-
1))).*(r1_1b.*exp(-(r1_1b.*(z-y)))).*H(z));
%
FTLR2_FTLR=@(z,y)(P0.*(r2_3a.*exp(-r_total_a.*y)).*(r1_1a.*exp(-
r1_1a.*(z-y))).*H(z));
FTLR2_FTR=@(z,y)(P0.*(r2_3a.*exp(-r_total_a.*(y))).*(r1_1b.*exp(-
r1_1a.*(1-y)).*exp(-(r1_1b.*(z-1)))).*H(z));
FTR2_FTR=@(z,y)(P0.*(r2_3b.*exp(-r_total_a).*exp(-r_total_b.*(y-
1))).*(r1_1b.*exp(-(r1_1b.*(z-y)))).*H(z));
%
```

```
FTLR_FTLR2=@(z,y)(P0.*(r1_3a.*exp(-r_total_a.*y)).*(r2_2a.*exp(-
r_total_2a.*(z-y))).*H(z));
FTLR_FTR2=@(z,y)(P0.*(r1_3a.*exp(-r_total_a.*(y))).*(r2_2b.*exp(-
r_total_2a.*(1-y)).*exp(-(r_total_2b.*(z-1)))).*H(z));
FTR_FTR2=@(z,y)(P0.*(r1_3b.*exp(-r_total_a).*exp(-r_total_b.*(y-
1))).*(r2_2b.*exp(-(r_total_2b.*(z-y)))).*H(z));
%
%% 1 random variable integrands
%
FTLR=@(z)(P4.*(r1_1a.*exp(-r1_1a.*z)).*H(z));
FTR=@(z)(P4.*(r1_1b.*exp(-r1_1a).*exp(-(r1_1b.*(z-1)))).*H(z));
%
FTLR2=@(z)(P1.*(r2_2a.*exp(-r_total_2a.*z)).*H(z));
FTR2=@(z)(P1.*(r2_2b.*exp(-r_total_2a).*exp(-r_total_2b.*(z-
1))).*H(z));
%
FTLR3=@(z)(P0.*(r3_3a.*exp(-r_total_a.*z)).*H(z));
FTR3=@(z)(P0.*(r3_3b.*exp(-r_total_a).*exp(-r_total_b.*(z-1))).*H(z));
%% evaluate the definite integral numerically
% define limits of integration
ymax = @(z) z;
xmax = @(z,y) y;
%% 1 random variable CDFs
%
P_FTS2_FTLR=3.*integral(FTLR,0,1);
P_FTS2_FTR=3.*integral(FTR,1,T);
%
P_FTS_FTLR2=3.*integral(FTLR2,0,1);
P_FTS_FTR2=3.*integral(FTR2,1,T);
%
P_FTLR3=integral(FTLR3,0,1);
P_FTR3=integral(FTR3,1,T);
%% 2 random variable CDFs
%
P_FTS_FTLR_FTLR=6.*integral2(FTLR_FTLR,0,1,0,ymax);
P_FTS_FTLR_FTR=6.*integral2(FTLR_FTR,1,T,0,1);
P_FTS_FTR_FTR=6.*integral2(FTR_FTR,1,T,1,ymax);
%
P_FTLR2_FTLR=3.*integral2(FTLR2_FTLR,0,1,0,ymax);
P_FTLR2_FTR=3.*integral2(FTLR2_FTR,1,T,0,1);
P_FTR2_FTR=3.*integral2(FTR2_FTR,1,T,1,ymax);
%
P_FTLR_FTLR2=3.*integral2(FTLR_FTLR2,0,1,0,ymax);
P_FTLR_FTR2=3.*integral2(FTLR_FTR2,1,T,0,1);
P_FTR_FTR2=3.*integral2(FTR_FTR2,1,T,1,ymax);
%% 3 random variable CDFs
% assume identical; x6 accounts for 123, 132, 213, 231, 312, and 321
P_FTLR_FTLR_FTLR=6.*integral3(FTLR_FTLR_FTLR,0,1,0,ymax,0,xmax); %
FTLR_FTLR_FTLR
P_FTLR_FTLR_FTR=6.*integral3(FTLR_FTLR_FTR,1,T,0,1,0,xmax);
P_FTLR_FTR_FTR=6.*integral3(FTLR_FTR_FTR,1,T,1,ymax,0,1);
```

```
P_FTR_FTR_FTR=6.*integral3(FTR_FTR_FTR,1,T,1,ymax,1,xmax); %
FTR_FTR_FTR
% %% 1 random variable CDFs
% %
% P_FTS2_FTLR=3.*integral(FTLR,0,1,'AbsTol',1e-16,'RelTol',1e-12);
% P_FTS2_FTR=3.*integral(FTR,1,T,'AbsTol',1e-16,'RelTol',1e-12);
% %
% P_FTS_FTLR2=3.*integral(FTLR2,0,1,'AbsTol',1e-16,'RelTol',1e-12);
% P_FTS_FTR2=3.*integral(FTR2,1,T,'AbsTol',1e-16,'RelTol',1e-12);
% %
% P_FTLR3=integral(FTLR3,0,1,'AbsTol',1e-16,'RelTol',1e-12);
% P_FTR3=integral(FTR3,1,T,'AbsTol',1e-16,'RelTol',1e-12);
% %% 2 random variable CDFs
% %
% P_FTS_FTLR_FTLR=6.*integral2(FTLR_FTLR,0,1,0,ymax,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTS_FTLR_FTR=6.*integral2(FTLR_FTR,1,T,0,1,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTS_FTR_FTR=6.*integral2(FTR_FTR,1,T,1,ymax,'AbsTol',1e-
16,'RelTol',1e-12);
% %
% P_FTLR2_FTLR=3.*integral2(FTLR2_FTLR,0,1,0,ymax,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTLR2_FTR=3.*integral2(FTLR2_FTR,1,T,0,1,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTR2_FTR=3.*integral2(FTR2_FTR,1,T,1,ymax,'AbsTol',1e-
16,'RelTol',1e-12);
% %
% P_FTLR_FTLR2=3.*integral2(FTLR_FTLR2,0,1,0,ymax,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTLR_FTR2=3.*integral2(FTLR_FTR2,1,T,0,1,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTR_FTR2=3.*integral2(FTR_FTR2,1,T,1,ymax,'AbsTol',1e-
16,'RelTol',1e-12);
% %% 3 random variable CDFs
% %
P_FTLR_FTLR_FTLR=6.*integral3(FTLR_FTLR_FTLR,0,1,0,ymax,0,xmax,'AbsTol'
,1e-16,'RelTol',1e-12);
%
P_FTLR_FTLR_FTR=6.*integral3(FTLR_FTLR_FTR,1,T,0,1,0,xmax,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTLR_FTR_FTR=6.*integral3(FTLR_FTR_FTR,1,T,1,ymax,0,1,'AbsTol',1e-
16,'RelTol',1e-12);
% P_FTR_FTR_FTR=6.*integral3(FTR_FTR_FTR,1,T,1,ymax,1,xmax,'AbsTol',1e-
16,'RelTol',1e-12);
%% no random variable
% CCFTS
P_FTS3=FTS3way;
%%
PCSBO1=P_FTS3+P_FTLR_FTLR_FTLR+P_FTS_FTLR_FTLR+P_FTS2_FTLR+P_FTLR2_FTLR
+P_FTLR_FTLR2+P_FTS_FTLR2+P_FTLR3;
```

