SANDIA REPORT

SAND 2014-4037
Unlimited Release
March 2014

Dynamical Systems Probabilistic Risk Assessment

Matthew R Denman, Arlo Ames

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2014-4037
Unlimited Release
March 2014

Dynamical Systems Probabilistic Risk Assessment

Matthew Denman and Arlo Ames
Department Names
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0748

Abstract

Probabilistic Risk Assessment (PRA) is the primary tool used to risk-inform nuclear power regulatory and licensing activities. Risk-informed regulations are intended to reduce inherent conservatism in regulatory metrics (e.g., allowable operating conditions and technical specifications) which are built into the regulatory framework by quantifying both the total risk profile as well as the change in the risk profile caused by an event or action (e.g., in-service inspection procedures or power uprates).

Dynamical Systems (DS) analysis has been used to understand unintended time-dependent feedbacks in both industrial and organizational settings. In dynamical systems analysis, feedback loops can be characterized and studied as a function of time to describe the changes to the reliability of plant Structures, Systems and Components (SSCs). While DS has been used in many subject areas, some even within the PRA community, it has not been applied toward creating long-time horizon, dynamic PRAs (with time scales ranging between days and decades depending upon the analysis). Understanding slowly developing dynamic effects, such as wear-out, on SSC reliabilities may be instrumental in ensuring a safely and reliably operating nuclear fleet. Improving the estimation of a plant's continuously changing risk profile will allow for more meaningful risk insights, greater stakeholder confidence in risk insights, and increased operational flexibility.

ACKNOWLEDGMENTS

This work was supported by the Laboratory Directed Research and Development program at Sandia National Laboratories. Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the US Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

The authors would like to thank Jeff Cardoni for his technical contributions to Chapter 4 of this report, as well as his work on the Three Mile Island MELCOR model.

CONTENTS

1. Introduction 1
   1.1 Purpose of this report 1
   1.2 Structure of this report 1
2. Methodology for Incorporating Dynamic Behavior into Fault Trees using System Dynamics ... 3
   2.1 Overview 3
   2.2 Methodology 3
      2.2.1 Fault Tree Formulation 3
      2.2.2 Dynamic Reliability Models 4
   2.3 Conclusions 7
   2.4 References 7
   2.A Preliminary Results 7
3. Dynamic Multi-Modal Safety Relief Valve Stocastic Failure Model 11
   3.1 Introduction 11
   3.2 DDET Approach with SRV failures 12
      3.2.1 Safety Relief Valve Branch Point Quantification Methodology 14
      3.2.2 Stochastic SRV Failure Modeling 16
      3.2.3 Selection of Branch Points 21
   3.3 Conclusions 22
   3.4 Acknowledgements 22
   3.5 References 22
   3.A Multi-Valve Extension of Safety Relief Valve Cyclic Failure Analysis 23
4. SRV Cycling Impliations for a MELCOR iPWR Model with CVCS Operator Interaction 29
   4.1 Impact of SRV failure on unmitigated accident progression 29
   4.2 Effects of Operator Action on Accident Progression 32
   4.3 Conclusions 34
   4.4 References 34
5. Conclusions 35
6. Distribution 36

FIGURES

Figure 1-1. Overall proposed dynamic system probabilistic risk assessment methodology……2

Figure 2-1. Reproduction of the Oconee High Pressure Injection System (HPSI) Fault Tree [5] [6]. Circled basic event probabilities can either be time averaged representations (Traditional) or be dynamic variables informed by SD models……..3

Figure 2-2. Schematic System Dynamic Model of the Functional Behavior of the Oconee HPIS……..5

Figure 2-3. Simple DS model for migration in the average pump failure rate. ……....8

Figure 2-4. HPIS Fault Tree with Failure to Start and Failure to Run events highlighted……..8

Figure 2-5. Dynamic conditional failure probability for the HPIS with a 30 min mission time at 40, 60 and 80 years of operation…….9

Figure 2-6. Dynamic conditional failure probability for the HPIS with a 25 hour mission time at 40, 60 and 80 years of operation……..10

Figure 3-1. A schematic representation of one dynamic situation that branches into many simulations as branching criterion are experienced……..……13

Figure 3-2. Aleatory and epistemic distribution discretization for Safety Relief Valve failures…..…..14

Figure 3-3. Aleatory SRV Failure (FTO+FTC) Probabilities are plotted as a function of SRV cycles (1 Cycle = Open + Close). The mean, 16th, 50th, and 83rd percentiles of the epistemic failure distribution are plotted. For comparison, the Point Estimates (P.E.) for the SOARCA Surry and Peach Bottom FTCs, and the NUREG/CR 6928 aleatory distributions (which were calculated using the mean cycle failure frequency) are also shown……..……..…18

Figure 3-4. Aleatory SRV FTO Probabilities are plotted as a function of SRV cycles (1 Cycle = Open + Close). The mean, 16^{th}, 50^{th}, and 83^{rd} percentiles of the epistemic failure distribution are plotted. For comparison, the Point Estimate (P.E.) SOARCA for the Surry and Peach Bottom FTC and the NUREG/CR 6928 aleatory distributions, which were calculated using the mean cycle failure frequency, are also shown…….….19

Figure 3-5. Aleatory SRV FTC probabilities are plotted as a function of SRV cycles (1 Cycle = Open + Close). The mean, 16^{th}, 50^{th}, and 83^{rd} percentiles of the epistemic failure distribution are plotted……...…….20

Figure 3-6. Number of SRV cycles before predicted failure, plotted as a function of epistemic and aleatory uncertainty……21

Figure 3-7. Three valve state transition diagram. Annotations near the transition lines show the split fraction of the probability mass vector for a given cycle, not the probability mass as a function of n……..24

Figure 3-8. Three valve system dynamics diagram.…….....…….…25

Figure 3-9. Important mean probability states for a 3 valve system. The black light blue and green curves represent the probability of existing in states 1, 2 and 3, respectively. The yellow curve represents the probability of existing in any SRV cycling state as a function of SRV cycles. The red curve represents probability of a valve existing in State 5 as a function of SRV cycles. The blue curve probability of a valve existing State 4 (i.e., State 1 to 4 transition + State 2 to 4 transition + State 3 to 4 transition)……..……..…..……...26

Figure 3.10 - Horse-tail plot of iid samples of the FTO and FTC probabilities from NUREG/CR-6928 for any valve FTC (stuck open, State 4). Note that while 7533 samples are plotted, the range of FTC curves covers nearly 10 orders of magnitude, illustrating the large degree of uncertainty in the FTC and FTO estimates……...…..….27

Figure 3-11. Illustration of the uncertainty around the mean FTC estimate (i.e., probability of existing in State 4)……...28

Figure 3-12. Illustration of the uncertainty around the mean FTO estimate (i.e., probability of existing in State 5)……..……..…28

Figure 4-1. RPV water level for DV-failure scenarios for various SRV operation……..30
Figure 4-2. RPV pressure for DV-failure scenarios for various SRV operation……31
Figure 4-3. Containment pressure for DV-failure scenarios for various SRV operation……..31

TABLES

Table 3-1. Selected industry distributions for variability of FTC and FTO per cycle failure probabilities for SRVs [5]……...15
Table 3-2. Equally weighted branch points for estimates of the number of SRV cycles before failure.
Table 4-1. Summary of findings from the initial capability study [1]……...22
Table 4-2. Accident bifurcations for DV-failure case study with no operator action; end states after 7 day simulation. …….32
Table 4-3. Accident bifurcations for DV-failure case study with operator failure branches; end states after 7 day simulation. ……....33
Table 4-4. Accident bifurcations for FV-failure case study; end states after 7 day simulation…….34

NOMENCLATURE

ADAPT – Analysis of Dynamic Accident Progression Trees

DDET – Discrete Dynamic Event Trees

DS – Dynamical Systems

DV – Depressurization Valves

ECCS – Emergency Core Cooling System

FV – Feed Valve

HPIS – High Pressure Injection System

iid – Independent identically distributed

MCS – Minimum Cut Sets

PRA – Probabilistic Risk Assessment

iPWR – integral Pressurized Water Reactor

MELCOR – Severe Accident Computer Code, not an acronym

SD – System Dynamics

SRV – Safety Relief Valves

SSC – Structures Systems and Components

1. INTRODUCTION

1.1 Purpose of this report

Probabilistic Risk Assessment (PRA) is the primary tool used to risk-inform nuclear power regulatory and licensing activities. Risk-informed regulations are intended to reduce inherent conservatism in regulatory metrics (e.g., allowable operating conditions and technical specifications) which are built into the regulatory framework by quantifying both the total risk profile as well as the change in the risk profile caused by an event or action (e.g., in-service inspection procedures or power uprates).

Dynamical Systems (DS) analysis has been used to understand unintended time-dependent feedbacks in both industrial and organizational settings. In dynamical systems analysis, feedback loops can be characterized and studied as a function of time to describe the changes to the reliability of plant Structures, Systems and Components (SSCs). While DS has been used in many subject areas, some even within the PRA community, it has not been applied toward creating long-time horizon, dynamic PRAs (with time scales ranging between days and decades depending upon the analysis). Understanding slowly developing dynamic effects on SSC reliabilities may be instrumental in ensuring a safely and reliably operating nuclear fleet. Improving the estimation of a plant's continuously changing risk profile will allow for more meaningful risk insights, greater stakeholder confidence in risk insights, and increased operational flexibility.

DS modeling of aging and maintenance can easily allow for the inclusion of various failure regimes, including “bathtub” effects, as well as accounting for unintended damage during maintenance to connected systems. It is possible that such correlations can be derived from the failure data reported by the U.S. Nuclear Regulatory Commission as part of their system reliability studies. Aging and maintenance dynamic models examine the evolving basic component reliabilities with time. Traditional PRAs utilize Markov Models to predict time-dependencies of component failure and repair, but these methods are typically only used for constant failure and repair rates and are typically averaged over a mission time before being included in the fault tree. DS models allow the decision maker greater flexibility in making risk-informed decisions by adjusting the fidelity of the model to meet their needs. In addition to modeling various failure behaviors and maintenance strategies, decision frameworks can be included in which maintenance rates can vary as a function of predicted system reliability and costs. A general DS PRA analysis organizational scheme can be seen in Figure 1-1.

It is hypothesized that metrics from a DS model of a nuclear plant, such as time-dependent SSC reliability, can provide input to a dynamically restructured PRA. The coupling between PRA and DS will both remove non-conservative approximations and improve stakeholder confidence in PRA.

1.2 Structure of this report

This report consolidates the results from a number of papers created using funding from the DS PRA LDRD project. Extensions of each paper are incorporated in an appendix sub-section for each paper when applicable. Chapter 2 overviews the DS PRA approach using System Dynamic (SD) models when analyzing the Oconee High Pressure Injection system (primarily from SAND2012-5500C). Chapter 3 describes how DS modeling can improve our current Safety Relief Valve (SRV) stochastic failure

modeling methodologies (primarily from SAND2013-3684C). Due to an equipment delay[1], planned case studies using the MELCOR Three Mile Island deck were not able to be conducted. Instead, Chapter 4 overviews how the DS SRV failure approach impacted an FY13 discrete dynamic event tree analysis for an iPWR (primarily from SAND2013-8324). Finally Chapter 5 discusses general conclusions which can be drawn from the work reported in this LDRD.

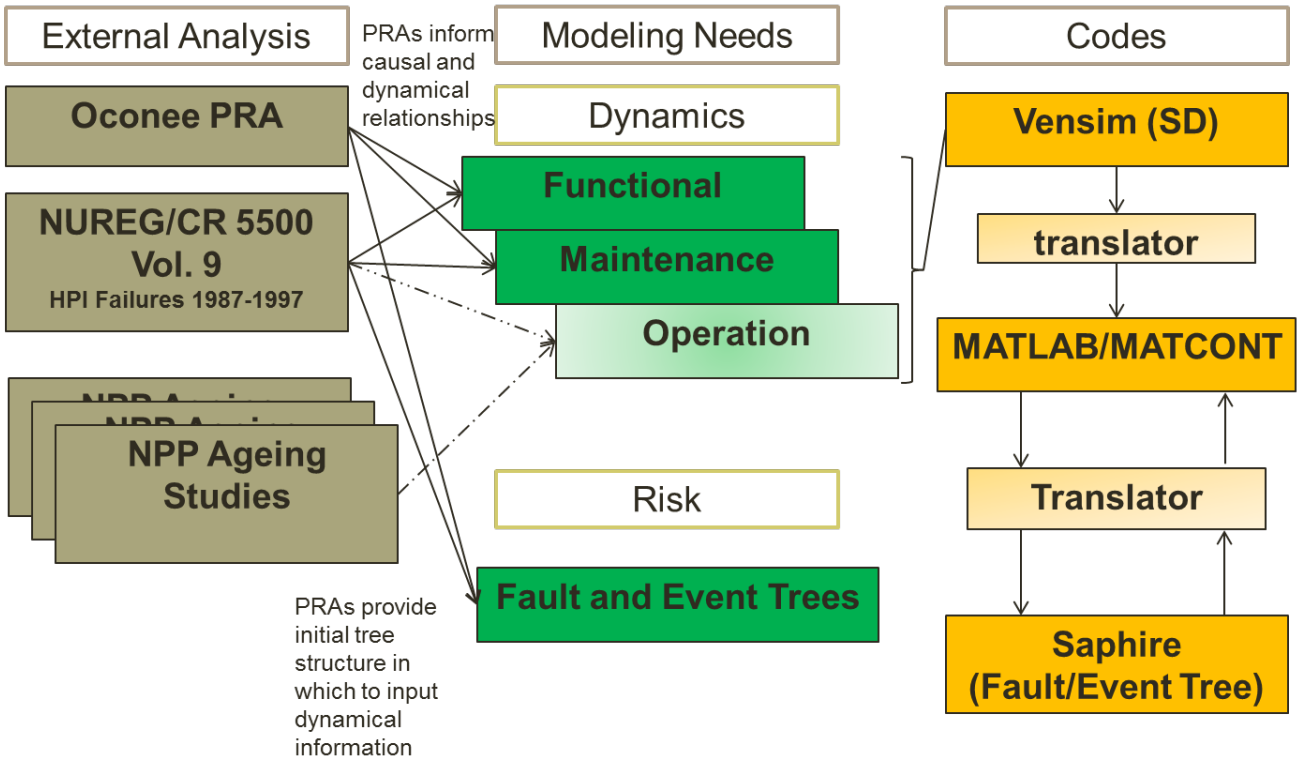

Figure 1- 2. Overall proposed dynamic system probabilistic risk assessment methodology

[1] Near the end of FY15, Center 6230's Linux cluster, Bankston, suffered fatal hardware failure which resulted in a new Linux system being procured. Unfortunately the new system not installed in enough time to complete an appropriate case study. Any case study would require the use of SNL's job scheduling software, ADAPT, which is not compatible with the MELCOR windows clusters. MELCOR runs in serial (one job per thread) which would not allow efficient simulation on SNLs larger distributed Linux clusters.

2. METHODOLOGY FOR INCORPORATING DYNAMIC BEHAVIOR INTO FAULT TREES USING SYSTEM DYNAMICS

2.1 Overview

This chapter explores the primary techniques used to conduct DS PRA analysis for nuclear power plants. Sections 2.2 thorough 2.4 provide the overall methodology for how the SD toolkit can be used to examine both slowing and quickly evolving changes to the basic event probabilities in fault trees. These sections were extracted from SAND2012-5500C. Section 2.A provides a small case study exploring the implications of pump aging on the in-accident time dependent performance of the High Pressure Injection System (HPIS).

2.2 Methodology

The approach explored in this chapter combines two analytical techniques:

1. Quasi-static Fault Trees with average time dependencies, e.g., HPIS Fault Tree in Figure 2-1, and
2. Dynamic methods with explicitly model time dependent changes in system behavior.

Each method employs unique computational tools and codes which will need to be utilized to maximize the usefulness of the output.

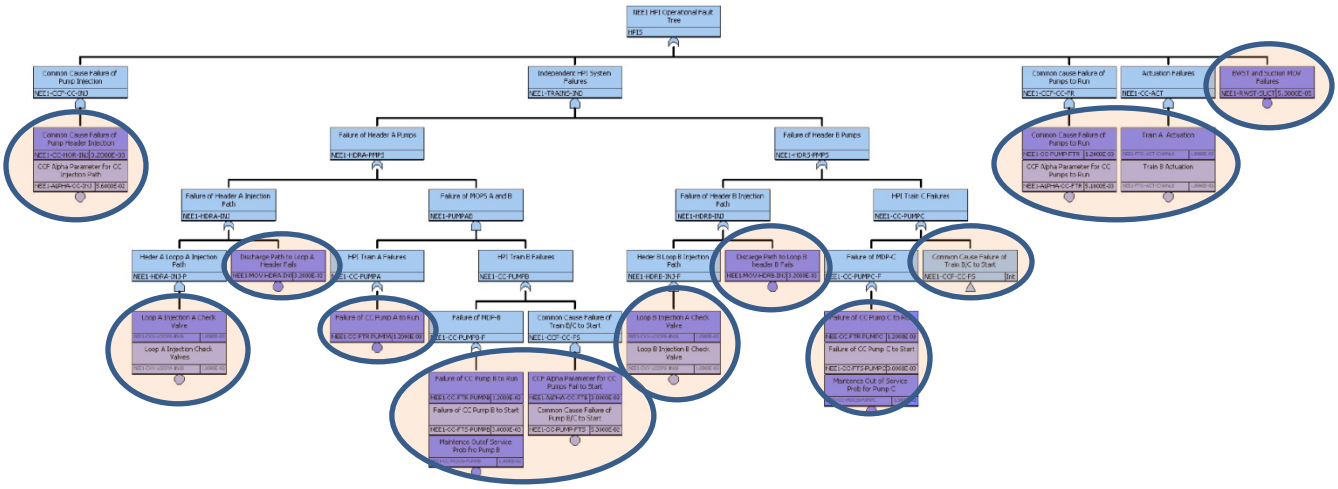

Figure 2-1. Reproduction of the Oconee High Pressure Injection System (HPSI) Fault Tree [5] [6]. Circled basic event probabilities can either be time averaged representations (Traditional) or be dynamic variables informed by SD models.

2.2.1 Fault Tree Formulation

The Fault Trees, which along with Event Trees comprise the building blocks of a nuclear PRA, compute average system failure probabilities from basic event probabilities. These basic event probabilities are, in turn, estimated directly from failure data. Some of these estimates can hide dynamic behavior through assumptions. For example, the failure-to-start probability for a pump is assumed to be independent of the number of demands on the pump instead of accumulating damage, and thus increasing the conditional failure probability, as the pump demands increase. Other estimates can hide dynamics

through discretization in time. For example, the failure-to-run probability for a pump is averaged over a given time interval instead of evolving the plant risk profile as the pump operates. Thus, each basic event probability, which has only one value that is propagated through the tree, fails to account for degradation due to use, as well as other parameters. In traditional PRAs, the resulting unreliability estimate is calculated by summing failure probabilities from all Minimum Cut-Set (MCS) in the system. Each MCS is a unique minimum group of component failures in the system which can cause overall system failure. For example, in the High Pressure Injection System (HPIS) modeled in Figure 2-2, one example of MCSs would be the failure of all three high pressure injection pumps. Eq. 1 is the mathematical formula for system unreliability using MCS.

$$F_{sys} = Pr\left(\sum_{n=1}^{N} MCS_n\right) \quad \text{Eq. 1}$$

In Eq. 1, F_{sys} is the system failure probability, P(*) is the probability transformation from Boolean logic to probability, and MCS_n is the n^{th} MCS. While these quasi-static representations of plant risk can be modeled in codes such as Saphire [6], it is hypothesized that dynamic models of basic event probabilities, such as making the probability of a given MCS_n a function of multiple parameters including time, may lead to a more accurate representation to evolving plant risk.

Dynamic models simulate time dependent changes in system behavior. System codes such as MELCOR or RELAP have been used in safety analysis to estimate the probabilistic response of complex systems. While these codes offer important insights concerning thermal-hydraulic, neutronic, and material changes during an accident, they generally are only used to calculate a branch probabilities within a given accident sequence. More general dynamic models can be created using SD modeling methods which can model both variations in basic event probabilities as well as branch probabilities. While SD models are typically created graphically, as shown in Figure 2-2, they ultimately reduce to a system of differential equations generalized in Eq. 2.

$$\begin{bmatrix} \dot{x}_1 = k_1 + k_2 x_1 + k_3 x_2 + \cdots \\ \vdots \\ \dot{x}_N = k_i + k_{i+1} x_1 + k_{i+2} x_2 + \cdots \end{bmatrix} \quad \text{Eq. 2}$$

In Eq. 2, x_i is the state variable *I*, $\dot{x}_i$ is the differential of state variable *I*, and k_i are constants which describe the relationships between variables. These variables can estimate both physical properties (e.g., temperatures, pressures, and flow-rates) and non-physical properties (e.g., probabilities and damage). Once the dynamic equations are integrated with the fault tree logic structure, both traditional PRA (e.g., importance measures) and dynamic analysis techniques (e.g., phase diagrams and bifurcation analysis) can be applied. Thus, these more generic dynamic modeling methods will allow the flexibility to model slowly evolving phenomena, such as aging or maintenance of components, while still allowing the analysts to examine the implication of those phenomena on system performance.

2.2.2 Dynamic Reliability Models

Dynamic models can interface with the PRA through many different approaches. For this study, the focus will be to identify plausible behavior modes for systems undergoing maintenance and aging, along

with dynamic events (e.g. startup, shutdown) that might benefit from analysis of reliability dynamics. In order to accomplish this goal, three different dynamic models are utilized:

1. Functional – How does the system work?
2. Aging and Maintenance – How does time affect component performance?
3. Operational – What decisions can the operator make given the information available?

2.2.2.1 Functional Dynamic Models

Functional dynamic models examine how a system operates to complete its mission. While traditionally PRAs only examine interdependencies through cut-sets and common cause factors, a functional dynamic model examines the system holistically. Figure 2-2 shows a functional dynamic model of the Oconee HPIS. This model is currently being coupled with the fault tree in Figure 2-1 to capture dynamic changes in plant risk upon system actuation.

While the fault tree can help assemble a functional dynamic model, the dynamic model is less rigid than the fault tree in determining success or failure of the system. For example, the fault tree shown in Figure 2-1 requires that one of the three trains of pumps not fail in order for the HPIS to succeed, but the fault tree views even partial loss of capacity as a failure. The functional dynamics model can simulate the performance of multiple degraded systems (through environmental effects or aging) acting cooperatively, a success path cannot easily be found through traditional fault trees. Additionally, the functional dynamics model can help identify and interrogate potential conditional and common cause failure modes within the system.

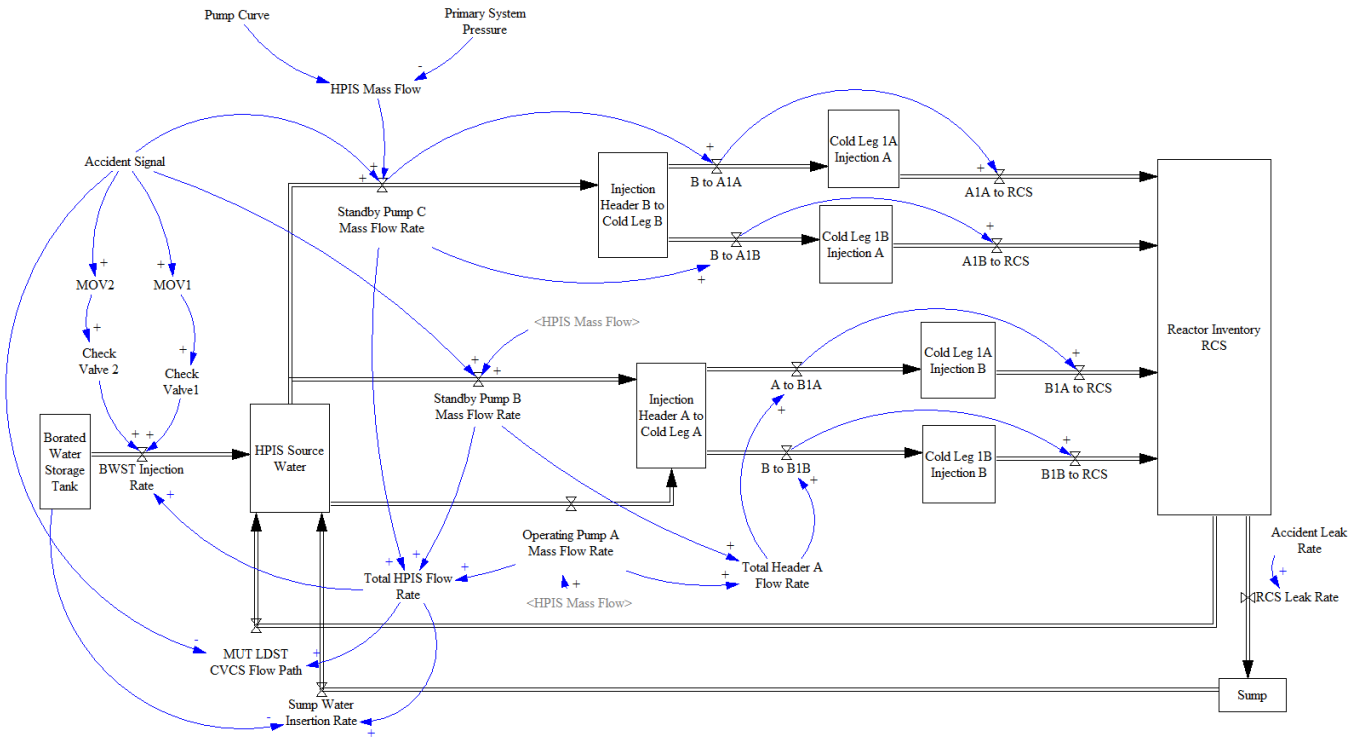

Figure 2-2. Schematic System Dynamic Model of the Functional Behavior of the Oconee HPIS.

This functional model can interface with the aging/maintenance and operational models, but in general the time scale of interest for the functional model is much shorter and thus only a loose coupling between the dynamic models are expected.

2.2.2.2 Aging and Maintenance Dynamic Models

Aging and maintenance dynamic models examine the evolution of basic component reliabilities with time. Traditional PRAs utilize Markov Models to predict time-dependencies of component failure and repair, but these methods are typically only used for constant failure and repair rates and are typically averaged over a mission time before being included in the fault tree [7].

SD modeling of aging and maintenance can easily allow for the inclusion of various failure regimes, including "bathtub" effects [7], as well as accounting for unintended damage during maintenance to connected systems. It is possible that such correlations can be derived from the failure data reported by the U.S. Nuclear Regulatory Commission as part of their system reliability studies [5] [8]. This data analysis effort will be conducted during the next year of this study.

In addition to modeling various failure behaviors and maintenance strategies, decision frameworks can be included in which maintenance rates can vary as a function of predicted system reliability and costs [3] [4]. Because this project does not have requisite expertise in group decision analysis, these areas will not be examined in detail as part of this project.

2.2.2.3 Operational Dynamic Models

Operational dynamic models examine system behavior when a component fails during steady-state operation. These models are similar to the aging and maintenance models, but differ due to the shorter time scale of interest and the higher potential for damage to adjacent systems. This additional potential for damage may be caused by additional propagated stresses in the system due to the initial component failure or by unintentional damage during maintenance being conducted under stress and time constraints.

One potential application of the operational dynamic model relates to applications of Reg. Guide 1.177 [9]. Reg. Guide 1.177 discusses a risk-informed approach to modifications to Technical Specifications, e.g., how long the power plant has to repair specific safety related components before the plant must shutdown. Due to increased maintenance efforts at the plant, the short-term potential for unintended damage to SSCs may potentially increase. Additionally, after the component has been repaired there may be an additional increase in unreliability as the newly repaired component resets to the "infant-mortality" failure regime [7]. These short-term increases in system unreliability are not currently captured in traditional Fault Tree analysis but can be incorporated through the dynamic system models.

2.3 Conclusions

A dynamic approach to calculating basic event probabilities can help improve confidence in PRA metrics as well as make better risk-informed decisions as the nuclear fleet moves to extend their operating licenses. Functional, aging and maintenance, and operational models can all be useful in capturing component damage modes which are neglected from traditional PRA analysis. Understanding these dynamic modes may influence decisions made by both plant operators and regulators.

In future work, the functional, aging and maintenance, and operational models of the Oconnee HPIS will be created and analyzed to illustrate the importance of incorporating dynamics into fault tree analysis. This paper presents a functional model of the Oconnee HPIS which is currently being coupled with a traditional fault tree to provide dynamic system reliability estimates.

2.4 References

[1] U.S. NRC, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, Reg. Guide 1.174, November (2002).

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

[3] J. Sterman, *Business Dynamics: Systems Thinking in a Complex World*, pp. 66-73, Irwin McGraw-Hill, Boston, MA, (2000).

[4] Z. Mohaghegh, R. Kazemi, and A. Mosleh, "Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization," *Reliability Engineering and System Safety*, **93**, pp.1000-1018, (2009).

[5] J. Poloski, J. Knudsen, C. Atwood, and W. Galyean, *Reliability Study: High-Pressure Safety Injection System, 1987-1997*, Idaho National Engineering and Environmental Laboratory, NUREG/CR-5500 Vol.**9**, INEEL/EXT-99-00373, Idaho Falls, ID, (2000).

[6] K.D. Russell, C.L. Atwood, W.J. Galyean, M.B. Sattison, D.M. Rasmuson, *Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE), U.S. Nuclear Regulatory Commission*, NUREG/CR-6116, Washington, DC, (1994).

[7] N. McCormick, *Reliability and Risk Analysis*, pp. 26,117-189, Academic Press, New York, NY, (1981)

[8] U.S. NRC, *High Pressure Safety Injection 1998–2010*, accessed at http://nrcoe.inel.gov/resultsdb/SysStudy/HPSI.aspx on June 12th (2012).

[9] U.S. NRC, *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications*, Reg. Guide 1.177, May (2011).

2.A Preliminary Results

This appendix discusses an initial assessment of aging impacts on HPIS performance using DS PRA modeling. A full modeling effort would model changes in component reliabilities using smaller DS models such as the one shown in Figure 2-3. These models will be plugged the basic event probabilities as shown in Figure 2-4 to calculate the age dependent reliability of the HPIS upon demand. Such models would need MELCOR derived time dependent variables, e.g., Temperature Pressure, Chemistry, in order to change the failure rate as a function of accident progression.

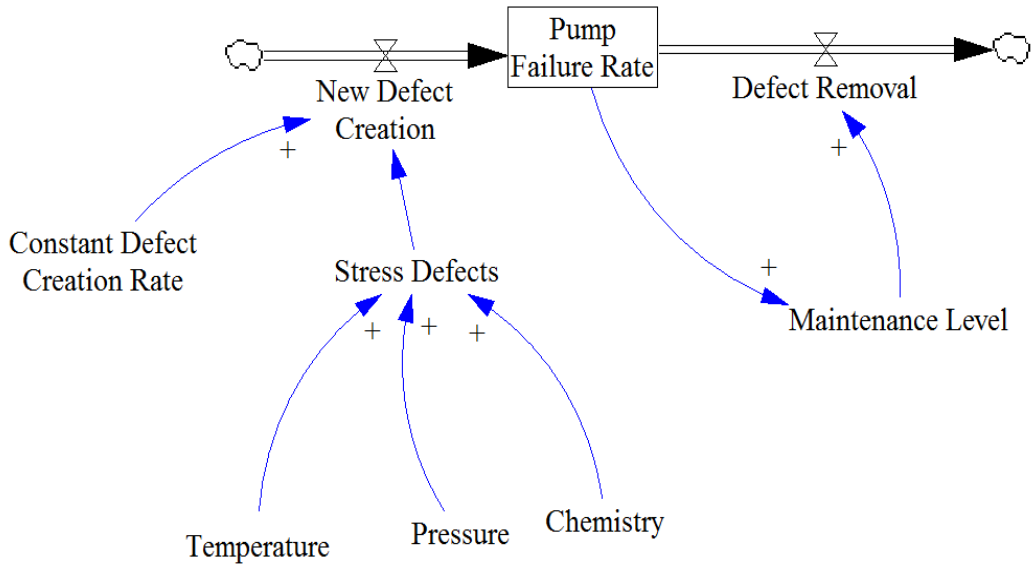

Figure 2-3. Simple DS model for migration in the average pump failure rate.