```
PCSBO2=P_FTLR_FTLR_FTR+P_FTLR_FTR_FTR+P_FTR_FTR_FTR+P_FTS_FTLR_FTR+P_FT
S_FTR_FTR+P_FTS2_FTR+...
  P_FTLR2_FTR+P_FTR2_FTR+P_FTLR_FTR2+P_FTR_FTR2+P_FTS_FTR2+P_FTR3;
% Total
if T==0
  PCSBO=P_FTS3;
elseif T<=1
  PCSBO=PCSBO1;  % may be incorrect for times between 0 and 1 hour
elseif T>1
  PCSBO=PCSBO1+PCSBO2;
end
```

## APPENDIX C

## FLEX DG (HOT) SYSTEM MATLAB MODELS

This appendix contains the MATLAB code for Section IV.5.1.

```
% 2iEDGs in hot standby & FLEX in hot standby; mission-time model of
load
clear all
tic
r=(1/1); % change for different "r-factor" cases
%
%% Input Data
% Failure to start data; failure-on-demand parameters
QFTS=3.24E-03;alpha1FTS=0.990656;alpha2FTS=1-
alpha1FTS;alphatFTS=alpha1FTS+2*alpha2FTS;
% Initial Conditions; failure on demand probabilities
P1=alpha1FTS.*QFTS/alphatFTS; % EDG "1" FTS
P2=P1;                        % EDG "2" FTS ; 1 and 2 are iEDGs
P3=(P1/2).*r;                       % FLEX EDG FTS
P4=2*alpha2FTS.*QFTS/alphatFTS; % both iEDG's CCFTS
P5=0;  % no possibility that EDG "1" and flex EDG CCFTS
P6=0;  % no possibility that EDG "2" and flex EDG CCFTS
P7=(P4/2).*r;  % all three EDGs FTS
P0=1-P1-P2-P3-P4-P5-P6-P7;
% Failure to load-and-run data
QFTLR=2.25E-03;alpha1FTLR=0.997015;alpha2FTLR=1-
alpha1FTLR;alphatFTLR=alpha1FTLR+2*alpha2FTLR;
% Failure to run data; constant failure rates
QFTR=7.12E-04; alpha1FTR=0.984593;alpha2FTR=1-
alpha1FTR;alphatFTR=alpha1FTR+2*alpha2FTR;
%% failure rates
% Designed
r1_3a=alpha1FTLR*QFTLR/alphatFTLR; r1_3b=alpha1FTR*QFTR/alphatFTR;
rF_3a=(r1_3a/2)*r;rF_3b=(r1_3b/2)*r;
r2_3aE=2*alpha2FTLR*QFTLR/alphatFTLR;
r2_3bE=2*alpha2FTR*QFTR/alphatFTR;
r2_3aC=r2_3aE/2; r2_3bC=r2_3bE/2;
r2_3a=r2_3aE+r2_3aC;r2_3b=r2_3bE+r2_3bC;
r3_3a=(r2_3aE/2)*r;r3_3b=(r2_3bE/2)*r;
% Influenced
r1_2a=r1_3a+r2_3aE+.5*r2_3aC; r1_2b=r1_3b+r2_3bE+.5*r2_3bC; % when one
iEDG is failed
rF_2a=rF_3a;rF_2b=rF_3b; % single FLEX failure given one iEDG is
already failed
r2_2a=r2_3a+r3_3a;r2_2b=r2_3b+r3_3b; % 2/2 failure (FLEX is already
failed)
```