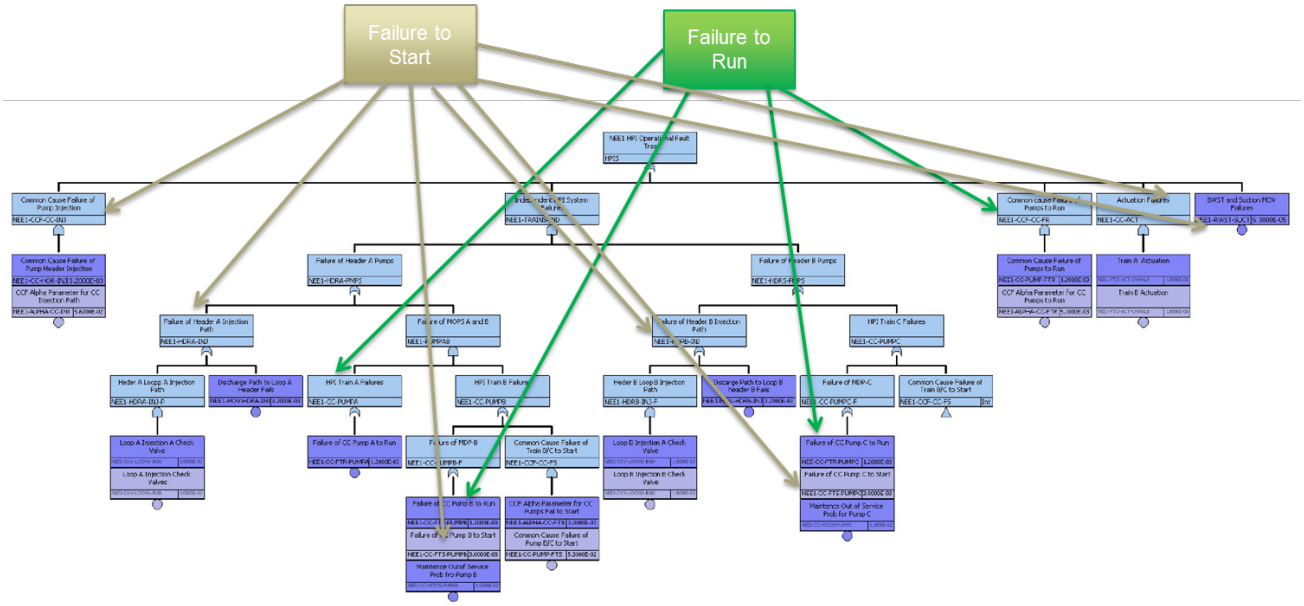

Figure 2-4. HPIS Fault Tree with Failure to Start and Failure to Run events highlighted.

Unfortunately, the computational resources were never available to fully link the DS models to the Three Mile Island MELCOR model. As a result, a simplified aging model derived from [5] was applied to the primary coolant pumps to examine first order aging effects. The results can be seen in Figure 2-5 and Figure 2-6 for various mission times. Before the HPIS system is activated, there is almost no change to plant risk due to pump aging. This is due to the large amount of redundancy in the initial fault tree, much of which is not effected by aging. When the system activates, success and failure of values and tanks (and failure to start probabilities for the HPIS pumps) are removed from

the reliability equation leaving only the aging pumps to dominate the conditional probability of failure. As can be seen from Figure 2-6, extending pump lifetime from 40 to 60 to 80 years has the potential of increasing the probability of failure anywhere from a factor of 2 to a factor of 10, depending on the number of pumps which successfully actuated and the age of the system. This initial result suggests that while aging may not affect the overall risk of a nuclear power plant, it may affect accident management due to the reduction in redundant systems. Thus, the authors suggest that the implications of aging should be included in any attempt to manage severe accidents.

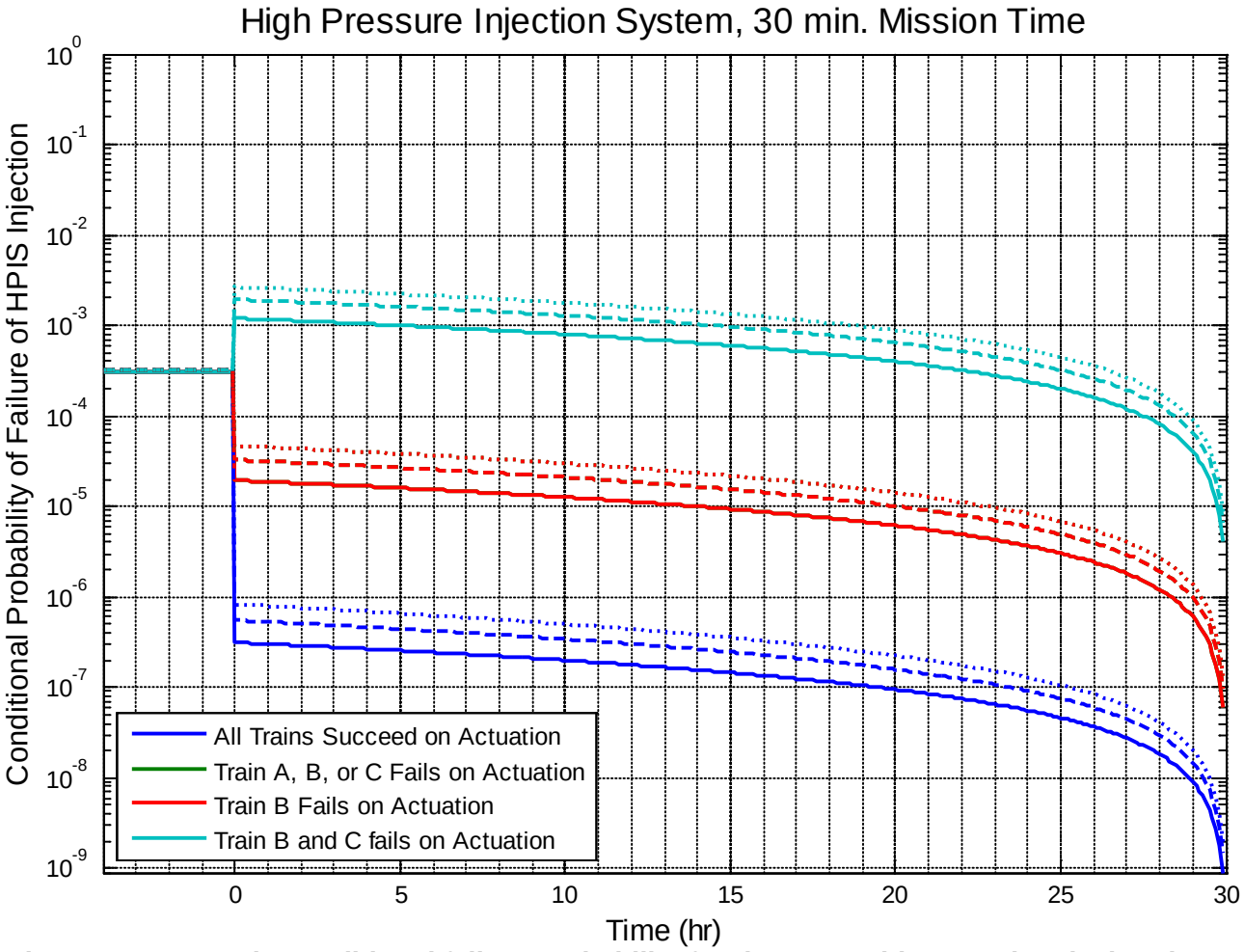

Figure 2-5. Dynamic conditional failure probability for the HPIS with a 30 min mission time at 40, 60 and 80 years of operation.

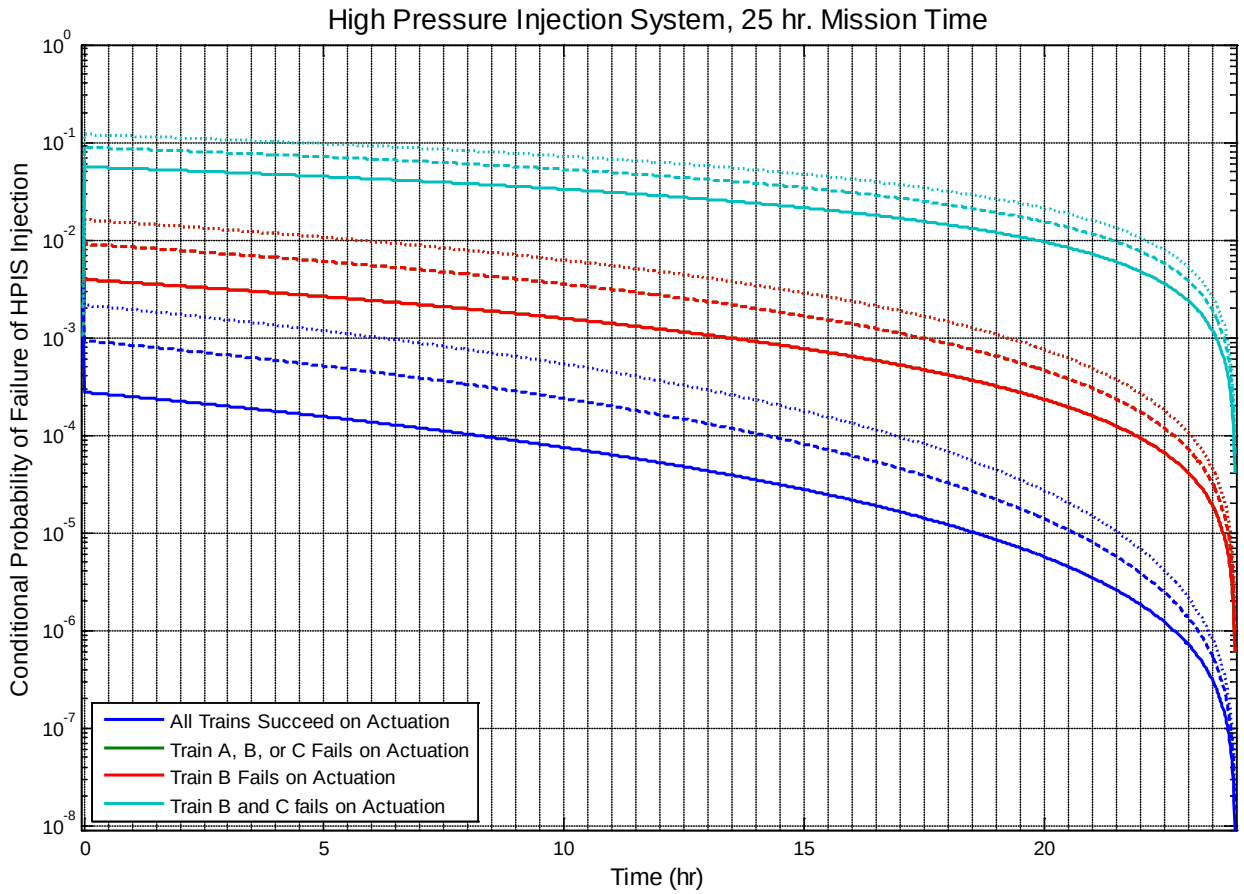

Figure 2-6. Dynamic conditional failure probability for the HPIS with a 25 hour mission time at 40, 60 and 80 years of operation.

3. DYNAMIC MULTI-MODAL SAFETY RELIEF VALVE STOCASTIC FAILURE MODEL

ABSTRACT

Safety Relief Valves (SRVs) are an important component of the safety case for a Light Water Reactor (LWR). The number and types of SRVs in LWRs vary from plant to plant, but they generally operate to perform the same safety function. During accidents in which the coolant pressurizes beyond a predetermined set-point, the SRV will open, releasing coolant from the primary system and into the containment. Once enough coolant has been released to lower the coolant pressure, the SRV will reset. This cycle will continue until pressure drops and remains below the set-point or until the SRV fails in either a Failed to Open (FTO) or Failure to Close (FTC) mode. These failures can be caused either through cyclic loading or as a result of thermal-induced stresses from the coolant passing through the valve. SRV failures can be important, because an SRV that has FTC will cause a small "Loss of Cooling Accident", which may depressurize the system or simply leak coolant out of the RCS. Alternatively, SRVs that have FTO will allow system pressure to rise until it reaches the next SRV set-point. If the pressure is not reduced through the successful operation of other safety systems, either creep rupture elsewhere in the system, such as in the steam line, or high-pressure core damage may occur. While some SRV failure data is recorded in NUREG/CR-6928, the spread of the epistemic uncertainty distributions for FTO and FTC are wide. These large uncertainties may cause an analyst to be overconfident in the results of a severe accident simulation that uses only point-estimates calculations of FTO and FTC.

3.1 Introduction

This paper reviews a DS SRV stochastic failure fault tree which can be used to implement a Discrete Dynamic Event Tree (DDET) assessment of nuclear power plant accident response [1][2]. The results presented in Sections 3.1-3.5 were published in SAND2013-3684C. Section 3.A presents follow-on work to generalize a single SRV failure model to multiple staged SRVs.

Application of the DDET methodology requires both the determination of the branching criteria and the quantification of branching probabilities. This paper will review the process for determining both the branching criteria and the probabilities for SRV failure. The timing of SRV failure (either in the open or closed position) has been demonstrated to be an important bifurcation parameter in severe accident response [3] [4] and therefore an important uncertainty to quantify in a DDET analysis.

This paper discusses cyclic loading-induced SRV failures and ignores thermal creep-induced failures. Thermal creep has been demonstrated to be an important failure mode [3] but will need to be examined separately. Finally, it should be noted that the majority of cyclic loading SRV failure data is taken from plant experience and not from controlled experiments [5]. Complete sticking of the SRV has not been recorded in plant operation, requiring the use of partial failure data and large resulting uncertainties in this study. The limitations of the underlying SRV-failure database should be taken into account when interpreting the results of a DDET analysis using the cyclic loading failure methodology described below.

3.2 DDET Approach with SRV failures

DDETs are an accelerated uncertainty propagation methodology that uses dynamic programming to build an event tree [6][5]. In a DDET analysis, the user pre-determines set-points that correspond to the initiation of an uncertain dynamic system response (e.g., component failure). These set points tell the dynamic analysis code (e.g., MELCOR) to stop in the middle of a simulation so that the uncertain parameter can be modified. Multiple simulations are then initiated with each simulation using:

1. A different value for the uncertain parameter, and
2. An associated branch weight corresponding to the degree of uncertainty that the varied parameter was intended to represent.

Ultimately, acceleration is experienced, because uncertainties in late-accident phenomena do not need to be simulated from transient initiation. Instead, one simulation can progress late into a transient, and then branch into multiple simulations to evaluate uncertainties in these late accident phenomena. Figure 3-2 illustrates a schematic representation of one dynamic situation that branches into many simulations as branching criteria are experienced.

Branching criteria can be defined across a wide array of system and code parameters. In the Analysis of Dynamic Accident Progression Trees (ADAPT) DDET driver code [3], the only limitation imposed on how branching criteria are defined is that all branching criteria need to be set before the DDET analysis is conducted. Thus, if the number of SRV cycles is a branching criterion, the number of cycles before the subsequent branch needs to be determined *a priori* and cannot be changed by the dynamic code.

In general, a DDET analysis is conducted using the following procedure:

1. Create stable dynamic model (e.g., the model needs to be robust enough to not crash when variables are changed mid-simulation)
2. Decide key uncertain parameters of interest, such as:
    a. Off-site power restoration time
    b. Decay Heat levels
    c. SRV failure timings
3. Create and discretize cumulative distribution functions for key parameters. This process is similar to traditional Latin-Hypercube sampling, except that each simulation is not started from the same point in time.
4. Program the binary branch points into the DDET code.
5. The DDET code starts, stops, and branches dynamic simulations, as necessary.

Appropriately creating and discretizing the uncertain dynamic parameters (i.e., Step 2 above) is extremely important in a DDET analysis. A robust DDET analysis will examine all epistemic (i.e., state of knowledge) and/or aleatory (i.e., random) uncertainties in the dynamic parameter of

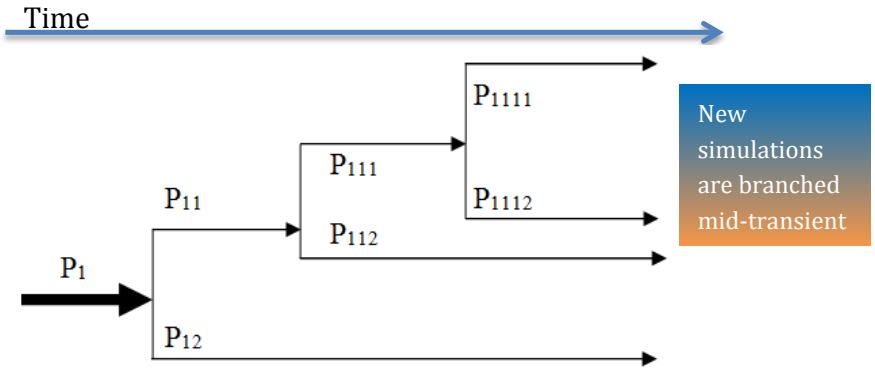

Figure 3-1. A schematic representation of one dynamic situation that branches into many simulations as branching criterion are experienced.

interest. The general approach for determining and discretizing uncertainties for cyclic SVR failures is described below.

First, the types of uncertainties related to cyclic SRV failure were considered. Cyclic SRV failure is typically modeled as a binomial distribution describing the random failure of the SRV. This binomial model is dependent on the "per-cycle" failure probability. The likelihood that an SRV will survive until cycle N is modeled as the Negative-Binomial distribution. Because cyclic SRV failures are rare, the industry's knowledge of the "true" per-cycle failure probability is low, and yields a high epistemic uncertainty for the per-cycle probability [5]. Each of these uncertainties, the aleatory failure model and the epistemic per-cycle failure probability, should be evaluated as part of an uncertainty analysis.

Figure 3-2 plots the cumulative SRV failure probability as a function of SRV cycles for the 16.6th, 50th, 83.3rd percentile estimates of the per-cycle SRV failure probability. The mean cumulative SRV failure probability is also plotted. The governing equations are described in Section 3.2.2. The thick, orange horizontal lines represent the 16.6th, 50th, 83.3rd percentiles of the family of negative binomial distributions. When the horizontal lines intersect the 16.6th, 50th, 83.3rd percentile negative binomial curves, nine intersection points are formed (only seven intersection points are shown in Figure 3-2 to the limited number of cycles shown). These nine intersection points represent three random failure points for each of the three representative estimates for the "true" per-cycle failure probability. The dashed blue lines relate the intersection point to the associated estimate regarding the number of SRV cycles. While the analysis described in this report only discretizes the epistemic and aleatory uncertainties into three bins each, a robust analysis would discretize each distribution until the final decision metrics do not appreciably change. If, in the course of the dynamic analysis, the SRVs are not simulated to cycle past a given number, any branch points that predict failure at a higher number of SRV cycles are not simulated. Thus, the DDET's ability to abstain from creating unnecessary branches can greatly decrease the runtime for the total analysis.

While both epistemic and aleatory uncertainties were analyzed to estimate SRV failures, the need to analyze each type of uncertainty can be "variable specific." For instance, failure rates on components with large quantities of data may only require aleatory uncertainties to be analyzed, because the epistemic uncertainty would be *de minimis*. Alternatively, uncertainties relating to

physical parameters (e.g., core degradation rates, mass flow rates) would only have epistemic uncertainties to analyze.

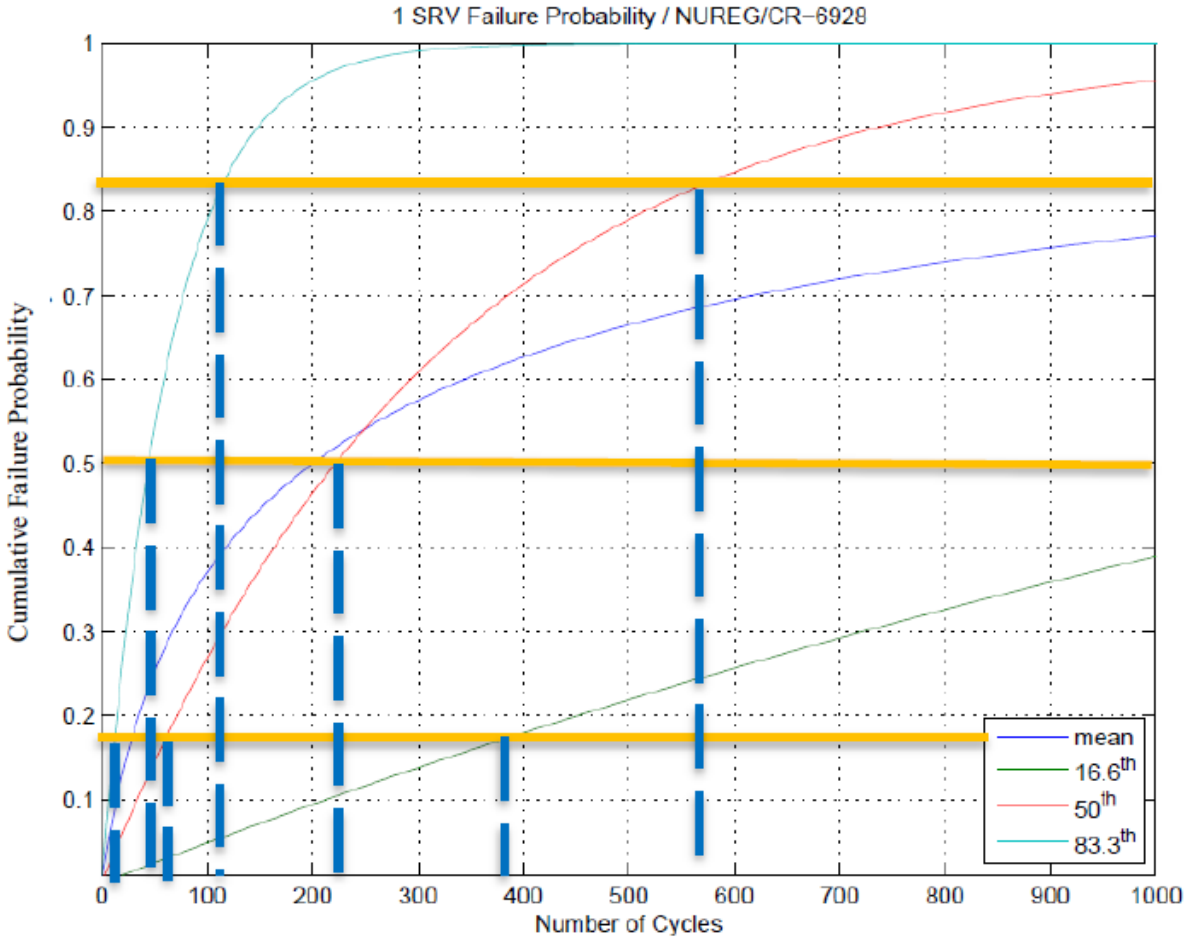

Figure 3-2. Aleatory and epistemic distribution discretization for Safety Relief Valve failures.

3.2.1 Safety Relief Valve Branch Point Quantification Methodology

During transient simulations in MELCOR, appropriately estimating the number of SRV cycles before SRV failure is important to producing a defensible safety analysis. This section describes SRV failure modes, and provides a stochastic model that can be used to estimate the number of the SRV cycles at which failure occurs (n). While a diverse array of SRV configurations exists, in general SRVs open and close to relieve high primary-system pressure by releasing primary coolant into the containment or suppression pool. NUREG/CR-6928 identifies three cycling failure modes:

- Failure To Open (FTO) – The SRV fails in the closed position.
- Failure To Close (FTC) – The SRV fails in the open position.
- Fail To Close after passing Liquid (FTCL) (a subset of FTC) –. This failure mode was not supported by the database used to supply data in NUREG/CR-6928, and was,

therefore, excluded from the stochastic analysis. It is assumed that FTCL consequences are subsumed by the FTC consequences.

It is assumed that the primary uncertain variable of interest is the number of SRV cycles (demands) that occur before failure of the SRV in either the FTO or the FTC mode. Failure is assumed to occur due to the inherent variability in the SRV cycling process. A parameter *p* denotes the probability of obtaining a failure on each demand. "*p*" will henceforth be referred to as the "per-cycle failure probability". It is further assumed that each demand on the SRV is independent of previous demands. Thus, *p* is constant for each demand on the SRV (i.e., the *p* is independent of cycle number, temperature, etc.). This is a Bernoulli process.

Because each cycle is assumed to be independent, the probability of failing on the N^{th} cycle is the product of the probability of failing on that cycle, *p*, multiplied by the probability of success in the previous (n-1) cycles:

$$f(n|p) = P(N = n|p) = p(1-p)^{n-1}, 0 \leq p \leq 1, n \sim [1,2,3 \ldots] \quad \text{Eq. 3}$$

This distribution describes the aleatory uncertainty about how many successful cycles will occur before failure at cycle N, given the parameter *p*. (In probability space, this is the probability distribution function (pdf) of the geometric distribution for *p*.)

The cumulative distribution function (cdf) of the geometric distribution expresses the likelihood that the valve will fail before N cycles:

$$F(n,p) = P(N \leq n|p) = 1-(1-p)^{n}, 0 \leq p \leq 1, n \sim [1,2,3 \ldots] \quad \text{Eq. 4}$$

However, there exists a large uncertainty about the value of *p* for SRV failures. This epistemic (i.e., state of knowledge) uncertainty for the per-cycle failure probability is modeled as a beta distribution.

The distributions for the per-cycle failure probabilities of the failure modes listed above are shown in Table 3-1. It should be noted that the SRV failure data used in NUREG/CR-6928 are fairly scarce. The FTO data was deemed sufficient for an Empirical Bayes analysis; however, the cumulative partial failure did not exceed 0.3 (α) was thus changed to 0.3 by the NUREG/CR-6028 authors. The β shape parameter reported in NUREG/CR-6028 is adjusted to preserve the mean of Empirical Bayes FTO distribution. FTC failure data is extremely scarce, so a Simplified Constrained Non-Informative Distribution was generated by producing a Jefferies mean of the industry data and using an assumed fraction failure of 0.5 (α) [5].

Table 3-1. Selected industry distributions for variability of FTC and FTO per cycle failure probabilities for SRVs [5]

Failure Mode	Distribution Type	A	β
FTO	Beta	0.3	38.9
FTC	Beta	0.5	628.2

Of these failure modes, only FTO and FTC were used in the SRV failure analysis. Instead of using the mean FTO and FTC values in this analysis, the entire FTC and FTO beta distributions were sampled to determine the number of cycles expected until SRV failure. By assuming the

independence of the FTO and FTC failure modes, a small probability of a total failure probability greater than 1.0 exists. Given the relatively small values of the FTC and FTO probabilities defined by the α and β parameters shown in Table 3-1, this non-physical result should not affect the final results.

3.2.2 Stochastic SRV Failure Modeling

To simplify the analysis, it is assumed that each trial of the binomial failure model refers to a complete cycle of the SRV (open and closed). Thus, the probability of failure, *p*, for each is defined in Equation 1 as the sum of the (assumed) independent FTO and FTC distributions. In reality, FTO and FTC are dependent parameters, because if the valve FTOs it cannot then FTC. While this assumption does introduce a small degree of error into the overall calculation, typically the per-cycle FTC and FTO probabilities are small enough to ensure that the error introduced by this dependency is negligible. In Eq. 5, p is the failure probability for each cycle, p_{FTO} is the failure to open probability for each cycle, and p_{FTC} is the failure to close probability for each cycle. Note: Lower case variables denote values within a distribution; upper case variables denote distributed variables.

Because the uncertainty propagation is conducted via Monte Carlo sampling, the differential transformations needed to normalize the distribution following the transformation of variables is not included in this derivation. Instead, the final distribution will be normalized numerically.

Historically, the mean of p was used to determine the cumulative distribution function of SRV failure, i.e., $P(N \leq n|p)$, but the non-linear nature of Eq. 5 prevents the high and low estimates of p from canceling each other out and producing the mean $P(N \leq n|p)$. Using the mean p to attempt to produce the mean $P(N \leq n|p)$ is referred to as the "Flaw of Averages" [7]. A more rigorous approach would be to sample from the distributions for p_{FTO} and p_{FTC} to obtain a range of values for *p*, and thus $P(N \leq n|p)$ curves. A given realization of $P(N \leq n|p)$ can be found by sampling p_{FTO} and p_{FTC} from the distributions $\pi_{P_{FTO}}(p_{FTO})$ and $\pi_{P_{FTC}}(p_{FTC})$, respectively. Thus, a given realization would produce a cumulative SRV failure curve using Eq. 6a. The corresponding cumulative failure distributions for the state of SRV can be determined by multiplying $P\left(N \leq n\middle|p_{FTO_i}, p_{FTC_i}\right)$ by the fractional component of each failure mode. This can be seen in Eq. 4a and 4b.

$$P\left(N \leq n\middle|p_{FTO_i}, p_{FTC_i}\right) = 1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n \quad \text{Eq. 5}$$

$$P_{FTO}\left(N \leq n\middle|p_{FTO_i}, p_{FTC_i}\right) = \left[1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n\right] * \frac{p_{FTO_i}}{p_{FTO_i} + p_{FTC_i}} \quad \text{Eq. 6a}$$

$$P_{FTC}\left(N \leq n\middle|p_{FTO_i}, p_{FTC_i}\right) = \left[1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n\right] * \frac{p_{FTC_i}}{p_{FTO_i} + p_{FTC_i}} \quad \text{Eq. 6b}$$

The expected value, or mean, of the $P_{FTC}\left(N \leq n\middle|p_{FTO_i}, p_{FTC_i}\right)$ curves can be calculated using Eq. 7. All distribution sampling, mean, and percentile calculations were conducted using intrinsic functions in MATLAB [8].

$$E[P(N \leq n)] = \frac{1}{m} * \sum_{i=1}^{m} P(N \leq n|p_i) = \frac{1}{m} * \sum_{i=1}^{m} 1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n \quad \text{Eq. 7}$$

Figure 3-3, Figure 3-4, and Figure 3-5 show the mean, 16.6th, 50th, and 83.3rd percentiles of the epistemic variations in $P(N \leq n|p_{FTO}, p_{FTC})$, $P_{FTC}(N \leq n|p_{FTO}, p_{FTC})$, and $P_{FTO}(N \leq n|p_{FTO}, p_{FTC})$, respectively. While the epistemic FTO and FTC probabilities are assumed to be independent, they are related ($p_{FTO_i} + p_{FTC_i} = p$) in each epistemic sample. Thus, while the expected value of the sum of both the FTO and FTC equal the expected value of all SRV failures, the percentiles cannot be expected to follow the same combinatorial rules.

In these plots, the y-axis shows the aleatory uncertainty for each curve. Figure and Figure also show the FTC aleatory failure curve used in Surry SOARCA analysis [3]. The Surry SOARCA analysis provides only a point estimate of the per-cycle failure probability, and further assumes that the SRVs can only fail in the open state. To determine the Best Estimate of the number of SRV cycles before failure, Surry SOARCA assumed that failure of the SRV occurs at the 50th percentile of the aleatory failure distribution, or 256 cycles. The Surry SOARCA estimate tracks closely with the 50th percentile epistemic estimate of $P(N \leq n|p_{FTO}, p_{FTC})$ in Figure 3-3, but under-predicts the 50th percentile epistemic estimate of $P_{FTO}(N \leq n|p_{FTO}, p_{FTC})$ in Figure 3-4 and over-predicts the 50th percentile epistemic estimate of $P_{FTC}(N \leq n|p_{FTO}, p_{FTC})$ in Figure 3-5. While there is no mathematical rational causing the SOARCA Surry results to track closely to either the 50th epistemic percentile or the mean failure curve, these curves do provide a reasonable point of reference between the two studies.