```
r1_1a=r1_3a+r2_3aE+.5*r2_3aC+r3_3a;r1_1b=r1_3b+r2_3bE+.5*r2_3bC+r3_3b;
% only 1 iEDG operating
rF_Fa=rF_3a+r3_3a;rF_Fb=rF_3b+r3_3b; % single failure, onle FLEX is
operating
r_total_a=2*r1_3a+r2_3a+rF_3a+r3_3a;
r_total_b=2*r1_3b+r2_3b+rF_3b+r3_3b;
%% three consecutive 'single' failures; written as 1 fails followed by
2 and 3
% _a=2iEDGs, then FLEX; _b=iEDG, FLEX, iEDG; _c=FLEX, then 2 iEDGs
% (z,y,x)=(t,t',tau)
FTLR_FTLR_FTLR_a=@(z,y,x)(P0.*(r1_3a.*exp(-
r_total_a.*x)).*(r1_2a.*exp(-(r1_2a+rF_2a+r3_3a).*(y-
x))).*(rF_Fa.*exp(-(rF_Fa).*(z-y))));% 2 iEDGs then FLEX; confirm (2/3)
and (1/3) in exp totals
FTLR_FTLR_FTLR_b=@(z,y,x)(P0.*(r1_3a.*exp(-
r_total_a.*x)).*(rF_2a.*exp(-(r1_2a+rF_2a+r3_3a).*(y-
x))).*(r1_1a.*exp(-(r1_1a).*(z-y))));% iEDG, FLEX, then iEDG;
FTLR_FTLR_FTLR_c=@(z,y,x)(P0.*(rF_3a.*exp(-
r_total_a.*x)).*(r1_3a.*exp(-(2*r1_3a+r2_2a).*(y-x))).*(r1_1a.*exp(-
(r1_1a).*(z-y))));% FLEX, iEDG, then iEDG;
%
FTLR_FTLR_FTR_a=@(z,y,x)(P0.*(r1_3a.*exp(-r_total_a.*x)).*(r1_2a.*exp(-
(r1_2a+rF_2a+r3_3a).*(y-x))).*(rF_Fb.*exp(-(rF_Fa).*(1-y)).*exp(-
(rF_Fb).*(z-1))));
FTLR_FTLR_FTR_b=@(z,y,x)(P0.*(r1_3a.*exp(-r_total_a.*x)).*(rF_2a.*exp(-
(r1_2a+rF_2a+r3_3a).*(y-x))).*(r1_1b.*exp(-(r1_1a).*(1-y)).*exp(-
(r1_1b).*(z-1))));
FTLR_FTLR_FTR_c=@(z,y,x)(P0.*(rF_3a.*exp(-r_total_a.*x)).*(r1_3a.*exp(-
(2*r1_3a+r2_2a).*(y-x))).*(r1_1b.*exp(-(r1_1a).*(1-y)).*exp(-
(r1_1b).*(z-1))));
%
FTLR_FTR_FTR_a=@(z,y,x)(P0.*(r1_3a.*exp(-r_total_a.*x)).*(r1_2b.*exp(-
(r1_2a+rF_2a+r3_3a).*(1-x)).*exp(-(r1_2b+rF_2b+r3_3b).*(y-
1))).*(rF_Fb.*exp(-(rF_Fb).*(z-y))));
FTLR_FTR_FTR_b=@(z,y,x)(P0.*(r1_3a.*exp(-r_total_a.*x)).*(rF_2b.*exp(-
(r1_2a+rF_2a+r3_3a).*(1-x)).*exp(-(r1_2b+rF_2b+r3_3b).*(y-
1))).*(r1_1b.*exp(-(r1_1b).*(z-y))));
FTLR_FTR_FTR_c=@(z,y,x)(P0.*(rF_3a.*exp(-r_total_a.*x)).*(r1_3b.*exp(-
(2*r1_3a+r2_2a).*(1-x)).*exp(-(2*r1_3b+r2_2b).*(y-1))).*(r1_1b.*exp(-
(r1_1b).*(z-y))));
%
FTR_FTR_FTR_a=@(z,y,x)(P0.*(r1_3b.*exp(-r_total_a).*exp(-r_total_b.*(x-
1))).*(r1_2b.*exp(-(r1_2b+rF_2b+r3_3b).*(y-x))).*(rF_Fb.*exp(-
(rF_Fb).*(z-y))));
FTR_FTR_FTR_b=@(z,y,x)(P0.*(r1_3b.*exp(-r_total_a).*exp(-r_total_b.*(x-
1))).*(rF_2b.*exp(-(r1_2b+rF_2b+r3_3b).*(y-x))).*(r1_1b.*exp(-
(r1_1b).*(z-y))));
FTR_FTR_FTR_c=@(z,y,x)(P0.*(rF_3b.*exp(-r_total_a).*exp(-r_total_b.*(x-
1))).*(r1_3b.*exp(-(2*r1_3b+r2_2b).*(y-x))).*(r1_1b.*exp(-(r1_1b).*(z-
y))));
% define limits of integration
ymax = @(z) z;
```

```
xmax = @(z,y) y;
%
%% 2 random variable integrands
% _a=2iEDGs, then FLEX; _b=iEDG, FLEX, iEDG; _c=FLEX, then 2 iEDGs
% FTS, 1/2, then 1/1
FTLR_FTLR_a=@(z,y)(P1.*(r1_2a.*exp(-
(r1_2a+rF_2a+r3_3a).*y)).*(rF_Fa.*exp(-rF_Fa.*(z-y))));
FTLR_FTLR_b=@(z,y)(P1.*(rF_2a.*exp(-
(r1_2a+rF_2a+r3_3a).*y)).*(r1_1a.*exp(-r1_1a.*(z-y))));
FTLR_FTLR_c=@(z,y)(P3.*(r1_3a.*exp(-(2*r1_3a+r2_2a).*y)).*(r1_1a.*exp(-
r1_1a.*(z-y))));
% FTS, 1/2, then 1/1
FTLR_FTR_a=@(z,y)(P1.*(r1_2a.*exp(-
(r1_2a+rF_2a+r3_3a).*y)).*(rF_Fb.*exp(-rF_Fa.*(1-y)).*exp(-(rF_Fb.*(z-
1)))));
FTLR_FTR_b=@(z,y)(P1.*(rF_2a.*exp(-
(r1_2a+rF_2a+r3_3a).*y)).*(r1_1b.*exp(-r1_1a.*(1-y)).*exp(-(r1_1b.*(z-
1)))));
FTLR_FTR_c=@(z,y)(P3.*(r1_3a.*exp(-(2*r1_3a+r2_2a).*y)).*(r1_1b.*exp(-
r1_1a.*(1-y)).*exp(-(r1_1b.*(z-1)))));
% FTS, 1/2, then 1/1
FTR_FTR_a=@(z,y)(P1.*(r1_2b.*exp(-(r1_2a+rF_2a+r3_3a)).*exp(-
(r1_2b+rF_2b+r3_3b).*(y-1))).*(rF_Fb.*exp(-(rF_Fb.*(z-y)))));
FTR_FTR_b=@(z,y)(P1.*(rF_2b.*exp(-(r1_2a+rF_2a+r3_3a)).*exp(-
(r1_2b+rF_2b+r3_3b).*(y-1))).*(r1_1b.*exp(-(r1_1b.*(z-y)))));
FTR_FTR_c=@(z,y)(P3.*(r1_3b.*exp(-(2*r1_3a+r2_2a)).*exp(-
(2*r1_3b+r2_2b).*(y-1))).*(r1_1b.*exp(-(r1_1b.*(z-y)))));
% 2i/3, then 1f/1
FTLR2_FTLR=@(z,y)(P0.*(r2_3a.*exp(-r_total_a.*y)).*(rF_Fa.*exp(-
rF_Fa.*(z-y))));
FTLR2_FTR=@(z,y)(P0.*(r2_3a.*exp(-r_total_a.*(y))).*(rF_Fb.*exp(-
rF_Fa.*(1-y)).*exp(-(rF_Fb.*(z-1)))));
FTR2_FTR=@(z,y)(P0.*(r2_3b.*exp(-r_total_a).*exp(-r_total_b.*(y-
1))).*(rF_Fb.*exp(-(rF_Fb.*(z-y)))));
% F/3, then 2/2
fFTLR_FTLR2=@(z,y)(P0.*(rF_3a.*exp(-r_total_a.*y)).*(r2_2a.*exp(-
(2*r1_3a+r2_2a).*(z-y))));
fFTLR_FTR2=@(z,y)(P0.*(rF_3a.*exp(-r_total_a.*(y))).*(r2_2b.*exp(-
(2*r1_3a+r2_2a).*(1-y)).*exp(-((2*r1_3b+r2_2b).*(z-1)))));
fFTR_FTR2=@(z,y)(P0.*(rF_3b.*exp(-r_total_a).*exp(-r_total_b.*(y-
1))).*(r2_2b.*exp(-((2*r1_3b+r2_2b).*(z-y)))));
% 1i/3, then iEDG/FLEX CCF
iFTLR_FTLR2=@(z,y)(P0.*(r1_3a.*exp(-r_total_a.*y)).*(r3_3a.*exp(-
(r1_2a+rF_Fa).*(z-y))));
iFTLR_FTR2=@(z,y)(P0.*(r1_3a.*exp(-r_total_a.*y)).*(r3_3b.*exp(-
(r1_2a+rF_Fa).*(1-y)).*exp(-((r1_2b+rF_Fb).*(z-1)))));
iFTR_FTR2=@(z,y)(P0.*(r1_3b.*exp(-r_total_a).*exp(-r_total_b.*(y-
1))).*(r3_3b.*exp(-((r1_2b+rF_Fb).*(z-y)))));
%% 1 random variable integrands
% iEDGs CCFTS, then single FLEX
FTLR=@(z)(P4.*(rF_Fa.*exp(-rF_Fa.*z)));
FTR=@(z)(P4.*(rF_Fb.*exp(-rF_Fa).*exp(-rF_Fb.*(z-1))));
```