Figure 3-6 shows the sensitivity of the predicted number of SRV cycles before failure to aleatory and epistemic uncertainty. As can be seen, the lower quartile of epistemic uncertainty produces the highest variability in potential SRV cycles until failure. Reducing this epistemic uncertainty with additional failure data would greatly decrease the total uncertainty, while predicting the number of cycles until SRV failure.

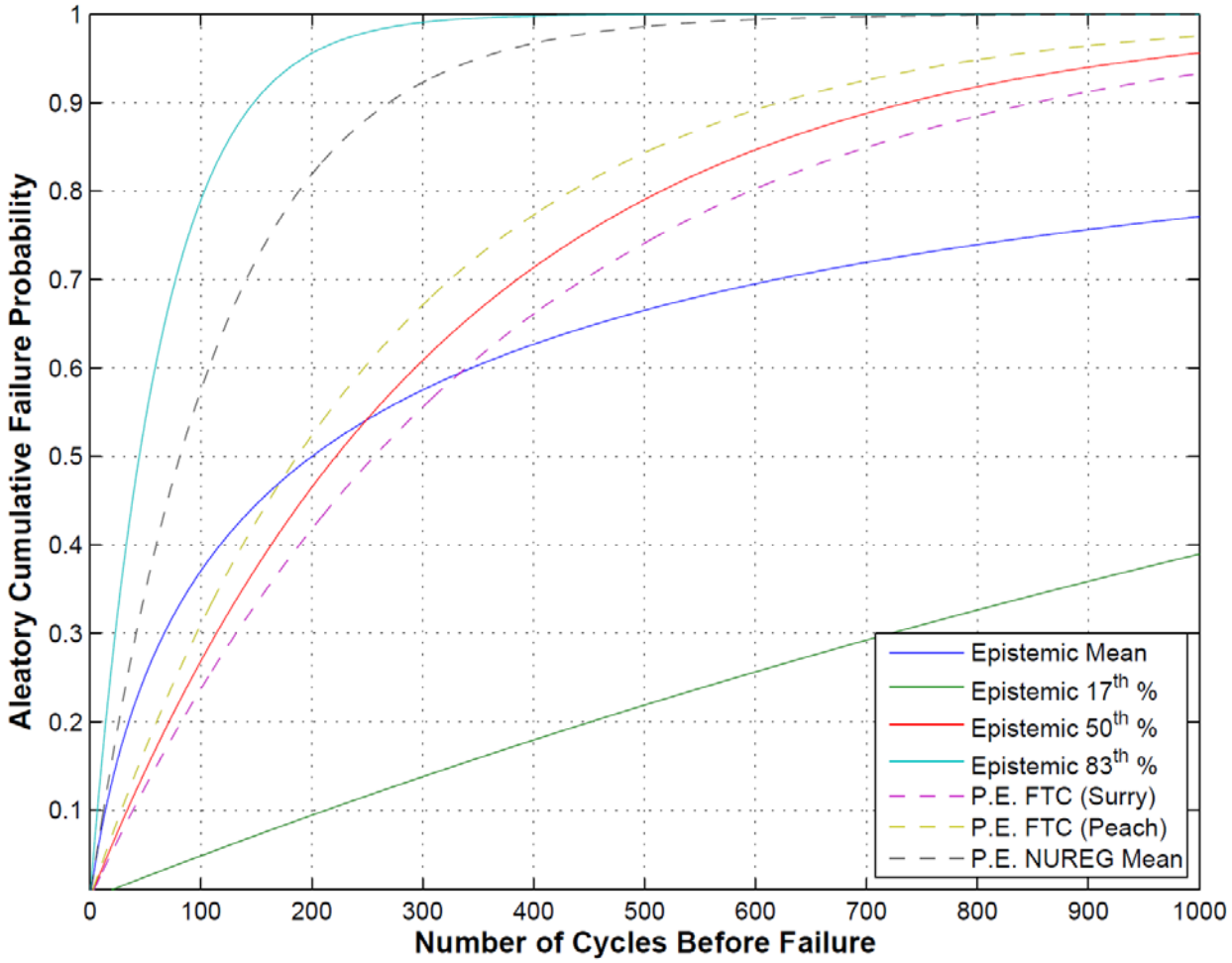

Figure 3-3. Aleatory SRV Failure (FTO+FTC) Probabilities are plotted as a function of SRV cycles (1 Cycle = Open + Close). The mean, 16th, 50th, and 83rd percentiles of the epistemic failure distribution are plotted. For comparison, the Point Estimates (P.E.) for the SOARCA Surry and Peach Bottom FTCs, and the NUREG/CR 6928 aleatory distributions (which were calculated using the mean cycle failure frequency) are also shown.

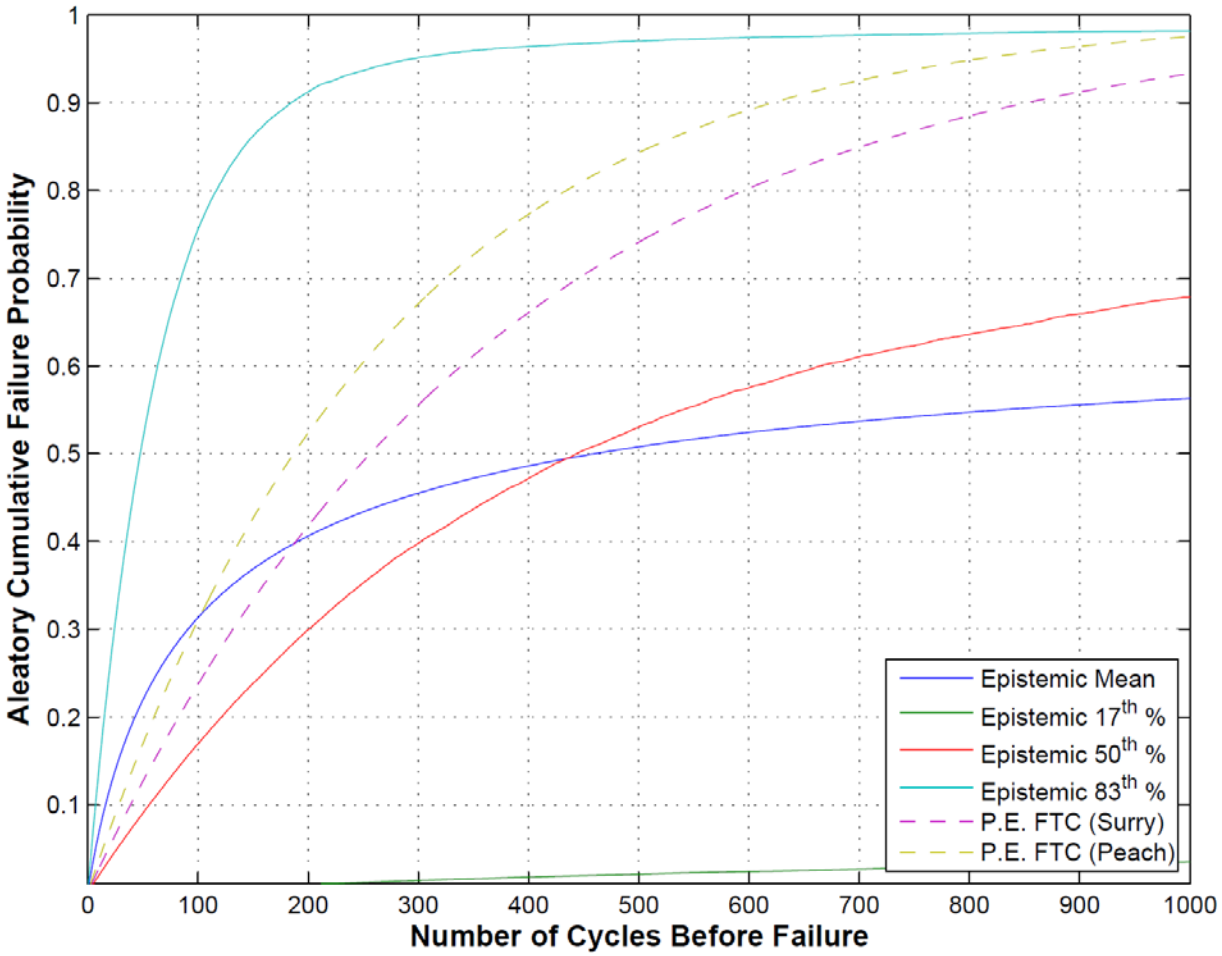

Figure 3-4. Aleatory SRV FTO Probabilities are plotted as a function of SRV cycles (1 Cycle = Open + Close). The mean, 16th, 50th, and 83rd percentiles of the epistemic failure distribution are plotted. For comparison, the Point Estimate (P.E.) SOARCA for the Surry and Peach Bottom FTC and the NUREG/CR 6928 aleatory distributions, which were calculated using the mean cycle failure frequency, are also shown.

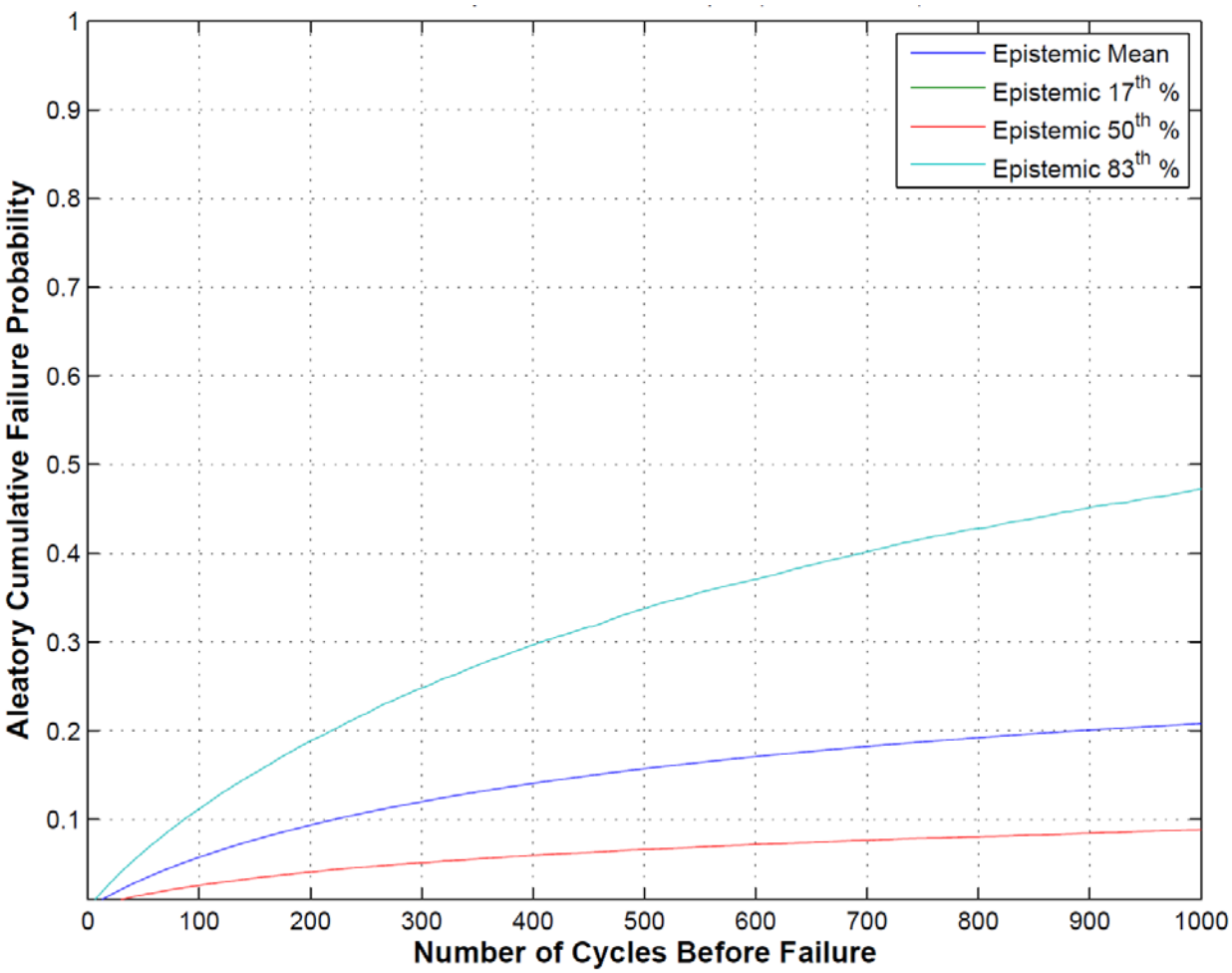

Figure 3-5. Aleatory SRV FTC probabilities are plotted as a function of SRV cycles (1 Cycle = Open + Close). The mean, 16th, 50th, and 83rd percentiles of the epistemic failure distribution are plotted.

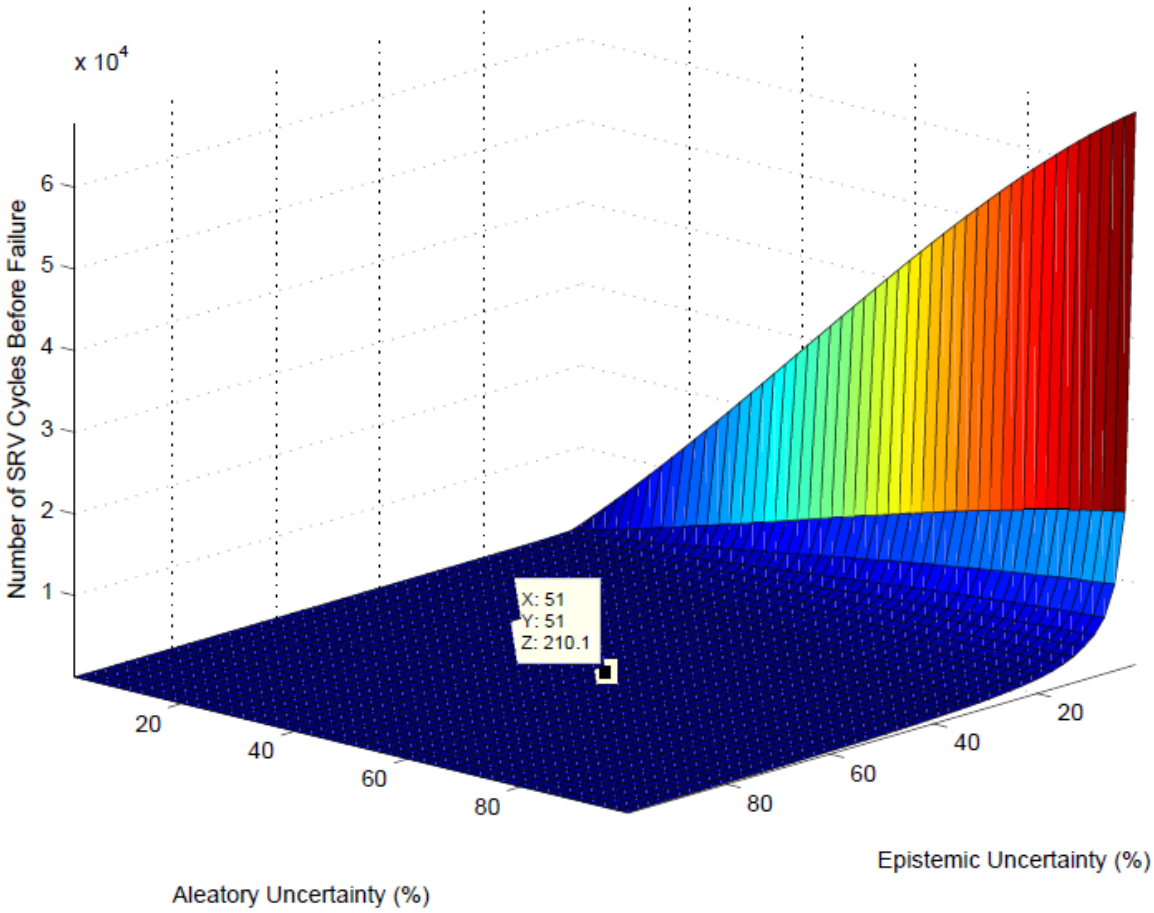

Figure 3-6. Number of SRV cycles before predicted failure, plotted as a function of epistemic and aleatory uncertainty.

3.2.3 Selection of Branch Points

While conducting a DDET analysis, multiple SRV cycle-until-failure numbers need to be calculated *a priori* to the MELCOR simulations. The easiest approach is to divide both the epistemic and aleatory uncertainties into equally weighted segments, then choose the probabilistic number of SRV cycles that represent the statistical mid-point of each segment. For example, if an analyst wants three epistemic branches and three aleatory branches for each epistemic branch, the three sections would occupy the following regions in epistemic probability space: 0 and 0.33, 0.33 and 0.66, and 0.66 and 1.0. The representative epistemic percentiles for each branch would then be 0.17, 0.5, and 0.83, respectively. Next, the aleatory space would be discretized into three regions with three corresponding representative values for each region (i.e., 0.17, 0.5, and 0.83).

Branch points developed using the SRV failure curves in Figure 3-2 can be found in Table 3-2. While the number of epistemic and aleatory regions need not be equivalent (or equal to 3), and because the relative size of each region is left to the analyst's judgment, the basic approach to selecting branch points, as described in this document, is applicable for all dynamic SRV failure applications.

Table 3-2. Equally weighted branch points for estimates of the number of SRV cycles before failure.

	Epistemic Variation			
Aleatory Variation		83rd %	50th %	17th %
	17th %	12	58	366
	50th %	44	213	1200
	83rd %	114	380	1986

3.3 Conclusions

This paper describes a methodology for selecting SRV cyclic loading branch points for DDET analysis. The timing of an SRV failure has been demonstrated to be important to severe accident response actions; SRV status may even affect severe accident management response. Future work will focus on 1) creating joint conditional probability distributions for p_{FTO} and p_{FTC}, given p, and 2) creating a unified method for combining the cyclic loading failure mode with the SRV creep failure mode to support DDET analysis.

3.4 Acknowledgements

The author would also like to extend a special thank you to Dr. Katrina Groth (SNL) for her consultation regarding equation formulation and Doug Osborn (SNL) for providing the base image in Figure 3-1.

3.5 References

[1] M. R. Denman, J. Cardoni, H. Laio, T. Wheeler, K. Groth, "Discrete Dynamic Event Tree Analysis of Small Modular Reactor Severe Accident Management," PSA 2013, **#191**, Columbia S.C., (2013).

[2] H. Liao, T. Wheeler, J. Cardoni, M. R. Denman, "Leveraging Existing Tools for Simulating Operator Performance in Discrete Dynamic Event Trees," PSA 2013, **#120**, Columbia S.C., (2013).

[3] U.S. NRC, "State-of-the-Art Reactor Consequence Analysis (SOARCA) Report," **NUREG/CR-7110**, U.S**.** Nuclear Regulatory Commission: Washington D.C. (2012).

[4] U.S. NRC, "State-of-the-Art Reactor Consequence Analyses Project, Uncertainty Analysis of the Unmitigated Long-Term Station Blackout of the Peach Bottom Atomic Power Station," **NUREG/CR-7155, DRAFT REPORT (SAND2012-10702P)**, (2012).

[5] S. Eide, T. Wierman, et al., "Industry-Average Performance for Components and Initiating Events at U.S. Nuclear Power Plants," **INL/EXT-01-01623**, Idaho National Laboratory, (2007).

[6] D. Kunsman, et al., "Development and Application of the Dynamic System Doctor to Nuclear Reactor Probabilistic Risk Assessments," **SAND2008-4746**, Sandia National Laboratories, Albuquerque, NM (2008).

[7] R. de Neufville, S. Scholtes, "Flexibility in Engineering Design," MIT Press, Cambridge Massachusetts, (2011).

[8] MATLAB 2013a, The MathWorks Inc., Natick, MA (2000).

3.A Multi-Valve Extension of Safety Relief Valve Cyclic Failure Analysis

For a single-SRV, it can be shown that the cumulative failure probabilities for a given sample (i) of the FTO and FTC probabilities are given by:

$$P\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) = 1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n \quad \text{Eq. 8}$$

$$P_{FTO}\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) = 1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n * \frac{p_{FTO_i}}{p_{FTO_i} + p_{FTC_i}} \quad \text{Eq. 9a}$$

$$P_{FTC}\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) = 1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n * \frac{p_{FTC_i}}{p_{FTO_i} + p_{FTC_i}} \quad \text{Eq. 10b}$$

Most nuclear reactor systems have multiple SRVs with staged set points to ensure that FTO of one valve does not prevent pressure relief from occurring. The subsequent valve would then continue to cycle until it fails or until pressure drops and remains below the setpoint. Any valve FTC could cause the reactor to depressurize sufficiently to stop further SRV cycling.. It should be noted that all SRVs are assumed to be redundant and independent but not diverse, thus the per-cycle failure probabilities are perfectly correlated for all SRVs in a sample. Mathematically, this process can be explained by Eq. 11, where j denotes the number of redundant valves cycling and i denotes a sampled valve.

$$P^j\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) = P_{FTC}^{j-1}\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right)\left[1 - \left(1 - \left(p_{FTO_i} + p_{FTC_i}\right)\right)^n\right] \quad \text{Eq. 11}$$

$$P_{FTO}^j\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) = P^j\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) * \frac{p_{FTO_i}}{p_{FTO_i} + p_{FTC_i}} \quad \text{Eq. 12a}$$

$$P_{FTC}^j\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) = P^j\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) * \frac{p_{FTC_i}}{p_{FTO_i} + p_{FTC_i}} \quad \text{Eq. 13b}$$

The expected value, or mean, of the $P_{FTC}\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right)$ curves can be calculated using Eq. 14. All distribution sampling, mean, and percentile calculations were conducted using intrinsic functions in MATLAB.

$$E\left[P^j(N \le n)\right] = \frac{1}{m} * \sum_{i=1}^{m} P^j(N \le n | p_i) \quad \text{Eq. 14}$$

$$E\left[P^j_{FTC}(N \le n)\right] = \frac{1}{m} * \sum_{i=1}^{m} P^j_{FTC}\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) \quad \text{Eq. 15a}$$

$$E\left[P^j(N \le n)\right] = \frac{1}{m} * \sum_{i=1}^{m} P^j_{FTO}\left(N \le n \middle| p_{FTO_i}, p_{FTC_i}\right) \quad \text{Eq. 15b}$$

It should be noted for a small number of SRV cycles, any SRV can exist in one of three states: functional, failed closed, or failed open. Figure 3-7 shows the state diagram for the transition matrix of a three valve system. States 4 and 5 are terminal end states, State 5 can only be reached when all three valves fail in the closed position (FTO) and State 4 can be reached from any valve state. It is assumed that valves cannot be recovered after a failure event occurs. The probability of existing in states 1 through 5 sums to unity (Eq. 16) and as the number of valve cycles approach infinity, the probability of states 1 through 3 approach zero and the probability of existing in states 4 and 5 sums to unity (Eq. 17). Figure 3-8 expresses the state transition diagram in Figure 3-7 as an SD model for incorporation into a DS PRA analysis as shown in Chapter 2.

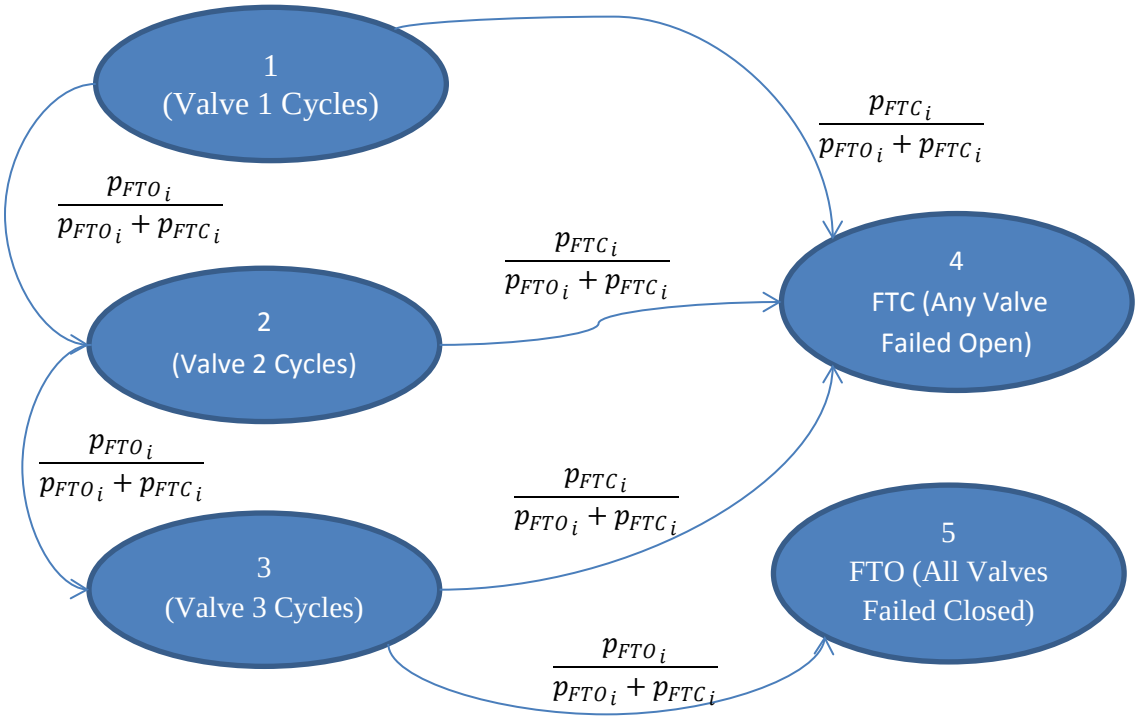

Figure 3-7. Three valve state transition diagram. Annotations near the transition lines show the split fraction of the probability mass vector for a given cycle, not the probability mass as a function of n.

$$\sum_{j=1}^{5} P^j(N \le n) = 1 \quad \text{Eq. 16}$$

$$\lim_{n\to\infty}\sum_{j=1}^{3} P^j(N \le n) = 0,$$

$$\lim_{n\to\infty}\sum_{j=4}^{5} P^j(N \le n) = 1$$

Eq. 17

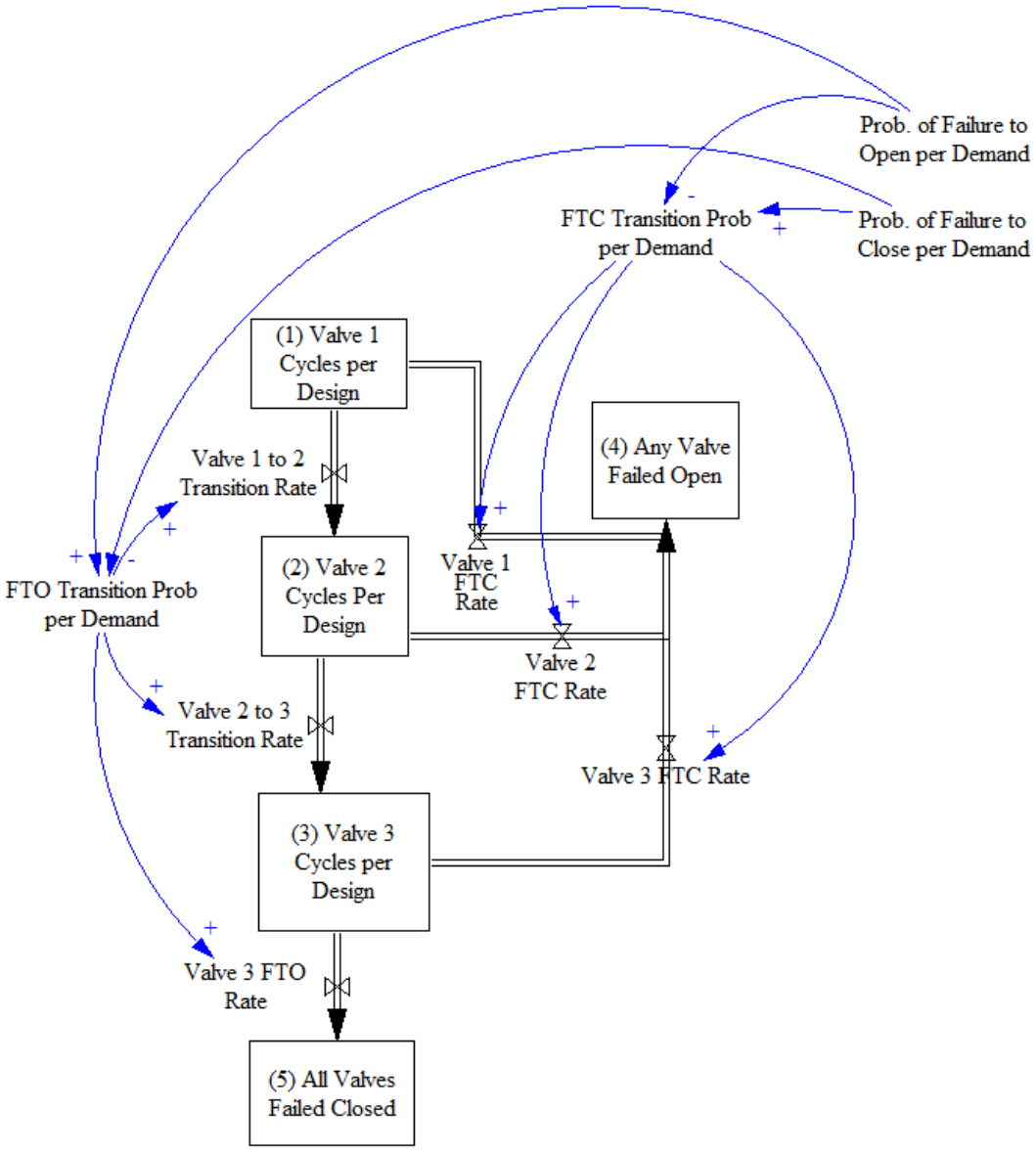

Figure 3-8. Three valve system dynamics diagram.

Figures 3-9 through 3-11 show summarize the sampling described in this Section 3.A for the three valve system shown in Figure 3-8. Figure 3-9 shows the mean valve states as a function of valve cycles. Figure 3-10 shows the horsetails of the independent identically distributed (iid)

samples from the epistemic FTO and FTC distributions. Figures 3-11 and 3-12 show the mean, 5th, 50th, 95th percentiles for the FTC (4) and FTO (5) end states respectively.