```
% FLEX FTS, then a CCF of both iEDGs
fFTS_FTLR2=@(z)(P3.*(r2_2a.*exp(-(2*r1_3a+r2_2a).*z)));
fFTS_FTR2=@(z)(P3.*(r2_2b.*exp(-(2*r1_3a+r2_2a)).*exp(-
(2*r1_3b+r2_2b).*(z-1))));
% iEDG FTS, then a CCF of iEDG/FLEX
iFTS_FTLR2=@(z)(P1.*(r3_3a.*exp(-(r1_2a+rF_2a+r3_3a).*z)));
iFTS_FTR2=@(z)(P1.*(r3_3b.*exp(-(r1_2a+rF_2a+r3_3a)).*exp(-
(r1_2b+rF_2b+r3_3b).*(z-1))));
% all 3 CCF
FTLR3=@(z)(P0.*(r3_3a.*exp(-r_total_a.*z)));
FTR3=@(z)(P0.*(r3_3b.*exp(-r_total_a).*exp(-r_total_b.*(z-1))));
%
%% no random variable
% CCFTS
P_FTS3=P7;
%% T=0
PCSBO(1)=P_FTS3;
%% T=1
P_FTLR_FTLR_FTLR_a=2.*integral3(FTLR_FTLR_FTLR_a,0,1,0,ymax,0,xmax); %
FTLR_FTLR_FTLR
P_FTLR_FTLR_FTLR_b=2.*integral3(FTLR_FTLR_FTLR_b,0,1,0,ymax,0,xmax);
P_FTLR_FTLR_FTLR_c=2.*integral3(FTLR_FTLR_FTLR_c,0,1,0,ymax,0,xmax);
P_FTLR_FTLR_FTLR=P_FTLR_FTLR_FTLR_a+P_FTLR_FTLR_FTLR_b+P_FTLR_FTLR_FTLR
_c;
%
P_FTS_FTLR_FTLR_a=2.*integral2(FTLR_FTLR_a,0,1,0,ymax);
P_FTS_FTLR_FTLR_b=2.*integral2(FTLR_FTLR_b,0,1,0,ymax);
P_FTS_FTLR_FTLR_c=2.*integral2(FTLR_FTLR_c,0,1,0,ymax);
P_FTS_FTLR_FTLR=P_FTS_FTLR_FTLR_a+P_FTS_FTLR_FTLR_b+P_FTS_FTLR_FTLR_c;
%
P_FTLR2_FTLR=integral2(FTLR2_FTLR,0,1,0,ymax);
P_fFTLR_FTLR2=integral2(fFTLR_FTLR2,0,1,0,ymax);
P_iFTLR_FTLR2=2.*integral2(iFTLR_FTLR2,0,1,0,ymax);
%
P_FTS2_FTLR=integral(FTLR,0,1);
P_FTLR3=integral(FTLR3,0,1);
%
P_iFTS_FTLR2=2.*integral(iFTS_FTLR2,0,1);
P_fFTS_FTLR2=integral(fFTS_FTLR2,0,1);
%
PCSBO(2)=P_FTS3+P_FTLR_FTLR_FTLR+P_FTS_FTLR_FTLR+P_FTLR2_FTLR+P_fFTLR_F
TLR2+P_iFTLR_FTLR2+P_FTS2_FTLR+P_FTLR3+P_iFTS_FTLR2+P_fFTS_FTLR2;
%% T>1
for i=3:769
% 3 random variable CDFs
P_FTLR_FTLR_FTR_a(i)=2.*integral3(FTLR_FTLR_FTR_a,1,i-1,0,1,0,xmax);
P_FTLR_FTLR_FTR_b(i)=2.*integral3(FTLR_FTLR_FTR_b,1,i-1,0,1,0,xmax);
P_FTLR_FTLR_FTR_c(i)=2.*integral3(FTLR_FTLR_FTR_c,1,i-1,0,1,0,xmax);
P_FTLR_FTLR_FTR(i)=P_FTLR_FTLR_FTR_a(i)+P_FTLR_FTLR_FTR_b(i)+P_FTLR_FTL
R_FTR_c(i);
%
P_FTLR_FTR_FTR_a(i)=2.*integral3(FTLR_FTR_FTR_a,1,i-1,1,ymax,0,1);
```

```
P_FTLR_FTR_FTR_b(i)=2.*integral3(FTLR_FTR_FTR_b,1,i-1,1,ymax,0,1);
P_FTLR_FTR_FTR_c(i)=2.*integral3(FTLR_FTR_FTR_c,1,i-1,1,ymax,0,1);
P_FTLR_FTR_FTR(i)=P_FTLR_FTR_FTR_a(i)+P_FTLR_FTR_FTR_b(i)+P_FTLR_FTR_FT
R_c(i);
%
P_FTR_FTR_FTR_a(i)=2.*integral3(FTR_FTR_FTR_a,1,i-1,1,ymax,1,xmax);  %
FTR_FTR_FTR
P_FTR_FTR_FTR_b(i)=2.*integral3(FTR_FTR_FTR_b,1,i-1,1,ymax,1,xmax);
P_FTR_FTR_FTR_c(i)=2.*integral3(FTR_FTR_FTR_c,1,i-1,1,ymax,1,xmax);
P_FTR_FTR_FTR(i)=P_FTR_FTR_FTR_a(i)+P_FTR_FTR_FTR_b(i)+P_FTR_FTR_FTR_c(
i);
% 2 random variable CDFs
P_FTS_FTLR_FTR_a(i)=2.*integral2(FTLR_FTR_a,1,i-1,0,1);
P_FTS_FTLR_FTR_b(i)=2.*integral2(FTLR_FTR_b,1,i-1,0,1);
P_FTS_FTLR_FTR_c(i)=2.*integral2(FTLR_FTR_c,1,i-1,0,1);
P_FTS_FTLR_FTR(i)=P_FTS_FTLR_FTR_a(i)+P_FTS_FTLR_FTR_b(i)+P_FTS_FTLR_FT
R_c(i);
%
P_FTS_FTR_FTR_a(i)=2.*integral2(FTR_FTR_a,1,i-1,1,ymax);
P_FTS_FTR_FTR_b(i)=2.*integral2(FTR_FTR_b,1,i-1,1,ymax);
P_FTS_FTR_FTR_c(i)=2.*integral2(FTR_FTR_c,1,i-1,1,ymax);
P_FTS_FTR_FTR(i)=P_FTS_FTR_FTR_a(i)+P_FTS_FTR_FTR_b(i)+P_FTS_FTR_FTR_c(
i);
%
P_FTLR2_FTR(i)=integral2(FTLR2_FTR,1,i-1,0,1);
P_FTR2_FTR(i)=integral2(FTR2_FTR,1,i-1,1,ymax);
%
P_fFTLR_FTR2(i)=integral2(fFTLR_FTR2,1,i-1,0,1);
P_fFTR_FTR2(i)=integral2(fFTR_FTR2,1,i-1,1,ymax);
%
P_iFTLR_FTR2(i)=2.*integral2(iFTLR_FTR2,1,i-1,0,1);
P_iFTR_FTR2(i)=2.*integral2(iFTR_FTR2,1,i-1,1,ymax);
% 1 random variable CDFs
P_FTS2_FTR(i)=integral(FTR,1,i-1);
P_iFTS_FTR2(i)=2.*integral(iFTS_FTR2,1,i-1);
P_fFTS_FTR2(i)=integral(fFTS_FTR2,1,i-1);
P_FTR3(i)=integral(FTR3,1,i-1);
PCSBO(i)=PCSBO(2)+P_FTLR_FTLR_FTR(i)+P_FTLR_FTR_FTR(i)+P_FTR_FTR_FTR(i)
+P_FTS_FTLR_FTR(i)+P_FTS_FTR_FTR(i)+P_FTLR2_FTR(i)...

+P_FTR2_FTR(i)+P_iFTLR_FTR2(i)+P_iFTR_FTR2(i)+P_FTS2_FTR(i)+P_FTR3(i)+P
_fFTLR_FTR2(i)+P_fFTR_FTR2(i)+P_iFTS_FTR2(i)+P_fFTS_FTR2(i);
end

toc
```

## APPENDIX D

## FLEX DG (COLD) SYSTEM MATLAB MODELS

This appendix contains the MATLAB code for Section IV.5.2.

```
% 2iEDGs in hot standby & FLEX in cold standby; mission-time model of
load
% 3/3 externally caused CCF is possible even though FLEX isnt started
clear all
%
T=768;
tic
r=(1/1); % change for different "r-factor" cases
%
%% Input data
% Failure to start data; failure-on-demand parameters
QFTS=3.24E-03;alpha1FTS=0.990656;alpha2FTS=1-
alpha1FTS;alphatFTS=alpha1FTS+2*alpha2FTS;
% Initial Conditions; failure on demand probabilities
P1=alpha1FTS*QFTS/alphatFTS; % EDG "1" FTS
P2=P1;                       % EDG "2" FTS ; 1 and 2 are iEDGs
P3=0;                        % FLEX EDG FTS at t=0
P4=2*alpha2FTS*QFTS/alphatFTS; % both iEDG's CCFTS
P5=0;  % no possibility that EDG "1" and flex EDG CCFTS
P6=0;  % no possibility that EDG "2" and flex EDG CCFTS
P7=(P4/2).*r;  % all three EDGs FTS; not possible for the cold standby
case
P0=1-P1-P2-P3-P4-P5-P6-P7;
%
P_3=(P1/2)*r;  % FLEX EDG FTS after both iEDGs failed
P_0=1-P_3;     % FLEX EDG successfully starts after both iEDGs failed
% Failure to load-and-run data
QFTLR=2.25E-03;alpha1FTLR=0.997015;alpha2FTLR=1-
alpha1FTLR;alphatFTLR=alpha1FTLR+2*alpha2FTLR;
% Failure to run data; constant failure rates
QFTR=7.12E-04; alpha1FTR=0.984593;alpha2FTR=1-
alpha1FTR;alphatFTR=alpha1FTR+2*alpha2FTR;
%% failure rates
% Designed
r1_2a=alpha1FTLR*QFTLR/alphatFTLR; r1_2b=alpha1FTR*QFTR/alphatFTR;
rFa=(r1_2a/2)*r;rFb=(r1_2b/2)*r;
r2_2aE=2*alpha2FTLR*QFTLR/alphatFTLR;
r2_2bE=2*alpha2FTR*QFTR/alphatFTR;
r2_2aC=r2_2aE/2; r2_2bC=r2_2bE/2;
r2_2a=r2_2aE+r2_2aC;r2_2b=r2_2bE+r2_2bC;
r3_3a=(r2_2aE/2)*r;r3_3b=(r2_2bE/2)*r;
% Influenced
```

```
r1_1a=r1_2a+r2_2aE+.5*r2_2aC; r1_1b=r1_2b+r2_2bE+.5*r2_2bC; % single
iEDG failure rate when one iEDG is failed
rF_Fa=rFa+r3_3a;rF_Fb=rFb+r3_3b;%%
r_total_a=2*r1_2a+r2_2a+r3_3a; r_total_b=2*r1_2b+r2_2b+r3_3b; % cold
mod
%% three consecutive 'single' failures; written as 1 fails followed by
2 and 3
% need to think about which rates compose the needed conditional hazard
functions for this joint pdf '3IND'
% define anonymous function for integrand
% (z,y,x)=(t,t',tau)
FTLR_FTLR_FTLR=@(z,y,x)(P0.*P_0.*(r1_2a.*exp(-
r_total_a.*x)).*(r1_1a.*exp(-(r1_1a+r3_3a).*(y-x))).*(rF_Fa.*exp(-
(rF_Fa).*(z-y))));% 2 iEDGs then FLEX; confirm (2/3) and (1/3) in exp
totals
FTLR_FTLR_FTR=@(z,y,x)(P0.*P_0.*(r1_2a.*exp(-
r_total_a.*x)).*(r1_1a.*exp(-(r1_1a+r3_3a).*(y-x))).*(rF_Fb.*exp(-
(rF_Fa).*(1)).*exp(-(rF_Fb).*(z-y-1))));
FTLR_FTR_FTLR=@(z,y,x)(P0.*P_0.*(r1_2a.*exp(-
r_total_a.*x)).*(r1_1b.*exp(-(r1_1b+r3_3b).*(y-x))).*(rF_Fa.*exp(-
(rF_Fa).*(z-y))));
FTLR_FTR_FTR=@(z,y,x)(P0.*P_0.*(r1_2a.*exp(-
r_total_a.*x)).*(r1_1b.*exp(-(r1_1b+r3_3b).*(y-x))).*(rF_Fb.*exp(-
(rF_Fa).*(1)).*exp(-(rF_Fb).*(z-y-1))));
FTR_FTR_FTLR=@(z,y,x)(P0.*P_0.*(r1_2b.*exp(-r_total_a).*exp(-
r_total_b.*(x-1))).*(r1_1b.*exp(-(r1_1b+r3_3b).*(y-x))).*(rF_Fa.*exp(-
(rF_Fa).*(z-y))));
FTR_FTR_FTR=@(z,y,x)(P0.*P_0.*(r1_2b.*exp(-r_total_a).*exp(-
r_total_b.*(x-1))).*(r1_1b.*exp(-(r1_1b+r3_3b).*(y-x))).*(rF_Fb.*exp(-
(rF_Fa).*(1)).*exp(-(rF_Fb).*(z-y-1))));
% define limits of integration
ymax = @(z) z;
xmax = @(z,y) y;
%
%% 2 random variable integrands
% iEDG FTS, iEDG running failure, FLEX running failure
FTLR_FTLR=@(z,y)(P1.*P_0.*(r1_1a.*exp(-
(r1_1a+r3_3a).*y)).*(rF_Fa.*exp(-rF_Fa.*(z-y))));
FTLR_FTR=@(z,y)(P1.*P_0.*(r1_1a.*exp(-(r1_1a+r3_3a).*y)).*(rF_Fb.*exp(-
rF_Fa.*(1)).*exp(-(rF_Fb.*(z-y-1)))));
FTR_FTLR=@(z,y)(P1.*P_0.*(r1_1b.*exp(-(r1_1a+r3_3a)).*exp(-
(r1_1b+r3_3b).*(y-1))).*(rF_Fa.*exp(-rF_Fa.*(z-y))));
FTR_FTR=@(z,y)(P1.*P_0.*(r1_1b.*exp(-(r1_1a+r3_3a)).*exp(-
(r1_1b+r3_3b).*(y-1))).*(rF_Fb.*exp(-rF_Fa.*(1)).*exp(-(rF_Fb.*(z-y-
1)))));
% iEDGs 2/2 running failure, FLEX running failure
FTLR2_FTLR=@(z,y)(P0.*P_0.*(r2_2a.*exp(-r_total_a.*y)).*(rF_Fa.*exp(-
rF_Fa.*(z-y))));
FTLR2_FTR=@(z,y)(P0.*P_0.*(r2_2a.*exp(-r_total_a.*(y))).*(rF_Fb.*exp(-
rF_Fa.*(1)).*exp(-(rF_Fb.*(z-y-1)))));
FTR2_FTLR=@(z,y)(P0.*P_0.*(r2_2b.*exp(-r_total_a).*exp(-r_total_b.*(y-
1))).*(rF_Fa.*exp(-rF_Fa.*(z-y))));
```

```
FTR2_FTR=@(z,y)(P0.*P_0.*(r2_2b.*exp(-r_total_a).*exp(-r_total_b.*(y-
1))).*(rF_Fb.*exp(-rF_Fa).*exp(-(rF_Fb.*(z-y-1)))));
% iEDG 1/2 running failure, iEDG 1/1 running failure, FLEX FTS
FTLR_FTLR_FTS=@(z,y)(P0.*P_3.*(r1_2a.*exp(-
(r_total_a).*y)).*(r1_1a.*exp(-(r1_1a+r3_3a).*(z-y))));
FTLR_FTR_FTS=@(z,y)(P0.*P_3.*(r1_2a.*exp(-
(r_total_a).*y)).*(r1_1b.*exp(-(r1_1a+r3_3a).*(1-y)).*exp(-
(r1_1b+r3_3b).*(z-1))));
FTR_FTR_FTS=@(z,y)(P0.*P_3.*(r1_2b.*exp(-(r_total_a)).*exp(-
(r_total_b).*(y-1))).*(r1_1b.*exp(-(r1_1b+r3_3b).*(z-y))));
% iEDG 1/2, iEDG and FLEX EDG CCF
FTLR_FTLR2=@(z,y)(P0.*(r1_2a.*exp(-(r_total_a).*y)).*(r3_3a.*exp(-
(r1_1a+r3_3a).*(z-y)))); % FLEX failure rate not included in "exp(-
(r1_1a+r3_3a)" because it hasnt turned on yet (cold)
FTLR_FTR2=@(z,y)(P0.*(r1_2a.*exp(-(r_total_a).*y)).*(r3_3b.*exp(-
(r1_1a+r3_3a).*(1-y)).*exp(-(r1_1b+r3_3b).*(z-1))));
FTR_FTR2=@(z,y)(P0.*(r1_2b.*exp(-(r_total_a)).*exp(-(r_total_b).*(y-
1))).*(r3_3b.*exp(-(r1_1b+r3_3b).*(z-y))));
%
%% 1 random variable integrands
% 2/2 FTS, FLEX failure while running
FTLR=@(z)(P4.*P_0.*(rF_Fa.*exp(-rF_Fa.*z)));
FTR=@(z)(P4.*P_0.*(rF_Fb.*exp(-rF_Fa).*exp(-rF_Fb.*(z-1))));
% 2/2 iEDG CCF, then FLEX FTS
FTLR2=@(z)(P0.*P_3.*(r2_2a.*exp(-(r_total_a).*z)));
FTR2=@(z)(P0.*P_3.*(r2_2b.*exp(-(r_total_a)).*exp(-(r_total_b).*(z-
1))));
% iEDG FTS, iEDG running failure, FLEX EDG FTS
FTS_FTLR_FTS=@(z)(P1.*P_3.*(r1_1a.*exp(-(r1_1a+r3_3a).*z)));
FTS_FTR_FTS=@(z)(P1.*P_3.*(r1_1b.*exp(-(r1_1a+r3_3a)).*exp(-
(r1_1b+r3_3b).*(z-1))));
% 3/3 CCF
FTLR3=@(z)(P0.*(r3_3a.*exp(-r_total_a.*z)));
FTR3=@(z)(P0.*(r3_3b.*exp(-r_total_a).*exp(-r_total_b.*(z-1))));
% iEDG 1/2 FTS, iEDG and FLEX CCF
FTS_FTLR2=@(z)(P1.*(r3_3a.*exp(-(r1_1a+r3_3a).*z)));
FTS_FTR2=@(z)(P1.*(r3_3b.*exp(-(r1_1a+r3_3a)).*exp(-(r1_1b+r3_3b).*(z-
1))));
%% no random variable
% CCFTS
P_FTS3=P7;
P_FTS2_FTS=P4.*P_3;
%%
P_FTLR_FTLR_FTLR=2.*integral3(FTLR_FTLR_FTLR,0,1,0,ymax,0,xmax); %
FTLR_FTLR_FTLR
P_FTS_FTLR_FTLR=2.*integral2(FTLR_FTLR,0,1,0,ymax);
P_FTLR2_FTLR=integral2(FTLR2_FTLR,0,1,0,ymax);
P_FTLR_FTLR_FTS=2.*integral2(FTLR_FTLR_FTS,0,1,0,ymax);
P_FTS2_FTLR=integral(FTLR,0,1);
P_FTLR2_FTS=integral(FTLR2,0,1);
P_FTLR3=integral(FTLR3,0,1);
P_FTS_FTLR2=2.*integral(FTS_FTLR2,0,1);
```

```
P_FTS_FTLR_FTS=2.*integral(FTS_FTLR_FTS,0,1);
P_FTLR_FTLR2=2.*integral2(FTLR_FTLR2,0,1,0,ymax);
%%
PCSBO(1)=P_FTS3+P_FTS2_FTS;
PCSBO(2)=PCSBO(1)+P_FTLR_FTLR_FTLR+P_FTS_FTLR_FTLR+P_FTLR2_FTLR+P_FTLR_
FTLR_FTS+P_FTS2_FTLR...
    +P_FTLR2_FTS+P_FTS_FTLR2+P_FTLR3+P_FTS_FTLR_FTS+P_FTLR_FTLR2;


%%
for i=3:T+1
% 3 random variable CDFs
P_FTLR_FTLR_FTR(i)=2.*integral3(FTLR_FTLR_FTR,1,i-1,0,1,0,xmax);
P_FTLR_FTR_FTLR(i)=2.*integral3(FTLR_FTR_FTLR,i-2,i-1,1,ymax,0,1);
P_FTLR_FTR_FTR(i)=2.*integral3(FTLR_FTR_FTR,1,i-1,1,ymax,0,1);
P_FTR_FTR_FTLR(i)=2.*integral3(FTR_FTR_FTLR,i-2,i-1,1,ymax,1,xmax);
P_FTR_FTR_FTR(i)=2.*integral3(FTR_FTR_FTR,1,i-1,1,ymax,1,xmax);  %
FTR_FTR_FTR
% 2 random variable CDFs
P_FTS_FTLR_FTR(i)=2.*integral2(FTLR_FTR,1,i-1,0,1);
P_FTS_FTR_FTLR(i)=2.*integral2(FTR_FTLR,i-2,i-1,1,ymax);
P_FTS_FTR_FTR(i)=2.*integral2(FTR_FTR,1,i-1,1,ymax);
P_FTLR2_FTR(i)=integral2(FTLR2_FTR,1,i-1,0,1);
P_FTR2_FTLR(i)=integral2(FTR2_FTLR,i-2,i-1,1,ymax);
P_FTR2_FTR(i)=integral2(FTR2_FTR,1,i-1,1,ymax);
P_FTLR_FTR_FTS(i)=2.*integral2(FTLR_FTR_FTS,1,i-1,0,1);
P_FTR_FTR_FTS(i)=2.*integral2(FTR_FTR_FTS,1,i-1,1,ymax);
P_FTLR_FTR2(i)=2.*integral2(FTLR_FTR2,1,i-1,1,ymax);
P_FTR_FTR2(i)=2.*integral2(FTR_FTR2,1,i-1,1,ymax);
% 1 random variable CDFs
P_FTS2_FTR(i)=integral(FTR,1,i-1);
P_FTR2_FTS(i)=integral(FTR2,1,i-1);
P_FTR3(i)=integral(FTR3,1,i-1);
P_FTS_FTR2(i)=2.*integral(FTS_FTR2,1,i-1);
P_FTS_FTR_FTS(i)=2.*integral(FTS_FTR_FTS,1,i-1);
%
PCSBO(i)=PCSBO(2)+P_FTLR_FTLR_FTR(i)+P_FTLR_FTR_FTLR(i)+P_FTLR_FTR_FTR(
i)+P_FTR_FTR_FTLR(i)+P_FTR_FTR_FTR(i)+P_FTS_FTLR_FTR(i)+P_FTS_FTR_FTR(i
)+P_FTLR2_FTR(i)+P_FTR2_FTR(i)...

+P_FTR2_FTLR(i)+P_FTR2_FTS(i)+P_FTLR_FTR_FTS(i)+P_FTR_FTR_FTS(i)+P_FTS2
_FTR(i)+P_FTS_FTR2(i)+P_FTR3(i)+P_FTS_FTR_FTS(i)+P_FTLR_FTR2(i)+P_FTR_F
TR2(i);
end
PCSBO_=PCSBO';
toc
```

# APPENDIX E

# FUTURE WORK MATLAB MODELS

## E.1 Semi-Markov Cold Standby Case

```
clear all
tic
syms x n k y t T
%% weibull parameters
r01=.1; r02=.01; r12=r01+r02;
syms r1 r2 r_12 B1 B2 B_12
assume (r1>0);assume(r2>0);assume(r_12>0);assume(B1>0)
;assume(B2>0);assume(B_12>0);
B01=1.3;B02=1.3;B12=1.3;
p01=symfun((r01.^B01).*B01.*(t.^(B01-1)).*exp(-(r01.*t).^B01),[t]);
p02=symfun((r02.^B02).*B02.*(t.^(B02-1)).*exp(-(r02.*t).^B02),[t]);
p12=symfun((r12.^B12).*B12.*(t.^(B12-1)).*exp(-(r12.*t).^B12),[t]);
cF01=symfun(exp(-(r01.*t).^B01),[t]);cF02=symfun(exp(-
(r02.*t).^B02),[t]);
cF12=symfun(exp(-(r12.*t).^B12),[t]);
%%
m=201;
dt=.1;tm=@(q)dt.*q;
Tm=tm(m)-dt;
%%
h01=symfun(p01(x).*cF02(x),[x]);
h02=symfun(p02(x).*cF01(x),[x]);
h12=symfun(p12(x),[x]);
%
W00=symfun(cF01(x).*cF02(x),[x]); % these w..'s check out
W11=symfun(cF12(x),[x]);
W22=1;
%%
H=[0 h01 h02;0 0 h12;0 0 0];
W=[W00 0 0;0 W11 0;0 0 W22];
%
H_0=double(H(0));           % for beta>=1
N=(eye(3)-(dt/2).*H_0); M=double(inv(N));
phi(:,:,1)=double(W(0)) % initialize phi(:,:,1)=phi(t=0),then
phi(:,:,2)=phi(t1), etc..
%%
for i = 2:m
  sum=zeros(3);
  for k=1:i-1
    y=i-k;
    sumfun=symfun(H(tm(x))*phi(:,:,y),[x]);
    count=double(sumfun(k));
    sum=double(count+sum);
  end
```

```
  P=symfun((M*(W(tm(x))+dt.*sum-(dt/2).*H(tm(x))*phi(:,:,1))),[x]);
  phi(:,:,i) = P(i-1);
  i
  toc
end
```

### E.2 Semi-Markov "Warm" Standby Case

```
clear all
tic
syms x n k y t T
%% weibull parameters
r01=.1; r02=.1; r03=.01; r13=.11; r23=.11;
syms r1 r2 r3 r_13 r_23 B1 B2 B3 B_13 B_23
assume (r1>0);assume(r2>0);assume (r3>0);assume(r_13>0);assume
(r_23>0);
assume(B1>0);assume(B2>0);assume(B3>0);assume(B_13>0);assume(B_23>0);
B01=1.3;B02=1.3;B03=1.3;B13=1.3;B23=1.3;
p01=symfun((r01.^B01).*B01.*(t.^(B01-1)).*exp(-(r01.*t).^B01),[t]);
p02=symfun((r02.^B02).*B02.*(t.^(B02-1)).*exp(-(r02.*t).^B02),[t]);
p03=symfun((r03.^B03).*B03.*(t.^(B03-1)).*exp(-(r03.*t).^B03),[t]);
p13=symfun((r13.^B13).*B13.*(t.^(B13-1)).*exp(-(r13.*t).^B13),[t]);
p23=symfun((r23.^B23).*B23.*(t.^(B23-1)).*exp(-(r23.*t).^B23),[t]);
cF01=symfun(exp(-(r01.*t).^B01),[t]);cF02=symfun(exp(-
(r02.*t).^B02),[t]);
cF03=symfun(exp(-(r03.*t).^B03),[t]);
cF13=symfun(exp(-(r13.*t).^B13),[t]);cF23=symfun(exp(-
(r23.*t).^B23),[t]);
%%
m=201;
dt=.1;tm=@(q)dt.*q;
Tm=tm(m)-dt;
%%
h01=symfun(p01(x).*cF02(x).*cF03(x),[x]);
h02=symfun(p02(x).*cF01(x).*cF03(x),[x]);
h03=symfun(p03(x).*cF01(x).*cF02(x),[x]);
h13=symfun(p13(x),[x]);
h23=symfun(p23(x),[x]);
%
W00=symfun(cF01(x).*cF02(x).*cF03(x),[x]);
W11=symfun(cF13(x),[x]);
W22=symfun(cF23(x),[x]);
W33=1;
%%
H=[0 h01 h02 h03;0 0 0 h13;0 0 0 h23;0 0 0 0];
W=[W00 0 0 0;0 W11 0 0;0 0 W22 0;0 0 0 W33];
%
H_0=double(H(0));          % for beta>=1
N=(eye(4)-(dt/2).*H_0); M=double(inv(N));
phi(:,:,1)=double(W(0));
%%
for i = 2:m
  sum=zeros(4);
```

```
  for k=1:i-1
    y=i-k;
    sumfun=symfun(H(tm(x))*phi(:,:,y),[x]);
    count=double(sumfun(k));
    sum=double(count+sum);
  end
  P=symfun((M*(W(tm(x))+dt.*sum-(dt/2).*H(tm(x))*phi(:,:,1))),[x]);
  phi(:,:,i) = P(i-1);
  i
  toc
end
```

### E.3 NRI Cold Standby Case

```
%% assume externally-caused CCF only
tic
clear all
syms z y w t r B
assume (r>0); assume(B>0);
m=200;dt=.1;
ymax = @(z) z;
%% Weibull parameters
r01=.1; r03=.01; r_=r01+r03;
B01=1.3;B02=1.3;B12=1.3;
r1=@(u)(r01.^B01).*B01.*u.^(B01-1); rcc=@(u)(r03.^B02).*B02.*u.^(B02-
1);
r13=@(u)(r_.^B12).*B12.*u.^(B12-1);
total=@(u)(r1(u)+rcc(u)); % cold
%%
total_sym=symfun(total(y),[y]);
total_int=matlabFunction(int(total_sym,0,y))
r_2_sym=symfun(r13(w),[w]);
r_2_int=matlabFunction(int(r_2_sym(w),y,z))
%%
for i=1:m+1
  j=i.*dt
FTR_FTR=@(z,y)(r1(y).*exp(-total_int(y)).*r13(z-y).*exp(-
r_2_int(y,z)));
P_FTR_FTR(i)=integral2(FTR_FTR,0,j-dt,0,ymax);
%
CCFTR = @(z)((rcc(z).*exp(-total_int(z))));
FTR_CCF(i) = integral(CCFTR,0,j-dt);
%
P_CSBO(i)=P_FTR_FTR(i)+FTR_CCF(i);
toc
end
```

### E.4 NRI Hot Standby Case

```
%% assume externally-caused CCF only
tic
clear all
syms z y w t r B
assume (r>0); assume(B>0);
m=200;dt=.1;
ymax = @(z) z;
%% Weibull parameters
r01=.1; r03=.01; r_=r01+r03;
B01=1.3;B02=1.3;B12=1.3;
r1=@(u)(r01.^B01).*B01.*u.^(B01-1); rcc=@(u)(r03.^B02).*B02.*u.^(B02-
1);
r13=@(u)(r_.^B12).*B12.*u.^(B12-1);
total=@(u)(2.*r1(u)+rcc(u));
%%
total_sym=symfun(total(y),[y]);
total_int=matlabFunction(int(total_sym,0,y))
r_2_sym=symfun(r13(w),[w]);
r_2_int=matlabFunction(int(r_2_sym(w),y,z))
for i=1:m+1
  j=i.*dt
FTR_FTR=@(z,y)(r1(y).*exp(-total_int(y)).*r13(z).*exp(-r_2_int(y,z)));
P_FTR_FTR(i)=2.*integral2(FTR_FTR,0,j-dt,0,ymax);
%
CCFTR = @(z)((rcc(z).*exp(-total_int(z))));
FTR_CCF(i) = integral(CCFTR,0,j-dt);
%
P_CSBO(i)=P_FTR_FTR(i)+FTR_CCF(i);
toc
end
```