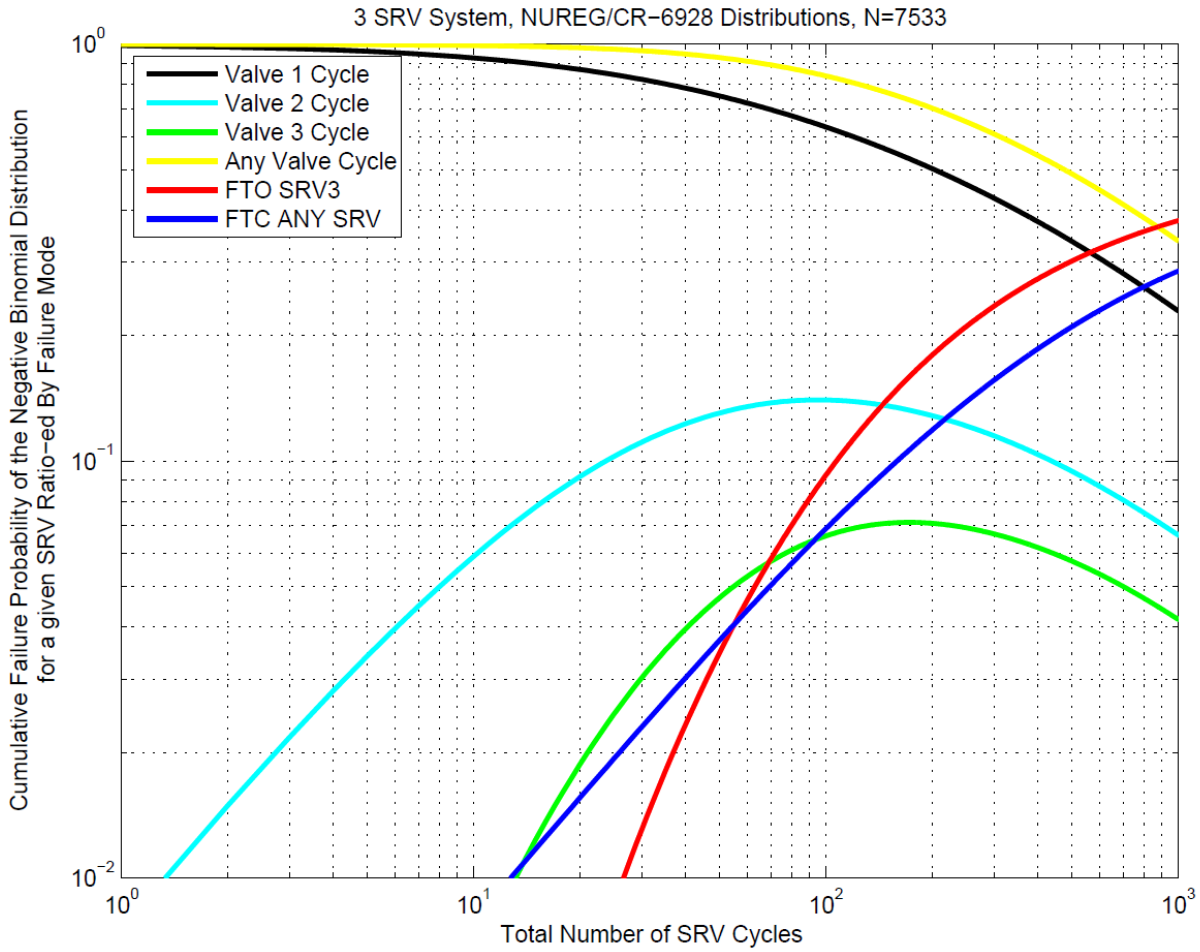

Figure 3-9. Important mean probability states for a 3 valve system. The black light blue and green curves represent the probability of existing in states 1, 2 and 3, respectively. The yellow curve represents the probability of existing in any SRV cycling state as a function of SRV cycles. The red curve represents probability of a valve existing in State 5 as a function of SRV cycles. The blue curve probability of a valve existing State 4 (i.e., State 1 to 4 transition + State 2 to 4 transition + State 3 to 4 transition).

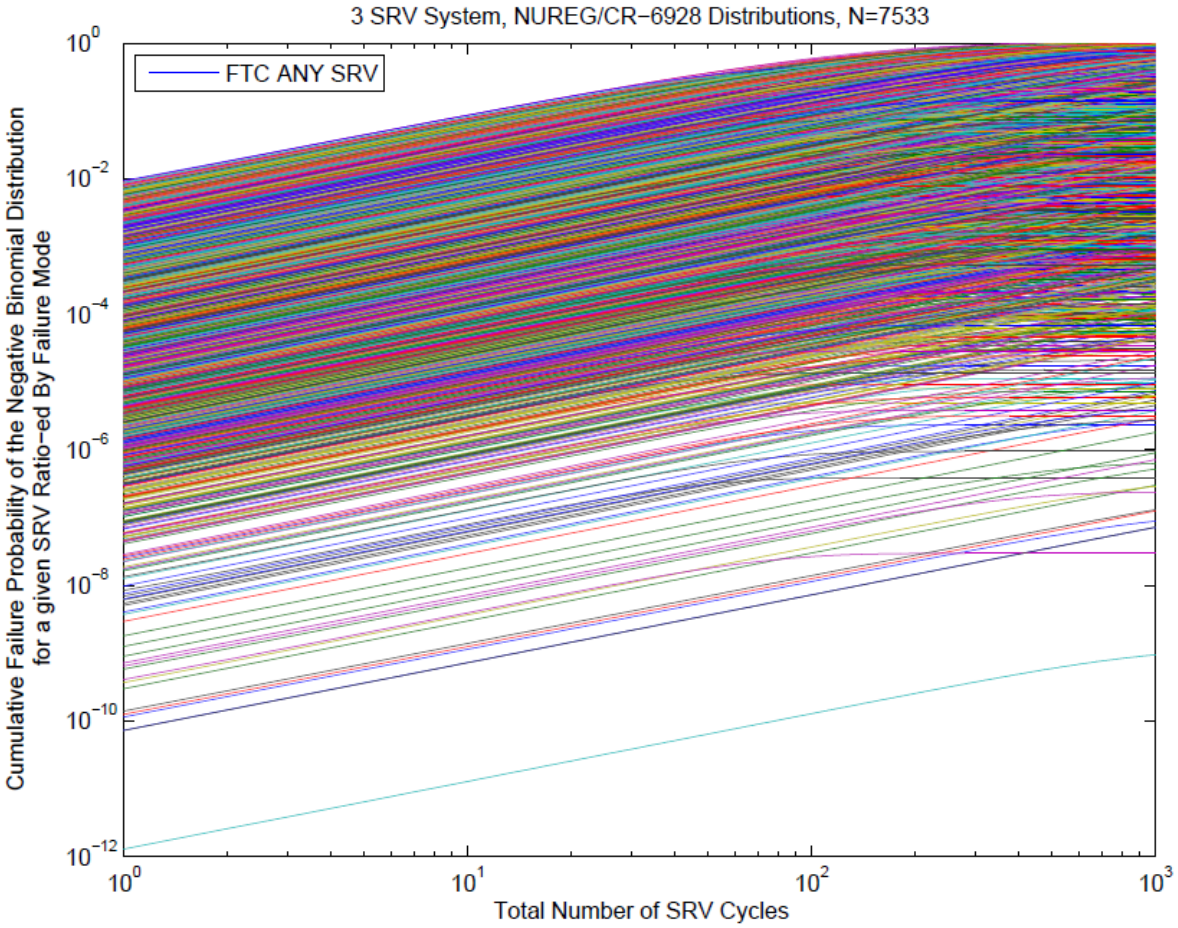

Figure 3.10 - Horse-tail plot of iid samples of the FTO and FTC probabilities from NUREG/CR-6928 for any valve FTC (stuck open, State 4). Note that while 7533 samples are plotted, the range of FTC curves covers nearly 10 orders of magnitude, illustrating the large degree of uncertainty in the FTC and FTO estimates.

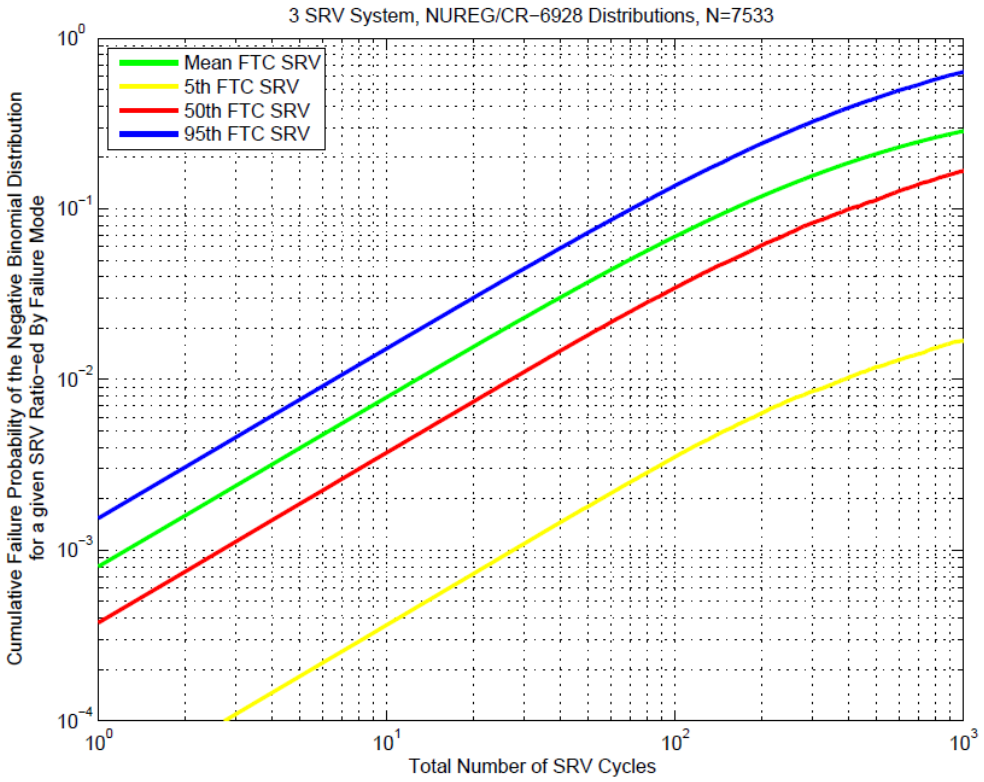

Figure 3-11. Illustration of the uncertainty around the mean FTC estimate (i.e., probability of existing in State 4)

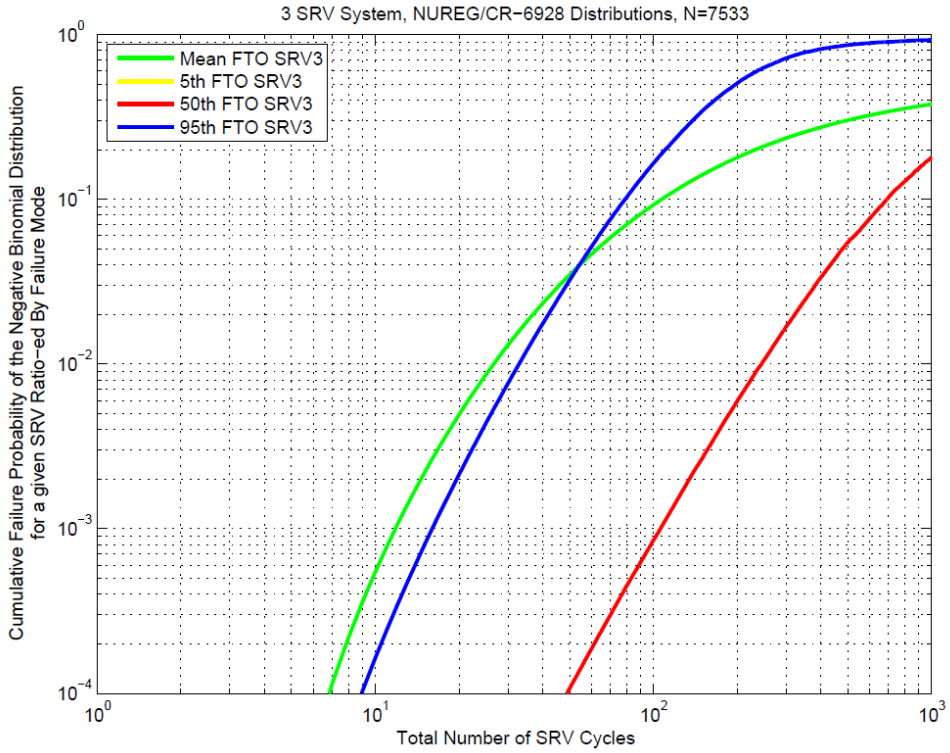

Figure 3-12. Illustration of the uncertainty around the mean FTO estimate (i.e., probability of existing in State 5)

4. SRV CYCLING IMPLIATIONS FOR A MELCOR IPWR MODEL WITH CVCS OPERATOR INTERACTION

Section 4 overviews how the LDRD-funded SRV stochastic failure model outlined in Section 3 was successfully modified to enhance the Discrete Dynamic Event Tree (DDET) analysis of a generic iPWR MELCOR model [1]. These results presented here are pulled from SAND2013-8324 which recognized the importance of, and subsequently incorporated, the independently developed SRV failure model described in Section 3.

4.1 Impact of SRV failure on unmitigated accident progression

A generic iPWR MELCOR model was developed for DS PRA study. This iPWR model features an Emergency Core Cooling System (ECCS) composed of Depressurization Valves (DVs) and Feed Valves (FVs) to allow natural circulation to transfer heat between the reactor and the ultimate heat sink. The results of the iPWR DDET study indicate that failure of FVs in the closed position provides a challenge to the system's accident response, while also reducing the combinatory effect of the DDET analysis by limiting the number of additional branches to analyze due to SRV failure. Thus, accidents relating to FV failure-to-open were selected for the initial study accident study, followed by accidents relating to DV failure-to-open. A summary of core damage states for various branches can be seen in Table 4-1.

Table 4-1. Summary of findings from DDET Study [1].

DVs fail to open on signal (FVs functional)		
# of available SRV cycles	SRV fails closed	SRV fails open
12	**Core damage with high decay power only**	**Core damage**
58	No core damage	**Core damage**
114	No core damage	No core damage
FVs fail to open on signal (DVs functional)		
# of available SRV cycles	SRV fails closed	SRV fails open
12	**Core damage**	**Core damage**
58	**Core damage**	**Core damage**
114	**Core damage**	**Core damage**
DVs and FVs fail to open (total ECCS failure)		
# of available SRV cycles	SRV fails closed	SRV fails open
12	**Core damage**	**Core damage**
58	No core damage	**Core damage**
114	No core damage	No core damage

The dynamic effects of SRV failure timing and state on two-phase water level can be seen in Figure 4-1, reactor vessel pressure in Figure 4-2, and containment pressure in Figure 4-3. Note the non-linear dynamics related to the functional SRV cycling time and the subsequent time until vessel. This behavior is due to increased heat transfer through the containment and lower decay heat generated later in the accident. Eventually, these dynamic cooling and heating effects will allow the graceful failure of SRVs, first in the closed and then in the open position. These trends will impact the time available to operators before they are forced to take extraordinary measures that will impact the performance shaping factors which can influence the likelihood of human error.

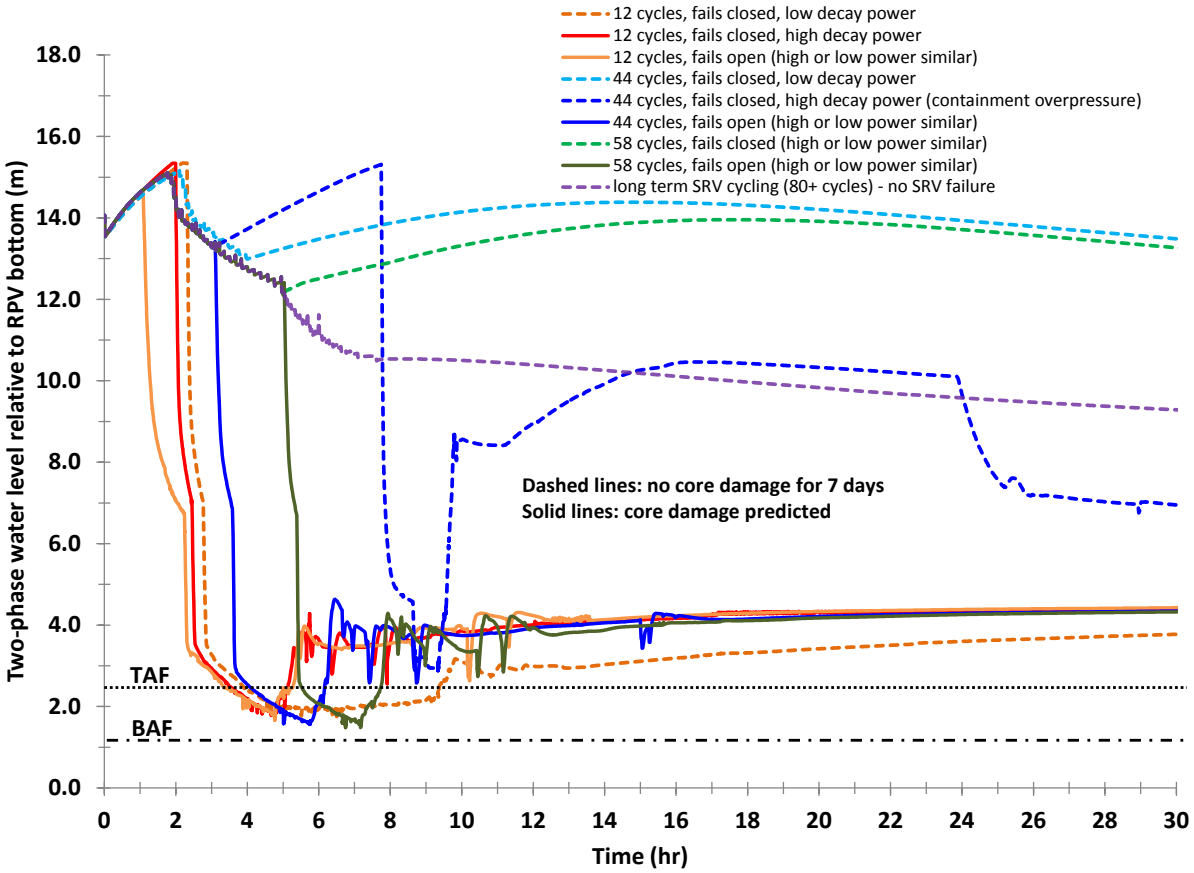

Figure 4-1. RPV water level for DV-failure scenarios for various SRV operation.

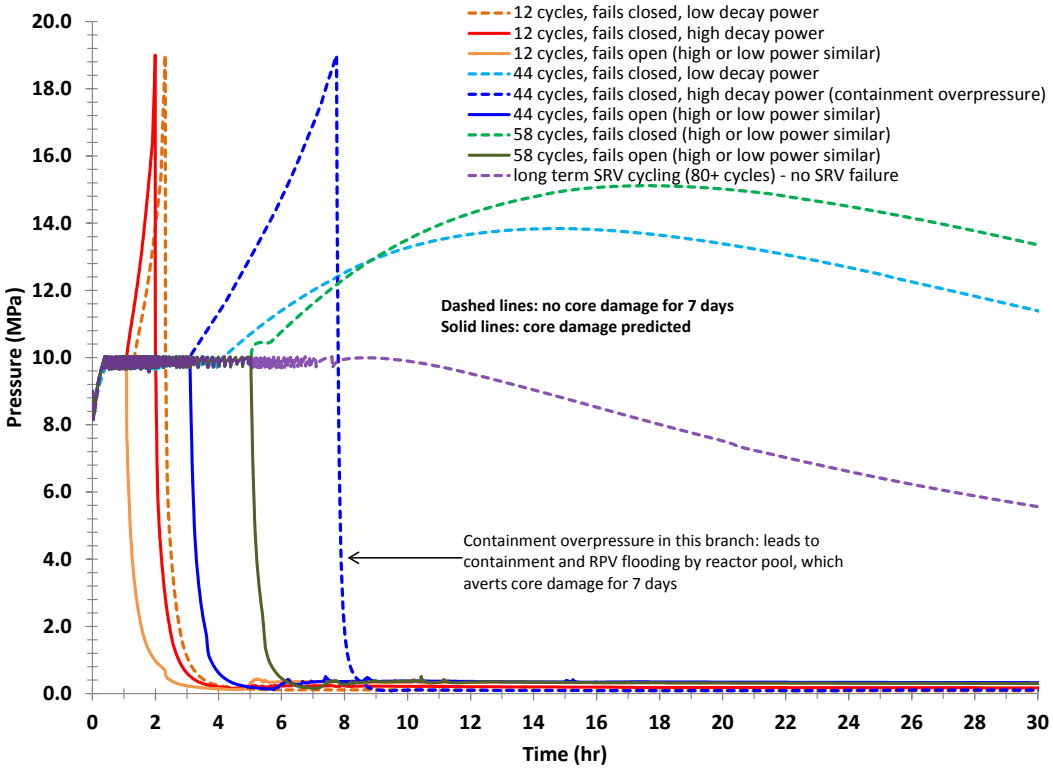

Figure 4-2. RPV pressure for DV-failure scenarios for various SRV operation.

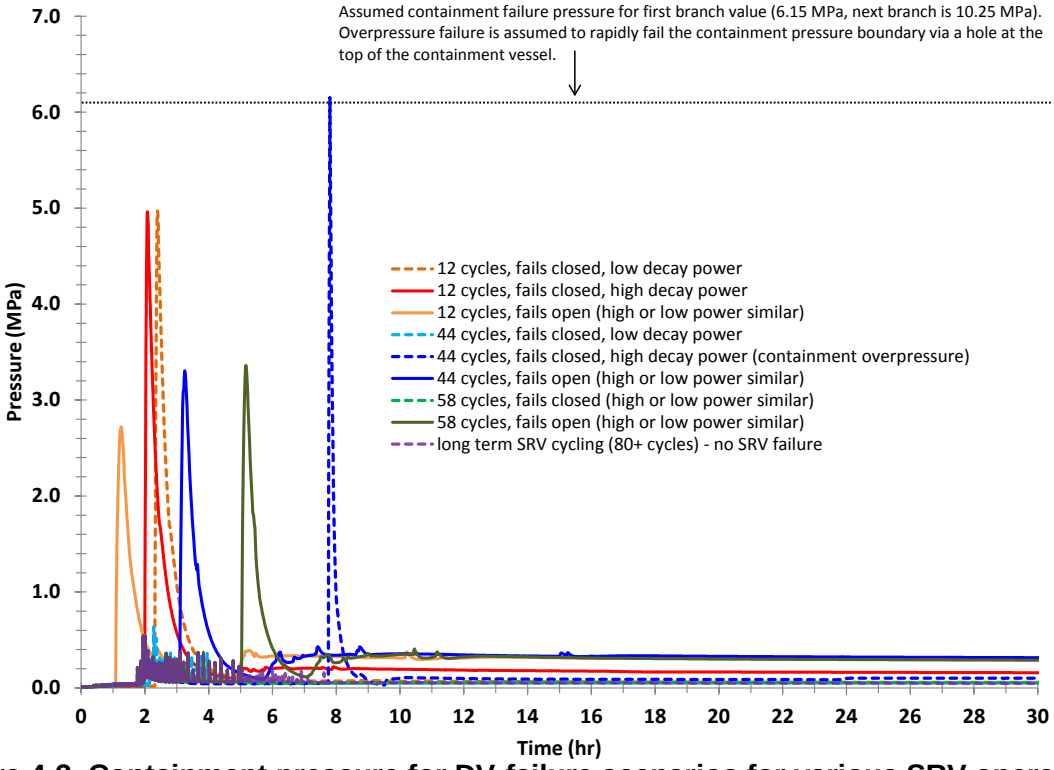

Figure 4-3. Containment pressure for DV-failure scenarios for various SRV operation.

4.2 Effects of Operator Action on Accident Progression

The DDET analysis further examined the impact of an operator aligning the Chemical Volume and Control System (CVCS) to introduce more cooling water into the iPWR while potentially opening a containment bypass pathway.

Depending upon the ECCS operation, decay power, and SRV operation, the operator failure branches with no CVCS injection and an uncontrolled letdown leak can lead to core damage, RPV damage (overpressure and lower head melt-through), and significant radionuclide releases to the environment, even for ECCS-failure branches that normally avert these end states with no operator action (e.g. branches with extended SRV cycling). To highlight these comparisons for the DV-failure scenario, Table 4-2 shows how decay power and SRV operation drive various bifurcations in plant end states for scenarios with no operator action.

Table 4-2. Accident bifurcations for DV-failure case study with no operator action; end states after 7 day simulation.

DV-failure scenario: bottom FVs available, no operator action						
Decay power	Number of SRV cycles	SRV failure position	Core damage?	RPV damage?	Containment failure?	Enviro. Release?
Low	12	Closed	**No**	**Yes: OP**	**No**	**No**
	12	*Open*	**Yes**	**No**	**No**	**No**
	44	Closed	**No**	**No**	**No**	**No**
	44	*Open*	**Yes**	**No**	**No**	**No**
	58	Closed	**No**	**No**	**No**	**No**
	58	*Open*	**Yes**	**No**	**No**	**No**
	Over 80	**NA**	**No**	**No**	**No**	**No**
High	12	Closed	**Yes**	**Yes: OP**	**No**	**No**
	12	*Open*	**Yes**	**No**	**No**	**No**
	44	Closed	**No**	**Yes: OP**	**Yes: OP**	**No**
	44	*Open*	**Yes**	**No**	**No**	**No**
	58	Closed	**No**	**No**	**No**	**No**
	58	*Open*	**Yes**	**No**	**No**	**No**
	Over 80	**NA**	**No**	**No**	**No**	**No**

OP = overpressure failure

Table 4-3 shows the impact that operator failure actions (CVCS leak and no charging) have on the accident end states. RPV lower head failure (melt-through) occurs for DV-failure scenarios with operator failure action at 1 hour, which is before any SRV branches are predicted to occur. Compared to Table 4-2 with no operator actions, Table 4-3 depicts how the CVCS leak can lead to core damage and environmental releases for several branches that normally avert one or both of these undesirable end states. It also worth noting that the 44 SRV cycle branch (failing closed) with high decay power still averts core damage and environmental releases due to the containment overpressure failure, even with the CVCS leak occurring at 5 hours. Successful

operator action always prevents core damage if the action branch occurs before significant core uncovering can initiate damage.

Table 4-3. Accident bifurcations for DV-failure case study with operator failure branches; end states after 7 day simulation.

DV-failure scenario: bottom FVs available, operator failure branch at 1 hour						
Decay power	Number of SRV cycles	SRV failure position	Core damage?	RPV damage?	Containment failure?	Enviro. Release?
Low	**NA**	**NA**	**Yes**	**Yes: MT**	**No**	**Yes**
High	**NA**	**NA**	**Yes**	**Yes: MT**	**No**	**Yes**
DV-failure scenario: bottom FVs available, operator failure branch at 5 hours or on low RPV water level						
Decay power	Number of SRV cycles	SRV failure position	Core damage?	RPV damage?	Containment failure?	Enviro. Release?
Low	12	Closed	**Yes**	**Yes: OP**	**No**	**Yes**
	12	*Open*	**Yes**	**No**	**No**	**Yes**
	44	Closed	**Yes**[2]	**No**[2]	**No**[2]	**Yes**[2]
	44	*Open*	**Yes**	**No**	**No**	**Yes**
	Over 44[1]	**NA**	**Yes**	**No**	**No**	**Yes**
High	12	Closed	**Yes**	**Yes: OP**	**No**	**Yes**
	12	*Open*	**Yes**	**No**	**No**	**Yes**
	44	Closed	**No**[2]	**Yes: OP**[2]	**Yes: OP**[2]	**No**[2]
	44	*Open*	**Yes**	**No**	**No**	**Yes**
	Over 44[1]	**NA**	**Yes**	**No**	**No**	**Yes**

OP = overpressure failure, MT = melt-through failure

[1] The first 58-cycle branch occurs at 6.4 hours for low decay power and 5.03 hours for high decay power; thus the RPV depressurization via the CVCS letdown leak at 5.0 hours for operator failure branches occurs first and prevents SRV branches beyond 44 cycles.

[2] With high decay power and 44 SRV cycles (failing closed), the unanticipated containment overpressure failure (flooding the RPV and containment with reactor pool water) prevents core damage and environmental releases even with an uncontrolled CVCS letdown leak. Conversely, the low decay power branch does not over-pressurize the containment, and therefore no pool water floods into the RPV/core to prevent damage and environmental releases.

Table 4-4 shows that the FV-failure scenario exhibits much simpler divisions in plant end states for various combinations of branching parameters. The operation of the DVs precludes most of the SRV branches from occurring. The operator failure branches simply affect the FV-failure scenarios by opening a containment bypass flow path, permitting environmental releases for branches that normally have zero releases for the 7 day simulation time. Again, successful operator action before core damage always results in end states with no core damage.

Table 4-4. Accident bifurcations for FV-failure case study; end states after 7 day simulation.

FV-failure scenario: top DVs available, no operator action						
Decay power	Number of SRV cycles	SRV failure position	Core damage?	RPV damage?	Containment failure?	Enviro. Release?
Low	12	Closed	**Yes**	**No**	**No**	**No**
	12	*Open*	**Yes**	**No**	**No**	**No**
	Over 35[1]	**NA**	**Yes**	**No**	**No**	**No**
High	12	Closed	**Yes**	**No**	**No**	**No**
	12	*Open*	**Yes**	**No**	**No**	**No**
	Over 35[1]	**NA**	**Yes**	**No**	**No**	**No**
FV-failure scenario: top DVs available, any operator failure branch						
Decay power	Number of SRV cycles	SRV failure position	Core damage?	RPV damage?	Containment failure?	Enviro. Release?
Low	12	Closed	**Yes**	**No**	**No**	**Yes**
	12	*Open*	**Yes**	**No**	**No**	**Yes**
	Over 35[1]	**NA**	**Yes**	**No**	**No**	**Yes**
High	12	Closed	**Yes**	**No**	**No**	**Yes**
	12	*Open*	**Yes**	**No**	**No**	**Yes**
	Over 35[1]	**NA**	**Yes**	**No**	**No**	**Yes**

[1]DV operation around 1-2 hours due to high RPV pressure, high containment pressure, or low RPV water level (i.e. for operator failure branches at 1 hour) precludes SRV cycling beyond about 35 cycles. Therefore, the SRV branches for 44 cycles and above are never simulated in the FV-failure scenario.

4.3 Conclusions

The iPWR DDET study again illustrates how a dynamic uncertainty model can impact the evolving risk of a nuclear facility during an accident progression. Here, SRV cycling time provides more opportunity for heat transfer and longer decision times for failure to open events. While detailed study of these results will be need to conduct probabilistic risk management to determine when operator action is appropriate, dynamic changes to the SRV failure likelihood will suggest that different actions may be taken for the same set of failures due to timing variations.

4.4 References

[1] Katrina M. Groth, Matthew R. Denman, Jeffrey N. Cardoni, Timothy A. Wheeler, “Proof of Principle Framework for Developing Dynamic Risk-Informed Severe Accident Management Guidelines”, SAND-2013-8324, Sandia National Laboratories, Albuquerque NM, Sept. 2013.

5. CONCLUSIONS

DS PRA provides powerful tools for evaluating evolving risks to nuclear power plants and may be especially powerful in evaluating the risk of nuclear facilities during accident management. Existing research at SNL on probabilistic accident management both have benefited from the techniques developed in this LDRD to dynamical quantify changing probabilities in both the long (e.g., plant life extensions) and short (e.g., accident mitigation) time frames.

Chapter 1 outlined the initially proposed DS approach to PRA. Chapter 2 explored that approach in greater detail and conducted an initial scoping evaluation of how aging risk may present themselves during risk management problems while hiding themselves in the results of overall risk assessments. Chapter 3 explored a new DS PRA derived stochastic SRV failure model. This model's potential has been recognized as important modeling improvement for current and future DOE and NRC studies. Chapter 4 presented initial iPWR DDET results using the DS PRA SRV fault tree to inform operator action decision-making.

The work of this LDRD will be extended into two program areas in DOE's NE7. These area are the advanced Small Modular Reactor (aSMR) program and DOE's Light Water Reactor Sustainability (LWRS) program. Through SNL's future programs with the aSMR program, DS PRA models of sodium reactor SSCs will be created explore uncertainties in the accident response of small sodium reactors to beyond design basis conditions. Under a slightly longer time horizon, potential new projects in the LWRS program may desire accident guidance to be tailored to both the long term degraded conditions of the plant as well as the rapidly evolving degradation of components and instruments during off-normal conditions. As demonstrated in this report, DS PRA is an excellent tool for provide these types of risk insights.

6. DISTRIBUTION

1	MS0359	D. Chavez, LDRD Office	1911
1	MS1027	Arlo Ames	6612
1	MS0748	Matthew Denman	6231
1	MS0748	Mitch McCrory	6231
1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories