U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-6985

A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

DISCLAIMER: This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-6985

A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems

Prepared by:

T. Aldemir[1], S. Guarro[2], J. Kirschenbaum[3], D. Mandelli[1], L.A. Mangan[1],
P. Bucci[3], M. Yau[2], B. Johnson[4], C. Elks[4], E. Ekici[5], M.P. Stovsky[1] ,
D.W. Miller[1], X. Sun[1], S.A. Arndt[6] , Q. Nguyen[6] , J, Dion[7]

[1]The Ohio State University, Nuclear Engineering Program,
Columbus, OH 43210

[2]ASCA, Inc., 1720 S. Catalina Avenue, Suite 220,
Redondo Beach, CA 90277-5501

[3]The Ohio State University, Department of Computer Science and
Engineering, Columbus, OH 43210

[4]University of Virginia, Department of Electrical and Computer Engineering,
Charlottesville, VA 22904

[5]The Ohio State University, Department of Electrical and Computer
Engineering, Columbus, OH 43210

[6]U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001

[7] Sandia National Laboratories, Department of Risk and Reliability
Analysis, Albuquerque, NM 87185

Manuscript Completed: September 2008
Date Published: February 2009

S.A. Arndt and Q. Nguyen, NRC Project Managers

NRC Job Code K6472

Office of Nuclear Regulatory Research

ABSTRACT

Two dynamic methodologies, dynamic flowgraph methodology (DFM) and the Markov/Cell-to-cell mapping technique (CCMT), are implemented on the benchmark Digital Feedwater Control System (DFWCS) specified in NUREG-6942, “Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments,” to demonstrate how an existing nuclear power plant probabilistic risk assessment (PRA) can incorporate a digital upgrade of the instrumentation and control system. The results obtained from the DFM and Markov/CCMT models of the DFWCS failure modes are compared, and the impact of scenarios directly related to the hypothetical digital upgrade on the core damage frequency (CDF) is assessed on a demonstrative basis, using a plant PRA from NUREG-1150, “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants.” The study shows that a DFWCS similar to that of an operating plant can be modeled using dynamic methodologies and that the results can be incorporated into an existing PRA to quantify the impact of a digital upgrade on the plant CDF.

This page is intentionally left blank

FOREWORD

In 1995, the U.S. Nuclear Regulatory Commission (NRC) issued its Probabilistic Risk Assessment (PRA) Policy Statement, which encourages increased use of PRA and associated analyses in all regulatory matters, to the extent supported by the state-of-art in PRA and the data. Toward that end, the NRC's Office of Nuclear Regulatory Research (RES) is sponsoring research to evaluate traditional PRA methods [e.g., event-tree/fault-tree (ET/FT) approaches] and dynamic PRA methods for use in modeling digital instrumentation and control (I&C) systems to quantify their overall risk contribution to the plant.

The PRA technical community has not yet agreed on how to model digital systems reliability in the context of a PRA and the level of detail that digital instrumentation and control systems require in reliability modeling. Nonetheless, it is clear that PRA models must adequately represent the complex system interactions that can contribute to digital system failure modes.

In NUREG/CR-6901, "Current State of Reliability Modeling Methods for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments", dynamic flowgraph methodology (DFM) and Markov/Cell-to-cell-mapping technique (CCMT) models were identified as promising dynamic methods for modeling digital systems. In NUREG/CR-6942, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments" a proof-of-concept was presented for the use of the Markov/CCMT and DFM methods to model a benchmark Digital Feedwater Control System (DFWS), illustrating how these dynamic models can be developed and integrated into an existing PRA model of a pressurized-water reactor. As part of the above series of NUREGs, this report is the conclusion of NRC-sponsored work addressing dynamic PRA modeling efforts in this specific study.

This report summarizes the key concepts of NUREG/CR-6942 and offers a discussion of the assumptions, capabilities, and limitations of the DFM and Markov/CCMT models. Additionally, in applying the proof-of-concept, as an objective of the study, the report also includes preliminary quantitative results that are demonstrative in nature and does not attempt to obtain complete and fully vetted results. Finally, it must be noted that the report, reflecting the authors' experience and reasoning, presents observations that may not represent the positions or technical conclusions of the NRC staff.

This page is intentionally left blank

CONTENTS

Page

Figures

Page

Tables

Page

EXECUTIVE SUMMARY

This Executive Summary is organized in three parts under the following subheadings:

- Background and Related Earlier Work
- Objectives and Results of This Study
- Findings and Observations

Background and Related Earlier Work

Nuclear power plants are in the process of replacing and upgrading aging and obsolete instrumentation and control (I&C) systems. Most of these replacements involve transitions from analog to digital technology. The results of a recent study published in NUREG/CR-6901(Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments) indicate that the traditional static methodologies for probabilistic risk assessment (PRA), such as event-tree (ET)/fault-tree (FT) methodology, may not yield satisfactory results when applied to these upgraded systems. More specifically, the NUREG/CR-6901 study indicated that the traditional PRA modeling paradigm is likely to have significant shortcomings when a digital I&C system:

- interacts with a process that, because of complex functionality, has multiple Top Events (i.e., system-level failure modes), logic loops, and/or substantial time delays between the initiation of the fault and the occurrence of the Top Event (relatively to the time scale of the characteristic system time constants),
- relies on sequential circuits that have memory,
- has tasks that compete for the I&C system resources, and/or,
- anticipates the future states of controlled/monitored processes.

Using subjective criteria based on reported experience and engineering knowledge, the NUREG/CR-6901 study has identified the dynamic flowgraph methodology (DFM) and the Markov methodology coupled with the cell-to-cell-mapping technique (CCMT) as the dynamic PRA methodologies that rank as the top two with the most positive features and least negative or uncertain features when evaluated against the requirements for the reliability modeling of digital I&C systems. NUREG/CR-6901 also concluded that benchmark systems should be defined to allow assessment of the methodologies proposed for the reliability modeling of digital I&C systems using a common set of hardware/software/firmware states and state transition data. It should be emphasized that throughout this study software is not addressed in detail as a separate entity as in operating system software or application software; instead it is treated as embedded in hardware and referred to as firmware. The term “hardware/software/firmware” refers to the software functionality that is embedded in the hardware.

As a follow-up to NUREG/CR-6901, NUREG/CR-6942 (Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments) defined a benchmark system that is similar to the steam generator digital feedwater control system (DFWCS) of an operating pressurized water reactor (PWR). Using the turbine trip of a NUREG-1150 (Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants) plant as an example of an initiating event, NUREG/CR-6942 also showed how:

1. the DFM and Markov/CCMT can be implemented for the reliability modeling of the benchmark system, and,
2. the outputs of the DFM and Markov/CCMT can be incorporated into the existing ET/FT based PRA of a NUREG-1150 (Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants) plant.

The study concluded that both the DFM and Markov/CCMT methodologies can account for all the features of the benchmark system with consistent results and that the results can be integrated into an existing PRA.

Some possible challenges were also identified with the methodologies including:

Challenge 1 - Analyst skill levels needed for the implementation of the methodologies,

Challenge 2 - Computational demand for the correct description of the coupling between failure events,

Challenge 3 - Acceptability of the data used for quantification by a significant portion of the technical community, and

Challenge 4 - Routine integration and processing of the results of these methodologies within the structure of existing PRAs.

These challenges originate primarily from the complexity and diverse nature of the phenomena to be accounted for (e.g. statistical dependence of failure events through Type I and Type II interactions[1]) and are not specific to DFM or the Markov/CCMT methodology. Other concerns that were raised in the review process of NUREG/CR-6942 were:

Concern 1 - Scalability of the methodologies to larger systems (in view of the simplifying assumptions implicit in the example initiating event)

Concern 2 - Estimation of the risk importance of the digital I&C system failures (in view of the fact that there was no quantification of the contribution of the benchmark system failure to core damage frequency)

Concern 3 - Impact of the hardware/software/firmware and process interactions on the risk significant events under consideration (in view of the fact that no comparison of dynamic versus traditional PRA approach results were available for the system and scenario considered).

Objectives and Results of This Study

[1] Type I interactions are those between the digital I&C system and the controlled/monitored plant physical processes (e.g., heatup, pressurization). Type II interactions are those among the components of the digital I&C system itself (e.g., communication between different components, multi-tasking, multiplexing).

With respect to the challenges and concerns identified in the course of the earlier stages of the project and during the NUREG/CR-6942 review process indicated in the previous section, this report addresses Challenges 1 (Analyst skill levels needed) , 2 (Computational demand) and, to a degree, 4 (Routine integration and processing of results). It also addresses Concern 1 (Scalability of the methodologies) and, partially, Concern 2 (Estimation of digital I&C systems risk importance). The data acceptability issue (Challenge 3) is the subject of broad conceptual and philosophical discussions in the PRA and related technical communities and, given its still open-ended status, remains beyond the direct scope of the work documented here. However, the report does show how failure data that can be utilized within the application of the dynamic PRA methodologies investigated can be generated for the benchmark digital I&C system DFWCS, which is a system quite representative of digital I&C systems actually used for nuclear power plant control and reactor protection functions. It also discusses a possible path for solution of this particular issue, also in light of recent developments in the field that have recently been produced and documented. The question at the core of Concern 3 (Impact of hardware/software/firmware interactions on risk-significant events) has been addressed in previous work by several researchers in the field. However, no conclusive results regarding Concern 3 have been reached at the time of this publication.

Regarding Challenge 1, the report uses the benchmark DFWCS originally defined in NUREG/CR-6942 to show how models (e.g. control logic models or process simulators) developed by different groups of specialists can be utilized within a system-level dynamic PRA framework. After different system function models have been produced, the PRA analyst only needs to be familiar with the linking process rather than with the detailed structure of a given dynamic methodology.

Regarding Challenge 2 and Concern 1, the study illustrates that a digital reactor control system similar to that of an operating plant can be modeled using dynamic methodologies and the results can be incorporated into an existing PRA to quantify the impact of the digital update of a control system on the plant core damage frequency. It should be emphasized that dynamic PRA methodologies have never been intended to be implemented for a whole nuclear power plant (NPP), but rather only for those systems that, because of their dynamic and complex characteristics, require such more sophisticated capabilities in the PRA model development effort. The integration process has been qualitatively demonstrated in NUREG/CR-6942 and is further expanded and quantitatively demonstrated in this report. In that respect, the report satisfactorily addresses both Challenge 2 and Concern 1.

Challenge 4 is addressed by leveraging the results of closely related studies that have been recently concluded and documented. This permits the identification of the key underlying issues as well as the identification and discussion of promising and technically feasible solutions for these issues.

Regarding Concern 2, this study provides a demonstration-level estimate of the impact that the digital upgrade of a main feedwater control system may have on accident scenarios originally included in the analysis of one of the NUREG-1150 plants. The demonstrative estimate scenario involves as the initiating event a turbine (and reactor) trip caused by high or low steam generator level. It is emphasized, however, that the quantitative aspects of the study results can at this time only be taken as partial indications, since the study objectives were demonstrative in nature and did not include obtaining complete and fully vetted quantitative results. To pursue more definitive quantitative indications, analyses more specifically focused on identifying capabilities and limitations of the current state of the art with respect to the quantification process and underlying data-collection processes would have to be planned and executed.

NUREG/CR-6942 had already qualitatively demonstrated the need to account for the timing of failures in the PRA modeling of digital I&C systems for a simplified scenario of the example DFWCS behavior. The present study uses the full DFWCS PRA model and addresses the dynamic conditions associated with a plant transient produced by a power maneuver (see Fig. 1.3.6) consisting of:

- 8 hour ramp up, starting from 70% of full power,
- 8 hour steady-state operation at 78% of full power, and,
- 8 hour power ramp-down, back to 70% of full power.

The maneuver constitutes good application ground because it exerts and challenges the main function of the DFWCS, i.e. maintaining the SG water level between set limits under changing power demand. The 24 hour period was chosen because it is the default reference-time period for standard PRA tools when modeling continuously operating systems. For assessing Top Event probabilities for different time periods, the DFWCS Top Event probabilities generated for this power maneuver should be regarded as a rate (i.e., per day).

The project has developed and completed data-gathering, modeling, and analytical activities, as summarized below:

1. Refinement of benchmark Digital Feedwater Control System (DFWCS) definition.
2. Determination of qualitative and quantitative basic component failure modes and probabilities via FMEA (Failure Modes and Effects Analysis), and fault-injection techniques.
3. Further development and refinement of the DFM and Markov/CCMT models of the DFWCS originally documented in NUREG/CR-6942.
4. DFM analyses and demonstrative risk quantification of selected DFWCS risk scenarios, carried out in both deductive mode (from defined Top Events to their root causes) and inductive mode (from hypothetical faults to Top Events of potential interest).
5. Markov/CCMT analyses and demonstrative risk quantification of selected DFWCS risk scenarios, carried out in inductive mode.
6. Integration, in demonstration mode, of DFM and Markov/CCMT analytical and quantitative results into the framework of the conventional ET/FT PRA of a reference NUREG-1150 plant.

Regarding the challenge of analyst skill levels needed for the implementation of dynamic methodologies, the report uses the benchmark DFWCS originally defined in NUREG/CR-6942 to show how models developed by different groups of specialists can be utilized within a system-level dynamic PRA modeling framework. After the submodels (e.g., DFM and/or Markov/CCMT) have been produced, the PRA analyst only needs to be familiar with the process of linking and integrating results into the PRA, rather than with the detailed inner structure of a given dynamic methodology.

In exploring the level of computational power and accuracy needed to model an important NPP control system with inclusion of its basic dynamic characteristics, the study illustrates how a digital reactor control system similar to that of an operating plant can be modeled using dynamic methodologies (i.e., through DFM and/or Markov/CCMT). Furthermore, this study also illustrates how the results can be incorporated into an existing traditional PRA to quantify the impact of the digital update of a control system on the core damage frequency. This is in line with the fact that dynamic PRA methodologies have not been developed with the intent of replacing traditional PRA techniques at the whole nuclear power plant (NPP) level, but rather to supplement them for those systems that, because of their dynamic and complex characteristics, require such capabilities. Thus the integration of dynamic PRA sub-modules into the conventional framework is an important aspect of the overall PRA analytical process when dynamic modeling is included. A demonstrative example of how such an integration process can be carried out for DFM and/or Markov/CCMT derived qualitative dynamic-PRA results – i.e., prime implicants to be integrated with ET/FT cut-sets – has been presented in NUREG/CR-6942 and is further expanded and quantitatively illustrated in this report.

Regarding the concern related to the risk importance of digital I&C system failures, this study uses the example benchmark system of NUREG/CR-6942 and a 24 hour power maneuver to show that, from a qualitative point of view, new risk-significant event sequences, associated with DFWCS failure modes identified by the dynamic analyses, may arise in a hypothetical conversion from an original analog control system to a digital platform. The quantitative contribution of these sequences to a plant-level risk figure-of-merit (e.g., core damage frequency or probability) was estimated to be modest in the context of this study demonstrative exercise. However, it must be noted that the quantitative aspects of the study results are at this time only preliminary and incomplete indications, since the study objectives were demonstrative in nature and did not include obtaining complete and fully vetted quantitative results. The report results are relative to the update of one control system and some of the related estimations are for scenarios conditioned upon the occurrence of a turbine trip. In these respects, the results are not necessarily representative of the impact of a digital upgrade of the whole reactor and plant protection and control system for all the initiating events under consideration, including possible digital I&C software design errors. Such errors have not been explicitly accounted for in the analyses carried out within this project due to the nature of available failure data. Thus it is premature to draw from this study any conclusions as to whether the overall risk impact from the digital system upgrade of an entire NPP protection and control system may be quantitatively significant in the positive or negative direction.

Findings and Observations

This study has produced useful indications concerning three basic questions that are, in the authors' view, central to the digital I&C PRA modeling and analysis issue:

Question 1: What modeling techniques are well suited to successfully represent and analyze the risk relevant failure modes of modern NPP digital I&C systems?

Question 2: Can quantitative reliability / risk measures be obtained for assessing the impact of the upgrade of a NPP control or protection system, from analog and relay-based to digital and software-based?

Question 3: Can a formally correct and practically implementable[2] approach be defined, to integrate the results of digital I&C dynamic PRA modeling and analysis techniques into a conventional PRA framework?

The current work has produced the following insights with respect to possible answers to Question 1:

A. The deductive analyses carried out with DFM appear to be well suited to span the search space for the prime-implicants of a given Top Event in logically complete[3] fashion.

B. The application of the DFM and Markov/CCMT has resulted in the identification of certain risk-relevant event sequences[4] specifically associated with DFWCS failure modes and reflecting the hypothetical conversion of the steam generator feedwater control system, from an original analog system to a digital one[5].

C. Combined application of deductive analysis and inductive analysis in comparative terms shows that different initial conditions and sequencing of events can cause the DFWCS system to fail in different modes, some of which have and some of which do not have safety implications. Because these failure modes depend on timing and logic combinations of underlying conditions, their individual probabilities can be significantly different. The improved qualitative insight capability of a combined deductive / inductive analysis holds whether this is achieved by the use of both types of analysis within DFM, or whether the DFM deductive analyses are complemented with Markov/CCMT inductive ones. However, with the level of modeling detail applied by each methodology in this study, Markov/CCMT inductive analysis may provide a better qualitative degree of analytical resolution to validate the quantitative insights for certain types of failures, such as Arbitrary Output, than DFM inductive analysis.

D. The inductive analyses of both methodologies, which can track dynamic scenarios by

[2] Formally correct here means that the technical means of execution of the approach preserve the logical integrity and information content of the PRA elements being integrated together. Practically implementable means that, given that the respective elements to be integrated have been already defined, the execution of the integration itself can be carried out with existing PRA implements and without adding an inordinate amount of additional effort.

[3] Logic completeness indicates that the set of prime implicants that can be identified via logic analysis of a model, executed inductively or deductively, is complete with respect to the definition of the logic model itself, i.e., no other prime implicants exist that the analytical process has not / can not identify.

[4] In the context of this discussion, risk-relevant does not necessarily imply quantitative significance. As stated earlier, the quantitative aspects of the risk sequences and of the underlying failure mode data have not been completely addressed in this study, nor validated, even when quantification has been carried out for demonstrative purposes.

[5] Given the demonstrative intent of the current analyses and associated quantification exercises, no claim is made as to whether the newly identified DFWCS risk scenario sequences constitute a comprehensive set, i.e., whether they characterize the risk associated with the hypothetical upgrade in satisfactory fashion from both a qualitative and quantitative point of view.

identifying associated time-dependent sequences of events may be effective for:

a. Validating the correctness of the respective models.

b. Performing sensitivity analyses starting from the baseline failure conditions identified by the prime implicant results of a DFM deductive analysis. Such sensitivity analyses may be carried out by varying initial conditions of certain parameters appearing in the prime implicant definitions, or in associated scenario boundary-condition definitions. For example, in Chapter 3, one such Markov/CCMT analysis has shown how, during a power ramp-up maneuver, the outcome of a frozen controller output or MFV stuck-at condition may change from the predominant Top Event outcome of low SG level to that of high SG level. This may occur if the transient starts at a time when the SG level happens to be 1% below normal, due to some unspecified earlier disturbance.

E. Similar to other modeling activities, there exist trade-offs between level of modeling detail and associated analytical power of resolution on one hand, and modeling and computational level of effort on the other. This is true for both methodologies. The effectiveness and efficiency of a deductive analysis mode has been explored in this study with the DFM methodology, but not with the Markov/CCMT because the Markov/CCMT analytical procedures do not currently include a deductive analysis algorithm that is practically implementable for system models as complex and detailed as the DFWCS model analyzed in this study. The Markov/CCMT inductive analyses appear to confirm its effectiveness in providing fine levels of resolution in the time tracking of dynamic sequences when compared to traditional techniques. With respect to the level-of-resolution vs. modeling and computational effort question, DFM offers the advantage of logic completeness at reasonable effort (e.g., within a maximum of three or four time steps) for a system similar to the DFWCS in complexity and dynamic characteristics. Markov/CCMT provides the analyst with the capability of tracking a larger number of time steps, if the analyst can restrict, on the basis of general engineering insight or of insights gained by means of some other type of analysis, the range of initial conditions from which a dynamic inductive analysis can be started.

The above insights are significant. However, there are several reasons why at this time no definitive conclusions may yet be drawn with regard to what technique, or combination of techniques, may be best suited for a specific digital I&C modeling and assessment purpose. One reason is that there are different conceivable contexts, objectives, and levels of depth for PRA analyses of digital I&C systems. Moreover, there has been to date limited experience with the estimation of reliability and risk for these systems by means of any type of analytical models. Furthermore, there has been limited experience with their operation such that reliability and risk relevant data, against which one may compare model predictions, are also not readily available.

With regard to Question 2, the study has demonstrated some means of quantification of the analytical results obtained via the application of the modeling techniques being investigated. This demonstration is not fully developed to cover all aspects of digital I&C risk that may be significant. The most important reasons why the study quantitative results should at this time be considered only as first-cut demonstrative values, and not real indicators of the possible risk impact of control system digital upgrades on a typical NPP, are:

A. The possibility of logic design errors, especially with respect to the design of any complex software that governs a digital I&C system was, by definition of project scope, left unexplored in the analyses carried out for the DFWCS benchmark.

B. The study models the digital update of just one control system and therefore does not cover, even in purely qualitative terms, the full potential extent of a full scale digital upgrade affecting all the elements of both the reactor protection and control systems of a given plant.

C. The quantitative results of the study relative to High and Low SG level probabilities are used in this report to quantify turbine-trip / reactor-trip types of traditional PRA scenarios, under the assumption that the values obtained in this study from the analysis of the power maneuver transient are representative of High and Low SG level probabilities for generic plant conditions. This is not necessarily true in all cases, and the probability of Top Events may depend on the plant regime at the time that certain types of component failures are assumed to occur. Thus, in a complete analysis, one would first need to carry out a classification of basic plant regimes, then conduct dynamic analyses like those executed in this study to cover all such regimes and finally use some appropriate averaging of probabilities if values for these probabilities were found to differ significantly from a plant regime to the next. In essence, the analyst needs to always treat dynamic scenario sequences and probabilities as being conditional upon the occurrence and probability of the initial plant state that is assumed to exist at the start of the dynamic sequence.

D. The results of the study do not necessarily reflect, besides the potential effect of system and software logic and/or algorithmic design errors already discussed above: a) possible statistical dependence among failures of different reactor protection and control functions due to common causes (e.g., platform and/or protocol commonality) and b) possible communication issues (e.g., data races, multitasking, multiplexing). Thus the potential probability of failure contributions from these types of failure modes and system interactions are not reflected in the demonstrative estimates documented in the study.

Within the above limitations, the study has provided the following insights with respect to Question 2:

A. Dynamic methods such as DFM and Markov/CCMT provide qualitative results in the form of prime implicants that are the multi-valued logic equivalent of binary cut-sets and can be quantified with data and techniques similar to those used to quantify conventional PRA models.

B. Failure probability and failure rate estimations relative to certain digital I&C components can be utilized, in both DFM and Markov/CCMT models and associated analytical failure-mode results, to generate quantitative risk estimations at a level of detail and depth comparable with the standards of practice encountered in traditional PRA. In this study, these estimates were generated primarily via the fault injection technique and combined in the dynamic PRA models with hardware failure mode probabilities and failure rates compiled from open literature sources. Overall digital risk estimates were produced for the DFWCS digital system and were then integrated and incorporated into traditional PRA event sequence estimations.

C. DFM results obtained in deductive or inductive analysis mode for the DFWCS benchmark, and Markov/CCMT inductively-obtained results appear to be consistent with the implemented modeling assumptions and quantification data.

D. Both DFM and Markov/CCMT analyses can be used to identify and rank-order event sequences with respect to their contribution to different DFWCS failure modes, as well as to identify and rank-order the corresponding contribution of individual basic events related to these sequences.

Regarding Question 3, the study has executed a demonstrative integration of the DFM and Markov/CCMT qualitative and quantitative results obtained for the DFWCS benchmark system with the relevant portions of an existing PRA. More specifically, this was done using the PRA framework and data pertaining to one of the NUREG-1150 plants. The results of this integration exercise support the following findings:

A. For point-estimation of risk figures of merit, the integration can be carried without particular difficulties for all three basic subcases of interface boundaries – i.e., at the ET initiating event level, at the ET pivotal event level, or at the FT intermediate event level – between the existing PRA structures and dynamic methodologies results cast in the form of prime implicants of a defined Top Event.

B. For the estimation of uncertainty ranges and importance measures, the integration can also be carried in straightforward fashion and without introducing errors, if an assumption of statistical independence of the basic events that appear across the conventional PRA – dynamic PRA model interface holds true in that the contribution of any such correlated basic events to overall plant risk metrics is small.

C. In cases of uncertainty or importance analysis where the limiting assumption stated in B above does not hold true, the integration of results is still possible if one applies the same post-processing techniques that need to be applied when integrating, under the same circumstances of correlated basic events, the model structures and results obtained from separate conventional PRA models and analyses.

All observations that can be made on the basis of the findings in this study cannot ignore the fact that the state of the art in the area of digital and software-intensive systems risk modeling is rapidly evolving and that important findings have also been identified and published by other researchers while this study was being executed. A full answer to the question of reliability and risk quantification for digital systems cannot be produced without covering ground that this study was not chartered to address. Most experts and organizations recognize that the identification of potential software-related digital system failure modes has not been evolved to the point of systematic classification and robustness that would make possible the high-confidence selection of the most appropriate modeling and quantification means for risk assessment purposes. The findings of this study and the associated insights essentially confirm this view. In order to fill this recognized gap, a systematic digital I&C failure-mode modeling activity should be eventually organized and executed to provide a substantive baseline with respect to this issue, specifically with regard to the more risk-relevant subsystems of a nuclear power plant.

It is perhaps worthwhile adding with respect to the above that any future failure mode identification and modeling effort should not be without a careful examination of the issue of software design errors. This issue has not thus far been investigated with sufficient attention in the context of nuclear power plant digital system applications, thus it is currently not possible to confirm whether the findings in this respect that have been documented in studies focused on other types of digital system applications, however theoretically similar to the ones of interest to the nuclear industry the latter may be, are transferable and have the same validity within the nuclear plant application area.

A closing observation is that, given the demonstration nature of this project, some of the key findings of the study, and some of the procedures that were identified and documented in the report, are yet to be validated and organized into repeatable processes, perhaps with the supplemental aid of suitable implementation aids, such as software tools. Achieving this would make both the analytical processes and the derived results more accessible and acceptable to users within the plant risk assessment and regulatory assessment communities.

ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
AFW	Auxiliary Feedwater System
API	Application Programming Interface
ATWS	Anticipated Transient Without Scram
ATVG	Automatic Test Vector Generation
BC	Backup Computer
BDD	Binary Decision Diagram
BE	Basic Event
BFV	Bypass Feedwater Regulating Valve
CAFTA	Computer-Assisted Fault Tree Analysis
CCMT	Cell-to-Cell Mapping Technique
Cdf	Cumulative distribution function
CST	Condensate Storage Tank
CVSS	Controlled Variable State Space
DET	Dynamic Event Tree
DFM	Dynamic Flowgraph Methodology
DFWCS	Digital Feedwater Control System
DST	Dynamic Scenario Tree
ES	End State
ET	Event Tree
FMEA	Failure Mode and Effect Analysis
FT	Fault Tree
FP	Feedwater Pump
HP	High Pressure
HPI	High Pressure Injection
LOCA	Loss of Coolant Accident
LOSP	Loss of Off-Site Power
MAR-D	Materials And Results Database
MC	Main Computer
MEI	Mutually Exclusive Implicant
MFV	Main Feedwater Regulating Valve
MFW	Main Feedwater System
MGL	Multiple Greek Letter
MOV	Motor Operated Valve
MS	Macro State
MW (e)	Megawatts (electric)
MW (th)	Megawatts (thermal)
PRA	Probabilistic Risk Assessment
PDI	Pressure Differential Indicator
PI	Prime Implicant
PI	Proportional Integral
PWR	Pressurized Water Reactor
RPS	Reactor Protection System
SAPHIRE	Systems Analysis Program for Hands-On Integrated Reliability Evaluations
SG	Steam Generator
SGM	Steam Generator Model

SRV	Safety Relief Valve
ST	Scenario Tree
TE	Top Event
TPI	Timed Prime Implicant

1. INTRODUCTION

1.1 Purpose of this Work

This report demonstrates how dynamic Probabilistic Risk Assessment (PRA) methodologies can be applied to a benchmark digital system with dynamic interactions between hardware/software/firmware and physical properties of a controlled/monitored process. In this work, the interactions are characterized as Type I or Type II. Type I interactions are those between the digital I&C system and the controlled/monitored plant physical processes (e.g., heatup, pressurization). Type II interactions are those among the components of the digital I&C system itself (e.g., communication between different components, multi-tasking, multiplexing).This work demonstrates the application of two dynamic PRA methods, Markov/Cell-to-cell-mapping-technique (CCMT) and Dynamic Flowgraph Methodology (DFM), to a benchmark Digital Feedwater Control System (DFWCS) of a generic pressurized water reactor (PWR). The dynamic model capabilities and limitations are presented in this report along with the assumptions made to develop the models. Furthermore, this work illustrates how the results from the dynamic models can be included into the framework of a traditional event tree (ET)/ fault-tree (FT) PRA.

1.1.1 Background

In 1995, the NRC issued the Probabilistic Risk Assessment (PRA) Policy Statement, which encourages the increased use of PRA and associated analyses in all regulatory matters to the extent supported by the state-of-the-art in PRA and the data [1]. This policy applies, in part, to the review of digital systems, which offer the potential to improve plant safety and reliability through such features as increased hardware reliability and stability and improved failure detection capability [2]. However, the demonstration of such safety and reliability improvements is presently hindered by the lack of universally accepted methods for modeling digital systems in current-generation PRAs.

As part of a cooperative agreement between the NRC and The Ohio State University (OSU), a study was initiated in 2004 to develop methods for inclusion of reliability models for digital systems into current generation nuclear power plant PRAs. The findings of the study regarding the current state of reliability modeling methodologies for digital systems were published as NUREG/CR-6901 (Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments) in February 2006 [3]. A conclusion of NUREG/CR-6901 is that none of the available methodologies satisfied all the requirements identified as minimum criteria for acceptance. Among the methodologies that were available at the time NUREG/CR-6901 was published, those that were found to rank as the top two with most positive features and least negative or uncertain features (using subjective criteria based on reported experience) were the DFM [4],[5-10] and the Markov/ CCMT [11-13], each with different advantages and limitations.

As a follow-up to NUREG/CR-6901, NUREG/CR-6942 (Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk

Assessments) [14] defined a benchmark system that is representative of the steam generator (SG) DFWCS of a currently operational PWR. Using a turbine trip as an example of initiating event, the NUREG/CR-6942 also showed how:

1. the DFM and Markov/CCMT can be implemented for the reliability modeling of the benchmark system, and,
2. the outputs of the DFM and Markov/CCMT can be incorporated into the existing ET/FT based PRA of a NUREG-1150 (Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants) [15] plant.

On the basis of the findings of the NUREG/CR-6942 study, it was concluded that both the DFM and Markov/CCMT methodologies can account for the features of the benchmark system with consistent results and that the results can be integrated into an existing PRA. At the same time, the following challenges/questions concerning a generalized use of the methodologies were identified:

Challenge 1 - Analyst skill levels needed for the implementation of the methodologies

Challenge 2 - Computational demand for the correct description of the coupling between failure events

Challenge 3 - Acceptability of the data used for quantification by a significant portion of the technical community

Challenge 4 - Routine integration and processing of the results of these methodologies within the structure of existing PRAs.

These challenges originate primarily from the complexity and diverse nature of the phenomena to be accounted for (e.g. statistical dependence of failure events through Type I and Type II interactions[6]) and are not specific to DFM or the Markov/CCMT methodology. Other concerns that were raised in the review process of NUREG/CR-6942 were:

Concern 1 - Scalability of the methodologies to larger systems (in view of the simplifying assumptions implicit in the example initiating event)

Concern 2 - Estimation of the risk importance of the digital I&C system failures (in view of the fact that there was no quantification of the contribution of the benchmark system failure to core damage frequency)

Concern 3 - Impact of the hardware/software/firmware/process interactions on the risk significant events under consideration (in view of the fact that no comparison of dynamic versus traditional PRA approach results were available for the system and scenario considered).

[6] Type I interactions are those between the digital I&C system and the controlled/monitored plant physical processes (e.g., heatup, pressurization). Type II interactions are those among the components of the digital I&C system itself (e.g., communication between different components, multi-tasking, multiplexing).

1.1.2 Organization of the Present Work and Results

With respect to the challenges and concerns identified in the course of the earlier stages of the project and during the NUREG/CR-6942 [14] review process indicated in the previous section, this report addresses Challenges 1 (Analyst skill levels needed) , 2 (Computational demand) and, to a degree, 4 (Routine integration and processing of results). It also addresses Concern 1 (Scalability of the methodologies) and, partially, Concern 2 (Estimation of digital I&C systems risk importance). The data acceptability issue (Challenge 3) is the subject of broad conceptual and philosophical discussions in the PRA and related technical communities and, given its still open-ended status, remains beyond the direct scope of the work documented here. However, the report does show how failure data that can be utilized within the application of the dynamic PRA methodologies investigated can be generated for the benchmark DFWCS, which is quite representative of digital I&C systems actually used for nuclear power plant control and reactor protection functions. It also discusses a possible path for solution of this particular issue, in light of recent developments in the field that have recently been produced and documented [7]. The question at the core of Concern 3 (Impact of hardware/software/firmware interactions on risk-significant events) has been addressed in previous work by several researchers in the field [3, 7, 16]. However, no conclusive results regarding Concern 3 have been reached at the time of this publication.

Regarding Challenge 1, the report uses the benchmark DFWCS originally defined in NUREG/CR-6942 to show how models (e.g. control logic models or process simulators) developed by different groups of specialists can be utilized within a system-level dynamic PRA framework. After different system function models have been produced, the PRA analyst only needs to be familiar with the linking process rather than with the detailed structure of a given dynamic methodology.

Regarding Challenge 2 and Concern 1, the study illustrates that a digital reactor control system similar to that of an operating plant can be modeled using dynamic methodologies and the results can be incorporated into an existing PRA to quantify the impact of the digital update of a control system on the plant core damage frequency. It should be emphasized that dynamic PRA methodologies have never been intended to be implemented for a whole nuclear power plant (NPP), but rather only for those systems that, because of their dynamic and complex characteristics, require such more sophisticated capabilities in the PRA model development effort. The integration process has been qualitatively demonstrated in NUREG/CR-6942 and is further expanded and quantitatively demonstrated in this report. In that respect, the report satisfactorily addresses both Challenge 2 and Concern 1.

Challenge 4 is addressed by leveraging the results of closely related studies that have been recently concluded and documented. This permits the identification of the key underlying issues as well as the identification and discussion of promising and technically feasible solutions for these issues.

Regarding Concern 2, this study provides a demonstration-level estimate of the impact that the digital upgrade of a main feedwater control system may have on accident scenarios originally included in the analysis of one of the NUREG-1150 plants. The demonstrative estimate scenario involves as the initiating event a turbine (and reactor) trip caused by high or low steam generator level. It is emphasized, however, that the quantitative aspects of the study results can at this time only be taken as partial indications, since the study objectives were demonstrative in nature and did not include obtaining complete and fully vetted quantitative results. To pursue more definitive quantitative indications, analyses more specifically focused on identifying capabilities and limitations of the current state of the art with respect to the quantification process and underlying data-collection processes would have to be planned and executed.

NUREG/CR-6942 had already qualitatively demonstrated the need to account for the timing of failures in the PRA modeling of digital I&C systems for a simplified scenario of the example DFWCS behavior. The present study uses the full DFWCS PRA model and addresses the dynamic conditions associated with a plant transient produced by a power maneuver (see Fig. 1.3.6) consisting of:

- 8 hour ramp up, starting from 70% of full power,
- 8 hour steady-state operation at 78% of full power, and,
- 8 hour power ramp-down, back to 70% of full power.

The maneuver constitutes good application ground because it exerts and challenges the main function of the DFWCS, i.e. maintaining the SG water level between set limits under changing power demand. The 24 hour period was chosen because it is the default reference-time period for standard PRA tools when modeling continuously operating systems. For assessing Top Event probabilities for different time periods, the DWFCS the Top Event probabilities generated for this power maneuver need to be regarded as rate (i.e., per day).In terms of the organization of the materials that follow, Section 1.2 describes the benchmark DFWCS. The project scope and development assumptions are outlined in Section 1.3 and include capabilities and limitations of the dynamic methodologies. The failure data utilized in this work is presented in Section 1.4 and includes the assumptions and limitations of the fault injection technique developed at the University of Virginia. Chapters 2 and 3, respectively, describe the implementation DFM and Markov/CCMT on the benchmark DFWCS. Chapter 4 discusses the Markov/CCMT and DFM results, summarizes the example NUREG-1150 PWR plant PRA, and discusses the integration of the DFM and Markov/CCMT model structures and associated quantifications into the example plant standard PRA framework and models. The summary and conclusions drawn from the study are given in Chapter 5.

1.2 The DFWCS

The purpose of the feedwater control system is to maintain SG water level within plus or minus 2 inches of an assigned setpoint (designated as 0). The feedwater system serves two SGs each controlled by its own digital controller as shown in Fig. 1.2.1 below. The controller is considered failed if the SG water becomes too high (over 30 inches above the setpoint level) or if the SG water level falls too low (less than 24 inches below the setpoint). Each digital feedwater controller is connected to a feedwater pump (FP), a main feedwater regulating valve (MFV), and a bypass feedwater regulating valve (BFV). The controller regulates the flow of feedwater to the steam generators to maintain a constant water level in the steam generator.

In addition to the FP, the FP seal water system, MFV and BFV, the feedwater control system contains high pressure (HP) feedwater heaters and associate piping and instrumentation which are not modeled in this report.

From an operational point of view, the DFWCS operates in different modes depending on the power generated in the primary system. These modes are the following:

- Low power automatic mode
- High power automatic mode
- Automatic transfer from low to high power mode
- Automatic transfer from high to low power mode

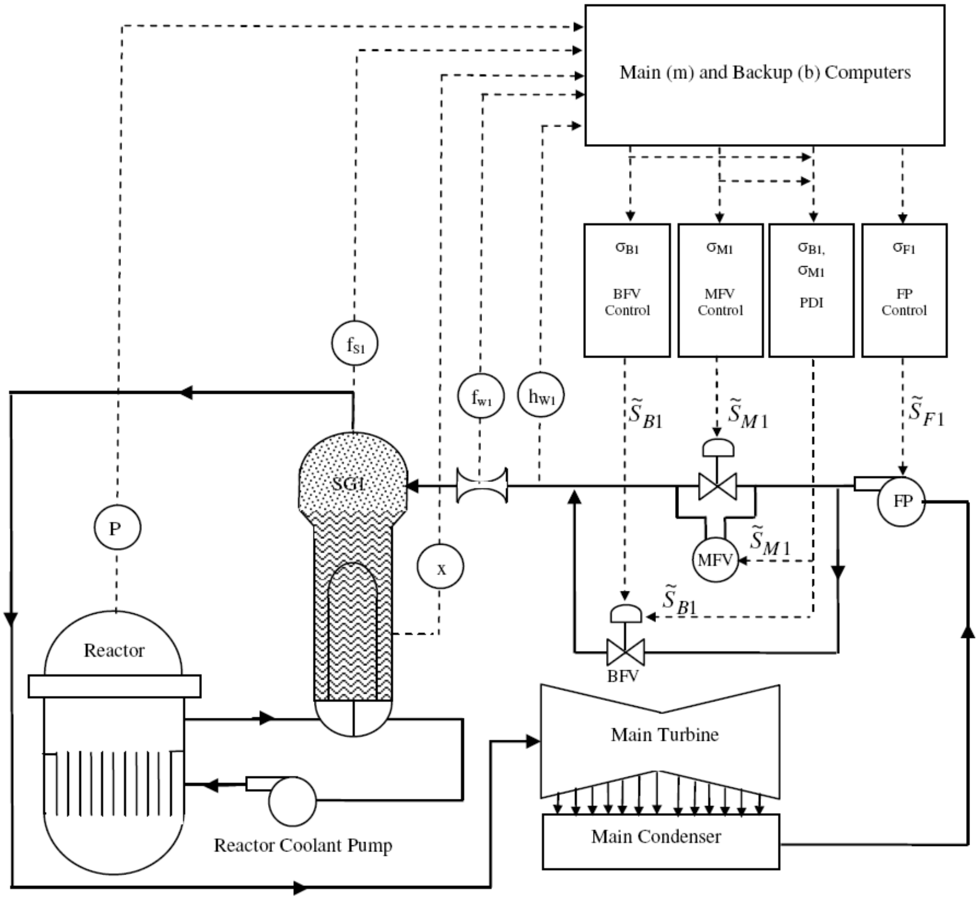


Figure 1.2.1: Detailed View of a Single Feedwater Controller. Solid lines indicate piping. Dashed lines indicate signals.

The low power mode of operation occurs when the reactor operates between 2% and 15% reactor power. In this mode, the BFV is used exclusively to control the feedwater flow. High power mode is used when the reactor power is between 15% and 100% reactor power. In this mode, the MFV and the FP are used to control the feedwater flow. The BFV is closed in a manner that is similar to low power mode.

1.3 Project Scope and Development Assumptions

As in any project, the scope of the study documented in this report was subject to practical constraints related to schedule and available resources. The technical objectives and boundaries of the project have been defined consistently with what appeared achievable in light of these constraints. The principal resulting limitations of scope are listed below:

1. The project was not intended to provide results, either qualitative or quantitative in nature, for direct use in the nuclear power plant risk assessment and/or regulatory arenas. Its main objective was instead an investigation and demonstration, as detailed and thorough as possible, of the DFM and Markov/CCMT techniques, to better identify their maturity and capabilities in view of a possible future use in such a capacity.
2. The project was not intended to seek any substantial development of the modeling and analytical capabilities of the DFM and/or Markov/CCMT techniques, beyond the level of capability already existing at the time of project inception.
3. In light of the above mentioned constraints, the project was set to utilize information and data produced by previous related work to the maximum extent possible. Consistently with this, the following technical assumptions have been applied in the modeling and analysis of the benchmark system described in Section 1.2 and of the interfacing plant:
    a) No explicit attempt is made to include system failure modes associated with possible design or specification errors concerning the system or software.

    b) Once valves, pumps, and controllers fail in a particular mode, it is assumed they will stay in that failure mode. No deliberate or fortuitous recovery action nor contingent repair is modeled.

    c) The plant is assumed to have 2 identical but isolated steam generators, so that modeling one steam generator with the associated control system is assumed sufficient to characterize the behavior of the overall SG system.

    d) The physical behavior of the steam generator modeled is assumed to be well represented by the simulator developed for NUREG/CR-6465.

    e) The SG control logic and control equations are those documented in NUREG/CR-6942.

    f) The set of failure modes of the valves, pumps, controllers and computers defined in the benchmark system is that identified in the FMEA (Failure Mode and Effects Analysis) performed specifically for this project.

    g) If a component fails in the “arbitrary failure mode,” the output it produces at the time of failure is assumed to be arbitrary within the theoretically possible range, and the output is assumed to remain at the arbitrary (random) value assumed at the time of failure. This applies to the main and back-up computers and controllers that are part of the DFWCS.

h) The failure rates of the benchmark system controllers and computers can be estimated by means of the fault-injection testing technique summarized in Section 1.4.

In the following, Section 1.3.1 describes how dynamic interactions were modeled for the DFWCS. Section 1.3.2 presents the unique characteristics of DFM and Markov/CCMT versus traditional PRA methods including capabilities and limitations.

1.3.1 Modeling Interactions

A discrete state representation of the benchmark system was developed in NUREG/CR-6942 [14] as a preliminary step with respect to the Markov/CCMT and DFM modeling processes, based on the availability of data for the benchmark system, the nature and detail of its associated failure modes and effects analysis, and the degree of connectivity between its major components. As described in NUREG/CR-6942, the DFWCS topology can be regarded as consisting of three layers of interactions:

- intra-computer interactions
- inter-computer interactions
- computer / controller / actuated-device interactions.

The intra-computer interactions layer consists of five states (see Fig.1.3.1). In State A, the computer is operating correctly and nominally. In State B, the computer detects a lost / invalid output for one sensor of any type (e.g., water level). State C represents detection of a loss / invalid output for two sensors of any one type. In State D, the computer has detected an internal problem but is signaling that the problem can be ignored. In State E, either a sensor output is invalid or there is an internal processing error in the computer; however, the computer does not detect the fault and transmits the wrong information to the controllers.

The inter-computer interaction layer represents the possible transfer of control of actuated devices among the main computer (MC), backup computer (BC), and controller. That is, the transfer of control from the MC to the BC is represented at this level of modeling, wherein three such computer-computer macro-states are represented (Fig.1.3.2). In State 1 both MC and BC are operating normally. In State 2, one computer is down but can be recovered. In State 3 again one computer is down but it is not recoverable. Transitions between the macro states (MSs) depend upon the state of the controlling computer as shown in Fig.1.3.2. Primary and secondary computers correspond, respectively, to the computer that is sending data to the controller and to the computer that is waiting in hot stand by. Either the MC or the BC can be the primary or the secondary computer. Recoverable and non-recoverable failures are defined as follows:

- Recoverable failure corresponds to the inability for the computer (which is still operating correctly) to send valid data to the controller (e.g., due to a loss of input from one or more sensors).
- Non-recoverable failure corresponds to an internal failure of the computer (e.g. the trip of the watchdog timer) or to a loss of output of the computer itself.

The fail-over action from MS 1 to MS 3 is a result of controller action via the watchdog timer or detecting the output failure from the computer. This action takes down the failed computer permanently and can occur in both the primary and secondary computer. If it occurs in the secondary, the transitions mimic the action of the secondary failure transitions from MS 1 to MS 3 by simply transitioning from a state in MS 1 to the respective state in MS 3. For example, State A in MS 1 would have a transition to State A in MS 3. If the primary computer fails in a non-recoverable manner when both MC and BC are operating (i.e., when the DFWCS is in MS1), then the DFWCS can go to any state in MS 3 except State D by the same rationale for transitions between MS1 and MS2. The transitions must take into account that the secondary computer may have already entered different states and these must be represented in the transitions to MS 3.

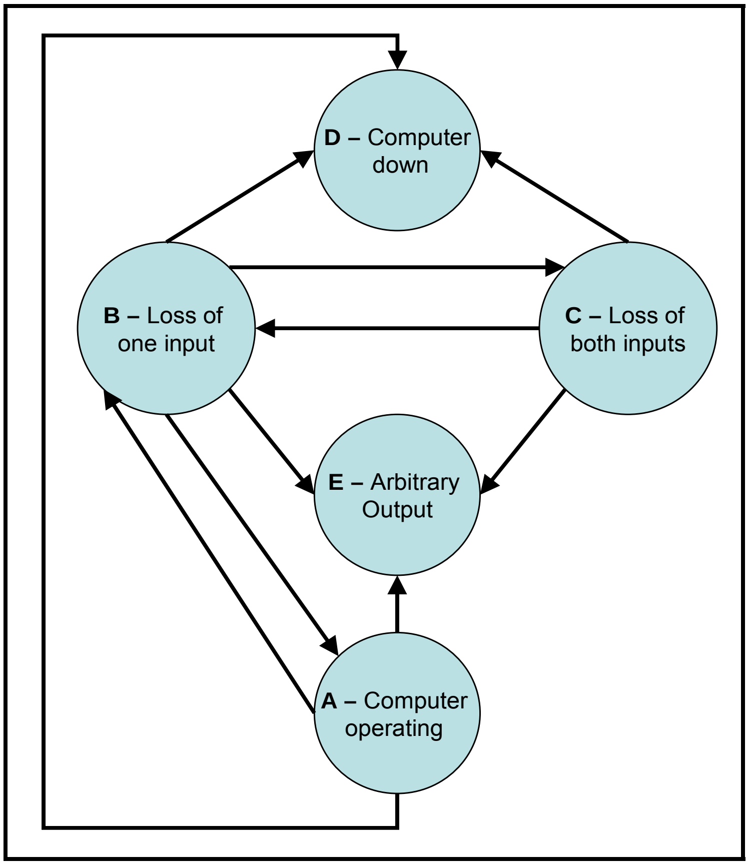
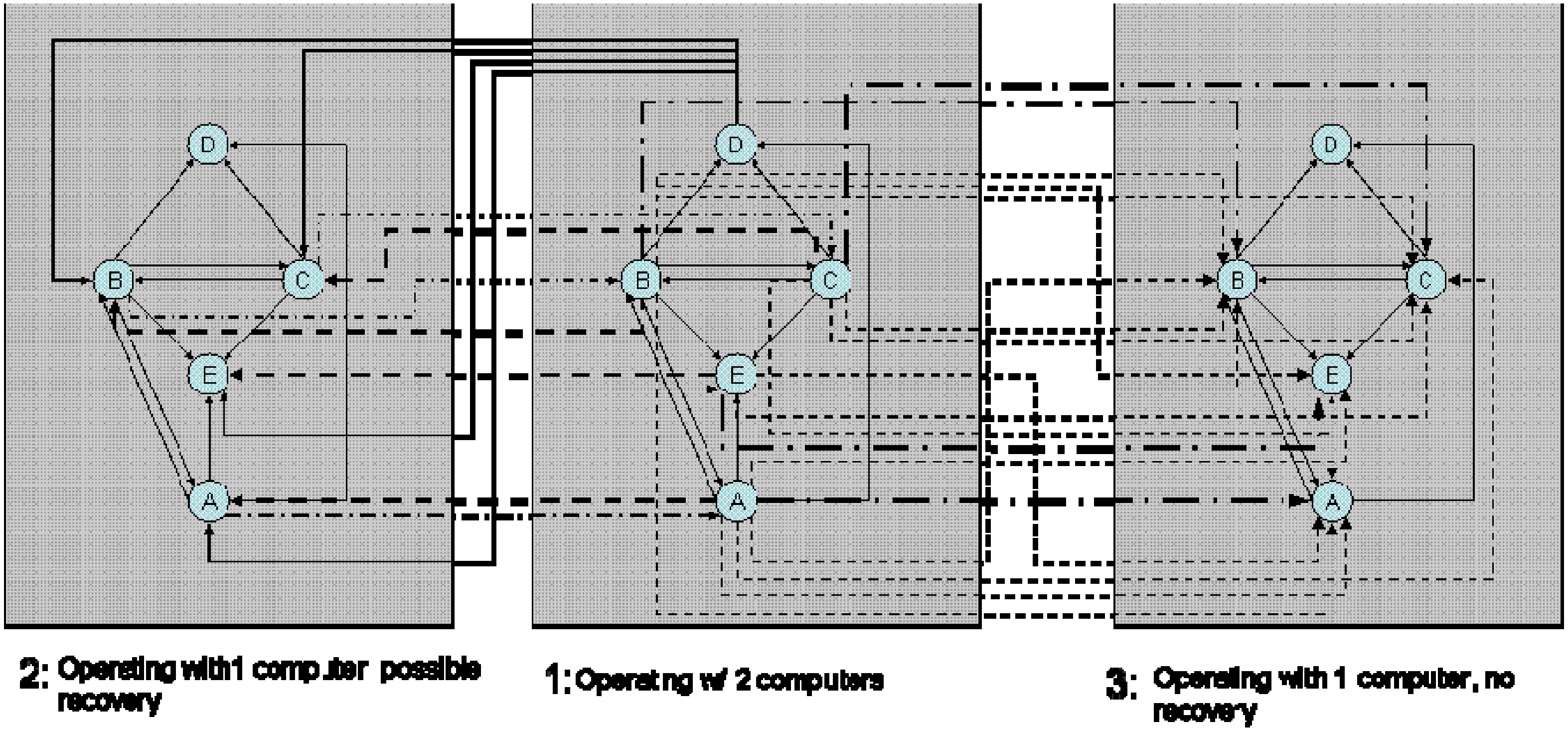

D – Computer down
B – Loss of one input
C – Loss of both inputs
E – Arbitrary Output
A – Computer operating

Figure 1.3.1: Intra-computer interactions

So far, the inter-computer and intra-computer interactions layers consider only the interaction between the computers. However, once the valve apertures and the pump speed are determined, those values pass through the controllers [14] which takes into account on the interactions between computers and controllers.

Fig. 1.3.3 shows all the possible controller-computer-actuated device interactions. The shaded circles represent signals to the actuated devices (e.g., MFV, BFV, FP) upon computer/controller failure, as well as the mechanical failure of the actuated device

(Device Stuck). Mechanical failure of the actuated device leads to the device maintaining its current position for the MFV and BFV or to its current speed for the FP. The planes represent the communication status between the controller and actuated devices. The two-way transitions between Planes I and II are necessary to keep track of the computer from which the controller is receiving data when the communications between the controllers are restored.


D
B
C
E
A
2: Operating with1 computer possible recovery
1: Operating w/ 2 computers
3: Operating with 1 computer, no recovery

Computer States

A: Operating	B: Loss of one input
C: Loss of both inputs	D: Computer down
E: Arbitrary output	

Macro States

1: Controller is receiving data from both computers

2: Controller is receiving data from 1 computer while the other one can be recovered

3: Controller is receiving data from 1 computer while the other one can not be recovered

Freeze: Controller sends the same data to the valves from the previous time step

— — — ·	Secondary goes down (recoverable)		Primary release control of the process.	— · — ·	Secondary computer watchdog timer trips or loss of output to controller		Common cause sensor failure
- · - · - · -	Secondary recovers	- - - - - - -	Primary computer watchdog timer trips or loss of output to controller.	▬ ▬ ·	Primary goes down. Secondary unavailable		

Figure 1.3.2: Inter-computer interactions

As presented in Fig.1.3.3, the following types of controller failures are under consideration:

- Arbitrary output: random data are generated and sent to the actuated device (i.e. pump or valves)
- Output high: output value is stuck at the maximum value (i.e. valve totally open or pump at the maximum speed)
- Output low: output value is stuck at the minimum value (i.e. valve totally closed or pump stopped)
- 0 vdc output: loss of communications between controller and actuated device.

Moreover, as a result of the failure of both computers, the controller can recognize the failure and send to the actuated devices (i.e. pump or valves) the old valid value (i.e. Freeze). If the controller does not recognize the failure, then it will simply pass on invalid information (Arbitrary Output) to the actuated device. Fig.1.3.3 also shows how the computer-computer interactions (presented in Fig.1.3.2) integrate with computer-controller and controller-actuated device interactions. The behavior of the controller under normal and failed operation can be described as follows:

- When both MC and BC are down, the controller transits to the Freeze state. The actuated device remains in the position corresponding to the last valid value.
- If the controller is operating and an Output High or an Output Low or an Arbitrary Output failure occurs, the controller transits to the corresponding state and the actuated device assumes the highest, the lowest or an arbitrary position respectively.
- If the controller is in the Freeze state and an Output High, Output Low or Arbitrary Output failure occurs, the controller transits to the corresponding state and the actuated device assumes the highest, the lowest or an arbitrary position, respectively.

If a loss of output occurs when the controller is failed (i.e. the controller is in Arbitrary Output, Output High or Output Low states), then the actuated device receives 0 vdc as input which corresponds to the lowest position.

The control laws for the DFWCS under both normal and off-normal condition may be described by a set of algebraic and first order differential equations which have been provided in NUREG/CR-6942. The DFWCS satisfies the benchmark requirements given in NUREG/CR-6942 [14], as well as being representative of the digital SG feedwater control systems used in operating PWRs. However, it does not represent digital I&C system features found in practice but not relevant to those used in the current nuclear reactor protection and control systems (e.g. networking, shared external resources). One particularly challenging feature of the benchmark system from a reliability modeling viewpoint is that modeling of some of its fault tolerance capabilities requires consideration of the system history. For example, when both the MC and BC have failed, FP speed as well as MFV and BFV positions are determined from system history data.

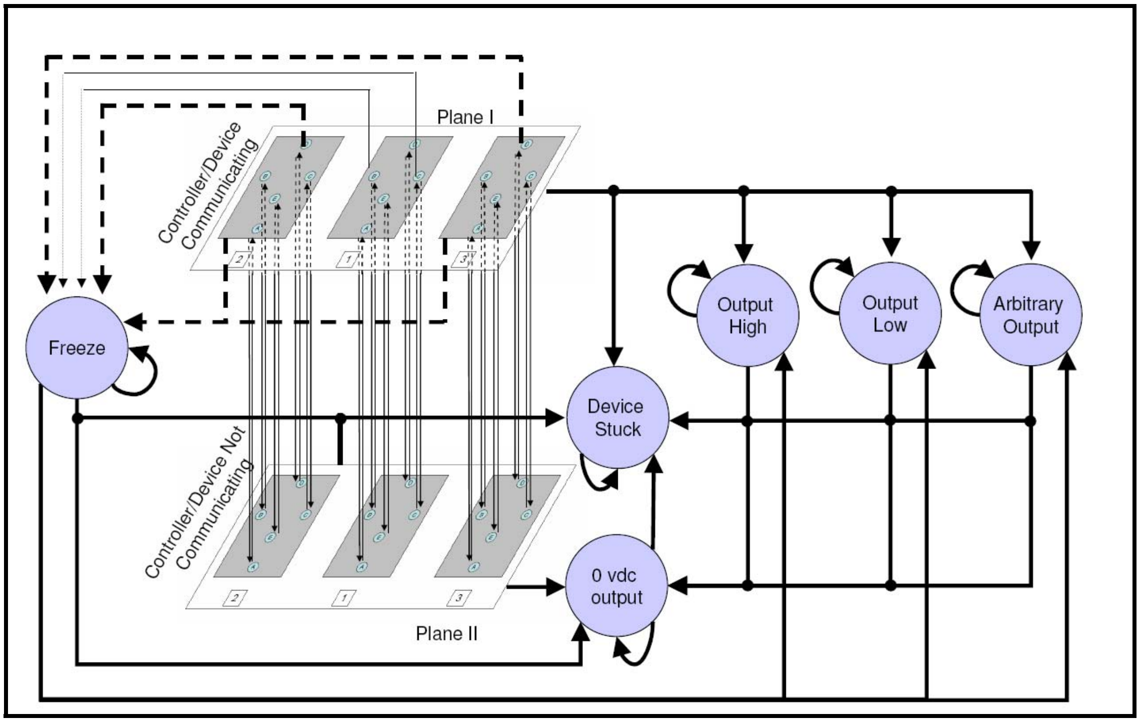


Figure 1.3.3: Computer-controller-actuated device interactions

1.3.2 Unique Characteristics of the Techniques Demonstrated

The limitations of the traditional PRA methodologies was discussed in detail in NUREG/CR-6901 [3] and the need to use dynamic methodologies to explicitly account for the timing of failure events to represent interactions among the digital I&C system hardware/software/firmware as well as the controlled/monitored process was illustrated in NUREG/CR-6942 [14] (also see Section 1.3.2.1). Similar to the ET/FT techniques utilized in a traditional PRA, both the DFM and Markov/CCMT utilized in the study rely on a three step approach to execute risk scenario analysis:

1. construction of a system model;
2. logic analysis of the system model and qualitative identification of risk-contributing combinations of events;
3. quantification of risk-relevant events and scenarios.

The principal common characteristics of the methodologies, both in terms of capabilities and limitations of these techniques are summarized below. Additional discussion of DFM or Markov/CCMT unique characteristics is provided respectively in Chapters 2 and 3.

1.3.2.1 Capabilities

The dynamic reliability models, DFM or Markov/CCMT, differ from traditional PRA models in the following ways:

- DFM or Markov/CCMT can represent system states with multi-valued logic, rather than binary logic
- DFM or Markov/CCMT can account for event timing and sequences whereas traditional PRA offers a limited static view of the system and its failures
- DFM or Markov/CCMT have the ability to model a system under many different conditions and scenarios whereas a traditional PRA approach requires a separate model to be manually recreated for each scenario specific situation. In addition, a DFM or Markov/CCMT model offers more flexibility in that they can be analyzed for either the success or failure of a system.

Once a system model has been constructed, both DFM and Markov/CCMT utilize computer assisted algorithms to either identify and track event time-ordered sequences resulting from certain user-identified initial conditions, or to obtain prime implicants[7] of interest. Quantification algorithms are also utilized by both methodologies to quantify this logic-qualitative information and obtain risk-scenario probabilities. More specific characteristics of the modeling, analysis and quantification processes associated with either technique are further discussed and summarized at the beginning of Chapters 2 and 3, respectively.

1.3.2.2 Limitations

As listed above, limitations of the demonstrated model applications result from either the constraints deliberately imposed on project scope or from explicit assumptions. Additional limitations are the product of intrinsic technical characteristics of the methodologies. Certain modeling and analysis trade-offs have to be made on the basis of these limitations. Limitations common for both DFM and Markov/CCMT models are discussed here, whereas the methodology-specific limitations are discussed respectively in Chapters 2 and 3.

The main limitation of both the DFM and Markov/CCMT modeling paradigms that an analyst must keep in mind is that, although capable of much greater fidelity and time-sequence representation than ET / FT binary models, both dynamic modeling environments are based on representing the system in terms of multiple discrete states (as opposed to binary success/failed states) and including the temporal characteristics of event timing and sequencing.

The number of states chosen to represent a specific system variable is in theory arbitrary, but in practice must reflect the definition of ranges in which the variable is subject to a certain type of control or safety regime. The overall number of variables modeled, the number of associated states, and the number of time-steps for which an analysis is desired conditions the computational speed with which a model can be analyzed to obtain risk-relevant prime-implicants. Thus an overly detailed model, or an analysis that is set to track an excessive number of system time steps, may run into computational problems because of the potential combinatorial explosion effect for the number of system variable states that must be tracked to execute the system analysis in a formally and logically complete[8] fashion.

[7] Multi-valued logic equivalent of binary minimal cut sets for user-defined Top Events

[8] Logic completeness indicates that the set of prime implicants that can be identified via logic analysis of a model, executed inductively or deductively, is complete with respect to the definition of the logic model itself, i.e., no other prime implicants exist that the analytical process has not / can not identify.

The user must also keep in mind that the power of the methodologies is not in identifying component failure modes unknown to the user, but in revealing how combinations of these failure modes, even across time boundaries, can result in system failure modes that would otherwise been very difficult for the user to identify and understand.

1.3.2.3 Dynamic Modeling within a PRA framework

The integration of advanced risk models and analyses developed by means of the dynamic methods DFM and Markov/CCMT with a traditional plant PRA developed with traditional ET/FT methodology, is the subject of a detailed discussion and demonstration presented in Chapter 4.

To examine and discuss how a traditional-PRA can be integrated with a DFM and/or Markov/CCMT modeling and analytical process, it is assumed that a PRA analysis is to be conducted with respect to a specific plant where one or more digital I&C systems with potential risk-relevant dynamic and interactive characteristics are present. Under these circumstances it can also be assumed that, besides the standard ET and FT models covering the conventional portions of the plant, a DFM and/or Markov/CCMT model may be developed to cover and represent, at a minimum, the digital I&C systems and any portions of other plant systems that may be directly interfacing, and closely interacting, with the latter.

The initial steps of the PRA execution process start and proceed as usual, i.e., developing master logic diagrams (MLDs), ET scenarios and system / subsystem FTs, until one or more of the following three situations is encountered:

1. The initiating event of an ET in the plant PRA concerns the failure of a digital I&C or other system that exhibits dynamic characteristics.
2. A pivotal event in an ET of the plant PRA concerns the failure of a digital I&C and/or dynamic system.
3. An intermediate event of a FT of the plant PRA concerns the failure of a digital I&C and/or dynamic system.

In all three cases, the underlying possible root causes and the probability (or frequency) of occurrence of the event(s) concerning the digital I&C / dynamic system can be derived by utilizing a DFM and/or Markov/CCMT model of that system. Such a model, as mentioned above, will have to have been developed in parallel with the standard PRA ET / FT models of the rest of the plant. More specifically, if DFM analysis is used here as an example, a model will have to be analyzed and its prime-implicant results quantified per the steps that will be outlined in Section 2.2 and illustrated in Section 2.3.

The reader is referred to Chapter 4 for a detailed discussion of the exact processes that can be applied to accomplish the integration of DFM and/or Markov/CCMT analysis with a traditional PRA and of the key technical issues related to the possible sub-cases of the situations that may be encountered. Here, however, a summarized version of that discussion is presented, essentially pointing out that in all three cases listed above a specific digital I&C / dynamic system event can be identified that can also be further defined, analyzed and quantified via

DFM and/or Markov/CCMT analysis. The translation of the definition of such a traditional PRA event into an equivalent dynamic model form is quite straightforward, especially so when utilizing the DFM paradigm because of the intrinsic inter-compatibility of the DFM multi-valued logic constructs with the PRA binary ones.

Using here DFM as an example, in all of the three cases, regardless of whether the event of interest appears in the PRA framework as an ET initiating or pivotal event, or as an FT intermediate event, a DFM analysis will be able to proceed by defining a DFM top event that is equivalent to the PRA event in both its engineering meaning and in its formal-logic definition. From such a definition a deductive DFM analysis can then proceed to the identification of its prime implicants, and in turn lead to quantification via procedures that are discussed in Section 2.2. DFM inductive analyses can also be applied as a means of validating the DFM model and deductive analysis, and of providing user-insight into the step by step sequencing of events and cause-effect chains in a given risk scenario.

1.3.2.3.1 DFWCS Events of Interest as PRA Scenario Initiating Events

In a typical plant PRA, a reactor trip or a turbine trip caused, respectively, by low SG level and high SG level are among the significant risk scenario initiating events considered. In terms of the DFWCS behavior, the low SG level event equates to the DFWCS failing Low and the high SG level event equates to the DFWCS failing High.

Conventional PRA ET models illustrating in simple form risk scenarios that proceed from these basic categories of DFWCS initiating events are shown, respectively, in Figs. 1.3.4 and 1.3.5.

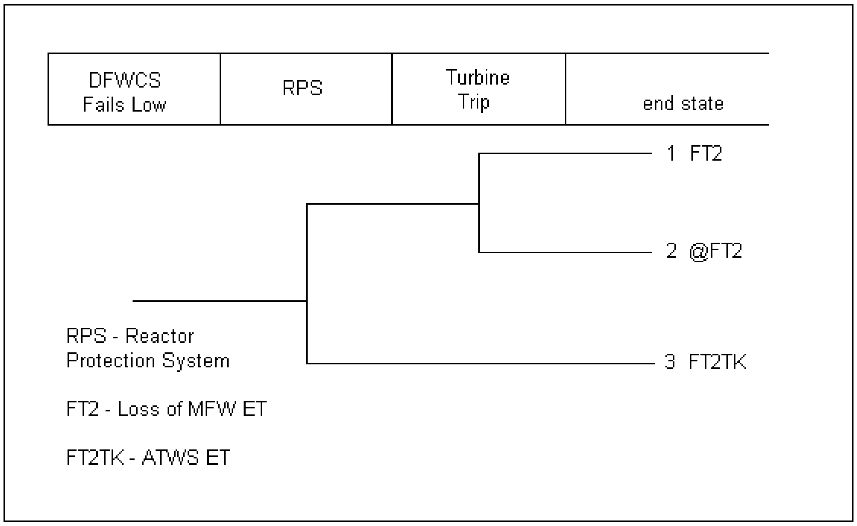


Figure 1.3.4: Event Tree for DFWCS Failing Low (MFW denotes Main Feed-Water, ATWS denotes Anticipated Transient Without Scram)

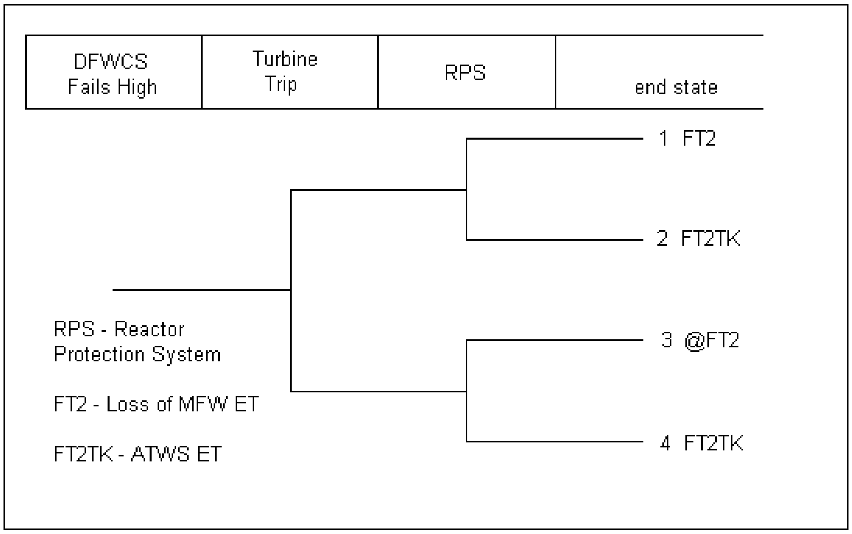


Figure 1.3.5: Event Tree for DFWCS Failing High (MFW denotes Main Feed-Water, ATWS = Anticipated Transient Without Scram)

The ET end states of the ET sequences shown in the figures are actually transfer-events linking the former to continuation ETs (indicated by the identifiers FT2, @FT2, FT2TK) which are not shown. The two ETs are very similar and lead to the same set of end-states / transfer-events. The difference between the two is determined by the plant-trip logic, which, upon a high steam generator condition calls immediately for a turbine trip first to prevent damage to the plant turbines from water behind carried along with the steam because of the high water level in the SGs; whereas, upon a low steam generator condition, it calls for a reactor trip (RPS actuation) to prevent drying out the SGs due to excessive power being transferred from the plant primary circuit. In the first situation a reactor trip follows automatically the turbine trip. In the latter the opposite occurs.

In line with the discussion above, if the ETs in Figs. 1.3.4 and 1.3.5 are assumed to be developed as part of a conventional PRA modeling effort, the development of the DFWCS Low and High SG level events would then be recognized to involve the modeling of a digital I&C system with potentially complex dynamic and interactive characteristics. Accordingly, to determine the prime implicants and probability for the two associated initiating events, DFM and Markov/CCMT models of the DFWCS benchmark system are utilized. This is done instead of expanding these events with FT models as would be normally done, at some level of detail, in a traditional PRA. In the demonstrations documented in Chapters 2 and 3, DFM and Markov/CCMT models of the DFWCS were constructed and solved with respect to the Low SG level failure top event and the High SG level failure top event. The results of the analyses were then incorporated into the traditional PRA models shown in Fig.1.3.4 and Fig.1.3.5, as will be shown in Chapter 4.

1.3.2.3.2 Dynamic Plant Conditions Associated with Example Initiating Event

The Markov/CCMT and DFM dynamic modeling methodologies are discussed in this report as a means to adequately address the interaction between dynamic and reliability characteristics of a system under consideration (in this case the DFWCS). Thus, as a background system condition against which the possible occurrence of an accident initiating event is to be modeled and assessed, a plant steady-state situation would be inadequate, because it will not necessarily reflect such interaction and system characteristics. For these reasons a plant transient, more specifically a plant power maneuver taking place within an overall time frame of 24 hours, was chosen as the background condition from which possible accident sequence initiating events may result. These events would manifest themselves at the DFWCS system level as either a low or high SG level event, normally followed in both cases by a turbine and reactor trip.

The plant output power maneuver referred to above is assumed to follow the course depicted in Fig.1.3.6.

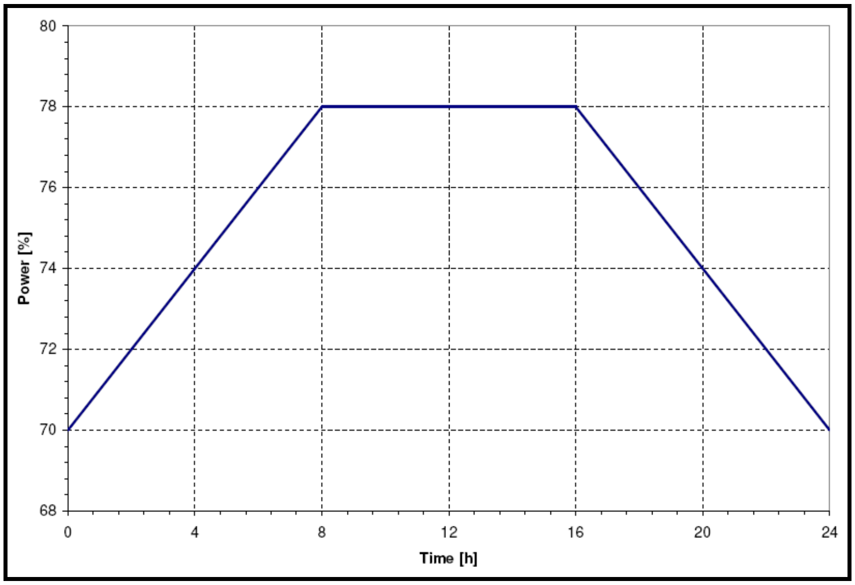


Figure 1.3.6: Power shape of the example plant transient condition

As shown in Fig.1.3.6, the maneuver overall timeline is 24 hours, divided into three 8 hour sub-periods defined as follows:

1. power ramp-up, starting from 70% of full power, at a rate of 1% of full power per hour,
2. steady-state at 78% of full power,
3. power ramp-down at the same rate as in 1, but in opposite direction, bringing the plant back to 70% of full power at the end of the 24 hr period.

The maneuver reflects the main function of the DFWCS, i.e. maintaining the SG water level between set limits under changing power demand. The 24 hour period was arbitrarily chosen, but mainly because it is the default time period to which failure rates and probabilities are normalized in the conventional PRA code SAPHIRE [17], which constitutes the PRA software environment that has been used to demonstrate the integration of the DFWCS models and associated results into an existing PRA (see Chapter 4). For assessing Top Event probabilities for different time periods, DWFCS Top Event probabilities generated for this entire power maneuver may be regarded as rate (i.e. probability per day).

The maneuver and resulting plant transient assume the following initial conditions:

1. Feedwater flow is at nominal level
2. Off-site power is available
3. All the components are operating correctly
4. Power generated by the primary circuit is shared equally by the two SGs

1.4 The DFWCS Failure Data

The data used in the in this study were obtained from the following sources:

- A fault injection based dependability assessment of I&C systems for the MC and BC failure modes,
- operating plant data for the controllers, and
- from the open-literature for the actuated devices.

1.4.1 Assumptions and Limitations

The following assumptions were made in obtaining the data for the MC and BC failure modes via the fault injection technique applied by the University of Virginia:

1. The fault space is assumed to be finite and discrete. This limits the injection process to only a portion of the fault space region.
2. All the faults in the fault space partition of the failure mode are equally likely to occur. This is also valid for the controller failure modes.
3. A statistics-of-extremes model [18] is used in situations when testing reveals no uncovered faults:
    a. The occurrence of an uncovered fault is a rare event (i.e., within the tail of the parent distribution)
    b. The maximum number of uncovered faults that can ever occur in a given system is *d* (this upper limit can be adjusted if the designer believes that the selected number of uncovered faults is too unrealistic).
    c. After each set of fault injection experiments is completed, one uncovered fault (if found) is removed from the system so that the resulting upper limit on the number R_f of uncovered faults in subsequent fault injection experiments is $d – 1$. Hence, the data for consists of $\{1, 2, …, d – 1, d\}$ uncovered faults
    d. At least one uncovered fault is assumed to exist
4. For the all covered case, the variance is estimated by converting one covered fault injection experiment to an uncovered fault injection experiment. This is a conservative assumption since it results in a larger variance estimate.
5. The failure modes are based on the FMEA presented in NUREG/CR-6942.

This study uses fault injection at the instruction set architecture of a microprocessor based computer. The following limitations apply to the application of the fault-injection technique to the MC and BC data gathering effort:

1. Requirements and design faults were not considered.
2. Software implementation faults were not considered.
3. Permanent hardware faults were not considered.
4. Possible non-uniform distribution of hardware faults and fault types was not considered.

5. Common-cause failure (CCF) effects were not considered.
6. Fault-injection testing was not carried out according to a representative operational (input) profile.

With respect to item 6, system start up conditions were not considered and the adopted operational profile (see Section 1.4.2, Step 4) was more representative of a light to heavy workload, a transition from low to high power operation. Finally, the use of the transient fault model was selected based upon historical and contemporary failure data (including operational data from the plant) of ground based systems. The permanent fault model represents a physical defect in the hardware that always is present and is activated when certain input and state conditions arise. The use of the permanent fault model is limited in this effort.

1.4.2 Fault Injection Based Dependability Assessment of I&C Systems

Fault Injection is a dependability validation technique based on the realization of controlled experiments where the observation of the system behavior in the presence of faults is explicitly induced by the deliberate introduction (injection) of faults into the system [19]. Fault injection stresses the fault handling and management aspects of the system under assessment to ultimately collect crucial data via fault injection campaigns. These typically include coverage of faults, error latency, and recovery time.

A fault is injected into a system by defining five parameters of the system.

1. external input and current system state σ,
2. fault occurrence time (or fault start time) t,
3. fault duration Δ
4. fault type f_m, and,
5. fault location l.

An extremely important parameter in the design and assessment of fault tolerant systems is fault coverage, C. Fault coverage can be defined as a measure of the system's ability to perform fault detection, fault isolation, and fault recovery. In that respect, fault coverage can capture Type II failure events such as communication failures and failures arising from competition for resources. Fault coverage can also capture common mode software failures in redundant systems (e.g., platform based) since system failure due to common mode is also part of un-coverage (*1-C*). The coverage of the system is typically obtained by sampling this five dimensional space and obtaining a statistical point estimate. The evaluation of each sampled data point in this space via fault injection results in either a 1 or 0 value for C. The binomial function is used to represent the system response. The point estimate for the system fault coverage is obtained

$$\hat{C} = \frac{1}{n}\sum_{i=1}^{n} y(t_i, \Delta_i, \sigma_i, l_i, f_{mi}) \qquad (1.4.1)$$

where $\hat{C}$ is the point estimate for the system fault coverage, and *n* is the number of fault injection experiment.

1.4.2.1 Methodology

Fig. 1.4.1 shows the flow of the quantitative dependability assessment methodology. The 8 steps are presented in this section.

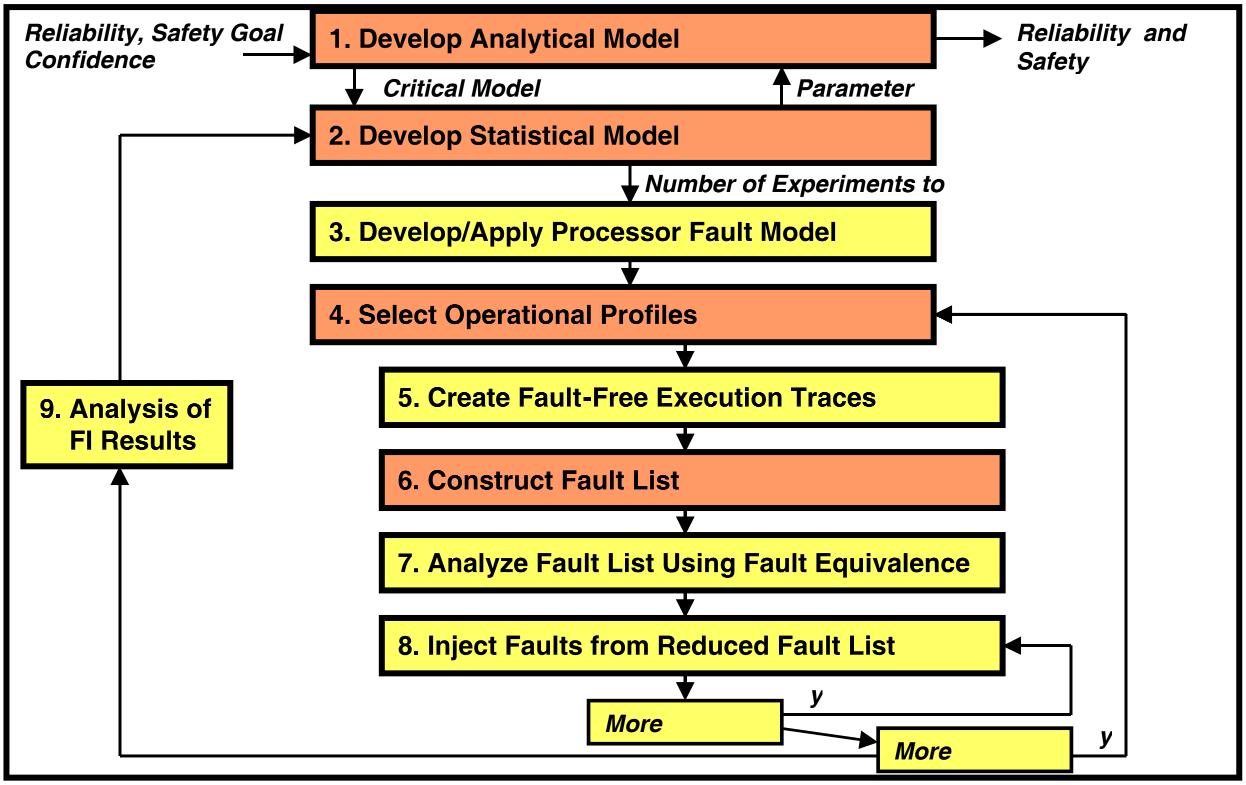

Reliability, Safety Goal
Confidence
1. Develop Analytical Model
Reliability and
Safety
Critical Model
Parameter
2. Develop Statistical Model
Number of Experiments to
3. Develop/Apply Processor Fault Model
4. Select Operational Profiles
5. Create Fault-Free Execution Traces
9. Analysis of
FI Results
6. Construct Fault List
7. Analyze Fault List Using Fault Equivalence
8. Inject Faults from Reduced Fault List
y
More
More
y

Figure 1.4.1: Step by Step View of the Quantitative Dependability Assessment Methodology.

Step 1 Develop Analytical Model: The analytical model is developed from the system architecture and inter-component dependencies. The input to the model development process are the architectural specifications, software specifications, fault tolerance specifications, operating systems specifications, control laws, and hazards analysis documents. These models are typically represented as dynamic fault trees, Markov models, dynamic flow graph models, finite state models to model functional behavior or combinatorial models.

Step 2 Develop Statistical Model: The statistical model provides formal basis for a estimating the critical model parameters (fault coverage values for components, recovery rates, and critical failure rates for the various components of the system) required by the analytical model. This statistical model supports following needs of the methodology:

- Quantify and characterize the uncertainty of model parameters.
- Characterize and define the assumptions of model parameters.
- Statistically estimate based on the assumptions of the model and model parameters the number of observations required to estimate a parameter to a known confidence level.
- Calculate the number of fault injection trials in a fault injection campaign required to calculate the coverage estimate of the component.

Step 3 Develop/Apply Processor Fault Model: The system is expected to encounter and tolerate certain faults, represented by the parameter f_m in Equation 1.4.1 above. A high level processor fault model is used to represent both transient and permanent faults. The fault model is used to generate the fault space, F, which is usually a multi-dimensional space whose dimensions can include fault characteristics such as location, time, and value. Here, time represents the time of occurrence and duration, location is where the fault occurs within the system under analysis, and value represents the form of the corruption.

A behavioral-level generic processor fault model represents the faulty behavior of a general-purpose, implementation-independent microprocessor [20]. The generic processor model considered performs a basic fetch-execute instruction cycle typical of a von Neumann architecture. As such, it contains a control unit, which operates as a synchronous finite state machine, and a data-path, consisting mainly of combinational logic and some storage elements, which performs the information processing within the processor. The data-path contains a register file that contains general-purpose and special-purpose registers, a program counter, an arithmetic and logic unit (ALU), and a fetch and decode logic block. In addition, the processor contains an interface that allows for communication with entities external to the processor. And finally, the processor contains internal signals that allow for communication between the data-path and control unit.

After the generic processor fault model was developed, it was analyzed to ensure that the experimental environment used to perform the fault injection experiments fully supports the fault model. The experimental fault injection environment developed to inject faults into the processors of the DFWCS is based on a software implemented fault injection method employing an in-circuit emulator to control and trace the execution flow of the processor

Step 4 Select Operational Profiles: The Operational Profile is the input and state space of the system under fault injection or the input operational domain of the system. In Equation 1.4.1, the σ represents the operational profile. Operational profiles to be used in the fault injection experiments must be selected to be representative of the system under various modes of operation and configuration.

Most real-time hardware/software systems operate on an event-triggered basis. If there is no event from the outside environment, only a reduced set of software and hardware resources may be used (cyclic idle tasks, diagnostics, and so forth). This portion of the operational profile will be referred to as a system light workload. The operational profile selection for the benchmark DFWCS is based upon actual plant data collected over a period of time. As indicated in Section 1.4.1, the profile on the benchmark DFWCS is more representative of a light to heavy workload, a transition from low to high power operation. This mode of operation invokes a substantial amount of the control processing.

Step 5: Create Fault-Free Execution Traces: For each operational profile that is selected, a fault-free execution trace must be created to support the analysis efforts in the safety evaluation process. The fault free trace is considered the correct operation of the system in the presence of no faults. The fault free trace is compared to the faulted trace after fault injection to determine if the fault was detected and properly mitigated by the system. In the assessment of the DFWCS three types of data logging are used to create fault free traces:

- a data dump routine that executes on the main and backup computers of the DFWCS,
- an external data logger that tracks selected sensor inputs and actuator commands, and,

- an assembly level instruction trace stored by the in-circuit emulator (ICE).

An ICE machine is a tool used by designers of embedded systems to debug embedded software. There is interface circuitry which provides a connection between an ICE machine and a terminal PC. This terminal can be used to run an interactive user interface application using which a designer can monitor the embedded system being designed.

Step 6 and 7 Construct Fault List and Analyze Using Fault Equivalence: One of the main issues when setting up fault injection experiments is how to construct the fault list. These failure used in this study were based on the FMEA presented in NUREG/CR-6942. The concept of fault equivalence and expansion [21] was used in the fault injection process.

Step 8 Inject Fault from Reduced Fault List: A fault injection tool was developed specifically to support precise controllability of the fault injection parameters given in Equation 1.4.1. The environment was designed to support the processor fault models described in Step 3. Faults are emulated by injecting single or multiple bit flip error patterns into the memory maps, registers, busses, and I/O registers of the microprocessor of the DFWCS computer modules. For this work, a unique method for fault injection was developed that employs an ICE as the heart of the fault injection environment.

1.4.2.2 Experiments

The experimental setup was designed and tested on the model of the DFWCS at the University of Virginia. Once sufficient confidence was obtained in the model fidelity regarding functionality through testing. the setup was deployed on the actual DFWCS. The response modes observed included:

- Fault covered due to masking[9] (or no-response faults),
- Fault covered by detection and recovery,
- Main CPU failure,
- Uncovered faults, and
- Invalid cases.

Fig. 1.4.2 shows a breakup of the relative percentages of each of the response modes that were observed from the experiments. Table 1.4.1 shows actual numbers obtained for each response mode.

[9] This is the case when the effect of a fault does not propagate as an error because after the fault is injected, the variable would be overwritten with a new, valid value.

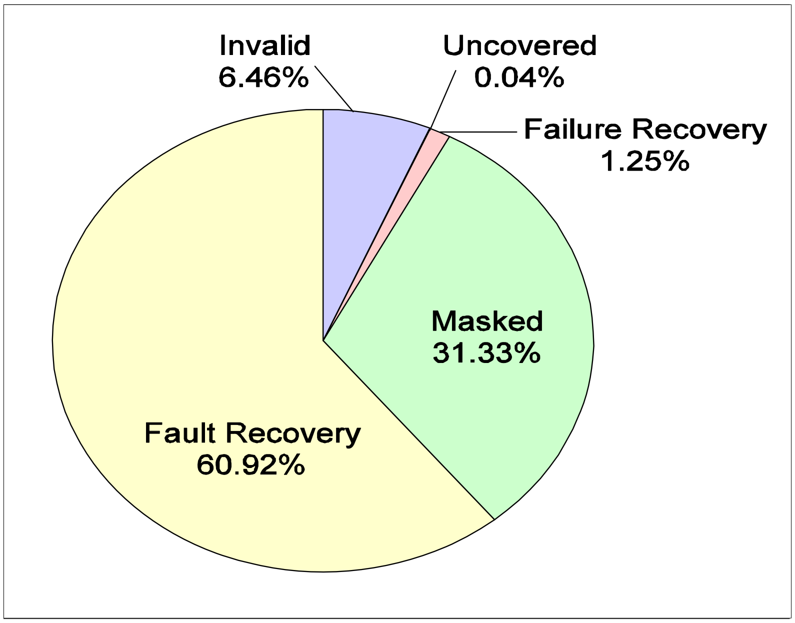


Figure 1.4.2: Relative Percentages of Observed Responses

Table 1.4.1: Break up of observed response modes

Response mode	Count
No-response faults	752
Recovered from Faults	1462
Recovered from Failure	30
Uncovered	1
Invalid Experiments	155
Total	2400

No response fault injections and invalid experiments were discarded in the analysis.

Table 1.4.2 shows the breakdown of the detected faults MC and BC for each of the specific failure modes:

- The down state accounts for faults that crashed the MC permanently
- The loss of one input state tabulates all faults where one of the inputs to the DFWCS was corrupted and detected.
- The loss of two inputs state is where both inputs are lost to duel redundant analog input pair.
- The arbitrary output state is defined as any fault that causes the output or the system functionality to deviate from the nominal.

Table 1.4.2: Tabulation of the Fault Response According to the Failure Mode States.

State	Recovered from fault by reconfiguration to BU	Local recovery from Fault on Main CPU	Uncovered fault	Total
Arbitrary Output	0	1281	1	1282
Loss of 1 Input	0	181	0	181
Loss of Both Analog Inputs	140*	0	0	140*
Down	30	0	0	30
				1493

1.4.2.3 Analysis

Two statistics are used to calculate the coverage parameters. The first statistic used is the simple Bernoulli model. The second is the statistics of the extreme model.

The simple Bernoulli model provides a point estimator for the fault coverage, given by the simple average, that is the arithmetic average of *n* observations of the random variable *Y*:

$$\hat{C}_{fm} = \frac{1}{n}\sum_{k=1}^{n}\underline{Y}_k \qquad (1.4.2)$$

where $\hat{C}_{fn}$ is point estimate for the faults associated with a particular failure mode. The mean of the estimator is calculated as

$$E[\hat{C}_{fm}] = E\left[\frac{1}{n}\cdot\sum_{k=1}^{n}\underline{Y}_k\right] = \frac{1}{n}\cdot\sum_{k=1}^{n}E[\underline{Y}_k] = \dot{C}_{fm} \qquad (1.4.3)$$

The unbiased estimator is given by

$$\hat{S}[\hat{C}_{fm}] = \frac{\hat{C}_{fm}(1-\hat{C}_{fm})}{n-1}$$

The single sided 100 γ% confidence interval is instead given by

$$\dot{C}_{fm} > \hat{C}_{fm} - z_{\gamma}\sqrt{\hat{S}[\hat{C}_{fm}]} \qquad (1.4.4)$$

where z_{γ} indicates the 100 γ % standard normal percentile.

For the special case where all the fault injection experiments are covered (e.g., no uncovered faults) the following conservative estimation of coverage was used [22]

$$C_{fn\_low} = 1 - z_{\gamma}\left[\frac{n-1}{n^3}\right]^{1/2} \qquad (1.4.5)$$

For a given desired coverage level, the number of experiments necessary to observe at least one uncovered fault with a certain confidence γ can be calculated as n in the following equation:

$$n = Log_c(1-\gamma) \tag{1.4.6}$$

To assess the confidence if a predicted or specified coverage value is greater or equal to the actual coverage value then the following equations can be used:

$$\begin{aligned} n &= \log_c(1-\gamma) \\ C^n &= (1-\gamma) \\ \gamma &= 1-C^n \end{aligned} \tag{1.4.7}$$

Where γ is the probability of revealing at least one uncovered fault for a given number of observations. In other words, this probability conveys how statistically confident the predicted or specified coverage value is to the actual coverage value.

Table 1.4.3 summarizes the calculations for coverage estimates associated for each state of the MC. The parameter γ is the probability that shows how statistically confident the predicted or specified coverage value is to the actual coverage value Table 1.4.3 that statistics of the extreme is the more pessimistic of the two models. In the last two columns, the low confidence shown in the numbers is due mainly to the low number of observed outcomes for some of the states (e.g. the down state had only 30 observations).

Table 1.4.3: Coverage Estimates for the MC Analytical Model

State	Bernoulli coverage estimate $\hat{C}_{fm\_low}$	Bernoulli Variance $\hat{S}[C_{fm\_low}]$	Bernoulli Single sided confidence interval (95%)	Statistics of the Extreme Coverage estimate with d=3 $\hat{C}_{fm\_ex}$	Statistics of the Extreme Confidence Factor □ Specified C=.9995	Statistics of the Extreme Confidence Factor □ Specified C=.995
Arbitrary output	.9992	6.24x10-7	C_{fm_low}> .9979	C_{fm_ex}=.998	.473	.998
Loss of 1 input	.994	3.31x10-5	C_{fm_low}>.984	C_{fm_ex}=.983	.086	.596
Loss of 2 inputs	.993	5.0x10-5	C_{fm_low}>.981	C_{fm_ex}=.979	.068	.5
Down	.967	1.1x10-3	C_{fm_low}>.912	C_{fm_ex}=.9	.015	.14

1.4.3 Data

Table 1.4.4 shows the the transition rates for MC and BC states based on Table 1.4.3 and the use of a state independent MC and BC failure rate of 3.3 x 10 $^{-6}$/hour that was obtained from the plant data.

Table 1.4.4: Transition rates for MC and BC States Based on Table 1.4.3

MC Transition Rates*	Statistics of the extreme method		Bernoulli method	
	Un-Coverage Parameters Estimates (d=3) $1-\hat{C}_{fm\_ex}$	Failure Rate (/hour) $3.3\text{x}10^{-6}(1-\hat{C}_{fm\_ex})$	Un-Coverage Parameters Estimates $1-\hat{C}_{fm\_low}$	Failure Rate (/hour) $3.3\text{x}10^{-6}(1-\hat{C}_{fm\_low})$
λ_{12}	.017	5.61x10-8	6x10-3	1.98x10-8
λ_{14}	.002	6.6x10-9	8x10-4	2.64x10-9
λ_{24}	.002	6.6x10-9	8x10-4	2.64x10-9
λ_{34}	.002	6.6x10-9	8x10-4	2.64x10-9
λ_{15}	.1	3.3x10-7	.033	1.089x10-7
λ_{23}	.021	6.93x10-8	7x10-3	2.31x10-8

*1:Operating 2: Loss of 1 Input 3:Loss of 2 inputs 4: Arbitrary Output 5: Down

Table 1.4.5 shows the data that were used to represent controller and actuated device failure rates and loss of power.

Table 1.4.5: Controller, Actuated Device and Power Failure Rates

DFWCS Component Name	Failure Rate (per hour)
Main Flow Valve PID controller[1]	3.3 X 10-7
Bypass Flow Valve PID controller [1]	3.3 X 10-7
Spare PID[1] of the PDI controller	3.3 X 10-7
Feed-Water Pump PID[1]	3.3 X 10-7
Main Flow Valve[2]	4.2 x 10-5
Bypass Flow Valve[2]	4.2 x 10-5
Feed-Water Pump [2]	4.2 x 10-5
Loss of power[2]	4.8 X 10-6

[1]Plant data, [2]From [17]

2. THE DFM MODEL

2.1 Introduction

DFM is a methodology implemented in an automated tool that allows an analyst to perform logic analyses and probabilistic assessments of complex systems. This specifically includes systems or subsystems, like digital I&Cs, that exhibit highly dynamic and interactive characteristics. For the DFWCS benchmark, the dynamic system characteristics that are of interest for inclusion in the DFM modeling and analysis are the temporal interactions between hardware/software/firmware, and the environment. The primary objective of the benchmark application documented in this chapter is to demonstrate the DFM capabilities in the specific context of digital I&C system risk modeling and analysis.

To provide the reader with essential information concerning the features and characteristics of the methodology, an overview of DFM is presented in Section 2.2. For more information on the methodology the reader is also referred to NUREG/CR-6942, as well as to a number of earlier publications which contain a variety of examples of modeling and analytical applications ranging from nuclear to space systems, including the modeling of dynamic control systems as well as of dynamic plant-system / human-operator interactions [4-10, 23].

Section 2.3 discusses briefly how DFM can be applied within a traditional plant PRA to focus on systems with dynamic features.

Section 2.4 presents the application of DFM to the DFWCS benchmark system, under the plant operational condition selected for this demonstration. More specifically, Section 2.4 introduces and illustrates the DFWCS DFM model and discusses the deductive and inductive analyses executed with the aid of the DFM DYMONDA^{TM} software tool. The result of these analyses is the identification of DFWCS-related critical event sequences and risk scenarios, along with their associated prime implicants[10]. DFM analytical results are equivalent in information content to the risk scenario and cut-set output provided by traditional PRA models and analytical methods, and as such, they can be similarly quantified and easily integrated into the logic structure of a traditional ET/FT plant PRA. An introductory discussion of how this can be achieved is provided in Section 2.4.4, but the reader should also refer to further discussion provided in Chapter 4 for a more complete illustration of how such an integration can be accomplished in practical terms for results obtained via both DFM and Markov/CCMT analyses.

Section 2.5 summarizes the insights gained in the application of DFM to the DFWCS.

2.2 Overview of DFM

DFM is a multi-valued logic based method, implemented in a graphical modeling environment, which can be used to represent and analyze the functional behavior of dynamic systems [4-10,

[10] In the multi-valued logic analysis of a system, a prime-implicant is a combination of individual conditions or events that automatically implies the occurrence of a system Top Event but which does not contain a smaller combination implying the Top Event. Prime-implicants are the multi-value logic equivalent of binary fault-tree minimal cut-sets.

23]. In DFM, system variables of interest are discretized into a finite number of states and are graphically represented by nodes. Causal and temporal relationships among variables are indicated by directed edges and decision mappings that can be tagged to indicate time transitions, which represent system time-sequential effects in terms of discrete time steps. The DFM model of a system can be analyzed in various modes, inductive and/or deductive, to explicitly identify both success and failure states and scenarios for that system. More specifically, the DFM software tool can be used to determine the system conditions that will lead to a failed or hazardous state (the Top Event). The conditions that lead to a given system state of interest are combinations of basic events and sequences which are called prime implicants. A system prime implicant is the multi-valued logic equivalent of a fault-tree minimal cut-set; the main difference between the two being that prime implicants are defined in terms of system model variables that may assume any logic value from across an arbitrary range of discrete values, as opposed to being limited to a binary set (i.e., true / false, or 0 / 1, etc.). The DFM prime implicants capture the dynamic characteristics of a system failure because they include both the states and timing of the events necessary to lead to a failed state. DFM has a set of integrated features that address both the modeling and quantitative aspects of digital systems safety and risk assessment, as summarized in Section 2.2.1.

The implementation of a DFM model within a traditional PRA framework can be achieved in relatively straightforward fashion by tying key events defined in the ET or FT PRA models to DFM Top Events, which can then be resolved and quantified within the DFM modeling and analysis environment. The basic steps of the DFM technique application are similar, in their most general terms, to those applied in the execution of a traditional PRA approach:

1. construction of a system model;
2. logic analysis of the system model;
3. quantification of risk-relevant events and scenarios.

The reader can refer to NUREG/CR-6942 for a more in-depth discussion of these three essential steps. The principal differences between a PRA and DFM model application can be summarized as follows:

1. a DFM model, unlike an ET and/or FT model, is not scenario or event-specific, but intends to represent the entire functionality of a given system;
2. a DFM model, because of its multi-valued logic and time-logic constructs, can represent system interactions and dynamic characteristics that are very difficult to explicitly model via conventional PRA techniques;
3. because of the characteristic stated in 1 above, and unlike any specific ET or FT model, a DFM model can be logically analyzed for success as well as for failure paths; this can also be done in both inductive (i.e., from cause to effect) and deductive (from effect back to possible causes) mode.

The principal characteristics, both in terms of capabilities and limitations, of the DFM technique are discussed in greater detail in the next section, along with the principal assumptions made in the specific application to the DFWCS system.

2.2.1 Capabilities

As mentioned above, beyond some basic similarities that have also been pointed out, DFM models differ from traditional PRA models in the following key characteristics:

1. Their system representation captures in one model the full range of system functionality, i.e., it is meant to cover both system success and fault space.
2. They employ a multi-valued, rather than binary, logic representation of variables and system states.
3. They explicitly represent, via certain specific features of their system representation constructs, the essential timing and sequencing characteristics of the cause-effect relationships among system variables and states.

Characteristic 1 implies that DFM models exhibit more information content than traditional ET / FT models. While the latter are scenario-specific, (i.e., separate event-trees and fault-trees have to be manually constructed for each initiating event and Top Event of interest) a DFM model is system-specific (i.e., one model constructed in DFM form can represent an entire system or subsystem) and can be analyzed with respect to many different Top Events to understand both success and failure scenarios of that system. Analyses of multiple Top Events with a single DFM model were illustrated in [4, 23]. This was also carried out for the DFWCS, for which two separate Top Events were explicitly analyzed using the same DFM model, as presented in Section 2.4.3.1.

Characteristics 2 and 3 affect the level of fidelity and detail resolution that the DFM methodology offers in comparison with the binary and static PRA model representation.

Because of their characteristics, DFM models offer the analyst the following capabilities:

- the capability to model and analyze feedback loops and time transitions;
- the capability to apply both deductive and inductive automated analyses to its detailed multi-valued logic system models to identify interactive failure modes which, in the analysis of digital I&C systems, often take the form of and have been referred to as software-error forcing contexts:
    - the deductive analysis explores the causality of the system model in reverse, starting from the definition of a system state representing the Top Event of interest, and generates prime implicants – i.e., the multi-valued logic equivalent of fault-tree minimal cut sets;
    - the inductive analysis follows the forward causality flow of the system model, starting from a user defined initial system state, and produces Dynamic Sequence Trees (DSTs), which are automatically generated event sequence scenarios, similar in logic format to system level ET and Event Sequence Diagram representations [24], but containing, unlike the latter, explicit event timing and sequence information[11].
- The capability to quantify, in probabilistic terms, the Top Events analyzed by the deductive analysis module.

[11] Another possible way of referring to DSTs would be dynamic event trees. However, the authors are not using this type of terminology for DFM inductively generated sequences, as the term dynamic event tree is already in use in the PRA community to refer to another specific type of inductive modeling, which presents both similarities and differences with respect to the DFM technique presented here.

- The capability to quantify, also in probabilistic terms, the scenario sequences identified in the inductive analysis mode.

One characteristic of DFM models that is quite important from the practical point of view of PRA framework integration and the analyst's ability to merge and combine DFM-derived analytical results with those of other logic models is that the DFM logic modeling paradigm can be adapted to logic forms that are completely equivalent to those of many other binary logic model environments, including reliability block diagrams (RBDs), event sequence diagrams (ESDs), event-trees (ETs), and fault-trees (FTs). This makes it fully compatible with most traditional reliability model and PRA software. For example, although a DFM model is normally expanded to include multi-valued logic system representation and the tracking of temporal interactions, a DFM model constructed with only binary variables and analyzed deductively will generate the logic structure of a traditional fault tree.

Other noteworthy characteristics of the DFM modeling environment are:

- DFM offers a graphical representation of the cause-effect and time-sequence characteristics of a given system. An analyst can understand and follow the causality and sequential flow within a system and its model.
- A DFM model can be modularized by defining system super-variables and states; this is useful to keep a system model from growing too large and difficult to visually follow and inspect. The underlying models for these super-variables and states can be grouped together to form a library of modeling templates from which DFM models of similar systems can be assembled. As more common logic structures are identified, modeling efforts can be reduced by making use of the available templates instead of constructing the model from the most basic modeling elements. The concept of constructing DFM models from sets of standard, pre-defined building blocks has been discussed at length in earlier publications [5, 25], and a few traditional DFM modeling templates for control systems are explicitly discussed [4].
- The DFM deductive algorithm can be utilized to provide logic analysis and qualitative solution (prime implicants) for both coherent and non-coherent logic structures[12]. This includes non-coherent varieties of the traditional ET and FT binary logic structures used in PRA, which require special, and often cumbersome, handling in current traditional PRA software packages.

[12] In layman terms, non-coherent logic structures are those where the transition of a basic component from one state to another can make the overall system either better or worse, depending on other conditions that may exist in the system itself. Traditional fault-trees are defined when possible to be coherent, i.e., if a basic event in the tree becomes true (binary value 1), the Top Event either remain false (binary value 0) or becomes true (binary value 1), but it will never change in the opposite direction, i.e., from true (binary value 1) to false (binary value 0), which is what may happen if the tree structure is non-coherent. Non-coherent logic models are relatively often encountered in Level 2 nuclear plant PRAs (more specifically in the modeling of post-core-melt containment sequences), and in the safety modeling of space systems and launch-vehicles.

2.2.2 Limitations

As mentioned earlier in the introductory statements concerning the methodology, the DFM modeling paradigm is based on:

1. the discretization into a limited number of states of the continuous variable characteristics of a plant or system, and,
2. the representation of time in terms of discrete time steps and time-transitions.

The number of states chosen to represent a specific system variable is, in theory, arbitrary, but in practice must reflect the definition of ranges in which the variable is subject to a certain type of control or safety regime. The overall number of variables modeled, the number of associated states, and the number of time-steps for a desired analysis condition the computational speed with which a model can be analyzed, especially in deductive mode, to obtain risk-relevant prime-implicants. Thus an overly detailed model, or an analysis that is set to track an excessive number of system time steps, may run into computational problems because there are too many system variable states that must be tracked to execute the system analysis.

DFM users should also be aware that the power of the methodology is in revealing how combinations of component failure modes, even across time boundaries, can result in system failure modes that would otherwise be very difficult to extract with traditional ET/FT PRA reliability models. However, similar to other modeling paradigm, DFM cannot be a substitute for user knowledge nor can it reveal system failure modes whose constituents, i.e., basic-component failure modes, the user has failed to account for at the individual system-component modeling level (i.e., in terms of corresponding variable nodes and states).

More limitations and caveats to keep in mind while constructing and analyzing a DFM model are summarized below:

- Creation of a DFM model requires technical knowledge of the behavior of the system being analyzed, and in some cases, the availability of system simulation results from a full blown continuous time/state simulator. This is not a true methodology limitation; rather it is a general pre-requisite when a need exists to represent the behavior of a system at a high level of fidelity. A system simulator would, for example, provide model validation and confirmation that would be necessary for application of the DFM technique in the nuclear regulatory and safety arena.
- The continuous variables represented in the model, for example the SG level in the benchmark DFWCS model, must be discretized in such a way as to balance the model fidelity versus complexity and analysis time. The user should not expect to use DFM to represent and track relatively small, and typically inconsequential, fluctuations of these continuous variables.
- Construction of the DFM decision tables that capture the detailed cause-effect relations among system variables is a process that requires time and care.
- The number of time steps that can be analyzed in deductive mode is limited by computational constraints.

2.2.3 General Considerations and Recommendation Concerning DFM Modeling

2.2.3.1 Model Level of Detail

There is no pre-set rule for the level of detail that the analyst should use in the representation of a system via DFM. The number of variable nodes and the number of discrete states selected to represent the range of each variable is what ultimately determines the model degree of fidelity, its complexity, and the computational power required to analyze it, especially in deductive mode when the backtracking desired is across a few time steps.

The DFWCS model analyzed in this study can be considered a good example of the level of complexity that can be handled by the current version of the DFM analytical engine without recurring to special modeling and analysis strategies, such as hierarchical modularization of the system model and of the associated analyses. That particular model includes approximately 40 variable nodes, each with an average of 4 discrete states, which yields a theoretical maximum overall number of system states that are represented within the model in the order of 40^4, i.e., about 2.6 million states.

2.2.3.2 Deductive and Inductive DFM analysis Modes

As mentioned earlier, a key characteristic of the DFM methodology is that its associated analytical engine (implemented in the commercially available DYMONDA^{TM} software) can execute both inductive (from cause to effect) and deductive (from effect to root-cause) logic analysis of a system model, once a system model has been constructed. In fact there are a few different types of analysis of either type that can be carried and have been documented in past studies, including a form of multi-valued logic ATVG[13.] Regardless of the type of analysis that is to be executed, the number of scenarios or system sequences that can be generated by the computer-assisted analysis from a DFM system model is theoretically unlimited. In practice, however, an upper limit for this number is determined once the level of detail applied in the modeling, i.e., the number of system variables explicitly represented and the number of states chosen to represent each individual variable, is set (see Section 2.2.3.1 above). Moreover, if a model is developed with exceedingly high level of detail, i.e., high combinatorial number of implicitly system states, it may become difficult for the DFM analytical software engine to analyze it in complete fashion, especially in the deductive, FT-like mode.

In the DFWCS application illustrated in Section 2.4, inductive and deductive DFM analyses were employed. In this chapter and in the rest of this report the terms inductive analysis and deductive analysis, when referred to DFM, shall be meant to indicate the types of analyses described immediately below in this section.

In the inductive analysis of a model, the DFM analytical algorithm can proceed from a system

[13] Automated Test Vector Generation: a process applied in its binary form in the generation of test sequences for digital circuits, specifically with the objective of detecting, exclusively via the application of external inputs and the observation of circuit outputs, possible faults within a device whose internal states cannot be otherwise determined. The DFM generalization of this process makes it possible to follow the same type of procedure for non-binary devices or systems, such as MEMS (Micro Electro-Mechanical Systems) and hybrid (i.e., mixed digital and analog) circuits.

initial condition (which may represent a PRA-style initiating event, or some other system initial state) and identify the system states evolution by marching forward in causal-chain and time-steps (qualitatively identified within the model as system state and variable state transitions). The product of this kind of analysis is the identification of system scenario event sequences, in a form that is similar to that produced by a discrete event simulation technique. In Section 2.2.1 the authors introduced the term Dynamic Sequence Tree (DST) to refer to the product of this type of inductive DFM model analysis.

In the deductive analysis, the DFM algorithm proceeds from a user-provided definition of Top Events of interest. The definition of a Top Event in the DFM paradigm is quite broader than what is normally seen in the fault-tree paradigm, in that a DFM Top Event can be defined as an arbitrary combination of variable states, including changes of states from one time-step to another. Given any such definition, the DFM deductive engine identifies all the possible Top Event prime implicants, which, as the authors have previously mentioned in Section 2.2.1, can be considered to be the multi-valued logic equivalent of binary-logic minimal cut sets.

The value of the deductive analysis mode is that the algorithms that implement it have been proven to provide the complete set of prime-implicants relative to a given Top Event. In contrast to this, the product of any inductive analysis, regardless whether applied within DFM or within another model paradigm, always depends on the definition of the user-provided, or combinatorially-constructed, sets of hypothesized initial conditions from which the analysis proceeds.

For the above reasons, it is recommended to use inductive and deductive analysis in combination. A possible practical and effective way of doing this, the detailed implementation of which will be clarified by the more detailed descriptions and discussions of DFM modeling provided in the remainder of this Chapter, is as follows:

1. While the model is being constructed and validated, use inductive analysis to verify that the model representation of the system corresponds to the known system functional behavior under nominal unfaulted conditions.
2. Once the model has been finalized and validated, perform deductive analyses for all system faulted states (i.e., Top Events) of interest.
3. If necessary to further explore and understand specific system failure scenarios and/or fault-space areas (for which the analyst felt that the initial level of detail of the model explored deductively may not have been completely adequate):
    a. refine the DFM model accordingly (e.g., by introducing a finer discretization of variable states and/or time steps in selected areas of the model suggested by the deductive analyses of Step 2), and
    b. inductively execute detailed system event sequence simulation analyses, using as initial system states the prime implicant definitions identified by the deductive analysis and introducing.

Another noteworthy characteristic of DFM concerns the quantification of results; more specifically, the process by which DFM can produce probability values for Top Events that have been deductively analyzed. The DFM quantification algorithm is capable of producing an exact probability calculation rather than a numerical approximation of the probability value (e.g., along the lines of the minimal cut-set upper bound approximation to Top Event probability commonly utilized in fault-tree analysis codes). This is done by logic manipulation of the Top Event prime implicants into a logically-equivalent set of mutually exclusive implicants (MEIs), so that the Top Event probability can be obtained as the sum of the MEI probabilities. This procedure is the multi-valued logic equivalent of the BDD (Binary Decision Diagram) quantification technique of binary fault-tree structures.

2.3 DFM Modeling within a PRA framework

The integration of advanced risk models and analyses developed by means of the dynamic methods DFM and Markov/CCMT, with a traditional plant PRA developed with traditional ET/FT methodology, is the subject of a detailed discussion and demonstration presented in Chapter 4. In this section the authors anticipate some of the concepts and processes discussed in that chapter, specifically with respect to those essential aspects that are pertinent to the integration and utilization of DFM models and results.

To discuss how a traditional-PRA / DFM model and analysis integration can be executed and handled, the authors may assume that a PRA analysis is to be conducted with respect to a specific plant where one or more digital I&C systems exist, with potential risk-relevant dynamic and interactive characteristics. Under these circumstances, the authors also assume that, besides the traditional ET and FT models covering the conventional portions of the plant, a DFM model may be developed to cover and represent, at a minimum, the digital I&C systems and any portions of other plant systems that may be directly interfacing, and closely interacting, with them.

The initial steps of the PRA execution process start and proceed as usual, i.e., developing master logic diagrams (MLDs), event tree scenarios and system / subsystem fault trees, until one or more of the following three situations is encountered:

1. The initiating event of an event-tree in the plant PRA concerns the failure of a digital I&C or other system that exhibits dynamic characteristics.
2. A pivotal event in an event-tree of the plant PRA concerns the failure of a digital I&C and/or dynamic system.
3. An intermediate event of a fault-tree of the plant PRA concerns the failure of a digital I&C and/or dynamic system.

In all three cases, the probability (or frequency) of occurrence of the event(s) concerning the digital I&C / dynamic system can be derived by utilizing a DFM model of that system that, as mentioned above, will have to have been developed in parallel with the traditional PRA ET / FT models of the rest of the plant. Such a model will have to be analyzed and its prime-implicant results quantified per the steps outlined in Section 2.2 above and illustrated below in Section 2.4.

The reader is referred to Chapter 4 for a detailed discussion of the exact processes that can be applied to accomplish a PRA / DFM integration, and of the key technical issues related to the possible sub-cases of the situations that may be encountered. Here, the authors provide a summarized version of that discussion, pointing out that in all three cases listed above, a specific digital I&C / dynamic system event can be identified that can also be further defined, analyzed, and quantified via DFM analysis. The translation of the definition of such a traditional PRA event into an equivalent DFM form is quite straightforward, because of the intrinsic inter-compatibility of the DFM multi-valued logic constructs with the PRA binary ones.

In all of the three cases, regardless of whether the event of interest appears in the PRA framework as an ET initiating or pivotal event, or as an FT intermediate event, the DFM analysis will be able to proceed by defining a DFM Top Event that is equivalent to it in both its engineering meaning and in its formal-logic definition. From such a definition, a deductive DFM analysis can then proceed to the identification of its prime implicants, and lead to quantification via the procedures discussed earlier in Section 2.2. DFM inductive analyses can also be applied as a means of validating the DFM model and deductive analysis, and of providing user-insight into the step-by-step sequencing of events and cause-effect chains in a given risk scenario.

2.3.1 DFWCS Event of Interest as PRA Scenario Initiating Events

In a typical plant PRA, a reactor trip or a turbine trip, respectively, caused by low steam generator level and high steam generator level, is one of the significant risk scenario initiating events considered in this study. In terms of the DFWCS behavior, the low steam generator level event equates to the DFWCS failing low and high steam generator level event equates to the DFWCS failing high.

Traditional PRA ET models illustrating risk scenarios that proceed from these basic categories of DFWCS initiating events are shown in Figs. 2.3.1 and 2.3.2.

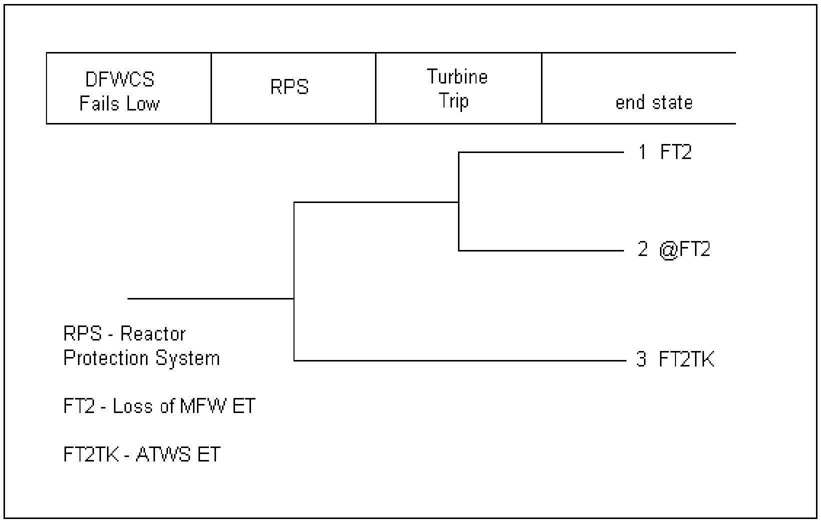


Figure 2.3.1: Event Tree for DFWCS Failing Low

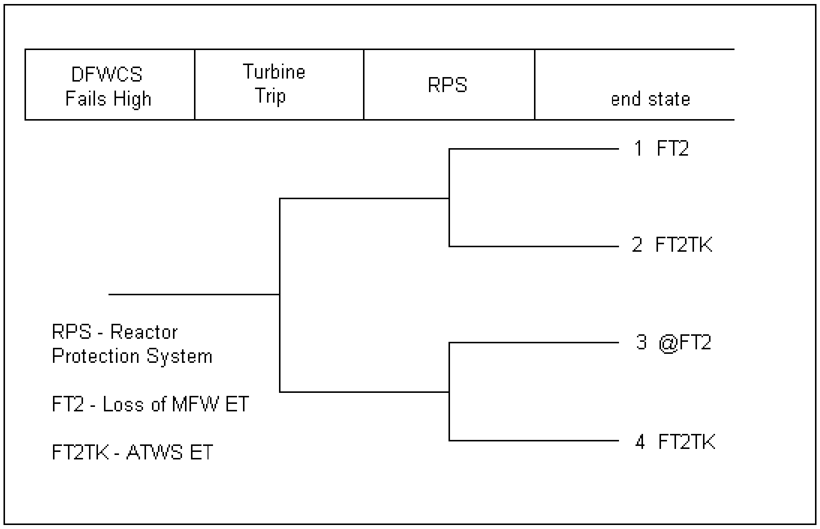


Figure 2.3.2: Event Tree for DFWCS Failing High

The ET end states of the event-tree sequences shown in the figures are transfer-events linking the former to continuation ETs (indicated by the identifiers FT2, @FT2, FT2TK), which are not shown. The two ETs are very similar and lead to the same set of end-states / transfer-events. The difference between the two is determined by the plant-trip logic; which, upon a high steam generator condition, calls immediately for a turbine trip to prevent damage to the plant turbines from water carried along with the steam because of the high water level in the SGs. Whereas, upon a low steam generator condition, this logic calls for a reactor trip (RPS actuation) to prevent drying out the SGs due to excessive power being transferred from the plant primary circuit. In the first situation, a reactor trip automatically follows the turbine trip. In the latter, the opposite occurs. Please note the following notation used in the figures:

MFW = Main Feed-Water
ATWS = Anticipated Transient Without Scram

In line with the discussion above, if the above ETs are assumed to have been developed as part of a conventional PRA modeling effort, the development of the DFWCS low and high events would then be recognized to involve the modeling of a digital I&C system with potentially complex dynamic and interactive characteristics. Accordingly, in order to determine the probability for the two associated initiating events, the DFM model of the DFWCS benchmark system is utilized. This is done instead of expanding these events with fault tree models as would be normally done, at some level of detail, in a traditional PRA. In this demonstration, a DFM model of the DFWCS was constructed and solved with respect to the low failure Top Event and the high failure Top Event. The results of the analyses were then incorporated into the traditional PRA models shown in Fig. 2.3.1 and Fig. 2.3.2.

2.4 Application of DFM to the Benchmark System Scenario

This section presents the application of DFM to the benchmark DFWCS. As mentioned earlier in Chapter 1, the DFWCS was selected as the benchmark system to be analyzed because, historically, the feed-water system of a nuclear power plant, although not a safety system by definition, has been a major contributor to plant trip events. Such events are potential challenges to the plant safety systems and, as such, are among the significant accident scenario initiating events analyzed in traditional plant PRAs.

The assumptions made in the DFM analysis are discussed below in Section 2.4.1. The construction of the system model is discussed in Section 2.4.2. The analysis and quantification of the system model is discussed in Section 2.4.3, and finally the incorporation of the solution into a hypothetical plant PRA is briefly discussed in Section 2.4.4.

2.4.1 Model Assumptions

In the following demonstration, it is assumed that the DFWCS of interest is the benchmark digital I&C system illustrated in Chapter 1. The DFWCS can either fail low, i.e. in such a way as to cause a low steam-generator level, or fail high, i.e. in such a way as to cause a high steam-generator level. These two conditions lead to the event sequences shown earlier in Fig.2.3.1 and Fig.2.3.2, respectively.

The development of the DFM model of the DFWCS benchmark system was executed under the set of general assumptions that have been discussed in Section 1.3. Accordingly, the model development reflects the following:

1. Because the reference DFWCS nuclear power plant is assumed to have two identical and independent steam generators, the DFM model only includes one steam generator and associated DFWCS control functions, along a relatively simple rendition of the power input from the plant primary side.
2. The physical behavior of the steam generator modeled is assumed to be well represented by the simulator developed for NUREG/CR-6465. Therefore, the definition of the discrete parameter state cause-effect relationships and time-dependencies represented in the DFM model is a discrete-state rendition of the equations and physical models included in that simulator.
3. The DFM model represents in discrete-state form the SG control logic and control equations documented in NUREG/CR-6942.
4. The DFM model includes the representation of hardware/software/firmware component failure modes. Hardware failure modes are assumed to be covered by the FMEA (Failure Mode and Effects Analysis) performed specifically for this project. Software is not being treated as a separate entity, but as embedded in hardware as firmware. Hardware components such as pumps and valves, once failed, are assumed to remain in the failed state. Software failure modes are assumed to affect certain DFWCS various kinds, e.g., high or low output, stuck-at values, and arbitrary values. If a software function failure is detectable and is backed up by a redundant controller or computer, the function is assumed to be recoverable via switch-over to the back-up unit that may be available. Only the failure modes covered by the failure rate derivations carried out by the University of Virginia (see Section 1.4) are included at the basic component level of the DFM model and utilized in the execution of the DFM analysis and quantification processes.
5. No attempt is made to explicitly pursue in the DFM model analysis the identification of system failure modes associated with possible design or specification errors concerning the system or software. However, the model does provide a partial validation of the design logic by showing that the DFWCS performs its functions successfully under the explored nominal condition, unless specific component faults are assumed to be present.

6. For its quantification process, the DFM analysis of the DFWCS system uses the failure rates of the benchmark system controllers and computers estimated by the University of Virginia by means of the fault-injection testing technique discussed in Section 1.4.
7. The power maneuver described in Section 1.3.2.3.2 is assumed to represent the typical behavior of the DFCWS.

2.4.2 DFM Model Construction for the Benchmark System

The DFM model developed to analyze the benchmark system is shown in Fig.2.4.1. This model encompasses the Main Computer, the Backup Computer, the BFV, the BFV controller, the FP, the FP controller, the MFV, the MFV controller, the PDI controller, the inputs and outputs for the main and backup computers, and the control law and logic for maintaining the SG level. Thus, the plant process and hardware, the digital hardware, the digital software, and their interactions are all included and represented in the same model.

The process variable nodes are used to represent the key process parameters or states of key components. These process variable nodes are listed in Table 2.4.1. For example, node L represents the SG Level, a key physical process parameter. Whereas, node MFV models the state of the Main Flow Valve/Controller, a key component of the system. These process variables nodes are each discretized into a finite number of states. The nodes highlighted in Table 2.4.1 are the ones that will be referred to later in this chapter, and the discretization schemes for these nodes are shown in Table 2.4.2 through Table 2.4.9. For process parameters, the discretization corresponds to a discrete representation of the possible range that the continuous variable can take, such as the one shown for the SG level in Table 2.4.4. On the other hand, for component states, the discretization reflects the failure modes that are assumed, such as the one shown for the Main Flow Valve/Controller in Table 2.4.6.

The DFM process variable nodes are graphically linked together to model the relationship between these nodes. In general, two types are relationships are represented:

1. Physical relationship with or without a timing element,
2. Logical.

An example of a temporal relationship is represented by the transfer box Tf2. This transfer box originally appears on the top center portion of the complete model (Fig.2.4.1), and a zoomed view is provided in Fig.2.4.2. Transfer box Tf2 shows that the current SG level depends on the steam flow, the total feed flow and the previous SG level. The detailed transfer function between the nodes is summarized in the associated decision table (Table 2.4 10).

An example of a logical relationship is represented by the transfer box Tf9. This transfer box originally appears on the bottom left portion of the complete model (Fig.2.4.1), and a zoomed view is provided in Fig.2.4.3. Transfer box Tf9 shows how the failure modes of the Main Flow Valve/Controller affect the system. In particular, the current state of the Main Flow Valve/Controller is determined by the failure transition of the MFV controller (MFV-T), the previous state of the MFV controller (MFV-P), and the power to the controllers (C-Pow). The reader should note that, since none of the failure modes were assumed to be repairable, the MFV controller, once failed in a particular mode, will stay in the same failure state. This is consistent with Assumption 4 discussed previously. The detailed transfer function between the nodes is summarized in the associated decision table (Table 2.4 11).

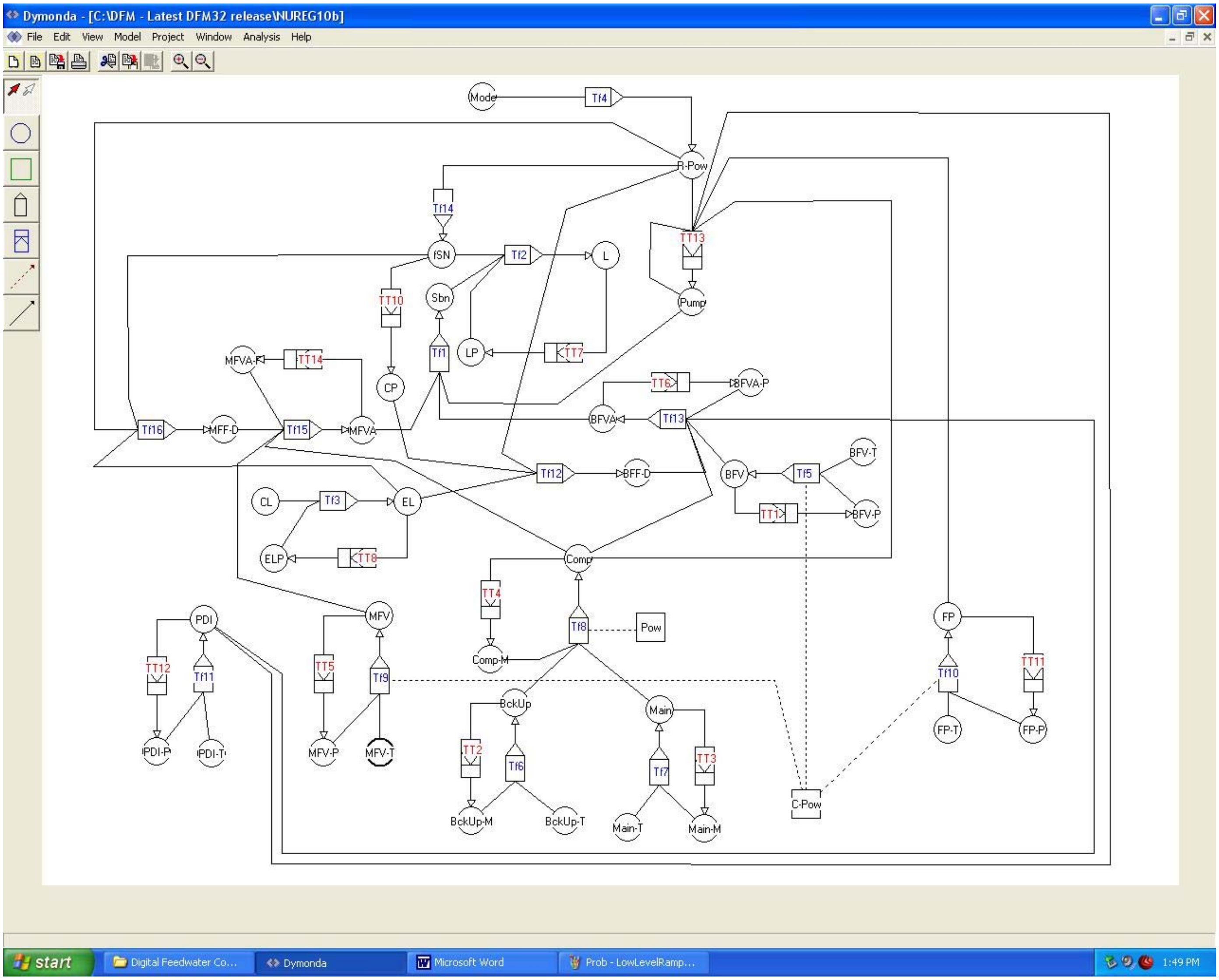


Figure 2.4.1: DFM Model of the Benchmark System

Table 2.4.1: List of Process Variable Nodes in the Benchmark System DFM Model

Node	Description
Bckup	Backup computer
Bckup-M	Previous state of the backup computer
Bckup-T	Transition of the backup computer
BFF-D	Bypass feed flow demand
BFV	Bypass flow valve and BFV controller
BFV-P	Previous state of BFV and BFV controller
BFV-T	Transition of BFV and BFV controller
BFVA	Bypass flow valve aperture
BFVA-P	Previous BFV aperture
C-Pow	Power to the controllers
CL	Compensated level
Comp	Computers (main & backup)
Comp-M	Previous state of the computers
CP	Compensated power
EL	SG level error
ELP	Previous SG level error
FP	Feed pump
FP-P	Previous state of the feed pump
FP-T	Transition of the feed pump
fSN	Steam flow
L	SG level
LP	Previous SG level
Main	Main computer
Main-M	Previous state of the main computer
Main-T	Transition of the main computer
MFF-D	Main feed flow demand
MFV	Main flow valve and MFV controller
MFV-P	Previous state of MFV and MFV controller
MFV-T	Transition of MFV and MFV controller
MFVA	Main flow valve aperture
MFVA-P	Previous MFV aperture
Mode	Operating mode of the reactor
PDI	PDI controller
PDI-P	Previous state of the PDI controller
PDI-T	Transition of the PDI controller
Pow	Power to the computers
Pump	Feed pump speed
R-Pow	Reactor power
Sbn	Total feed flow

Table 2.4.2: Discretization of the Controller Power (Node C-Pow)

State	Description
Op	Operating
No	No power

Table 2.4.3: Discretization of the Steam Flow (Node fSN)

State	Description
0	< 15% of Maximum
1	[15, 70%) of Maximum
2	[70, 74%) of Maximum
3	[74, 78%) of Maximum
4	[78, 100%] of Maximum

Table 2.4.4: Discretization of the SG Level (Node L)

State	Description
-2	< -2 ft
-1	[-2, -0.17) ft
0	[-0.17, 0.17) ft
+1	[0.17, 2.5] ft
+2	> 2.5 ft

Table 2.4.5: Discretization of the Previous SG Level (Node LP)

State	Description
-2	< -2 ft
-1	[-2, -0.17) ft
0	[-0.17, 0.17) ft
+1	[0.17, 2.5] ft
+2	> 2.5 ft

Table 2.4.6: Discretization of the Main Flow Valve/Controller (Node MFV)

State	Description
Comm	Operating and communicating
No-Comm	Not communicating
High	Output high
Low	Output low
Arb	Arbitrary output
Zero	Zero output
Stuck	Stuck

Table 2.4.7: Discretization of the Previous State of the Main Flow Valve/Controller (Node MFV-P)

State	Description
Comm	Operating and communicating
No-Comm	Not communicating
High	Output high
Low	Output low
Arb	Arbitrary output
Zero	Zero output
Stuck	Stuck

Table 2.4.8: Discretization of the State Transition of the Main Flow Valve/Controller (Node MFV-T)

State	Description
Comm	Transition to operating & communicating
No-Comm	Transition to not communicating
High	Transition to output high
Low	Transition to output low
Arb	Transition to arbitrary output
Zero	Transition to zero output
Stuck	Transition to stuck

Table 2.4.9: Discretization of the Total Feed Flow (Node Sbn)

State	Description
0	< 15% of Maximum
1	[15, 70%) of Maximum
2	[70, 74%) of Maximum
3	[74, 78%) of Maximum
4	[78, 100%] of Maximum

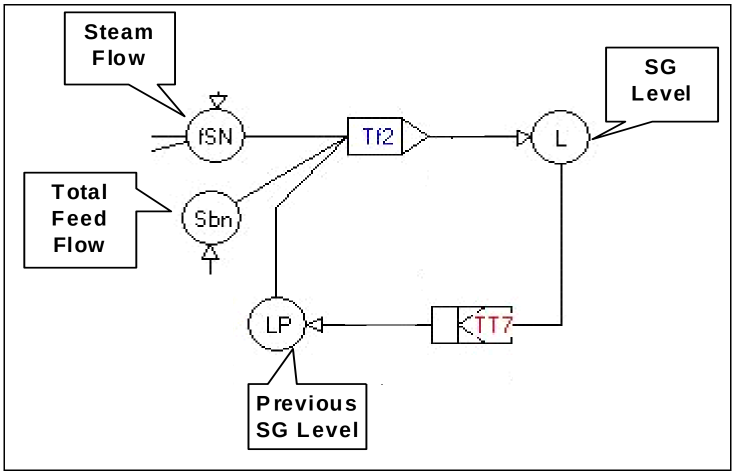


Figure 2.4.2: Zoomed View of Transfer Box Tf2

Table 2.4.10: Decision Table for the Transfer Box Tf2

Total Feed Flow (Sbn)	Steam Flow (fSN)	Previous SG Level (LP)	**Current SG Level (L)**
0	0	-2	**-2**
0	0	-1	**-1**
0	0	0	**0**
0	0	+1	**+1**
0	0	+2	**+2**
0	1	-2	**-2**
0	1	-1	**-2**
0	1	0	**-1**
0	1	+1	**0**
0	1	+2	**+1**
:	:	:	**:**

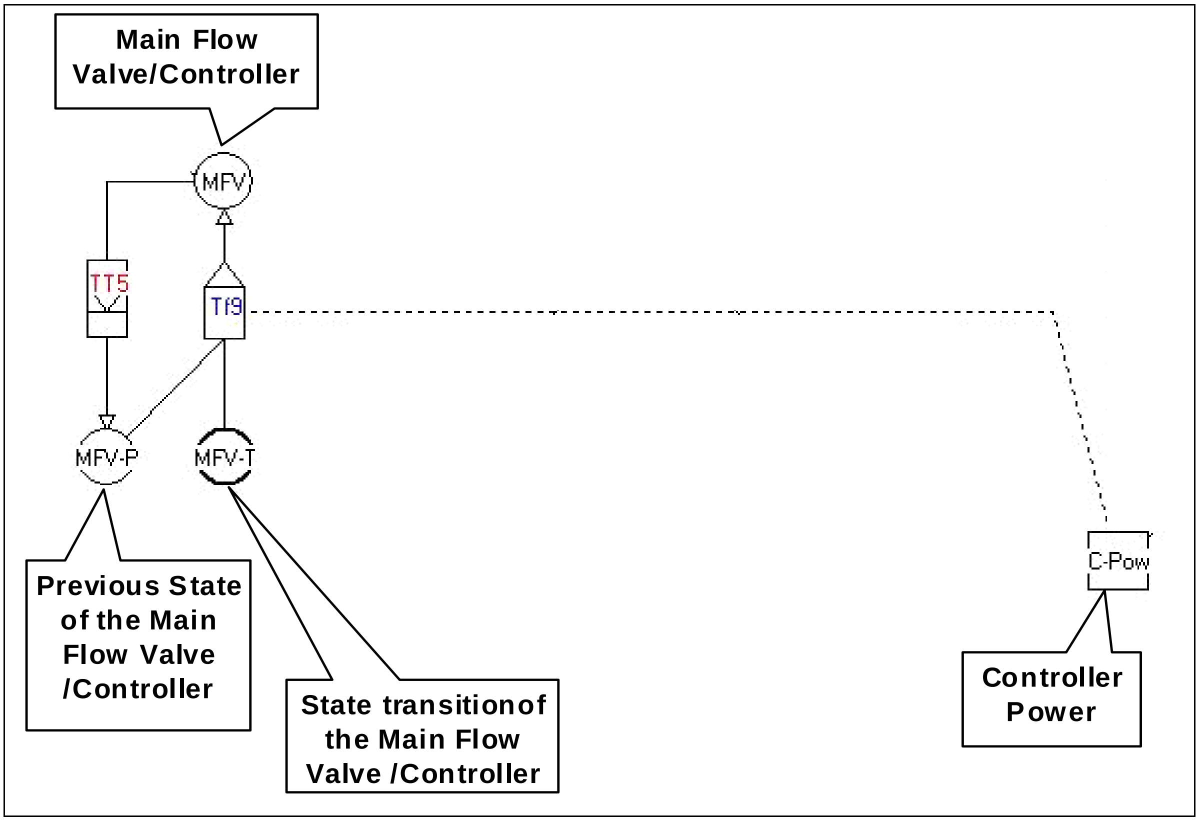

Main Flow Valve/Controller
MFV
TT5
Tf9
MFV-P
MFV-T
C-Pow
Previous State of the Main Flow Valve /Controller
State transitionof the Main Flow Valve /Controller
Controller Power

Figure 2.4.3: Zoomed View of Transfer Box Tf9

Table 2.4.11: Decision Table for the Transfer Box Tf9

Previous state of the Main Flow Valve /Controller (MFV-P)	State transition of the Main Flow Valve /Controller (MFV-T)	Controller power (C-Pow)	**Current state of the Main Flow Valve /Controller (MFV)**
Comm	Comm	Op	**Comm**
Comm	No-Comm	Op	**No-Comm**
Comm	High	Op	**High**
Comm	Low	Op	**Low**
Comm	Arb	Op	**Arb**
Comm	Zero	-	**Zero**
Comm	Stuck	Op	**Stuck**
No-Comm	-	Op	**No-Comm**
Stuck	-	Op	**Stuck**
Zero	-	-	**Zero**
Arb	-	Op	**Arb**
Low	-	Op	**Low**
High	-	Op	**High**
-	-	No	**Zero**

2.4.3 DFM Model Analysis for the Power Excursion Scenario

This section presents a demonstration of the two ways, deductive and inductive, in which a DFM model can be analyzed. Deductive analysis is performed backwards by tracing effects to their respective causes while inductive analysis is performed by following the causes to their effects. As discussed previously in this chapter, the power of the deductive analysis mode is in the fact that the algorithms that implement it have been proven to provide the complete set of prime-implicants relative to a given Top Event. In contrast to this, the product of any inductive analysis, regardless whether applied within DFM or within another model paradigm, always depends on the definition of the user-provided, or combinatorially-constructed, sets of hypothesized initial conditions from which the analysis proceeds. Earlier in this chapter, the authors suggested that a practical and effective way of combining the deductive and inductive techniques is to first identify and quantify the failure modes via the deductive technique, and then confirm the failure modes identified by using the inductive technique with those failure modes assumed as initial conditions.

Once the DFM model and the decision tables are constructed, deductive and inductive DFM analysis techniques are applied to identify potential faults in the system and to investigate the effects of basic component failure modes on the system performance. Two deductive analysis examples are provided in Section 2.4.3.1. These two deductive analyses explore the Top Events corresponding to a low SG level and a high SG level. In addition, two inductive analysis examples are presented in Section 2.4.3.2. These two inductive analyses confirm the failure modes identified by the low SG level deductive analysis and the high SG level deductive analysis. In addition, the inductive analyses provide insights with respect to the sequence of intermediate events that progress from the initial failures to the final outcomes. These analyses illustrate that multiple Top Events and multiple initial conditions can be investigated with a single DFM model.

The reader should note that the deductive and inductive techniques demonstrated here, are not the only analysis supported by DFM. In fact, DFM supports a range of analysis techniques, from failure and fault analysis to automated test vector generation. Readers interested in these other techniques should refer to the more in-depth discussion in NUREG/CR-6942.

2.4.3.1 Deductive Analysis and Quantification for the Power Excursion Scenario

For the benchmark system, failure and fault analyses using the deductive technique were carried out to derive the prime implicants for a failed state of the DFWCS. In support of the initiating events for the event trees shown in Fig.2.3.1 and Fig.2.3.2, the two Top Events of interest are low SG level and high SG level. The deductive analysis and quantification of these two Top Events are discussed in Section 2.4.3.1.1 and Section 2.4.3.1.2.

2.4.3.1.1 Deductive Analysis and Quantification for Low SG Level

The Top Event defined here describes failure of the DFWCS by allowing the level in SG to become too low. A failure and fault analysis was conducted in deductive mode to identify the digital system prime implicants for a low SG level during the power excursion maneuver identified in Chapter 1. The reactor power profile is repeated here in Fig.2.4.4. The analysis concentrated on identifying prime implicants for a SG low level failure state occurring in the eight hours of the power ramp-up maneuver, given the system starts in a state with no failed components. The focus is on the ramp-up phase because the DFWCS is most vulnerable to the low failure during this phase. Specifically, if the change in feed flow cannot match the increase in steam flow, the SG level can drop and lead to a reactor trip condition. The assumption regarding no prior failed components forces the analysis to identify the absolute minimum conditions that would lead to the undesirable low SG level outcome.

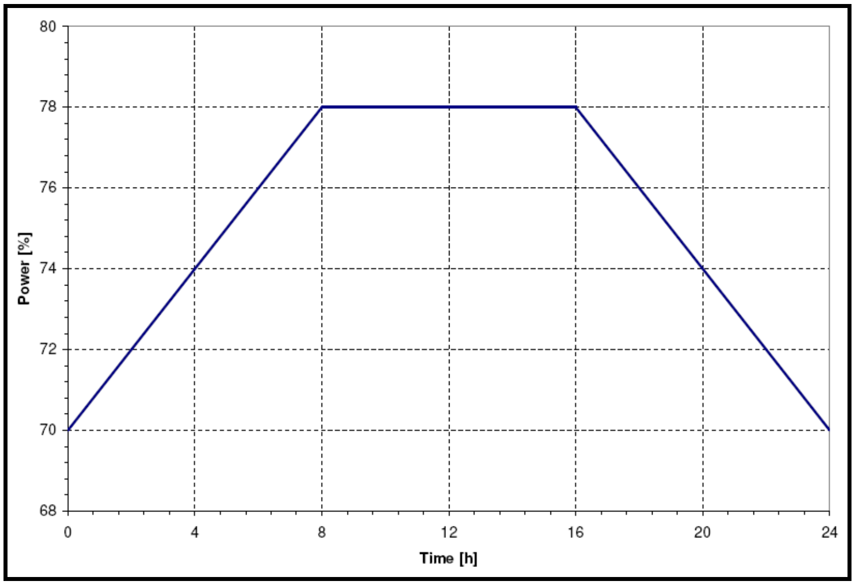


Figure 2.4.4: Reactor Power Profile for the Power Excursion Scenario

In this analysis, the time step *t = 0* refers to the 78% power steady-state that follows the end of the initial 8 hour ramp-up period, whereas the time step *t = -1* refers to the initial 8 hour ramp-up period. With these time-step definitions, the SG Low Level Top Event was defined in detail to include the definition of corollary plant parameter states and conditions. Table 2.4.12 provides the description of the conditions that are included in the Top Event definition.

Table 2.4.12: Low SG Level Top Event Definition (Deductive analysis)

DFM Node State	Time Stamp	Meaning
L = -2	0	SG level reaches the lowest state
LP = 0	-1	SG level was at the nominal state
C-Pow = Op	-1	Power to the controllers was initially available
Pow = Op	-1	Power to the computers was initially available
BckUp-M = OP	-1	Backup computer was initially operational
BFV-P = Comm	-1	Bypass flow valve/controller was initially operational
Comp-M = OP-MC	-1	The main computer was initially working as the primary
FP-P = Comm	-1	Feed pump controller was initially operational
Main-M = OP	-1	Main computer was initially operational
MFVA-P = 2	-1	Main feed flow was initially at 70% prior to the ramp-up maneuver
MFV-P = Comm	-1	Main flow valve/controller was initially operational
PDI-P = OP	-1	PDI controller was initially operational

The key transition in this Top Event is summarized in the first 2 rows highlighted in yellow. It corresponds to the progression of the SG level from normal (state 0) to low (state –2). In the DFM terminology, the Top Event definition is represented in the transition table format shown in Table 2.4.13. The header row shows the nodes and their associated time stamp and row 1 shows the combination of the states for the nodes of interest.

Table 2.4.13: Transition Table for the Top Event

L t = 0	LP t = -1	C-Pow t = -1	Pow t = -1	…	PDI-P t = 0
-2	0	Op	Op	…	Op

In the deductive analysis, the DFM software tool analytical engine starts at the Top Event and then tracks the DFWCS model backwards in time and causality. An illustration of deductive analysis is given here. With the analysis time set to 0, the decision table for transfer box Tf2 is first used to expand the initial state combination shown in Table 2.4.13. This expansion spells out the combinations of steam flow, feed flow and previous SG level that give rise to the lowest SG level state. The result of the expansion is the transition table shown in Table 2.4.14.

Table 2.4.14: Transition Table for after the first expansion

fSN t = 0	Sbn t = 0	LP t = 0	LP t = -1	C-Pow t = -1	…	PDI-P t = 0
-	0	-2	0	Op	…	Op
4	2	-1	0	Op	…	Op
1	0	-1	0	Op	…	Op
1	1	-2	0	Op	…	Op
4	-	-2	0	Op	…	Op
:	:	:	:	:	:	:

To continue the deductive analysis, the causality shown in the model is further backtracked. For the transition table shown in Table 2.4.14, the column corresponding to Sbn @ t = 0 is next expanded with the decision table for transfer box Tf1.

The deductive state expansion process is repeated, along with the application of logic reduction and static and dynamic logic consistency rules that are implemented in the DFM solution engine, until the whole model is traversed backwards for the number of time steps specified. In the example discussed here, this corresponded to one 8 hr timespan. For the Top Event specified, the DFM analysis yielded 1197 prime implicants. These prime implicants contain the combinations of basic events that could cause the Top Event, with none of these implicants being contained in another (hence the denomination prime). As mentioned earlier, prime implicants are essentially the multi-valued logic equivalent of binary minimal cut sets appearing in a fault tree analysis.

The prime implicants for the Low SG Level Top Event found via the DFM deductive analysis were ordered from the highest to lowest probability of occurrence. The 6 top prime implicants (each with the probability of occurrence > 1% of the top contributor) are shown in Table 2.4.15. The events corresponding to components remaining in the good states are filtered out from the raw prime implicants, leaving the key component failure transition(s) (highlighted in red in Table 2.4.15), the boundary conditions (the initial SG level and the reactor power profile), and essential states for distinguishing prime implicants with the same failure transition(s). For example, examination of the prime implicants listed in Table 2.4.15 shows that the key failure event in the primary contributor to the low SG level is the failure of the main feed valve being stuck in the 70 –74% position (MFV-T = Stuck @ t = -1 $\cap$ MFVA-P = 2 @ t = -1 in prime implicants #1 and 2). The increase in steam flow cannot be matched by an increase in feed flow, causing the SG level to drop and to eventually reach the low level. In addition, the key failure events in the secondary contributors to the low SG level are the failure of the controller power (prime implicants #3 and 4, C-Pow transitioning from operating to no power) and the failure of the computer power (prime implicants #5 and 6, Pow transitioning from operating to no power). Either failure will cause the main feed valve to close, and neither failure can be recovered by the PDI controller, causing the SG level to drop and to eventually reach the low level.

Table 2.4.15: Top Prime Implicants for Low Steam Generator Level

(Key failure transition shown in red, distinguishing boundary condition shown in blue)

#	Prime Implicant	Probability

1	Mode = 1 @ t = 0
	PDI-T = Op @ t = -1
	MFV-T = Stuck @ t = -1
	MFV-P = Comm @ t = -1
	MFVA-P = 2 @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		3.33E-04

2	Mode = 1 @ t = 0
	BFV-T = Comm @ t = -1
	MFV-T = Stuck @ t = -1
	MFV-P = Comm @ t = -1
	MFVA-P = 2 @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		3.33E-04

3	Mode = 1 @ t = 0
	PDI-T = Op @ t = -1
	C-Pow = No @ t = 0
	C-Pow = Op @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		3.86E-05

4	Mode = 1 @ t = 0
	BFV-T = Comm @ t = 0
	C-Pow = No @ t = 0
	C-Pow = Op @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		3.86E-05

5	Mode = 1 @ t = 0
	PDI-T = Op @ t = -1
	Pow = No @ t = 0
	Pow = Op @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		3.86E-05

6	Mode = 1 @ t = 0
	BFV-T = Comm @ t = -1
	Pow = No @ t = 0
	Pow = Op @ t = -1
	LP = 0 @ t = -1
	7. Mode = 1 @ t = -1
		3.86E-05

In addition to quantifying the individual prime implicants, the DFM analysis also produces an exact (as opposed to computationally approximated) estimation of the probability of the Top Event. As discussed in NUREG/CR-6942, the DFM software tool first converts the set of prime implicants into a set of mutually exclusive implicants and then sums the probabilities for the mutually exclusive implicants to obtain the Top Event probability, as symbolically summarized below:

Step 1 – Prime implicant results of deductive analysis:

$$Top\ Event = \bigcup_{i=1}^{1197} \mathrm{Pr}\,ime\ \mathrm{Im}\,plicant_i\ ,$$

where

Prime Implicant #i $\not\subset$ Prime Implicant #j for $i \neq j$
Step 2 – Expression of Top Event as set of Mutually Exclusive Implicants (MEIs):

$$Top\ Event = \bigcup_{j=1}^{m} Mutually\ EDxclusive\ \mathrm{Im}\, plicant_j\ ,$$

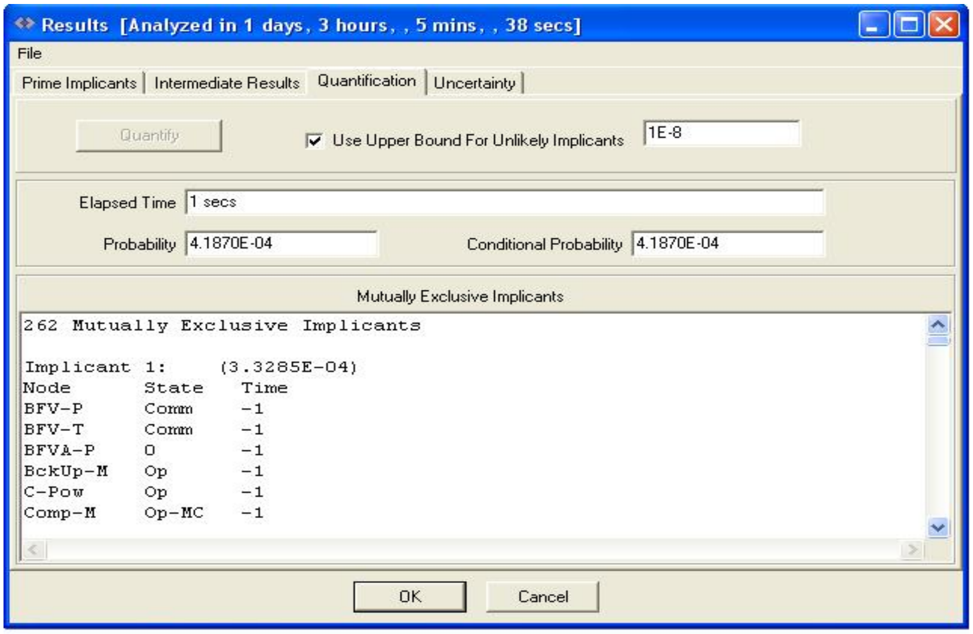
where

Mutually Exclusively Implicant #i $\cap$ Mutually Exclusive Implicant #j = $\varnothing$ for $i \neq j$

Step 3 – Expression of Top Event probability as sum of Mutually Exclusive Implicant probabilities:

$$Top\ Event\ \mathrm{Pr}\, obability = \sum_{j=1}^{m} \mathrm{Pr}\, obability\ of\ \ Mutually\ Exclusive\ \mathrm{Im}\, plicant_j$$

For the low SG level Top Event, the Top Event probability of 4.19E-04 is obtained in this fashion, as shown in Fig.2.4.5.


Results [Analyzed in 1 days, 3 hours, , 5 mins, , 38 secs]
File
Prime Implicants
Intermediate Results
Quantification
Uncertainty
Quantify
Mutually Exclusive Implicants
OK
Cancel

☑ Use Upper Bound For Unlikely Implicants: 1E-8

Elapsed Time: 1 secs

Probability: 4.1870E-04   Conditional Probability: 4.1870E-04

```
262 Mutually Exclusive Implicants

Implicant 1:     (3.3285E-04)
Node        State    Time
BFV-P       Comm     -1
BFV-T       Comm     -1
BFVA-P      O        -1
BckUp-M     Op       -1
C-Pow       Op       -1
Comp-M      Op-MC    -1
```

Figure 2.4.5: Quantification for Low SG Level Top Event

2.4.3.1.2 Deductive Analysis and Quantification for High SG Level

As noted earlier, once a system DFM model is constructed, it can be analyzed for many different Top Events. Thus, for example, the same DFWCS DFM model that the authors have used for the analysis discussed in Section 2.4.3.1.1 can also be analyzed for a Top Event concerning a high SG level occurring in the 8 hours of the ramp-down power maneuver, again assuming that the system starts in a state with no failed components. The focus is on the ramp-down phase because the DFWCS is most vulnerable to the high failure during this phase. Specifically, if the change in feed flow cannot match the reduction in steam flow, the SG level can rise and lead to a turbine trip condition. The assumption regarding no prior failed components forces the analysis to identify the absolute minimum conditions that would lead to the undesirable high SG level outcome.

In this analysis, the time step *t = 0* refers to the 70% power steady-state that follows the end of the closing 8 hour ramp-down period, whereas the time step *t = -1* refers to the 8 hr window of the power ramp down during the plant maneuver. With these time-step definitions, the SG High Level Top Event was defined in detail to include the definition of corollary plant parameter states and conditions. Table 2.4.16 provides the description of the conditions that are included in the Top Event definition.

Table 2.4.16: High SG Level Top Event Definition (Deductive analysis)

DFM Node State	Time Stamp	Meaning
L = +2	0	SG level reaches the highest state
LP = 0	-1	SG level was at the nominal state
C-Pow = Op	-1	Power to the controllers was initially available
Pow = Op	-1	Power to the computers was initially available
BckUp-M = OP	-1	Backup computer was initially operational
BFV-P = Comm	-1	Bypass flow valve/controller was initially operational
Comp-M = OP-MC	-1	The main computer was initially working as the primary
FP-P = Comm	-1	Feed pump controller was initially operational
Main-M = OP	-1	Main computer was initially operational
MFVA-P = 4	-1	Main feed flow was initially at 78% prior to the ramp-down maneuver
MFV-P = Comm	-1	Main flow valve/controller was initially operational
PDI-P = OP	-1	PDI controller was initially operational

The key transition in this Top Event is summarized in the first 2 rows highlighted in yellow. It corresponds to the progression of the SG level from normal (state 0) to high (state +2). For the Top Event specified, the DFM analysis yielded 138 prime implicants. These prime implicants contain the combinations of basic events that could cause the Top Event, with none of these implicants being contained in another (hence the denomination prime). As mentioned earlier, prime implicants are essentially the multi-valued logic equivalent of binary minimal cut sets appearing in a fault tree analysis.

The prime implicants for the High SG Level Top Event found via the DFM deductive analysis were ordered from the highest to lowest probability of occurrence. Only 2 prime implicants are associated with a probability > 1E-06. Instead of showing just these 2 prime implicants, the top 6 prime implicants are shown in Table 2.4.17 to provide additional information regarding secondary contributors. The events corresponding to components remaining in the good states are filtered out from the raw prime implicants, leaving the key component failure transition(s) (highlighted in red in Table 2.4.17), the boundary conditions (the initial SG level and the reactor power profile), and the essential states for distinguishing prime implicants with the same failure transition(s) (highlighted in blue in Table 2.4.17). For example, examination of the prime implicants listed in Table 2.4.17 shows that the key failure event in the primary contributor to the high SG level is the failure of the main feed valve being stuck in the 78% position (MFV-T = Stuck @ t = -1 $\cap$ MFVA-P = 4 @ t = -1 in prime implicants #1 and 2). The decrease in steam flow cannot be matched by a reduction in feed flow, causing the SG level to rise and to eventually reach the high level. In addition, the key failure events in the secondary contributors are the failure of the MFV controller in arbitrary mode and in high mode. More specifically, Table 2.4.17 summarizes the subset of failures within that family that would cause the controller to generate a high MFV position command signal (prime implicants #3 and 4, the MFV controller transitioning from the previous communicating state, MFV-P = Comm, to the arbitrary state, MFV-T = Arb). This would cause the main feed valve to open to its full position, causing the SG level to rise and eventually reach the high level.

The reader should note that the top contributor identified here (MFV failed stuck) is the same top contributor for the low SG level during ramp up. This shows that for dynamic systems, when subjected to different timing and boundary conditions (power ramp up versus power ramp down), the same failure mode could lead to drastically different outcomes.

Table 2.4.17: Top Prime Implicants for High Steam Generator Level

(Key failure transition shown in red, distinguishing boundary condition shown in blue)

#	Prime Implicant	Probability

1	Mode = 1 @ t = 0
	MFV-T = Stuck @ t = -1
	MFV-P = Comm @ t = -1
	MFVA-P = 4 @ t = -1
	Main-T = OP @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		3.33E-04

2	Mode = 1 @ t = 0
	MFV-T = Stuck @ t = -1
	MFV-P = Comm @ t = -1
	MFVA-P = 4 @ t = -1
	Bckup-T = OP @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		3.33E-04

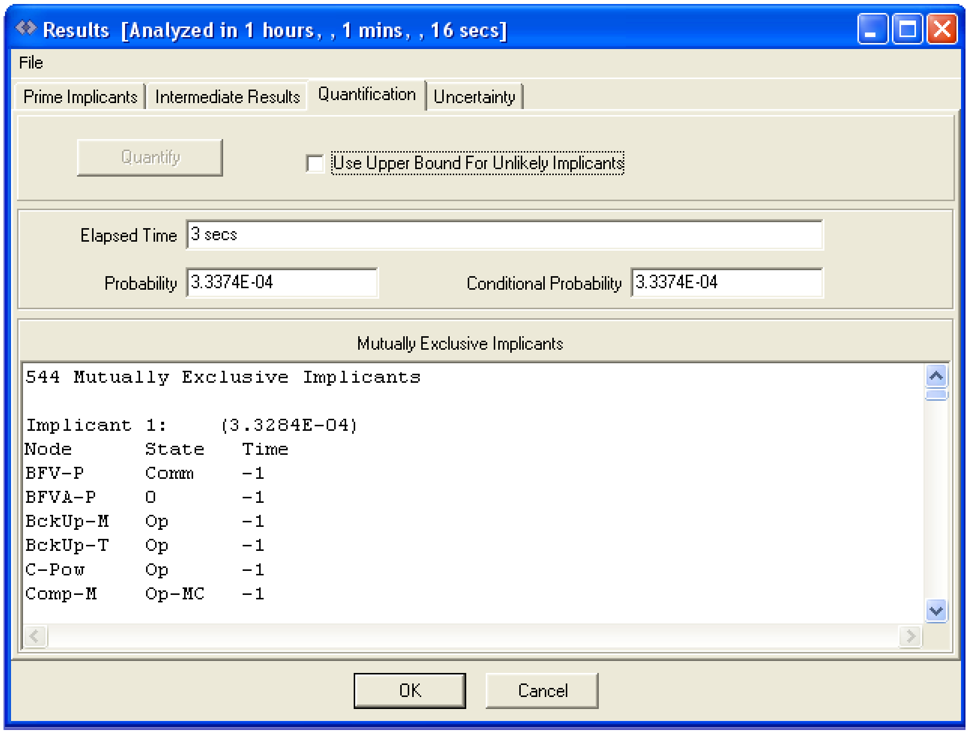
3	Mode = 1 @ t = 0
	MFV-T = Arb @ t = -1
	MFV-P = Comm @ t = -1
	Main-T = OP @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		4.37E-07

4	Mode = 1 @ t = 0
	MFV-T = Arb @ t = -1
	MFV-P = Comm @ t = -1
	Backup-T = OP @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		4.37E-07

5	Mode = 1 @ t = 0
	MFV-T = High @ t = -1
	MFV-P = Comm @ t = -1
	Main-T = OP @ t = -1
	LP = 0 @ t = -1
	Mode = 1 @ t = -1
		4.37E-07

6	Mode = 1 @ t = 0
	MFV-T = High @ t = -1
	MFV-P = Comm @ t = -1
	Backup-T = OP @ t = -1
	LP = 0 @ t = -1
	8. Mode = 1 @ t = -1
		4.37E-07

As shown in Fig.2.4.6, the probability of the Top Event, obtained via the transformation of the initial prime implicant set into a set of mutually exclusive implicants, was estimated to be 3.34E-04.



□ Use Upper Bound For Unlikely Implicants

Elapsed Time: 3 secs

Probability: 3.3374E-04

Conditional Probability: 3.3374E-04

Mutually Exclusive Implicants

```
544 Mutually Exclusive Implicants

Implicant 1:     (3.3284E-04)
Node       State    Time
BFV-P      Comm     -1
BFVA-P     0        -1
BckUp-M    Op       -1
BckUp-T    Op       -1
C-Pow      Op       -1
Comp-M     Op-MC    -1
```

Figure 2.4.6: Quantification for High SG Level Top Event

2.4.3.2 Inductive Analysis and Quantification for the Power Excursion Scenario

For this demonstration, inductive failure and fault analyses were also executed for the benchmark system in addition to the deductive analyses presented in the preceding section. These analyses were carried out to confirm the key contributor identified in the low SG level deductive analysis and the key contributor identified in the high SG level deductive analysis, and to gain insights regarding the progression of intermediate events, from the initial failure to the final outcome. In particular, these inductive analyses generated DSTs that show the progression of system and key process parameter states, starting from different combinations of initial conditions and component states, to the low SG level and high SG level, respectively.

Two scenario-initiating failure conditions were investigated:

A. the MFV failing stuck in a given position during the eight hours of the ramp-up maneuver. This inductive analysis is carried out to confirm the key prime implicant identified for the low SG level Top Event as discussed in Section 2.4.3.1.1, and
B. the MFV failing stuck in a given position during the eight hours of the ramp down maneuver. This inductive analysis is carried out to confirm the key prime implicant identified for the high SG level Top Event as discussed in Section 2.4.3.1.2.

For both of the above scenarios, the other components were assumed to be in the nominal operational states. The inductive analysis and quantification of these two DSTs are discussed in Section 2.4.3.2.1 and Section 2.4.3.2.2.

2.4.3.2.1 Inductive Analysis and Quantification for MFV Failed Stuck During Ramp Up

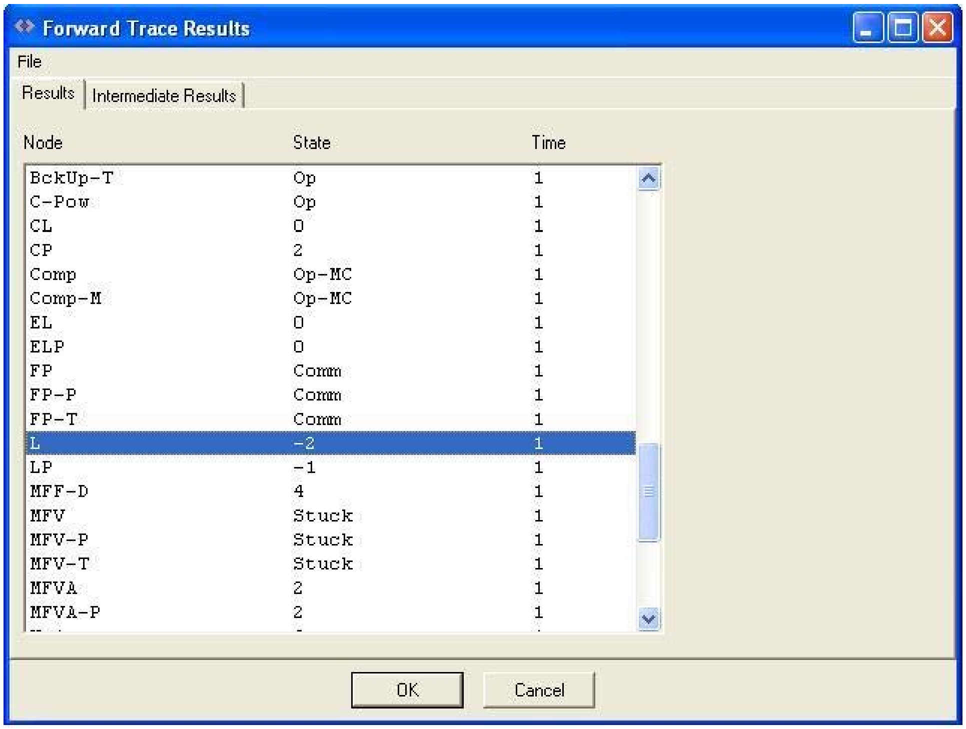
Table 2.4.18 lists the initial/boundary conditions that were defined for input into the DFM inductive analytical engine to develop a DST resulting from a stuck-at failure of the MFV during the 8 hours of the ramp up maneuver (the top contributor to the low SG level during ramp up), given the system starts in a state with no failed components.

Table 2.4.18: Initial/Boundary Conditions for DFM (Inductive – Ramp Up)

DFM Node State	Meaning
At time 0, BckUp-M = OP At times 0 & 1, BckUp-T = OP	The backup computer was operating initially and remains operating
At time 0, BFV-P = Comm At times 0 & 1, BFV-T = Comm	The bypass flow valve/controller was operating initially and remains operating
At time 0, BFVA-P = 0	The BFV was closed
At times 0 & 1, C-Pow = Op	Controller power is available
At time 0, CL = 0	Compensated level was nominal
At time 0, Comp-M = OP-MC	The main computer was the primary
At time 0, CP = 1	Compensated power was nominal
At time 0, ELP = 0	No accumulated level error
At time 0, FP-P = Comm At times 0 & 1, FP-T = Comm	The FP controller was operating initially and remains operating
At time 0, LP = 0	SG level was nominal initially
At time 0, Main-M = OP At times 0 & 1, Main-T = OP	The main computer was operating initially and remains operating
At time 0, MFV-P = Comm At times 0 & 1, MFV-T = Stuck	The MFV was operating initially, but transitioned to the stuck at failure state
At time 0, MFVA-P = 2	The MFV aperture was initially at 70%
At time 0, PDI-P = Op At times 0 & 1, PDI-T = Op	The PDI controller was operating initially and remains operating
At time 0, Pump = High	The pump was operating at high speed
At times 0 & 1, Pow = Op	Computer power is available
At time 0, R-Pow = 3 At time 1, R-Pow = 4	The reactor power increases from 70% to 78%

The initiating failure event represented by the transition of the MFV from its full operational state to the stuck-at state is highlighted in red. The inductive analysis engine was used to trace through the causality of the model. First, the states of the nodes included in the initial condition were used to determine the states of the nodes immediately downstream. After that, the states of these immediately downstream nodes were used to determine the states of the nodes further downstream. When the forward tracing was completed for 1 time step, the nodes were updated and the process was repeated for the next time step. The final result of the inductive analysis is shown in Fig. 2.4.7. This shows that, although the feedflow demand tries to follow the increase in power (MFF-D = 4, 6th row from the bottom in Fig. 2.4.7), the MFV failed stuck causes the MFV aperture to stay in the previous position (MFVA = 2, 2nd row from the bottom in Fig.2.4.7). As a result, the SG level decreases (L = -2, the highlighted row in Fig.2.4.7).

As discussed previously in NUREG/CR-6942, this DST can be quantified by multiplying the probabilities of the basic events in this sequence. The probability of this DST and its ultimate outcome (SG level decreases to state -2 in the eight hours period after start of the ramp-up maneuver) via this process is estimated to be 3.34E-04.



Node	State	Time
BckUp-T	Op	1
C-Pow	Op	1
CL	0	1
CP	2	1
Comp	Op-MC	1
Comp-M	Op-MC	1
EL	0	1
ELP	0	1
FP	Comm	1
FP-P	Comm	1
FP-T	Comm	1
L	-2	1
LP	-1	1
MFF-D	4	1
MFV	Stuck	1
MFV-P	Stuck	1
MFV-T	Stuck	1
MFVA	2	1
MFVA-P	2	1

Figure 2.4.7: Inductive Analysis Result for MFV Failed Stuck

2.4.3.2.2 Inductive Analysis and Quantification for MFV Failed Stuck During Ramp Down

The development of the second DST that the authors discuss in this section again underscores that, once a system DFM model is constructed, it can be analyzed for any variety of different system conditions and scenarios, in either inductive or deductive mode. In the case discussed in this section, the same DFWCS DFM model is analyzed to generate a DST relative to the initiating failure condition represented by the stuck-at failure of the MFV during the 8 hours of the ramp-down maneuver (the top contributor to the high SG level during ramp down), given that the system starts the maneuver in a state with no failed components. For generating a DST relative to this scenario, Table 2.4.19 lists the initial/boundary conditions that were defined and used as initial input to the DFM inductive engine.

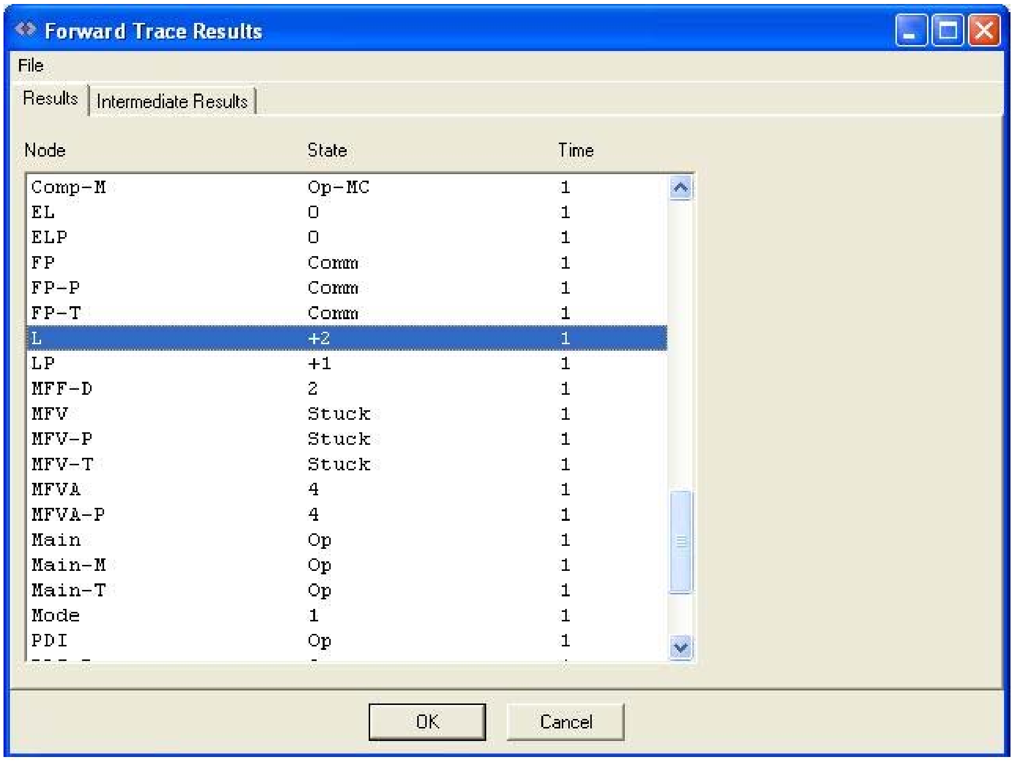
Table 2.4.19: Initial/Boundary Conditions for DFM (Inductive – Ramp Down)

DFM Node State	Meaning
At time 0, BckUp-M = OP At times 0 & 1, BckUp-T = OP	The backup computer was operating initially and remains operating
At time 0, BFV-P = Comm At times 0 & 1, BFV-T = Comm	The bypass flow valve/controller was operating initially and remains operating
At time 0, BFVA-P = 0	The BFV was closed
At times 0 & 1, C-Pow = Op	Controller power is available
At time 0, CL = 0	Compensated level was nominal
At time 0, Comp-M = OP-MC	The main computer was the primary
At time 0, CP = 1	Compensated power was nominal
At time 0, ELP = 0	No accumulated level error
At time 0, FP-P = Comm At times 0 & 1, FP-T = Comm	The FP controller was operating initially and remains operating
At time 0, LP = 0	SG level was nominal initially
At time 0, Main-M = OP At times 0 & 1, Main-T = OP	The main computer was operating initially and remains operating
At time 0, MFV-P = Comm At times 0 & 1, MFV-T = Stuck	The MFV was operating initially, but transitioned to the stuck at failure state
At time 0, MFVA-P = 4	The MFV aperture was initially at 78%
At time 0, PDI-P = Op At times 0 & 1, PDI-T = Op	The PDI controller was operating initially and remains operating
At time 0, Pump = High	The pump was operating at high speed
At times 0 & 1, Pow = Op	Computer power is available
At time 0, R-Pow = 3 At time 1, R-Pow = 2	The reactor power decreases from 78% to 70%

In Table 2.4.19, the failure event constituted by the transition of the MFV from its operational state to a stuck-at state is highlighted in red.

As in the previous inductive analysis example, the states of the nodes included in the initial condition were first used to determine the states of the nodes immediately downstream. After that, the states of these immediately downstream nodes were used to determine the states of the nodes further downstream. When the forward tracing was completed for 1 time step, the nodes were updated and the process was repeated for the next time step.

The final result of the inductive analysis is shown in Fig. 2.4.8. One can see that, although the feedflow demand tries to follow the decrease in power (MFF-D = 2, 9th row from the top in Fig. 2.4.8), the MFV failed stuck causes the MFV aperture to stay in the previous position (MFVA = 4, 7th row from the bottom in Fig. 2.4.8) and the SG level increases (L = +2, highlighted row in Fig. 2.4.8). Quantification of this DST produces a scenario probability of 3.34E-04.



Node	State	Time
Comp-M	Op-MC	1
EL	0	1
ELP	0	1
FP	Comm	1
FP-P	Comm	1
FP-T	Comm	1
L	+2	1
LP	+1	1
MFF-D	2	1
MFV	Stuck	1
MFV-P	Stuck	1
MFV-T	Stuck	1
MFVA	4	1
MFVA-P	4	1
Main	Op	1
Main-M	Op	1
Main-T	Op	1
Mode	1	1
PDI	Op	1

Figure 2.4.8: Inductive Analysis Result for MFV Controller Low Output

2.4.4 Incorporation of DFM Analytical Results into Plant PRA

As discussed in the beginning of Section 2.4, the DFM model was solved to address the low DFWCS failure initiating event (Fig.2.3.1) and the high DFWCS failure initiating event (Fig.2.3.2). In an actual PRA application, the deductive analyses results (probability of occurrence) obtained for the low SG level Top Event and the high SG level Top Event would be incorporated into the two event tree models and the remainder of the PRA analyses would be carried out as usual.

It is noted that, although for brevity and simplicity this is not been shown in the preceding discussion, the results from the DFM analysis may include uncertainty and sensitivity analysis results. These results can also be integrated in relatively straightforward fashion into the conventional PRA models. Some caveats apply to how this can be correctly done, as discussed in Section 4.3.

2.5 Insights and Observations

Several important insights were gained as a result of applying DFM to the benchmark system.

At the risk scenario interpretation level, the application of dynamic methods such as DFM to digital I&C analysis may be essential to understanding the plant risk-related event sequences and to support the PRA efforts. This is demonstrated by some of the results obtained in the DFM analysis. In the deductive analysis carried out for the low SG level Top Event during ramp up, the top contributor is identified to be the MFV (main feedwater valve) failed in the stuck-at mode. This same failure mode was also identified in the deductive analysis for the high SG level Top Event during ramp down. This illustrates that timing, as well as the systems dynamics, are crucial in the identification of root causes and the determination of what sequences may develop and how from certain component failure modes. The timing issue and the system dynamics issue cannot be straightforwardly addressed and quantified exclusively with a traditional ET/FT analysis. The support offered to a traditional PRA by an advanced logic-analytical methodology with dynamic and interactive modeling capabilities to analyze dynamically-characterized initiating events, pivotal events, and/or intermediate events, provides a viable solution to this issue.

At the methodology level:

1. The analysis conducted with DFM has given us confirmation that there is a practical and effective way of combining the deductive and inductive techniques. In the DFM model construction and refinement process, the inductive technique can be used to validate the model. In the DFM analysis process, the deductive technique can be applied first to identify and to quantify the failure modes. These failure modes can then be confirmed with the inductive technique (or other simulation technique for that matter). In addition, the inductive technique (or simulation) can provide the details regarding the sequence of events from the initial failure to the final outcome, which is not easily visible to the user from the deductive analysis.
2. The deductive analysis results (prime implicants and their associated probability) are confirmed to be completely compatible and easily integrated with the results obtained from a traditional PRA (cutsets and their associated probability). This, as mentioned earlier, could be expected, as the DFM results are the multi-valued logic equivalence of ET/FT results. Hence, the execution of a traditional PRA supported by the selective insertion of DFM technique models and procedures (to analyze and solve dynamic portions of the system of interest) represents a viably implemented solution. This is elaborated further below in the discussion of insights at the implementation level.

At the implementation level:

1. The deductive analyses of the DFWCS system model (a complex models that included tens of variable nodes with multi-state range definitions) were allowed to run without interruption for a maximum of ~72 hours. This allowed the DYMONDA^{TM} software to track two (current and earlier) major system time steps. The early indications from current work being carried out to optimize the deductive search capabilities of the DYMONDA^{TM} software are that it will be possible to extend the backward-in-time deductive search for such a model to 3 or 4 system time steps with the computational power of a current dual-core CPU desktop computer.
2. The prime implicants and/or probability estimates obtained with DFM analyses can be incorporated into a plant PRA model in the same fashion as it would be done with the minimal cut sets and probabilities of a typical fault tree. In this demonstration, the DFM results were obtained by means of the DYMONDA^{TM} DFM software tool, and then transferred into the SAPHIRE PRA code via the data transfer feature of the latter. More direct interfaces between the DFM software and traditional PRA tools like CAFTA and SAPHIRE via Application Programming Interfaces (APIs) are possible and have been demonstrated in proof-of-concept mode in other studies [26].

3. THE MARKOV/CCMT MODEL

3.1 Introduction

Markov/CCMT is an approach [27, 28] that combines the conventional discrete state Markov methodology with CCMT to represent the possible coupling between failure events that can originate from the dynamic (time-dependent) interactions:

1. between the digital I&C system and the controlled/monitored process, and,
2. among the different constituents of the digital I&C system.

As indicated in Section 1.3, the DFM and Markov/CCMT are proposed to be used in a complementary fashion in the PRA modeling of digital I&C systems with

- DFM implemented in the deductive mode to identify possible failure sequences/initiating events that lead to a specified Top Event, and,
- Markov/CCMT implemented in the inductive mode to assure completeness and verification of the quantification of these failure sequences that may require more detailed modeling (e.g. those involving Arbitrary Output as explained in Section 3.4)

This chapter presents the Markov/CCMT and illustrates its application on the benchmark DFWCS system presented in Section 1.2 for the power maneuver described in Section 1.3.2.3.2 of the report. The DFWCS failures under consideration are when an operating PWR's steam generator (SG) level becomes too high or low (High and Low SG Level failures). The analysis performed yields the minimal hardware/software/firmware failure sequences (or prime implicants) that lead to these failed system states, or Top Events, as well as the probability of occurrence of the sequences. These sequences then can be integrated into an existing plant PRA performed using the traditional ET/FT approach to assess the impact of the presence of the DFWCS on the risk metrics under consideration.

Section 3.2 gives a general overview of the Markov/CCMT methodology and lists the assumptions made in the Markov/CCMT implementation for the example initiating event under consideration (see Section 1.3.2.3.2) as well as the capabilities and the limitations of the Markov/CCMT methodology. Section 3.3 shows the application of the Markov/CCMT methodology to DFWCS under the power maneuver presented in Section 1.3.2.3.2. Section 3.4 investigates the sensitivity of the results to the modeling of Arbitrary Output by the computers and controllers by sampling over the range of possible outputs from either type of components.

3.2 Overview of the Markov/CCMT Methodology

The CCMT [29] is a systematic procedure to describe the dynamics of both linear and non-linear systems in discrete time and discretized system state space[14]. The CCMT provides a very effective means to account for epistemic uncertainties, non-linear aspects of the system

[14] The system state space is a space in which all possible states of the system are represented. Each possible state of the system corresponds to a unique point in the state space.

dynamics and stochastic fluctuations in dynamic system operation. The CCMT produces a model that is compatible with the conventional discrete-state Markov approach for representing hardware/software/firmware failures The conventional discrete-state Markov approach represents the stochastic evolution of a system through the transition probabilities (often obtained from experimental data) among the possible system states. The transitions between the states (nodes) can be represented graphically by directional links (edges) through Markov transition diagrams. Even if failure data are not available, a Markov/CCMT model can be used in both the inductive and deductive modes to produce, respectively:

- the cause-consequence relations (event sequences, scenarios) between initiating events and Top Events or operational states [30], and
- the prime implicants leading to specified Top Events or operational states [31]

The event sequences or scenarios then can be rank ordered according to their frequency of occurrence, and/or the frequency of occurrence of specified events within the sequence using standard PRA tools such as SAPHIRE [17], CAFTA [32] or RISKMAN [33]. If failure data are available, then the scenario and Top Event likelihoods can be quantified. Whether failure data are available or not the, Markov/CCMT model can be integrated into standard PRAs using standard PRA tools [34].

The inputs needed by the Markov/CCMT methodology are:

i. a model of system dynamics (simulator),
ii. control laws and control logic of the system under operational and failed conditions,
iii. discretized system states as inferred from a failure modes and events analysis (FMEA), the system dynamics and control laws,
iv. hardware/software/firmware state transition rates or failure probabilities per demand, and
v. a modeling time step.

3.2.1 Capabilitites

A full Markov/CCMT model accounts for transitions between all system states defined by the user and hence represents a complete picture of the system structure in terms of these discrete states. Subsequently, once the model is constructed it can be used for analyzing sequence of events of different Top Events or the consequences of different initiating events, in contrast to the conventional ET/FT models which are scenario and initiating event specific. For systems with a large number of states (more than several thousand) construction of a full Markov/CCMT model may not be computationally feasible. In these situations, the use of Markov/CCMT is more effective in the inductive mode where a limited range of initial conditions are considered rather that all possible conditions (see Section 3.1).

Whether used in its full or more limited inductive mode, Markov/CCMT can represent

- memory effects (by adding auxiliary states or auxiliary variables),
- logic loops along with time dependent and system state dependent transitions,
- epistemic uncertainties, non-linear aspects of the system dynamics and stochastic fluctuations in dynamic system operation,

- logic interactions within the digital I&C system components (failover),
- statistically dependent failure probabilities/rates, and,
- failure probabilities/rates that may be affected by the environment (e.g. pressure, temperature)

3.2.2 Limitations

Some limitations of the methodology are the following:

- The construction of a Markov/CCMT model for any system requires a substantially larger amount of technical knowledge compared to that needed for a traditional ET/FT analysis.
- The Markov/CCMT approach may require significant computational effort in order to solve the model and generate event sequences. Factors that affect the computational requirements of the model include:
    - the overall number of system states (which may be reduced by merging states),
    - size of the modeling time step (i.e. Input (v) above),
    - mission time of the simulation,
    - complexity and size of the system model.
- As the methodology produces a large amount of data, some post processing of the results is required.

3.2.3 Procedures

The steps in applying Markov/CCMT in a PRA framework consist of the following:

1. *Construct the Markov/CCMT model to represent the system of interest*. As indicated above, an input to Markov/CCMT model construction is discretized system states (Input (ii)). The discretized system states for hardware/software/firmware are inferred from a FMEA, as well as the control logic for the system [14]. For the continuous process variables, the discretization is accomplished by defining sets of mutually exclusive intervals of the continuous process variables[15] (cells) in a manner to those used by the finite difference or finite element methods [14]. Model construction first requires finding the cell-to-cell transition probabilities by:

   a) sampling points in each cell as initial conditions, and
   b) using the system simulator (Input (i) above) to find their arrival cells at the end of the modeling time step (Input (v) above).

   Then these transition probabilities are combined with the hardware/software/firmware state transition rates or failure probabilities per demand (Input (iv) above) to find the transition probabilities between system states [14]. It should also be indicated that while some of the steps in model construction have been mechanized, general purpose software for model construction is not available at this point in time.

[15] Such as pressure, temperature and liquid level

2. *Analyze the Markov/CCMT model*. A Markov/CCMT model obtained through Step 1 above is a probabilistic analogue of the decision tables used by DFM. It can be utilized to construct dynamic event trees (DETs) for specified initiating events [30] for inductive reasoning or dynamic fault trees (DFTs) [31] for deductive reasoning to obtain timed prime implicants. Software is available for the construction of DETs and DFTs from the Markov/CCMT models. The DETs and DFTs can be integrated into standard PRA using conventional PRA tools [34]} such as SAPHIRE [17], CAFTA [32] or RISKMAN [33]. The Markov/CCMT models can be also used to find statistical properties of the system such as mean residence time in a specified state or the mean time for transition to a specified Top Event.
3. *Quantify the deductive and the inductive analytical results*. If failure data are available, quantification of the risk significance of events can be performed following the integration of the DETs and DFTs into standard PRA again using standard tools. If data are not available, again these software can be used to rank order the DETs as a function of specified basic events or find the prime implicants for specified Top Events [14].

3.3 Application of Markov/CCMT to the Example Initiating Event

3.3.1 Model Assumptions

The development of the Markov/CCMT model of the DFWCS benchmark system was also executed under the set of general assumptions that have been discussed in Section 1.3. Accordingly, the model development reflects the following:

1. The model only includes one steam generator and associated DFWCS control functions, along a relatively simple rendition of the power input from the plant primary side.
2. The physical behavior of the steam generator modeled is assumed to be well represented by the simulator developed for NUREG/CR-6465 [4].
3. The model represents in discrete-state form the SG control logic and control equations documented in NUREG/CR-6942 [14].
4. The model includes the representation of hardware and software component failure modes as described in [14]:
    a. Because of the limited availability of quantification data, software is not modeled in full detail but as embedded in hardware; this limitation can be removed if the purpose of the analysis is purely qualitative, or if quantification data is made available.
    b. Hardware components such as pumps and valves, once failed, are assumed to remain in the failed state.
    c. Software failure modes are assumed to affect certain DFWCS states of various kinds, e.g., high or low output, stuck-at values, and arbitrary values.
    d. If a software function failure is detectable and is backed up by a redundant controller or computer, the function is assumed to be recoverable via switch-over to the back-up unit that may be available. If failure is detected but backup is not available, the previous output from that device is used,

    The resulting finite state machine model is shown in Figs. 1.3.2 and 1.3.3.
5. No attempt is made to explicitly pursue in the Markov/CCMT an analysis for the identification of system failure modes associated with possible design or specification errors concerning the system or software.

6. For its quantification process, the Markov/CCMT analysis of the DFWCS system uses the failure rates of the benchmark system controllers and computers reported in Section 1.4.3.
7. The power maneuver described in Section 1.3.2.3.2 is assumed to provide a satisfactory representation of the DFCWS behavior in terms of identification of typical failure modes and associated probabilities.

In addition, the following Markov/CCMT specific assumptions are made for the modeling and analysis process:

1. The sample points used in the determination of the cell-to-cell transition probabilities (see Section 3.2.3, Step 1) are assumed to adequately represent the entire cell-to-cell transition behavior.
2. The system is initially in the nominal operating range for the SG level (i.e., ± 2 in. around the set point designated as 0 in.)
3. All the other controlled variables (i.e. level error, compensated level, compensated power, compensated flow error, MFV position, FP speed, BFV position) are initially in their nominal ranges.
4. The time horizon of interest is 24 hours, and a single Markov/CCMT modeling time step is chosen to be 8 hours, which corresponds to each of the phases of the power maneuver described in Section 1.3.2.3.2.

3.3.2 Model Construction

As indicated in Section 3.2, the inputs for Markov/CCMT model construction are:

i. Information about the system dynamics (e.g., from basic engineering knowledge, or, in more detailed form, from a system simulator),
ii. control laws and control logic of the system under nominal and off-nominal conditions,
iii. discretized system states as inferred from a failure modes and effects analysis (FMEA), the system dynamics and control laws,
iv. hardware/software/firmware state transition rates or failure probabilities per demand, and,
v. the definition of a modeling time step.

Along with the control laws and control logic of the system under operational and failed conditions, engineering knowledge, or output from a system simulator, is used to determine the transition probabilities between the cells that are defined by the discretized controlled variable states and that partition the system state space [14]. In a full Markov/CCMT model using the complete system state space, these transition probabilities also provide a mapping between the cells to represent the system dynamics under normal and fault conditions and constitute a probabilistic version of the decision tables used by DFM (Section 2.4.2). In the inductive mode of utilization of Markov/CCMT as it is done in this study, the cell-to-cell transition probabilities are conditional upon the range of initial conditions assumed (i.e., ± 2 in round the set point designated as 0 in by Assumptions 2 and 3 in Section 3.3.1). In either case, the cell-to-cell transition probabilities are combined with the hardware/software/firmware transition probabilities to determine the probability of finding the system in a specified state at a specific time step [14].

For the generation of the cell-to-cell transition probabilities, The SG dynamics is assumed to be adequately represented by the simulator developed for NUREG/CR-6465 [4] (Assumption 2 in

Section 3.3.1). The modeling time step is chosen as 8 hours (Assumption 4 in Section 3.3.1). The SG level is partitioned into three ranges consisting of:

- Low level (less than 24 in. below level setpoint),
- High level (more than 30 in. above level setpoint), and
- Allowed level range (between -24 in. and +30 in. with respect to reference level).

The control laws and control logic of the system under nominal and off-nominal conditions is described by a Matlab® SIMULINK model. The control logic module also models automatic transition from High to Low power and from Low to High power (see Section 1.2). The SG model is implemented using a C/C++ proprietary code from ASCA Inc. Figs. 3.3.1 and 3.3.2 show, respectively, the control logic and actuated device Matlab® SIMULINK modules.

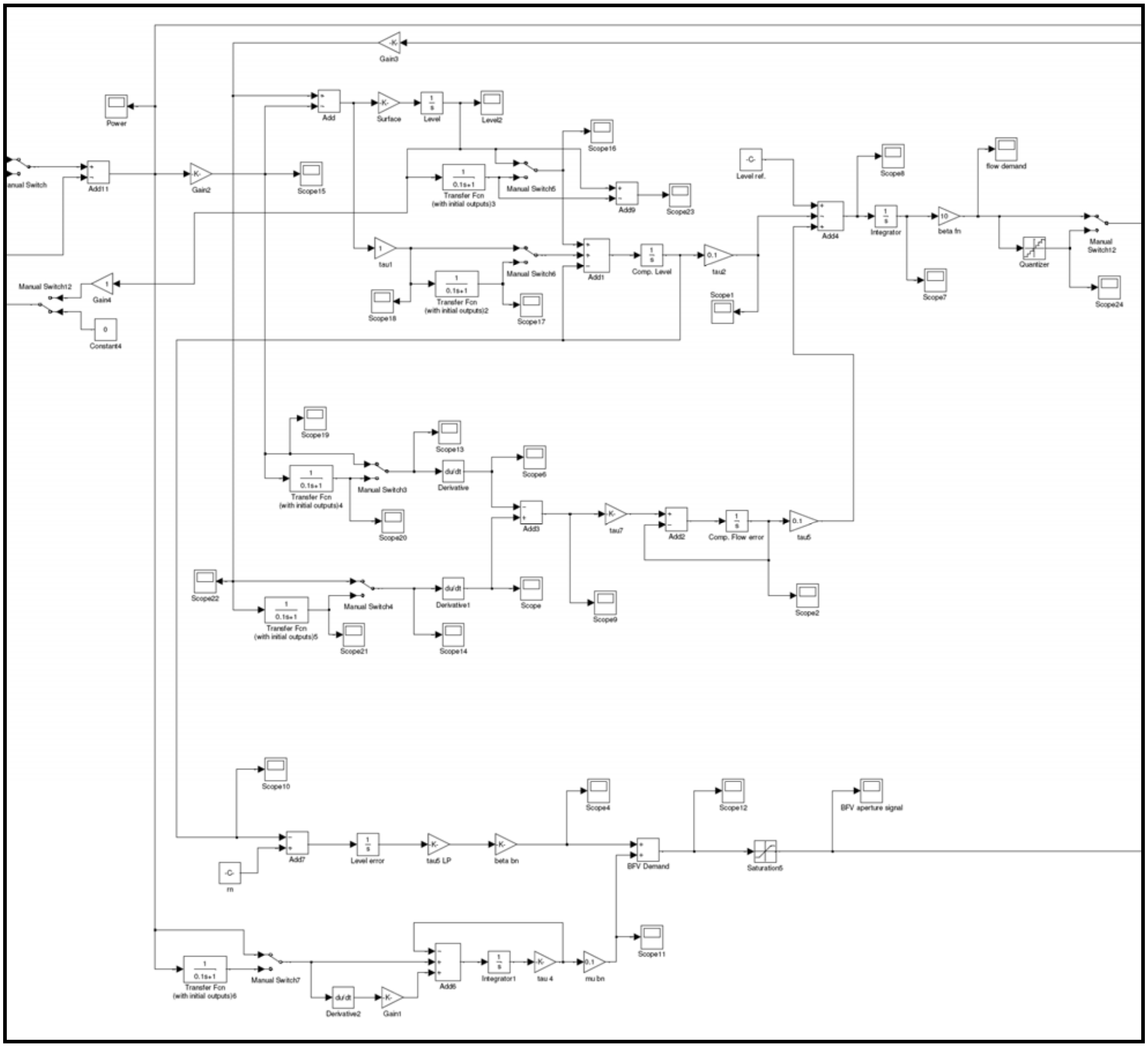


Figure 3.3.1: SIMULINK control logic module

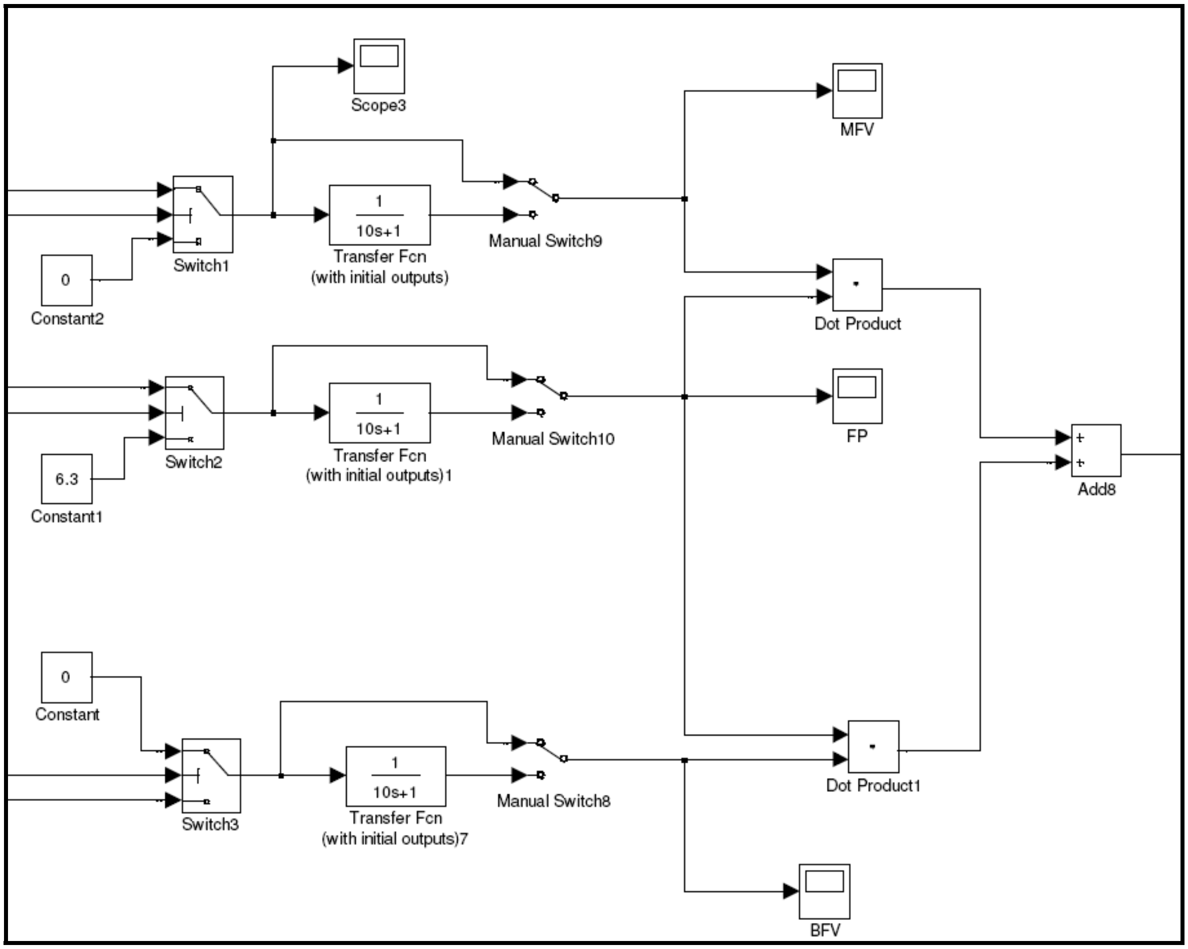


Figure 3.3.2: SIMULINK module for actuated devices of the DFWCS (MFV, BFV and FP)

The choice of the hardware/software/firmware states is based on Figs. 1.3.2 and 1.3.3 as stated in the assumption s in Section 3.3.1. Figs. 3.3.3 - 3.3.7 show the Markov transition diagrams for the DFWCS components (MC, BC, BFV controllers, PDI controller, and the controllers' power source). Note that although Figs. 3.3.3 and 3.3.4 are very similar, individual models MC and BC are shown for fidelity with the finite-state machine representation of the system they are both shown here to retain fidelity with Fig.1.3.1 and also to illustrate their combination into Fig.3.3.8 more clearly. The Markov transition diagrams for MFV and FP controllers are similar to that shown in Fig.3.3.5 for BFV controllers. The Markov transition diagram for the power source of the MFV, BFV and FP controllers is presented in Fig.3.3.7.

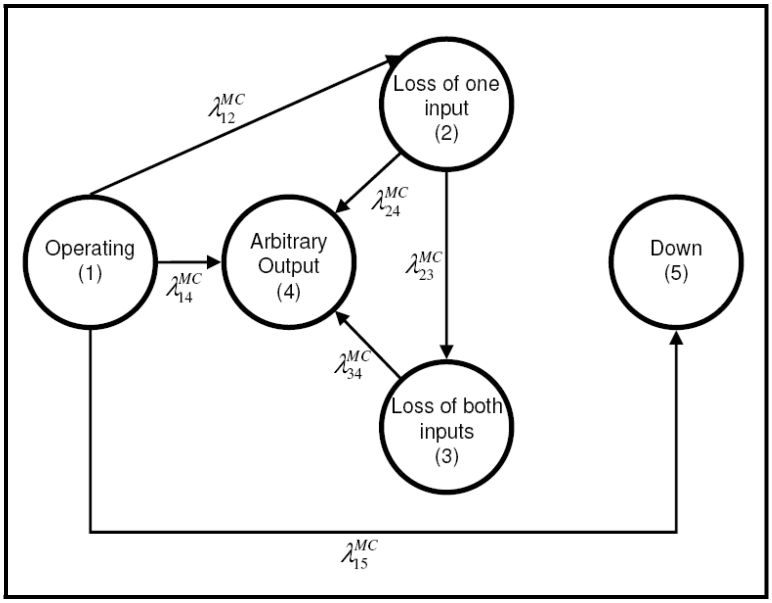


Figure 3.3.3: Markov transition diagram for the MC

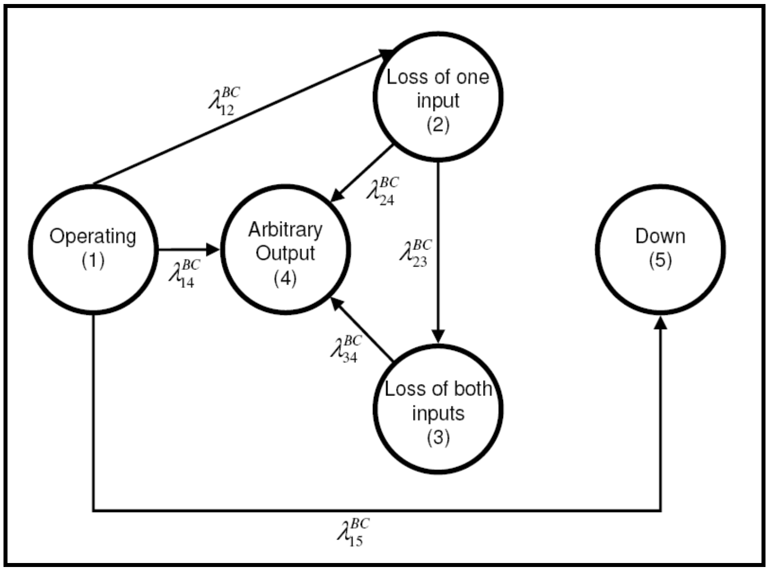


Figure 3.3.4: Markov transition diagram for the BC

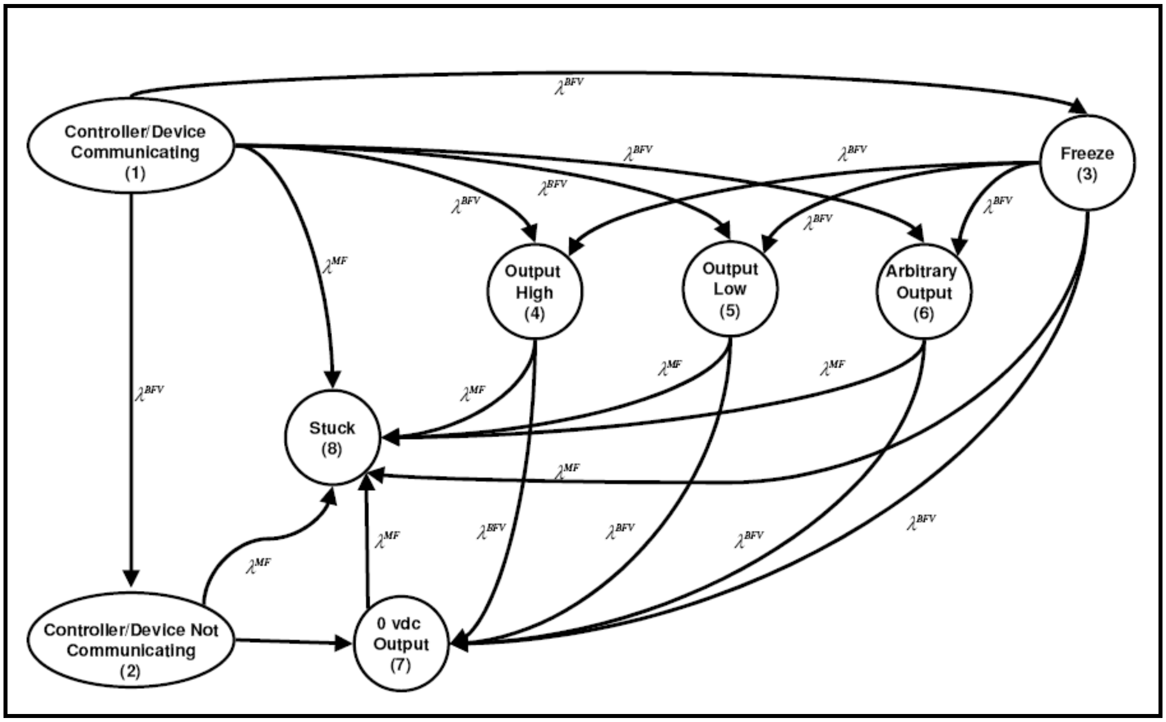


Figure 3.3.5: Markov transition diagram for the BFV controller (the Markov transition diagrams for the MFV and FP controllers are similar)

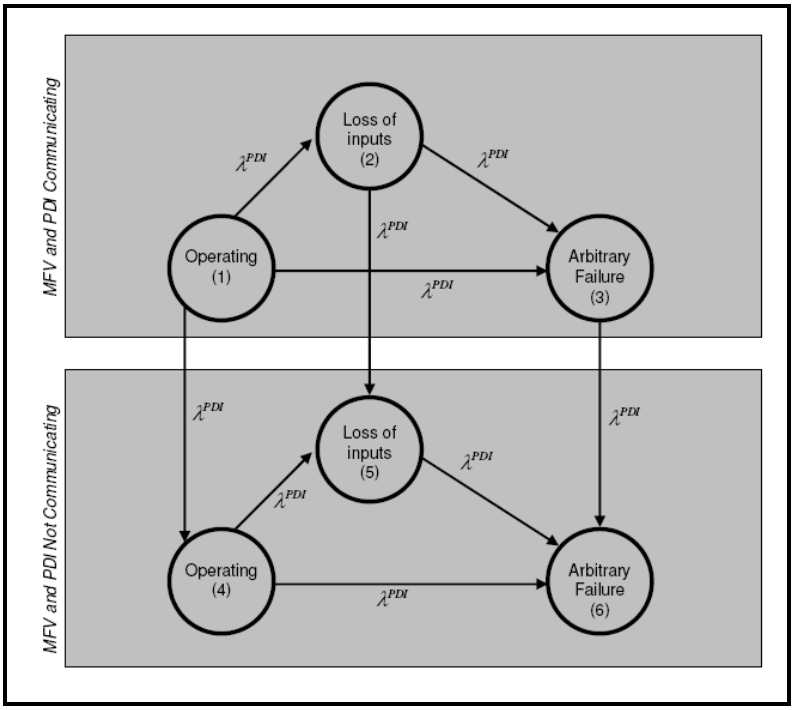


Figure 3.3.6: Markov transition diagram for the PDI Controller

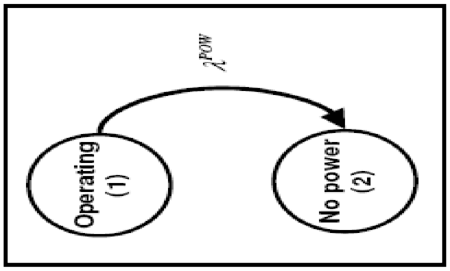


Figure 3.3.7: Markov transition diagram for the power source of the MFV, BFV and FP controllers

The transition rates shown in Figs. 3.3.3 and 3.3.4 for the MC and BC refer to the failure rates listed in Table 1.3.4.

According to Assumption 2 in Section 1.4.1, the failure rates for all the controllers are equally likely to occur. From Table 1.4.5, the failure rates for the MFV, BFV and FP PID controllers are 3.3 10^{-7} /hr. Moreover, from Fig.3.3.5, the number of failure modes (i.e. the number of failure states) is 6. This implies that, for the Markov transition diagram of the BFV controller shown in Fig.3.3.5:

- λ^{BFV} = 3.3 10^{-7} /hr / 6 = 5.5 X 10^{-8} /hr.
- the transition rates that lead to state 8 (Stuck) of Fig.3.3.5 are λ^{MF} = 4.2 10^{-5} /hr (mechanical failure of the actuated device),

The reasoning is similar for the MFV and FP controllers. In an analogous manner, there are 3 failure modes for the Markov transition diagram of the PDI controller shown in Fig.3.3.6. From Table 1.4.5, the failure rate for the PDI controller is 3.3 10^{-7} /hr. Thus, since the transition rates for the PDI controller are equally like to occur, λ^{PDI} = 3.3 10^{-7} / 3 /hr = 1.09 10^{-7} /hr.

The failure rate of the power source (for the MFV, BFV and FP controllers) is listed in Table 1.4.5, i.e. λ^{POW} = 4.8 10^{-6} /hr (Fig.3.3.7).

Table 3.3.1 summarizes the states in Figs. 3.3.3 – 3.3.8 and indicates that there are 15*8*8*8*6*2 = 92160 possible states. For Markov/CCMT modeling purposes, these states can be reduced as shown in Table 3.3.2 by combining states with similar effects on the steam generator feedwater level evolution.

Table 3.3.1: List of hardware/software/firmware states

Components	**Number of States**
Computers	15
MFV Controller	8
BFV Controller	8
FP Controller	8
PDI Controller	6
Controller power	2

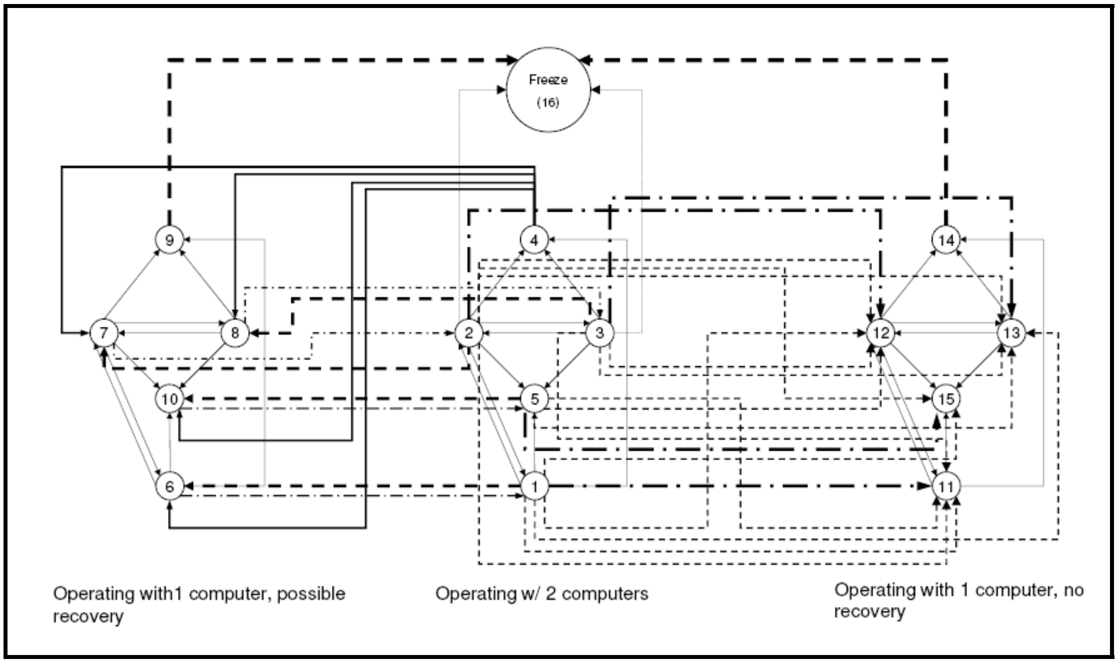

Freeze
(16)
9
4
14
7
8
2
3
12
13
10
5
15
6
1
11
Operating with1 computer, possible recovery
Operating w/ 2 computers
Operating with 1 computer, no recovery

Figure 3.3.8: Markov transition diagram for the computers MC and BC.

Table 3.3.2: List of reduced hardware/software/firmware states

Component	**New State**	**Combines/Renames**
Computers	Correct Output	States 1, 6, and 11 of Fig.3.3.8
	Previous Output	States 2, 3, 4, 7, 8, 9, 12, 13, and 14 of Fig.3.3.8
	Arbitrary Output	States 5, 10, and 15 of Fig.3.3.8
MFV, BFV, FP Controller	Correct Output	State 1 of Fig.3.3.5
	Previous Output	State 3, 8 of Fig. 3.3.5
	Output High	State 4 of Fig. 3.3.5
	Output Low	States 2, 5 and 7 of Fig. 3.3.5
	Arbitrary Output	State 6 of Fig. 3.3.5
PDI Controller	Correct Output	State 1 of Fig.3.3.6
	Previous Output	State 2 of Fig.3.3.6
	Arbitrary Output	State 3 of Fig.3.3.6
	Output Low	States 4,5,6 of Fig.3.3.6

Figs. 3.3.9 – 3.3.11 show the corresponding reduced Markov transition diagrams. Fig. 3.3.9 accounts for all the interactions shown in Fig.3.3.8 through time dependent failure rates determined from a separate auxiliary Markov model of which uses Fig.3.3.8 as a Markov transition diagram.

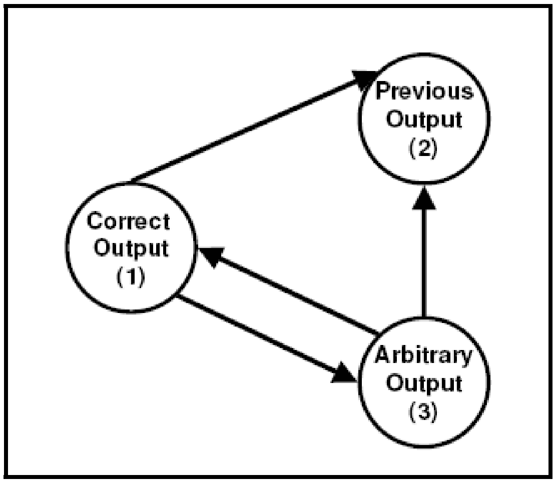


Figure 3.3.9: Reduced Markov transition diagrams for the computers

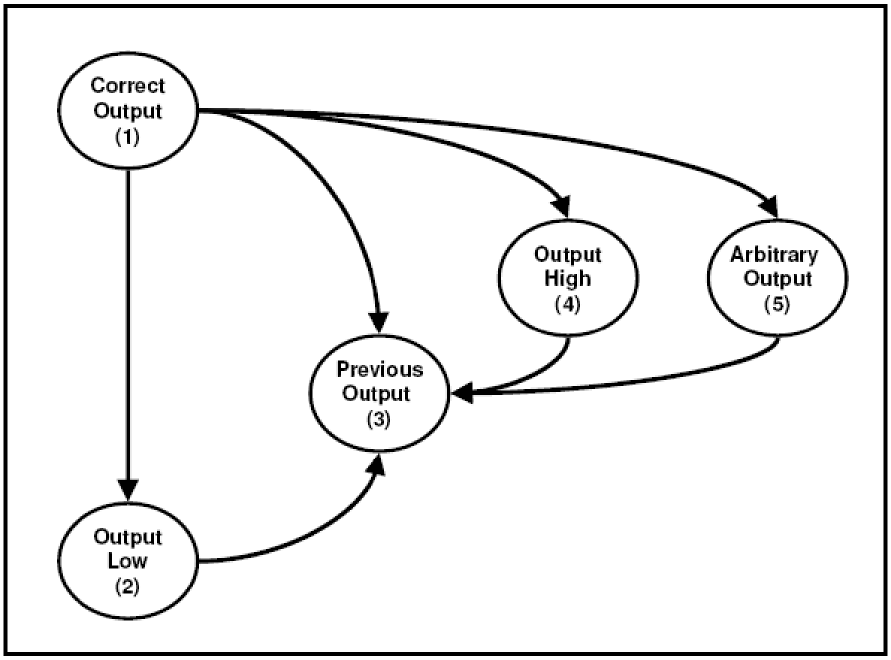


Figure 3.3.10: Reduced Markov transition diagram for the MFV, BFV and FP controllers

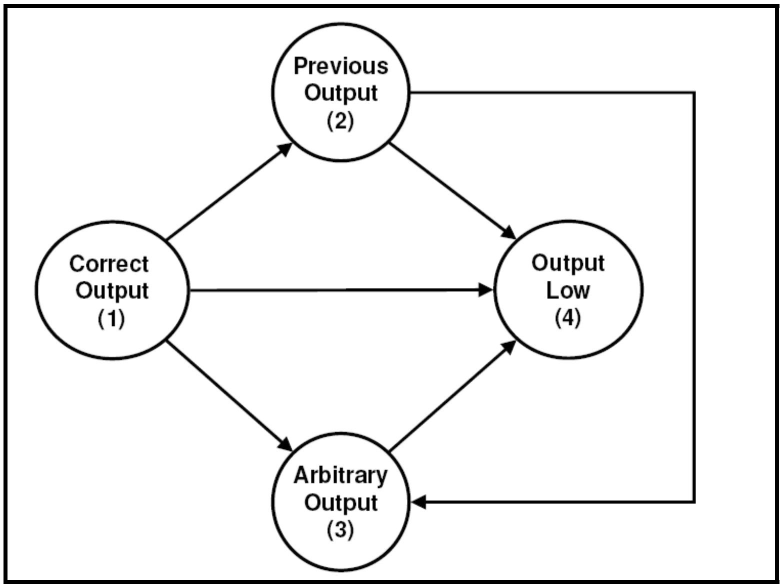


Figure 3.3.11: Reduced Markov transition diagram for the PDI controller

The two computers (MC and BC) and the three controllers (MFV, BFV, and FP) share the same power sources [14]. Thus, a failure in the power source of the computer or the controller, affects all the computers or all the controllers, respectively.

The controller power source has been modeled as a two-state Markov transition diagram as shown in Fig.3.3.7. Regarding the computers, a failure in the computer power source causes the failure of both MC and BC and, subsequently, the controllers freeze their own outputs (see Section 1.3.1). Since both the computers are modeled in a single Markov transition diagram which accounts for their interaction shown in Fig.3.3.8, the failure of the computer power source can be simply represented with a transition to the Previous Output from every other state of Fig.3.3.9. As stated in Assumption 4.d in Section 3.1, once a device failure is detected the last output from that device is used.

Table 3.3.3 list the number of reduced hardware/software/firmware states and shows that the reduction leads to 3*5*5*5*4*2 =3000 states.

Table 3.3.3: List of reduced hardware/software/firmware states

Components	**Number of States**
Computers	3
MFV Controller	5
BFV Controller	5
FP Controller	5
PDI Controller	4
Controller power	2

For the determination of the transition probabilities between the hardware/software/ firmware states, the data presented in Section 1.4.3 are used along with auxiliary Markov models for the reduced states to determine the transition rates between these reduced states. For the generation of the cell-to-cell transition probabilities, the cells corresponding to the Top Events are regarded as sink cells (where there is zero probability that the state will transition from a failed state to an operational state). The allowed level range is represented by 3 level values, chosen from the normal operating range (i.e., ±2 in). This choice of limited range of initial conditions restricts the use of the model to the inductive mode.

3.3.3 Markov/CCMT Model Analysis for the Power Excursion Scenario

As stated in Assumption 7 in Section 3.3.1, The DFWCS behavior is assumed to be represented by the power transient, described in Section 1.4, for this analysis. The reactor power ramps up from 70% to 78% at 8 hours, remains constant for 8 hours, them ramps down from 78% to 70% at 16 to 24 hours.

Fig. 3.3.12 shows the Top Events (High and Low level failure) cumulative distribution functions (CDFs) as a function of time.

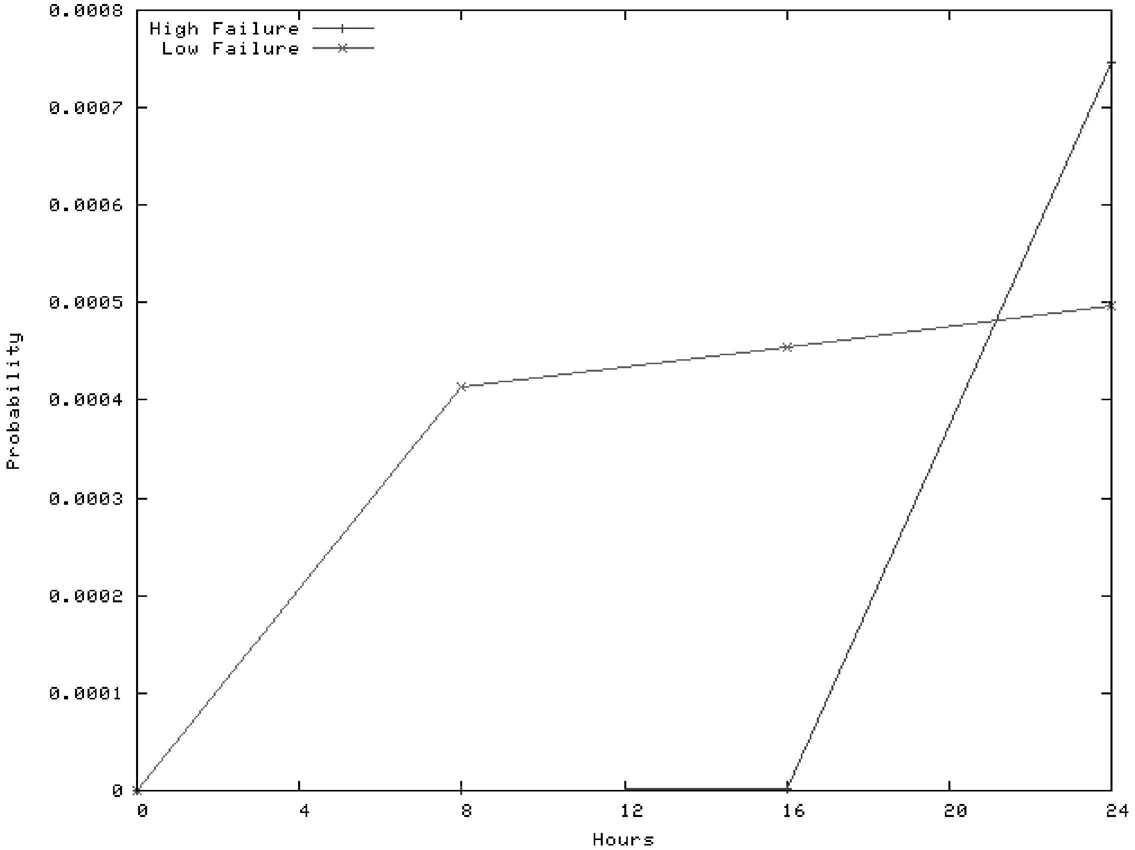


Figure 3.3.12: Failure Probability as a Function of Time

The High failure probability is shown in more detail in Fig.3.3.13. The stepwise nature of the CDFs reflects the contribution of the system dynamics to the evolution of the CDFs due to the time lag between the initiation of the fault and occurrence of the Top Event.

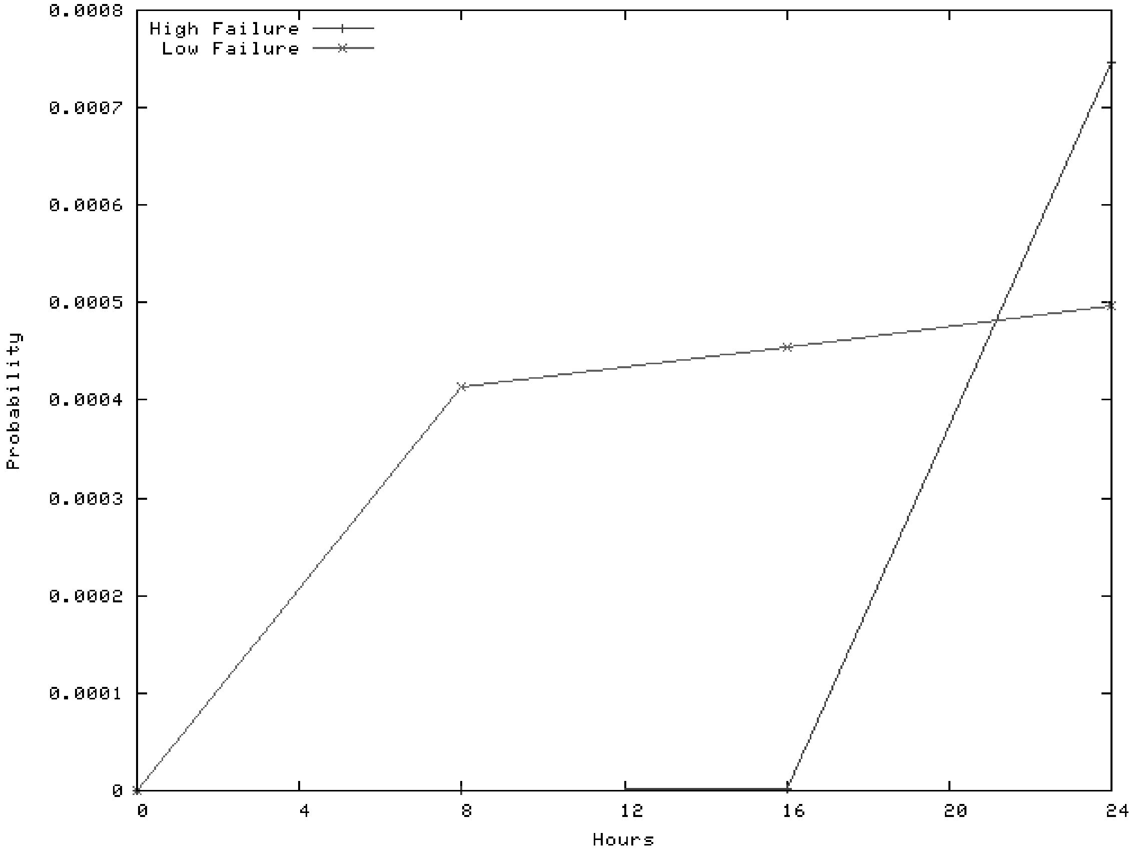


Figure 3.3.13: High Level Probability as a Function of Time

Tables 3.3.4 and 3.3.5 list the top 10 event sequences with the highest probability of occurrence for Low and High failure respectively. The event names in the sequences identify the component (FP, MFV, etc), followed by the state (Stuck, Arbitrary Output, etc), and finally a time tag identifying the order in which the events occur.

As can be seen from Table 3.3.4, MFV in the Stuck state is the dominant event for Low Level failure and Power-Power-Off (i.e., failure of the power source of the MFV, BFV and FP controllers shown in Fig.3.3.7) is the second most dominant event. From Table 3.3.5, MFV Stuck (i.e. the mechanical failure of the MFV shown in Fig.3.3.5) is again the most dominant failure sequence for High Level failure followed by Computer in the Freeze state (e.g., due to a failure in the power source of the computers or a permanent loss of communications between sensors and computers) as the second most dominant sequence.

Table 3.3.4: Low Level Failure Scenarios Ranked By Probability of Occurrence

Cut Set Number	Cut Set Probability	% Total Probability	Component	State	Order
1	3.33E-04	67.02	MFV	Stuck	1
2	1.15E-04	23.25	Power	Off	1
3	3.85E-05	7.76	Comp	Freeze	1
4	3.70E-06	0.74	Comp	Arbitrary Output	1
5	2.61E-06	0.53	FP	Output Low	1
6	1.31E-06	0.26	FP	Arbitrary Output	1
7	8.72E-07	0.18	MFV	Output Low	1
8	8.70E-07	0.18	MFV	Arbitrary Output	1
9	1.11E-07	0.02	MFV	Stuck	1
			FP	Stuck	2
10	1.11E-07	0.02	MFV	Stuck	1
			BFV	Stuck	2

Table 3.3.5: High Level Failure Scenarios Ranked By Probability of Occurrence

Cut Set Number	Cut Set Probability	% Total Probability	Component	State	Order
1	6.64E-04	89.02	MFV	Stuck	1
2	7.69E-05	10.3	Comp	Freeze	1
3	1.74E-06	0.23	MFV	Output Low	1
4	1.31E-06	0.18	MFV	Output High	1
5	4.36E-07	0.06	MFV	Arbitrary Output	1
6	3.32E-07	0.04	FP	Stuck	1
			MFV	Stuck	2
7	3.32E-07	0.04	BFV	Stuck	1
			MFV	Stuck	2
8	3.32E-07	0.04	MFV	Stuck	1
			BFV	Stuck	2
9	3.32E-07	0.04	MFV	Stuck	1
			FP	Stuck	2
10	3.85E-08	0.01	BFV	Stuck	1
			Comp	Freeze	2

Events which occur the most frequently in the failure sequences, without regard to their probability of occurrence, are given in Tables 3.3.6, 3.3.7, 3.3.8 and 3.3.9. Tables 3.3.6 and 3.3.7 list the 5 most commonly occurring events (components and their respective states) and include the time/ order in which that event appears in the sequence. For example, Power in the Off state appears as the third event in 937 sequences or scenarios leading to Low Level failure. Tables 3.3.8 and 3.3.9 list all events without regard to the order in which events occur in a given sequence.

Tables 3.3.6 and 3.3.8 indicate that Power in the Off state, the Computer in the Arbitrary Output state (i.e., the computers are sending random values to the controllers as shown in Fig.3.3.8), and the PDI in the Stuck state (e.g., the PDI is not receiving any data in input and it wrongly recognizes that the MFV controller is not communicating with the MFV) are significant events in the Low Level failure sequences. Tables 3.3.7 and 3.3.9 identify the Computer in the Freeze state and the FP in the Output High state (i.e., the FP controller is sending the highest value to the FP) as the most common event appearing in the High Level failure sequences.

The differences between Tables 3.3.6 and 3.3.8 and between 3.3.7 and 3.3.9 indicate that the occurrence rank order changes when the timing of failure events is considered and hence timing is significant regarding their contribution of the basic events to the occurrence of a given Top Event.

Table 3.3.6: Low Failure Events Ranked by Number of Occurrences (Timing Included)

Low Failure			
Component	**State**	**Order**	**Number of Occurrences**
Power	Off	3	937
Comp	Arbitrary Output	3	781
PDI	Arbitrary Output	1	629
PDI	Stuck	1	616
BFV	Output High	1	563

Table 3.3.7: High Failure Events Ranked by Number of Occurrences (Timing Included)

High Failure			
Component	**State**	**Order**	**Number of Occurrences**
Comp	Freeze	2	825
FP	Output High	1	775
Comp	Freeze	3	760
MFV	Output High	3	669
BFV	Output High	1	651

Table 3.3.8: Low Failure Events Ranked by Number of Occurrences (No Timing)

Low Failure		
Component	**State**	**Number of Occurrences**
Power	Off	1400
PDI	Output Low	1355
PDI	Stuck	1337
BFV	Stuck	1238
Comp	Arbitrary Output	1228

Table 3.3.9: High Failure Events Ranked by Number of Occurrences (No Timing)

High Failure		
Component	**State**	**Number of Occurrences**
Comp	Freeze	2016
FP	Stuck	1585
MFV	Stuck	1576
FP	Output High	1490
PDI	Arbitrary Output	1373

Finally, the Fussell-Vesely (FV) Importance for Low and High Level failure sequences is presented in Table 3.3.10 and 3.3.11 respectively. In both cases, only the top five most significant events are shown. These tables consider both individual events in the sequences as well as their order in the entire sequence. As seen from Table 3.3.10, the MFV in the Stuck state, Power in the Off state, and the Computer in the Freeze state are all significant events for Low Level failure. This agrees with the information presented above in Table 3.3.4. Similarly, Table 3.3.11 indicates the MFV in the Stuck state, the Computer in the Freeze state, and the MFV in the Output Low state are significant events leading to High Level failure, in agreement with Table 3.3.5.

Table 3.3.10: Fussell-Vesely Importance for Low Failure Sequences

Low Failure			
Component	**State**	**Order**	**FV**
MFV	Stuck	1	6.71E-01
Power	Off	1	2.33E-01
Comp	Freeze	1	7.76E-02
Comp	Arbitrary Output	1	7.45E-03
FP	Output Low	1	5.27E-03

Table 3.3.11: Fussell-Vesely Importance for High Failure Sequences

High Failure			
Component	**State**	**Order**	**FV**
MFV	Stuck	1	8.91E-01
Comp	Freeze	1	1.03E-01
MFV	Output Low	1	2.33E-03
MFV	Output High	1	1.75E-03
MFV	Stuck	2	9.50E-04

3.4 Sensitivity Analysis of the Arbitrary Output Implementation

As discussed in Chapter 1, the proposed utilization of the Markov/CCMT is in the inductive mode to verify the prime implicants identified by DFM and their quantification. The Arbitrary

Output mode is a particularly challenging situation since it affects both structure of the decision tables of DFM and the cell-to-cell transition probabilities of Markov/CCMT. The impact of the Arbitrary Output failure for both the computers and all the controllers is evaluated by randomly choosing values between 0-100% for the action of the actuated devices (e.g., 10% aperture for MFV or BFV or 10% of nominal speed for the FP). To determine the effect the choice of the random numbers has on the results, confidence intervals were determined for a set of analyses. Thirty different analyses were run, each with a different random seed used for the Arbitrary Output state valve and pump positions. A 95%- confidence interval was computed based on the information gathered from each of the analyses. This information is shown in Figs. 3.4.1 and 3.4.2 where both graphs are shown in log scale. For High Level failure, the confidence intervals after 8, 16 and 24 hours are 21.64%, 23.25% and 0.048% of the mean respectively. For Low Level failure, the confidence intervals after 8, 16 and 24 hours are 0.041% 0.066% and 0.065% of the mean respectively.

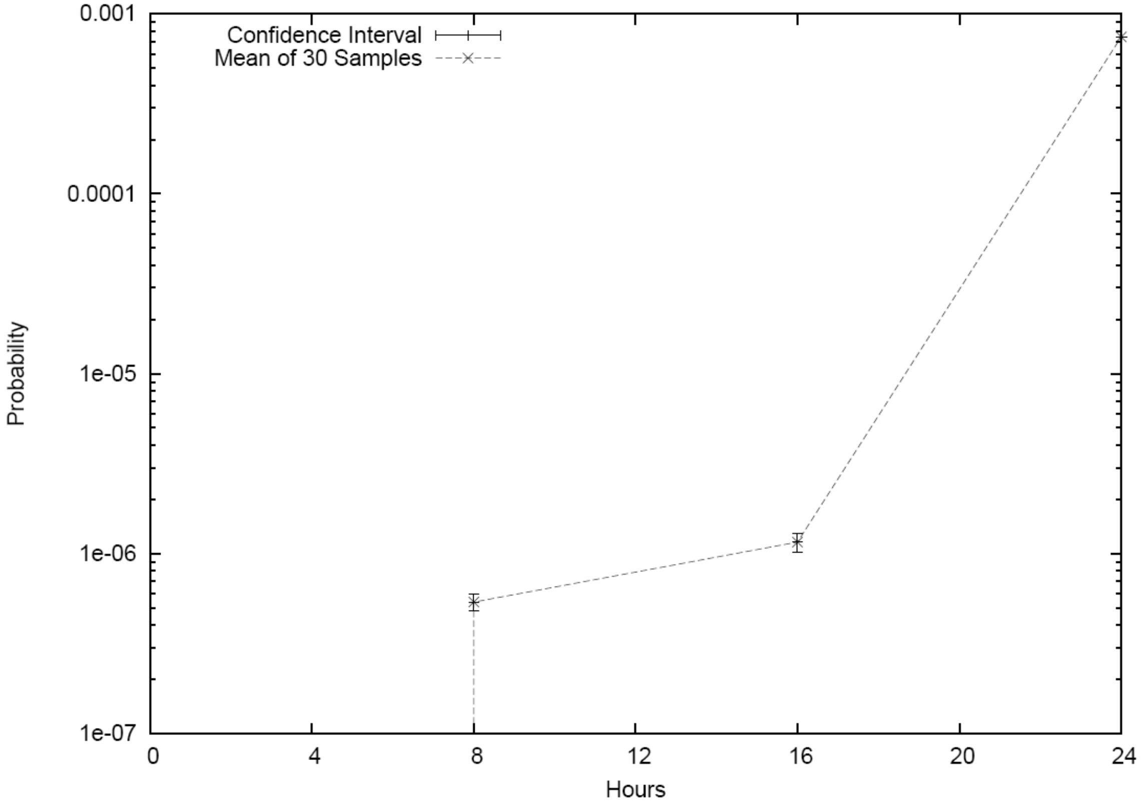


Figure 3.4.1: High Failure Arbitrary Output Confidence Interval

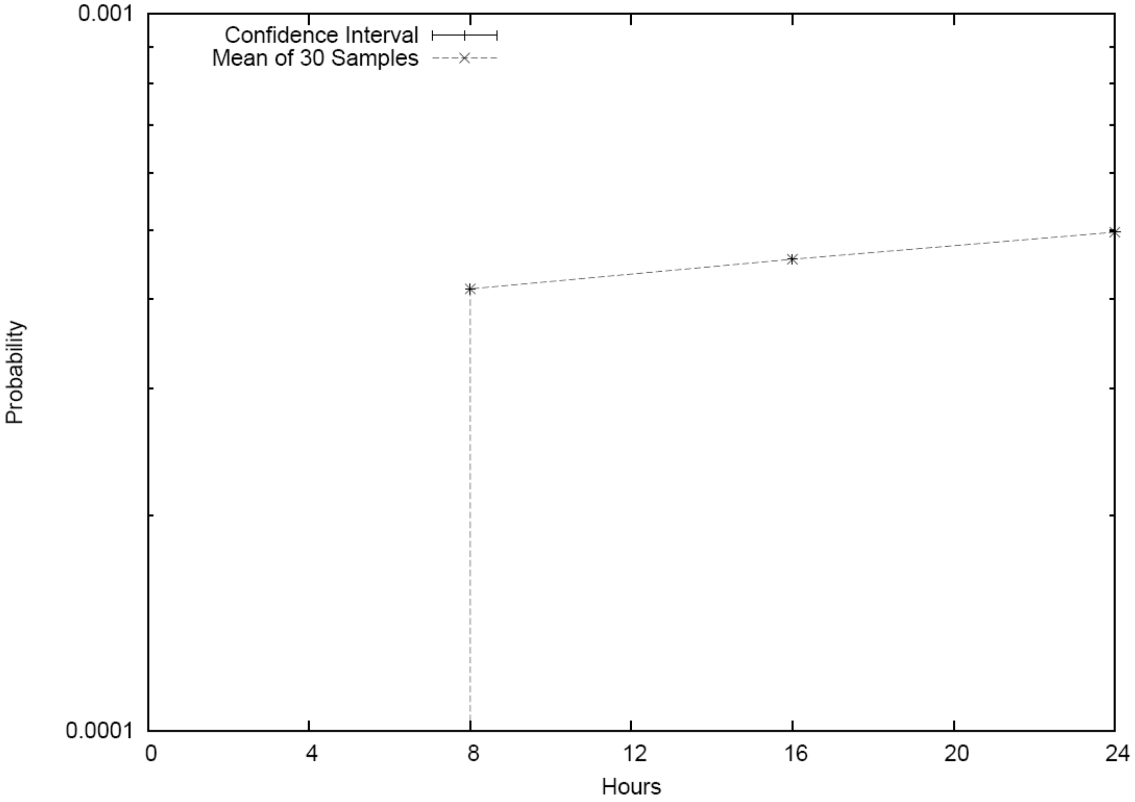


Figure 3.4.2: Low Failure Arbitrary Output Confidence Interval

Table 3.4.1, below, gives the mean probability found for both Low and High failure. These values were found using the total failure probability after 24 hours for low and high failure from each of the 30 samples. Also reported are the minimum and maximum values found.

For Low Level failure, an average probability of 4.963E-4 was found, with a minimum of 4.952E-4 and a maximum of 4.969E-4. For High failure an average probability of 7.461E-4 was found, with a minimum of 7.459E-4 and a maximum of 7.472E-4. The standard deviation from the 30 samples is small.

Table 3.4.1: Probability Data from 30 Samples

	Low	High
Mean	4.963E-04	7.461E-04
Max	4.969E-04	7.472E-04
Min	4.952E-04	7.459E-04
Std Dev	2.771E-19	7.522E-19

The size of the confidence interval changing as the number of samples used increases was also examined. Figs. 3.4.3 and 3.4.4 show these results for Low and High Level failures, respectively. These graphs show several properties of the analysis. The first and most important property is that the confidence interval is shrinking as the number of samples used increases.

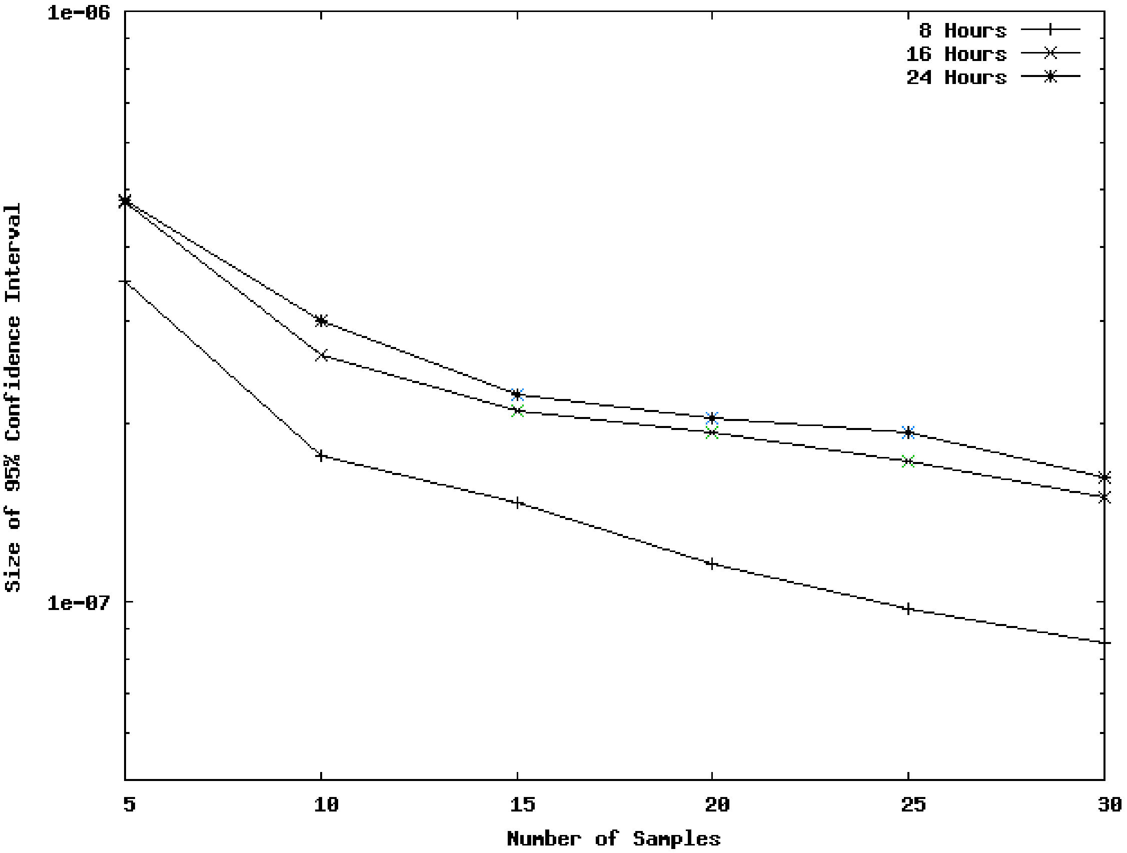


Figure 3.4.3: Size of the 95% Confidence Interval for Low Failure

The 30 samples were averaged together to from a single series of event sequences for analysis. The averaging was performed using an algorithm that compared each sequence to every other sequence to create a master/averaged list of sequences, as well as the number of times each sequence appeared. The probability $\overline{P}(j)$ in Equation 3.4.1 for a given sequence was found by summing the probability generated for that event sequence from each of the 30 runs.

$$\overline{P}(j) = \frac{\sum_{i=1}^{30} P_i(j)}{30} \qquad (3.4.1)$$

where $\overline{P}(j)$ is the averaged probability for the *j*-th sequence, and P_i is the probability found for the sequence *j* in the run *i* (*i*=1,…,30). If the sequence was not found in the run *i*, then P_i=0.

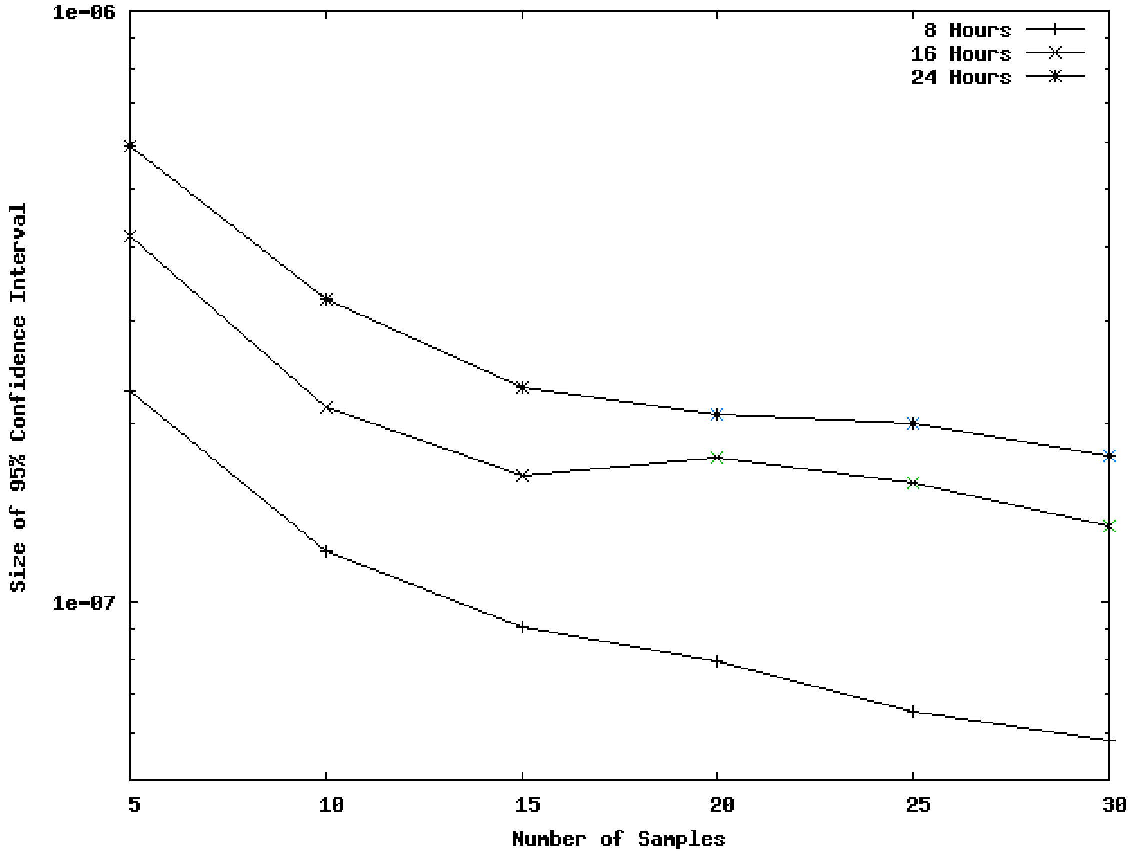


Figure 3.4.4: Size of the 95% Confidence Interval for High Failure

As presented in Section 3.3, the event names in the sequences identify the component (FP, MFV, etc), followed by the state (Stuck, Arbitrary Output, etc), and finally a time tag identifying the order in which the events occur.

The post processing was performed by SAPHIRE [17]. From the Low Level failure scenarios, a total of 142,763 event sequences are generated, with 7,740 unique sequences. The averaged Low Level failure scenarios have an overall probability of occurrence of 4.963e-4, which is consistent with the value reported in Table 3.4.1. Table 3.4.2 shows that 2,626 of the 7,740 sequences appear in each of the 30 samples, and account for over 99% of the total probability (4.962e-4 for the combined 2,626 sequences). Table 3.4.2 also lists how many sequences were repeated in a given number of runs, along with the probability contribution from those sequences. Note that for certain entries, the probability was to low for SAPHIRE to calculate, and thus only an approximation is given.

From the High Level failure scenarios, a total of 152,070 event sequences were generated, with 7,543 unique sequences. The averaged High Level failure scenarios have an overall probability of occurrence of 7.460e-4, which is consistent with the value reported in Table 3.4.1. Table 3.4.2 also shows that 3,542 sequences appear in all 30 samples.

Table 3.4.2: Sequence Information from Averaged Sample

	Low Failure		High Failure	
	Number of Sequences	**Probability**	**Number of Sequences**	**Probability**
Total Sequences	142763	-	152070	-
Unique Sequences	7740	4.963E-04	7543	7.460E-04
30 Occurrences	2626	4.962E-04	3542	7.454E-04
29 Occurrences	211	3.361E-10	90	2.020E-12
28 Occurrences	120	7.401E-10	13	1.0E-17*
27 Occurrences	87	3.235E-13	62	5.992E-11
26 Occurrences	104	5.835E-13	77	5.680E-13
25 Occurrences	196	1.510E-14	66	2.444E-13
24 Occurrences	193	2.445E-10	119	7.311E-10
23 Occurrences	224	2.560E-11	118	2.594E-11
22 Occurrences	95	1.243E-14	128	9.437E-15
21 Occurrences	152	7.594E-14	59	8.327E-15
20 Occurrences	118	3.320E-14	170	3.632E-07
19 Occurrences	121	3.295E-13	57	3.806E-13
18 Occurrences	219	7.772E-16	87	8.241E-13
17 Occurrences	100	2.220E-16	106	1.113E-10
16 Occurrences	76	3.109E-15	147	1.019E-10
15 Occurrences	74	2.322E-10	77	2.443E-17
14 Occurrences	139	2.240E-11	112	2.153E-13
13 Occurrences	70	4.197E-14	132	3.331E-16
12 Occurrences	192	1.372E-13	243	5.551E-16
11 Occurrences	136	5.662E-14	101	1.0E-16*
10 Occurrences	195	1.361E-13	128	2.087E-14
9 Occurrences	114	3.231E-14	141	8.729E-11
8 Occurrences	191	1.110E-16	116	3.740E-13
7 Occurrences	172	2.387E-14	201	1.299E-14
6 Occurrences	110	1.954E-14	181	2.701E-13
5 Occurrences	59	1.887E-15	204	6.783E-11
4 Occurrences	202	1.443E-15	214	1.643E-07
3 Occurrences	419	1.0E-18*	148	8.694E-08
2 Occurrences	449	1.0E-18*	222	2.531E-14
1 Occurrences	576	1.0E-17*	482	5.903E-13

*: Approximation, the probability is too low for SAPHIRE to calculate

Table 3.4.3 presents the 10 most dominant sequences leading to Low Level failure. Table 3.4.4 presents the 10 most dominant sequences leading to High Level failure. The sequence tag presented for each sequence indicates the first occurrence for that particular sequence. For both High and Low Level failures, MFV Stuck is the most dominant failure sequence.

From Table 3.4.3, the sequence with the MFV in the Stuck state as the only event (i.e., the mechanical failure of the MFV as shown in Fig. 3.3.5) dominates, with a probability of 3.33E-4. It accounts for over 67% of the total probability. The sequence with Power in the Off state as the only event (i.e., a failure in the power source of the MFV, BFV and FP controllers) is also significant with a probability of 1.154e-4, accounting for 23.25% of the total probability. The Computer in the Freeze state as the only event (e.g., due to a failure in the power source of the computers or a permanent loss of communications between sensors and computers) is also notable, with a probability of 3.85E-5, 7.76% of the total probability. Each of these sequences appears in all 30 runs. The other 7,737 sequences account for the remaining 2% of the total probability.

From Table 3.4.4, the dominant event sequence for High Level failure is MFV-Stuck-1, with a probability of 6.64e-4. This sequence accounts for 89% of the total probability. Comp-Freeze-1 is also significant, with a probability of 7.69E-5, accounting for 10.3% of the total probability.

These dominant sequences are consistent with what is reported in Section 3.3.2 for a single sample. Table 3.4.3 is similar to Table 3.3.4, and Table 3.4.4 is similar to Table 3.3.5. The differences indicate that there is some sensitivity of the system to the randomness associated with the Arbitrary Output. This data serves as a check to the single run and shows that its results are statistically valid.

Table 3.4.3: Low Level Failure Scenarios from Averaged Sample

Cut Set Number	Cut Set Probability	% Total Probability	Number of Occurrences	Component	State	Order
1	3.33E-04	67.04	30	MFV	Stuck	1
2	1.15E-04	23.25	30	Power	Off	1
3	3.85E-05	7.76	30	Comp	Freeze	1
4	3.53E-06	0.71	30	Comp	Arbitrary Output	1
5	2.61E-06	0.53	30	FP	Output Low	1
6	1.22E-06	0.25	30	FP	Arbitrary Output	1
7	9.43E-07	0.19	30	MFV	Arbitrary Output	1
8	8.72E-07	0.18	30	MFV	Output Low	1
9	1.11E-07	0.02	30	MFV FP	Stuck Stuck	1 2
10	1.11E-07	0.02	30	MFV BFV	Stuck Stuck	1 2

Table 3.4.4: High Level Failure Scenarios from Averaged Sample

Cut Set Number	Cut Set Probability	% Total Probability	Number of Occurrences	Component	State	Order
1	6.64E-04	89	30	MFV	Stuck	1
2	7.69E-05	10.3	30	Comp	Freeze	1
3	1.74E-06	0.23	30	MFV	Output Low	1
4	1.31E-06	0.18	30	MFV	Output High	1
5	3.63E-07	0.05	20	MFV	Arbitrary Output	1

6	3.32E-07	0.04	30	FP	Stuck	1
				MFV	Stuck	2
7	3.32E-07	0.04	30	BFV	Stuck	1
				MFV	Stuck	2
8	3.32E-07	0.04	30	MFV	Stuck	1
				BFV	Stuck	2
9	3.32E-07	0.04	30	MFV	Stuck	1
				FP	Stuck	2
10	1.64E-07	0.02	4	Comp	Arbitrary Output	1

Events which appear frequently in the averaged failure sequences, without regard to their probability of occurrence, are given in Tables 3.4.5, 3.4.6, 3.4.7, and 3.4.8. Table 3.4.5 shows that Power in the Off state is the most commonly appearing event as the third event in a sequence, followed by the Computer in the Arbitrary Output state as again the third failure, and the PDI in the Arbitrary Output state (e.g., due to an internal failure the PDI controller is sending random generated values to the MFV as shown in Fig. 3.3.6) as the first failure. The ranking of the most frequently occurring three events (i.e. Power-Off, Comp-Arbitrary Output, PDI-Arbitrary Output) match those reported in Table 3.3.6 for the single run.

Table 3.4.5: Low Level Failure Events Ranked by Number of Occurrences

Low Failure			
Component	**State**	**Order**	**Number of Occurrences**
Power	Off	3	1215
Comp	Arbitrary Output	3	1143
PDI	Arbitrary Output	1	1076
FP	Arbitrary Output	1	989
FP	Arbitrary Output	2	919

Table 3.4.6 indicates that the PDI in the Arbitrary Output state is the most significant event leading to High Level failure as the first failure. The FP in the Output High state as the first failure and the Computer in the Freeze state as the third failure are also significant events leading to High Level failure. For High failure there is discrepancy between Table 3.4.6 and Table 3.3.7. Table 3.3.7 identifies the Computer in the Freeze state as the second failure as the most dominant event, while the PDI in the Arbitrary Output state is much lower in the list.

Table 3.4.6: High Level Failure Events Ranked by Number of Occurrences

High Failure			
Component	**State**	**Order**	**Number of Occurrences**
PDI	Arbitrary Output	1	1180
FP	Output High	1	938
Comp	Freeze	3	910
BFV	Output High	1	898
Comp	Arbitrary Output	3	892

Tables 3.4.7 and 3.4.8 list all events that appear in the averaged failure sequences, without regarding their ordering information. Table 3.4.7 indicates that the FP in the Arbitrary Output state is the most common event for Low failure, followed by the PDI in the Arbitrary Output state. Table 3.4.8 indicates the PDI in the Arbitrary Output state is the most common event for High failure. There is some variance between these tables and Tables 3.3.8 and 3.3.9 for the single run. However, when ignoring all Arbitrary Output state events, the data from Tables 3.4.7 and 3.4.8 is more consistent with that from Tables 3.3.8 and 3.3.9. As previously noted, a large number of sequences appearing in only a small number of runs contains an Arbitrary Output failure event. If the sample size is increased, it is expected that Arbitrary Output events will appear increasingly dominant.

Table 3.4.7: Low Failure Events Ranked by Number of Occurrences (No Time)

	Low Failure	
Component	**State**	**Number of Occurrences**
FP	Arbitrary Output	2622
PDI	Arbitrary Output	2259
PDI	Output Low	2021
PDI	Stuck	1960
Comp	Arbitrary Output	1941

Table 3.4.8: High Failure Events Ranked by Number of Occurrences (No Time)

	High Failure	
Component	**State**	**Number of Occurrences**
PDI	Arbitrary Output	2478
Comp	Freeze	2420
FP	Stuck	2129
FP	Output High	2022
MFV	Stuck	1973

3.5 Closing Remarks

The Markov/CCMT analysis described in this chapter emphasizes the relevance of the timing of failures to the Top Events (Section 3.3.3), as well as the need to conduct inductive analyses to assure the completeness of event sequences leading to Top Events (Section 3.4) for digital I&C systems. Chapter 4 discusses these issues in more detail and shows that the Markov/CCMT results are in good agreement with the DFM results.

4. DISCUSSION AND PRA-INTEGRATION OF DFM AND MARKOV/CCMT RESULTS

This chapter discusses the features and results of the DFM and Markov/CCMT analyses from both a qualitative and quantitative viewpoint and on a comparative basis, drawing insights from the modeling experience that has been covered by both the DFM and Markov/CCMT analysis teams in the activities documented in NUREG/CR-6942 and in this report. The chapter also discusses how these results can be operatively integrated into the standard framework of a conventional PRA.

Although further insights may emerge from a more extensive range of methodology application experience, the insights gained from the benchmark DFWCS DFM and Markov/CCMT analyses already provide a good level of understanding of the respective modeling capabilities and potential issues. This understanding is sufficient to draw recommendations relative to the future use of the methodologies and to their integration with the framework of a nuclear power plant conventional PRA, and with the standard ET/FT models within it.

Section 4.1 presents general observations comparing and contrasting the application of the two methodologies. Section 4.2 compares the qualitative and quantitative results from DFM and Markov/CCMT for Low and High SG level failures. The incorporation of the Dynamic results into a traditional FT/ET PRA is presented in Section 4.3.

4.1 General Observations on the Methodologies and Their Application

DFM and Markov/CCMT are methodologies that present both similarities and differences from the point of view of their practical application modes. From a top level perspective, on the basis of the current application experience for both methodologies, one can make some comparative observations relative to the areas of:

a. Modeling resolution
b. Nature and depth of analytical results
c. Ease of model quantification
d. Ease of use and availability of application software
e. Integration of results with traditional PRA models

Specific observations concerning the above are presented in the following subsections. A possible overall synthesis of these observations is that DFM can be viewed, in the typical and predictable conditions of trade-off between ease of application and degree of analytical resolution of the produced results, as standing in between the traditional PRA binary logic models (FT/ET) and the multi-valued logic Markov/CCMT models. This observation is generically valid across the range of features, such as those listed above, that may be of interest to a PRA analyst and potential user of the methodologies. As one may expect, however, DFM and Markov/CCMT have their own specific strengths in distinct areas. Therefore, a user who is focused on certain aspects of dynamic modeling and analysis may find one methodology to be more attractive than the other depending on the criteria and features that the user believes to be more important for his/her application.

DFM is available in a relatively mature computerized tool form. This provides potential users with access to the methodology and its capability of blending together, in multi-valued logic representation, both analog and discrete system characteristics, and of unraveling the associated causality flow in both deductive, i.e., from effect to underlying causes, and inductive, i.e., from cause to effect, analysis mode. Markov/CCMT, on the other hand, is a newer development with a less mature set of implementation aids. However, its use in the inductive mode can provide more detailed insight and modeling resolution of reversible state transitions and highly time-dependent effects such as bi-stable or intermittent faults and any dynamic effects that may need to be tracked over a relatively high number of distinct time steps or intervals.

From a conceptual point of view the two methods embody, respectively, different balance points in the trade-off between modeling ease and power of resolution. DFM works best with a coarser time-discretization, enabling deductive analysis at the expense of full dynamic fidelity, whereas Markov/CCMT users can use a finer discretization in the model set-up, which enables greater dynamic effect fidelity at the expense of deductive analytical capability and the associated logic completeness[16] of the identified prime implicant sets. This suggests that the two methodologies should be viewed as being mutually-complementing, i.e., used in combination with the blending strategy for implementation to be determined on the basis of the specific nature of the system to be modeled and type of results that may be of interest. This is stated here simply as an anticipation of further discussion, which the reader will find in Chapter 5.

4.1.1 Modeling Resolution

Although the characteristics of the respective modeling constructs are such that it is actually possible to mimic with one methodology the fundamental characteristics of the other, the natural dispositions of the two types of models are such that DFM is primarily oriented towards the description of cause-effect flows with moderate capability of following time progressions via discrete time step approximations, whereas Markov/CCMT offers a much greater time resolution capability, obtained at the expense of computational complexity. Markov/CCMT, however, can also more compactly represent bi-stable and flip-flop parameter conditions, such as those that occur in the presence of intermittent failures. The inductive analysis process applied in conjunction with the Markov/CCMT modeling is also well suited for the representation of arbitrary output from a digital component or device.

4.1.2 Nature and Depth of Analytical Results

Consistently with its greater time-dependence representation capabilities, Markov/CCMT can produce very detailed inductive analyses involving a relatively large number of forward time steps. In principle, it is capable of deductive analysis [35]. However, its use in deductive analysis can be computationally costly for a large system (e.g., similar in complexity to the benchmark DFWCS system introduced in Section 1.2), due to the multiple point representations

[16] Logic completeness indicates that the set of prime implicants that can be identified via logic analysis of a model, executed inductively or deductively, is complete with respect to the definition of the logic model itself, i.e., no other prime implicants exist that the analytical process has not / can not identify.

of cells in the generation of cell-to-cell transition probabilities (see Section 3.2). For the DFM, on the other hand, the model generation time is shorter and the analytical process permits complex deductive analyses, such as those discussed in Chapter 2, to be completed with a few hours of computation time. However, large models with variables discretized into many separate states for dynamic effect fidelity cannot be backtracked in time for more than a couple of reverse time steps without running against the computational speed limits of current-generation personal computers.

4.1.3 Modeling Complexity and Availability of Application Software

Both methodologies are objectively more complex and more difficult to apply in effective fashion than a typical PRA ET/FT paradigm. However, the construction of a system model with Markov/CCMT is arguably by level of abstraction more difficult to conceptualize than a corresponding DFM model, although as stated earlier the former type of model will typically provide more time-related resolution power in inductive analysis mode than the latter. Markov/CCMT is also a newer development and thus the associated implementation software tool presently exists only in prototype research edition. To facilitate DFM applications, a software tool called DYMONDA^{TM} exists in commercial beta-version form, and provides both model editing capabilities and inductive / deductive analytical capabilities, although its proper use requires a fair amount of user-training effort.

4.1.4 Ease of Model Quantification

One of the perceived difficulties of digital I&C and/or software-intensive system modeling and analysis is in the quantification aspects.

DFM permits quantification of its models in both inductive and deductive analysis mode, as discussed and illustrated in Chapter 2. DFM quantification is no more difficult than an ET/FT cut-set quantification since the DFM analyses produce prime implicant results that are the multi-valued logic equivalent of binary cut-sets prior to quantification.

Markov/CCMT produces results also in prime implicant form, but arrives at this via the solution of combinations of state-transition equations that need to be quantified via the definition of state transition frequencies or conditional probabilities at each modeling time step. While providing greater fidelity in the representation of the interaction of the digital I&C system under consideration with the controlled/monitored process, such quantification may represent a computational challenge for the users. In the case of the application discussed in Chapter 3, the challenge has been addressed via a two step process that has as primary objective the condensation of system model states into a reduced number of super- or macro -states. This approach is viable also from the point of view of reducing the complexity of the initial system model and thus streamlining the computational solution burden. However, it does introduce one additional step in the application of the methodology and correspondingly increases the model complexity for validation and verification purposes.

4.1.5 Integration of results with traditional PRA models

The utilization of DFM deductive analysis results within framework of a conventional PRA and relative ET/FT system models is a straightforward matter, given the conceptual and practical similarity between multi-valued logic DFM prime implicants and binary ET/FT cut-sets. The associated integration process typically mimics the process of integrating an ET model quantification with the quantification of fault-trees developed for its initiating and/or pivotal events. This process is discussed in detail in Section 4.3, and has also been extensively demonstrated and discussed in a recent NASA study [36].

Inductive analysis results from DFM or both the deductive and inductive analysis results from Markov/CCMT can also be successfully integrated with a PRA framework and associated ET/FT models. This is also discussed in Section 4.3 of this chapter. As is always the case with inductive analyses, the question of completeness (see footnote on page 4.2) in identifying all significant contributors to a given risk scenario remains here more open than in the case of a set of contributors that are deductively-obtained for the same scenario. To put this in perspective, however, it must also be said that the completeness of a deductively-obtained set of prime-implicants may come at a price, since the coarser DFM discretization process that makes a deductive solution possible in the first place may potentially limit the fidelity of the models and impact the degree of accuracy of the associated results. This potential issue of formal logic completeness versus practical model fidelity is not unique to the Markov/CCMT and DFM approaches discussed here, but affects all approaches that rely on either a march-forward or march-backward analytical solution algorithm. Full time-dependent simulation or randomized-sequence generation approaches that have been discussed in the dynamic-PRA literature over the course of the past decade are examples of inductive analyses that have high model fidelity for any given initial system condition that is used to start a simulation, but remain open-ended in terms of demonstrating completeness in the identification of possible initial conditions/faults that may lead to a pre-defined end state. Binary (i.e., fault / no-fault representations) used in fault-tree models are at the opposite end of the spectrum, in that they can only offer a very coarse system representation, but, within that, are capable of providing a complete and exhaustive identification of system component events that can lead to a pre-defined Top Event system condition.

4.2 Comparison of Results

The comparison presented here completes the overview of what has been learned from the application of the two methodologies to the DFWCS benchmark, before proceeding in the next section to discussing the integration of DFM and Markov/CCMT results with conventional PRA models.

It should be kept in mind that the DFM and Markov/CCMT teams operated separately in performing the respective DFWCS analyses. This resulted in modeling flexibility that is reflected in the formats in which the respective results have been obtained. This mode of operation was chosen to minimize cross-influencing of the teams in modeling choices and subsequently to maximize the likelihood of identifying potential challenges in the future applications other dynamic methodologies to the PRA modeling of digital I&C systems. To facilitate the correct interpretation by the reader, an explicit effort has been made here to explain the why and how some additional analyses were executed when it appeared necessary to do so. For example, as more specifically discussed below, a more direct and consistent comparison between the DFM and Markov/CCMT quantitative results for the High SG Level Top Event was made possible by extending the DFM deductive analysis by an additional time step with respect to the initial baseline analysis performed in the DFM deductive mode and discussed in Chapter 2.

In general, the results obtained from the DFM and Markov/CCMT analyses exhibit close consistency. The qualitative and quantitative comparison of the results for the Low SG Level and High SG Level events are summarized in Tables 4.2.1 and 4.2.2, respectively. The DFM baseline analyses leading to these results and considered in this discussion are the deductive analyses presented in Sections 2.3.2.1.1 and 2.3.2.1.2. These analyses cover potential faults occurring in successive 8 hour long time-steps. More specifically, for the Low SG Level failure scenario, the baseline DFM deductive analysis covers two time steps, identifying those basic fault conditions that may occur during the power ramp-up phase (from 70% to 78% power) and cause the low SG level Top Event to occur during the 8 hour ramp up or the 8 hour 78% power steady state period. For the High SG Level Top Event, the initial DFM baseline analysis identified basic fault conditions to occur during the ramp-down phase (78% to 70% power) which would lead to the High SG Level Top Event to occur during the 8 hour ramp down or the 8 hour steady state period immediately following the ramp down.

Table 4.2.1: Comparison of Low SG Level Results

Comp Attribute	**DFM**	**Markov/CCMT**
Probability (8 hr ramp-up only)	4.19E-04	4.15E-04
Highest Contributor	Main feed valve stuck	Main feed valve stuck
2nd Contributor	Computer & Controller Power	Computer Power
Time of Basic Failure Event Covered by Analysis	8 hour ramp-up period	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)
Time interval for Top Event to occur	8 hour ramp up (70% to 78%), or 8 hour steady state (78%)	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)

Table 4.2.2: Comparison of High SG Level Results

Comp Attribute	**DFM** **Baseline Analysis**	**DFM** **Extended Analysis**	**Markov/CCMT**
Probability (high level manifestation during 8 hr ramp-down only)	3.34E-04	6.68E-04	7.40E-04
Highest Contributor	Main feed valve stuck	Main feed valve stuck	Main feed valve stuck
2nd Contributor	Main feed valve controller (arbitrary pos & high) pos)	Main feed valve controller (arbitrary pos & high) pos)	Comp Freeze
Time of Basic Failure Event Covered by Analysis	8 hour ramp down (78% to 70%)	8 hour steady state (78%) and 8 hour ramp down (78% to 70%)	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)
Time interval for Top Event to occur	8 hour ramp down (78% to 70%) or 8 hour steady state (70%)	8 hour steady state (78%), 8 hour ramp down (78% to 70%), or final steady state (70%)	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)

The extended analysis for the DFM case for High SG Level Top Event was carried out for an extra 8 hour time step to obtain quantitative results more directly comparable with the Markov/CCMT results. The analyst's choice of time intervals for the baseline DFM deductive analysis coverage, on the other hand, was made on the basis of two primary considerations of a different nature from the comparison objective stated above. The first of these two factors was the desire to focus analytical attention on the power maneuver time intervals where the failure of interest (i.e., the basic events causing a Low or High SG Level Top Event) would be expected to occur. For example, one would expect that a feedwater and SG level deficiency would be more likely to originate during a power ramp up, since in such a regime most types of faults in the DFWCS would likely cause the SG to dry up. Conversely an excess in feedwater and SG level would more likely be originated during a power ramp down. The second contributor to the time span analysis choice was the need to limit the computational load of the deductive analysis by controlling the number of time steps backtracked in the analysis. For example, once it was found by the High SG Level Top Event analysis that a main feedwater valve stuck condition would be a primary cause for the event during the ramp-down period, the analysts reasoned that an explicit DFM analysis was not necessary to be able to conclude that a main feedwater valve stuck condition during the preceding steady-state at 78% power would also produce the High SG Level Top Event once power started to decrease during the ramp-down period. In addition, it was also concluded that this would not be true during the initial ramp-up period, since the same condition would lead to a Low SG Level event, as already identified and confirmed by the DFM deductive and inductive analyses for the Low SG Level Top Event. In other words, combining direct DFM deductive results from the baseline analyses with the analyst's reasoned interpretation of these, it was possible to conclude that the above mentioned basic event leading to a High SG level failure could be a leading contributor in the 78% steady state or in the ramp down interval from 78% to 70% power, but not in the ramp up time interval.

In quantitative terms, since the failure rate for the main feedwater valve stuck failure mode is constant in time, all of the above indicated that the probability contributed by the main feedwater failure mode to the High SG Level Top Event during the overall 24 hour power maneuver (ramp up, steady state, ramp down), could be expected to be twice the contribution of the 8 hour ramp-down, since no contribution could be expected during the 8 hour ramp up interval. This was in substantial agreement with the quantitative results of the Markov/CCMT inductive analysis of the High SG Level Top Event, which covered the entire 24 hour maneuver (but showed the probability to remain practically nil during the initial ramp-up interval). This agreement, as explained above, was partially deduced, rather than directly proven by the baseline analysis. To obtain a direct analytical confirmation and a more direct comparison with the Markov/CCMT results, the analysts deemed useful to extend the original DFM deductive analysis of the High SG Level Top Event by an additional 8 hour time step, covering the 78% 8-hour steady-state period as well as the ramp-down and the final 70% power steady state condition. The results of the two DFM analyses for the High SG Level Top Event, referred to respectively as the DFM Baseline Analysis and DFM Extended Analysis, are shown in Table 4.2.2, together with the Markov/CCMT results.

The baseline DFM deductive analyses focused primarily on two 8 hour successive time-windows rather than an entire 24 hour power maneuver cycle, on the basis of the practical engineering judgment that, everything else being equal, a low SG level failure is much more likely to occur during a power ramp-up transient than during any other plant condition, and that, conversely, a high SG level failure is much more likely to occur during a power ramp-down transient than during any other plant condition. By focusing the analysis in such a fashion the analysts were able to avoid unnecessary computational burdens.

For the comparison of quantitative results, Markov/CCMT results relative to certain 8 hour spans (e.g., those which appear in Table 4.2.1) are obtained from the failure probability versus time plots over 24 hours that are presented in Chapter 3. The Tables 4.2.1 and 4.2.2 also summarize a qualitative comparison of results by showing the key contributors to the Top Events of interest identified, respectively, by the DFM and Markov/CCMT analyses. In this latter respect the comparison in the tables is not strictly speaking in completely equivalent terms, because the Top Event contributors identified in the Markov/CCMT analyses are relative to the entire 24-hour power maneuver, whereas the corresponding DFM qualitative results are relative to an 8 hour or 16 hour time span.

Keeping all of the above in mind, one can nevertheless see from the data summarized in the tables that:

- The DFM and Markov/CCMT probability values and qualitative results (i.e., contributor rankings) produced for the Low SG Level events are unconditionally in good agreement.

- The DFM and Markov/CCMT quantitative and qualitative results for the High SG Level event need to be interpreted carefully but are also essentially in agreement when appropriately re-baselined to account for the underlying modeling and analytical coverage, i.e., the DFM Extended Analysis case, rather than the Baseline case originally discussed in Chapter 2, is developed and compared with the Markov/CCMT analysis.
- The qualitative difference that appears to exist in the 2nd highest contributor to the High SG Level Top Event, is the result of a Markov/CCMT modeling choice. In fact the Comp Freeze state that appears in the qualitative portion of the Markov/CCMT results is a super-state produced by the state-reduction step of the Markov/CCMT modeling procedure. This super-state groups together a set of lesser contributors, which appear individually in lower rank positions of the DFM list of importance, and makes them as an aggregate appear as a larger and more important contributor in the Markov/CCMT ranking. It is worthwhile noting, however, that the 3rd Markov/CCMT contributor corresponds to the DFM 2nd contributor, and that this contributor, without the introduction of the Comp Freeze super-state, would actually rank as the 2nd most important contributor in the Markov/CCMT list as well.

In summary it can be concluded that the results produced by the application of the two methodologies to the DFWCS benchmark system, although obtained by means of substantially different modeling and logic analysis processes, are in close qualitative and quantitative agreement.

4.3. Incorporation of Dynamic Model Results into a PRA

This section discusses how the dynamic methods, DFM and Markov/CCMT, can be integrated with a traditional plant PRA developed with binary ET/FT methodology.

Three distinct cases cover the entire range of situations for which integration of dynamic results may need to be performed. These cases are when the failure of the dynamic system is:

A. the initiating event of an event-tree of the plant PRA (Section 4.3.1),

B. a pivotal event/Top Event in an event tree of the plant PRA (Section 4.3.2), or

C. an intermediate event of a fault-tree of the plant PRA (Section 4.3.3)

In all three cases, the probability (or frequency) of occurrence of the dynamic system failure can be derived by applying the DFM and/or Markov techniques as illustrated in Chapters 2 and 3. If the basic events identified by the dynamic models do not also appear as basic events elsewhere in the standard PRA models, the dynamic model result integration into the standard PRA models is straightforward as shown in Sections 4.3.1, 4.3.2 and 4.3.3. This process is illustrated in Section 4.3.1 for the case where the initiating event of an event tree is assumed to be the failure of a dynamic system modeled via DFM and Markov/CCMT. Section 4.3.2 shows the case where the failure of the dynamic system is a pivotal event in a PRA event tree. Section 4.3.3 illustrates the case, reproduced from NUREG/CR-6942 [14], where the failure of a dynamically modeled system constitutes the intermediate event of a conventional PRA. The traditional PRA models used here are based on one of the nuclear power plants studied in the

NUREG-1150 [15] PRA study. Finally, PRA/dynamic model integration when common basic events are present is described in Section 4.3.4.

One more factor that needs to be considered, in order to carry out the PRA integration of a dynamic model in a way that correctly preserves all its necessary qualitative and quantitative aspects, is the existence of correlation – i.e., common basic events – across the interface between the conventional PRA models and the dynamic models. This situation is discussed in Section 4.3.4.

4.3.1 PRA/Dynamic Model Integration through an ET Initiating Event (Case A)

When the initiating event of a traditional PRA event tree is the failure of a dynamic system, dynamic models such as DFM and/or Markov/CCMT models can be constructed and solved to obtain the probability, or frequency, of the initiating event. If the prime implicants of the initiating event do not contain basic events that also appear elsewhere in the overall PRA model, the probability of occurrence of the initiating event from the dynamic models can be used in the traditional PRA event tree. This is illustrated with the examples given below for DFWCS High SG Level Failure and Low SG Level Failure states.

Standard ETs are used to describe the plant response to initiating events corresponding to steam generator High Failure and Low Failure modes. Incorporation of the DFWCS initiating events in the ETs is straightforward, as only the failure frequency of the DFWCS events needs to be used in the ETs themselves.

In this case, new ETs are created to model the plant's response to the initiating event/failure of the dynamic system. One ET is created for each failure mode of the dynamic system. Thus for the DFWCS two ETs are required: one for High Failure and one for Low Failure. End states for these new ETs will transfer to other ETs present in the PRA as discussed below. The initiating event frequency for each failure mode is the failure frequency obtained from the DFM or Markov/CCMT model; no other information is retained.

Fig. 4.3.1, below, models the plant response to the DFWCS failing from a High SG Level state. In this scenario, the high water level in the steam generator would lead to a turbine trip. The turbine trips to protect the turbine from damage. The reactor then trips in response to the turbine trip. If both the turbine and reactor trips occur, the ET will transfer to End State 1, and leads to the Loss of Main Feedwater event tree FT2. If the reactor trip does not occur, the ET transfers to the End State 2, and leads to the Anticipated Transient Without Scram (ATWS) ET. Event sequences 3 and 4 of Fig.4.3.1 are not further investigated in this report as the PRA is only focused on core damage sequences.

Fig. 4.3.2, below, models the plant response to the DFWCS failing in the Low SG Level state. In this scenario, the low water level in the steam generator would lead directly to a reactor trip. The reactor trip occurs in order to protect the reactor core as the reactor heat sink, the SG, has been lost. A turbine trip is also supposed to follow in response to the reactor trip. If both the reactor trip and turbine trip occur, the ET transfers to the Loss of Main Feedwater ET, FT2. If the reactor does not trip, the ET transfers to the ATWS ET, FT2TK. Again, scenarios in which the turbine does not trip are ignored in this illustration analysis.

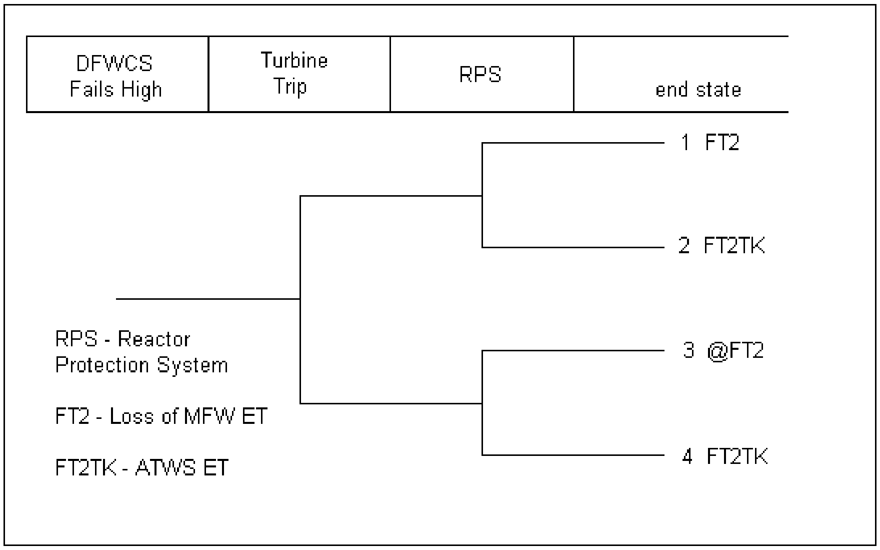


Figure 4.3.1: DFWCS Fails High ET

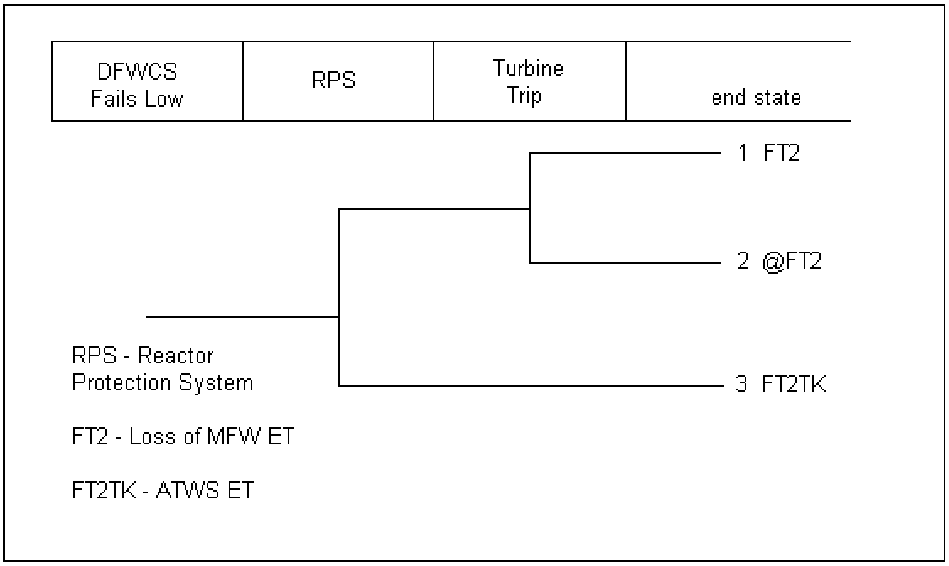


Figure 4.3.2: DFWCS Fails Low ET

Fig. 4.3.3 shows the Loss of Main Feedwater ET that is linked to both the DFWCS High and Low failure ETs in Figs. 4.3.1 and 4.3.2. This ET is used in both above cases as the DFWCS has failed, compromising the MFW system. From Fig.4.3.3, it is seen that the plant will first attempt to close safety relief valves (SRV) and pressure relief valves (PORV) to keep coolant in the vessel. Failure to do so will result in a loss of coolant accident, and ET logic is transferred to an ATWS ET. If the SRVs and PORVs successfully close, then the auxiliary feedwater system (AFW) will attempt to maintain a supply of water to the reactor vessel. If the AFW system should fail, high pressure injection (HPI) and/or PORVs will open for feed and bleed to provide coolant to the core. Should these systems fail the low pressure recirculation (LPR) and high pressure recirculation (HPR) systems will be needed to protect the core from damage.

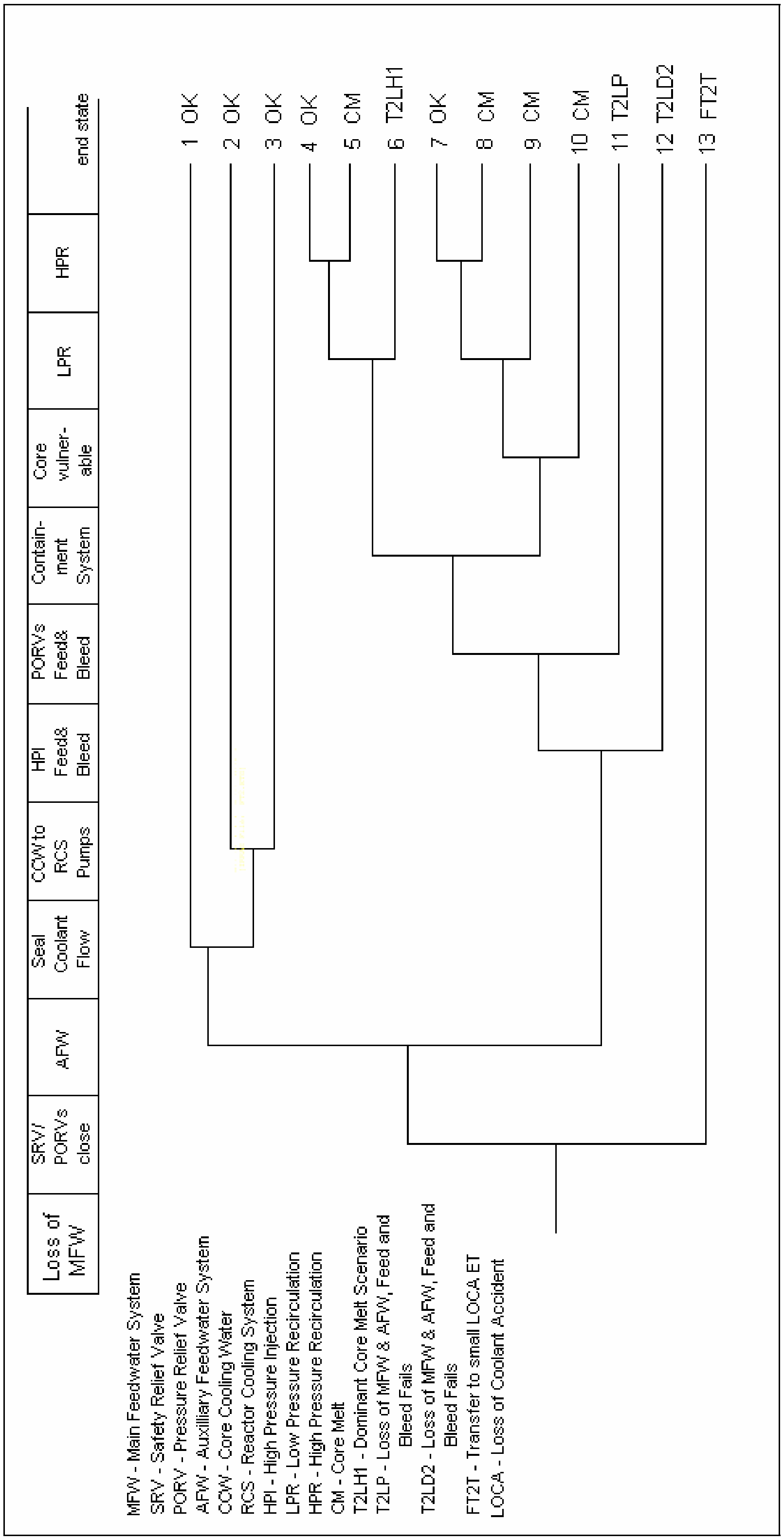

Loss of MFW
SRV/ PORVs close
AFW
Seal Coolant Flow
CCW to RCS Pumps
HPI Feed& Bleed
PORVs Feed& Bleed
Contain-ment System
Core vulner-able
LPR
HPR
end state
1 OK
2 OK
3 OK
4 OK
5 CM
6 T2LH1
7 OK
8 CM
9 CM
10 CM
11 T2LP
12 T2LD2
13 FT2T
MFW - Main Feedwater System
SRV - Safety Relief Valve
PORV - Pressure Relief Valve
AFW - Auxilliary Feedwater System
CCW - Core Cooling Water
RCS - Reactor Cooling System
HPI - High Pressure Injection
LPR - Low Pressure Recirculation
HPR - High Pressure Recirculation
CM - Core Melt
T2LH1 - Dominant Core Melt Scenario
T2LP - Loss of MFW & AFW, Feed and Bleed Fails
T2LD2 - Loss of MFW & AFW, Feed and Bleed Fails
FT2T - Transfer to small LOCA ET
LOCA - Loss of Coolant Accident

Figure 4.3.3: Loss of Main Feedwater ET

]

Note that the ET described in Fig.4.3.3 has been slightly modified from the original version presented in the example plant PRA [Reference NUREG 1150]. In the original PRA from NUREG-1150, the first Top Event following the Initiating Event (Loss of Main Feedwater) is the RPS. The RPS Top Event has been removed from the ET in Fig.4.3.3 as this event already appears in the previous event trees for DFWCS High and Low failure (Figs. 4.3.1 and 4.3.2) and should not be double-counted. This minor change to the original PRA is needed to maintain the overall logical consistency of the combined models.

Failure frequencies for High and Low (SG level) failure (as determined from either the Markov/CCMT model or the DFM model) will need to be input as the initiating event frequencies. As mentioned above, the RPS system was removed from the Loss of MFW ET. It is also noted that the ATWS ET called by the DFWCS High and Low failure ETs is also already present in the PRA and needs no adjustments.

The DFM and Markov/CCMT results, originally generated as frequency/day, are converted to be frequency/year before they are inserted as the IE in the DFWCS failure ETs. The core damage end state probabilities are calculated and shown in Table 4.3.1. The sequence numbers identify the sequences from the loss of MFW ET in Fig.4.3.3. In Table 4.3.1, the core damage end state frequencies are per year. These sequence results may be gathered into end states as normally done in a traditional PRA, combining the results with similar end states from other ETs in the PRA. Uncertainty, Importance, and Sensitivity analysis may all be performed as normal in a traditional tool such as SAPHIRE, RISKMAN, or CAFTA.

Table 4.3.1: Sequence Failure Frequencies per Year

Sequence	End State	Frequency
High-5	CM	2.586E-10
High-6	dominant CM	1.530E-07
High-8	CM	5.171E-10
High-9	CM	3.061E-07
High-10	CM	3.233E-06
High-11	CM	5.901E-06
High-12	feed & bleed fails	5.834E-06
High-13	small LOCA	7.039E-04
Low-5	CM	1.720E-10
Low-6	dominant CM	1.018E-07
Low-8	CM	3.441E-10
Low-9	CM	2.037E-07
Low-10	CM	2.152E-06
Low-11	CM	3.927E-06
Low-12	feed & bleed fails	3.882E-06
Low-13	small LOCA	4.684E-04

4.3.2 PRA/Dynamic Model Integration through an ET Pivotal Event (Case B)

When a pivotal or Top Event of an event tree (in the plant PRA model) is the failure of a dynamic system, dynamic models such as DFM and/or Markov/CCMT models can be constructed and appended to the plant PRA, so that the prime implicants/cut sets and the probability of occurrence of that pivotal event can be derived and integrated back into the plant PRA.

In this case, the dynamic system is viewed as another system being called upon as the plant responds to an initiating event (such as a turbine trip, station blackout, or loss of coolant accident). From a modeling perspective, one or more ETs present in the existing plant PRA are modified to include new Top Events. These Top Events model the failures of the dynamic system. New FT logic will be required to describe the new ETs. This information will be obtained from the DFM and Markov/CCMT models as described below. This is illustrated with the DFWCS High Failure and Low Failure states under a turbine trip initiating event.

In this example, failure of the DFWCS is viewed as another failure mode for the entire MFW system. This results in three failure modes for the MFW system: High Failure resulting from failures to the DFWCS, Low Failure resulting from failures to the DFWCS, and Low Failure resulting from mechanical failures to the MFW itself (as modeled in the existing plant PRA using a standard FT). In this approach, an ET modeling the plant response to a turbine trip is modified to incorporate failure effects of the DFWCS.

It should be noted that the DFM and Markov/CCMT models discussed in Chapters 2 and 3 analyzed a power maneuver under high power conditions, as discussed in Section 1.4. However, for the current scenario a more appropriate model would be one considering low power conditions, since, after a turbine trip, the reactor is shut down and the plant enters its low power operating mode. Although models specifically accounting for post-trip mode of DFWCS and auxiliary feedwater system operation may actually yield different prime-implicants and probabilities from those documented in Chapters 2 and 3 and relative to DFWCS high power mode, the process of integrating the results is the same. Thus, in the following purely demonstrative illustration of the process, the DFWCS failure modes and probabilities obtained in Chapters 2 and 3 from the DFM and Markov/CCMT models are used as substitutes for the corresponding system failure modes and probabilities that would apply under turbine trip conditions.

Section 4.3.2.1 describes the portion of the example plant PRA used in this case. Section 4.3.2.2 describes the process to import the dynamic model results into a PRA tool. Section 4.3.2.3 describes the procedure to link the dynamic model with the plant PRA. Section 4.3.2.4 discusses quantification of the integrated dynamic model and existing PRA, and Section 4.3.2.5 discusses further analysis.

4.3.2.1 Description of Relevant PRA Models

An example ET in which the status of the MFW system is a pivotal event is given in Fig.4.3.4 [15]. This ET models the plant's response to a turbine trip, while assuming that MFW is still available in the event that the AFW system fails (this may be the case in plants where the MFW pumps are electrically driven and electric power is not lost as a result of the turbine trip initiating event). This ET was described in detail in NUREG/CR-6942 and so will only be summarized here.

As can be seen by the ET, the plant first response to the turbine trip would be to scram the reactor through the reactor protection system (RPS). Failure of the RPS to scram the reactor will lead to an anticipated transient without scram (ATWS), and is modeled in a separate event tree (not shown here). After a successful reactor scram, the SRVs must close (failure to do so leads to another separate event tree modeling further plant actions in this scenario). With the reactor scrammed and the relief valves closed, the AFW system must then provide water to the steam generators, maintaining a heat sink for the reactor core.

If the AFW system is unable to provided adequate water to the steam generators, then the MFW is brought back online to provide cooling water to the generators. Failure of both of these systems will require High Pressure Injection (HPI), and opening of the relief valves for feed and bleed, and could possibly lead to core damage. Successful operation of the auxiliary or main feedwater system will result in a safe condition for the plant, as water is supplied to the steam generators to carry away decay heat from the reactor core.

It is important to note that the example plant PRA model represents a simplified PRA and is not complete. The MFW included in the NUREG-1150 [15] models takes a black-box approach; it is simply a basic event with a given failure probability (2.900E-03). Therefore, a simplified MFW fault tree was constructed to provide a more detailed PRA to integrate with the DFM and Markov/CCMT models.

A generic MFW system was modeled representative of a typical plant MFW system but is not based on any one plant. Water is drawn from three condensers and is pumped to the two steam generators. Make-up water to the condensers is supplied from the condensate storage tank. The system has numerous motor-operated valves, as well as two check valves, one per steam generator. The motor operated valves control the flow from the water sources to the steam generators. The check valves help to protect against backflow from the steam generators. The system has a total of five motor-operated pumps.

The failure data for all system components were taken from the NUREG-1150 example plant PRA data. The resulting MFW fault tree has 123 minimum cut sets, with a failure probability of 3.051e-03. This is comparable to the value of 2.90e-03 presented in the NUREG-1150 example plant for the MFW.

4.3.2.2 Importing the Dynamic Model

The Markov/CCMT and DFM methodologies identify additional event sequences (corresponding to the failure of the DFWCS) which would lead to failure of the MFW system. These event sequences can be combined with an existing plant PRA in order to produce a full-scale model. While in NUREG/CR-6942 [14], the Markov/CCMT and DFM results were used to generate FTs which were then linked with the existing PRA, here the failure sequences are simply combined with the FT cut sets from the existing PRA. This approach may be simpler and less memory-intensive in case one may be dealing already with relatively large PRA FT models.

The following basic procedure can be used to generate cut sets for the complete PRA:

1 – Import FT cut sets and Basic Event data through the MAR-D toolset.
2 – Edit plant ETs to include newly imported FTs.
3 – Solve pre-existing FTs to generate cut sets.
4 – Solve ET sequences for Cut Sets, using the Cut Set method.

5 – Gather End State cut sets.
6 – Perform any additional analysis desired.

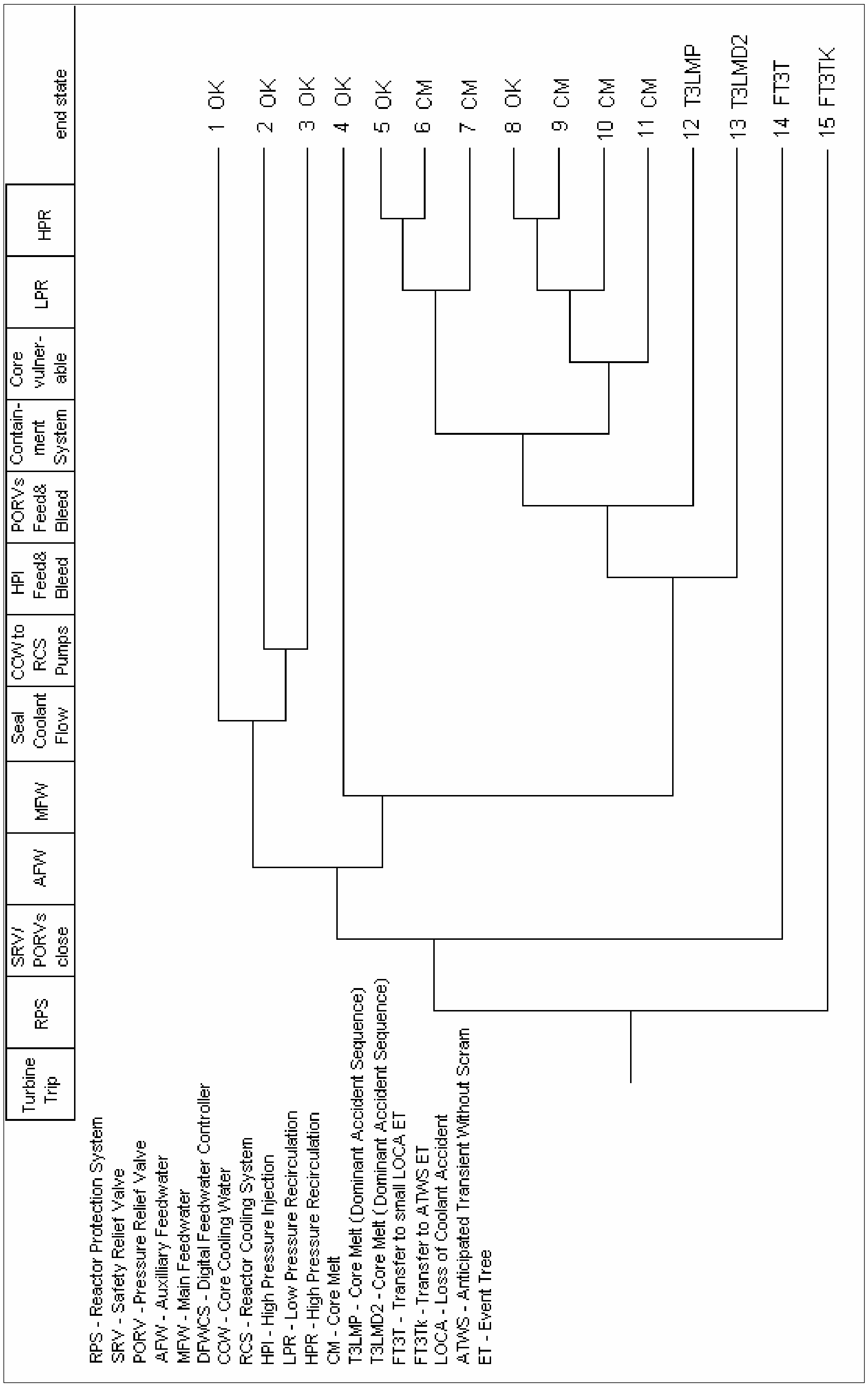

Turbine Trip
RPS
SRV/ PORVs close
AFW
MFW
Seal Coolant Flow
CCW to RCS Pumps
HPI Feed& Bleed
PORVs Feed& Bleed
Contain-ment System
Core vulner-able
LPR
HPR
end state
1 OK
2 OK
3 OK
4 OK
5 OK
6 CM
7 CM
8 OK
9 CM
10 CM
11 CM
12 T3LMP
13 T3LMD2
14 FT3T
15 FT3TK
RPS - Reactor Protection System
SRV - Safety Relief Valve
PORV - Pressure Relief Valve
AFW - Auxilliary Feedwater
MFW - Main Feedwater
DFWCS - Digital Feedwater Controller
CCW - Core Cooling Water
RCS - Reactor Cooling System
HPI - High Pressure Injection
LPR - Low Pressure Recirculation
HPR - High Pressure Recirculation
CM - Core Melt
T3LMP - Core Melt (Dominant Accident Sequence)
T3LMD2 - Core Melt (Dominant Accident Sequence)
FT3T - Transfer to small LOCA ET
FT3Tk - Transfer to ATWS ET
LOCA - Loss of Coolant Accident
ATWS - Anticipated Transient Without Scram
ET - Event Tree

Figure 4.3.4: Example Plant Event Tree for Turbine Trip, Part One

First, the information generated from the dynamic model must be imported into a PRA code's project file. In this example, the information will be imported as fault tree cut sets. A section of the DFWCS FT cut set model is given below. This model gives 15 event sequences that will result in the digital controller being in the Low Failure state. An additional basic event, *LOW-SEQ-#*, was added to each sequence to serve as a time tag. These time tags give the order in which the events in the sequence occur. They do not indicate the time step in which the failure occurs.

Failure, Low_Failure, 0001=
comp-Freeze1 * LOW-SEQ-0 +
comp-Freeze1 * mfv-Output_High2 * LOW-SEQ-1+
comp-Freeze1 * mfv-Output_Low2 * LOW-SEQ-2 +
comp-Freeze1 * mfv-Stuck2 * LOW-SEQ-3 +
comp-Freeze1 * mfv-Arbitrary_Output2 * LOW-SEQ-4 +
comp-Freeze1 * mfv-Arbitrary_Output2 * mfv-Stuck3 * LOW-SEQ-5 +
comp-Freeze1 * mfv-Arbitrary_Output2 * bfv-Output_High3 * LOW-SEQ-6 +
comp-Freeze1 * mfv-Arbitrary_Output2 * bfv-Output_Low3 * LOW-SEQ-7 +
comp-Freeze1 * mfv-Arbitrary_Output2 * bfv-Stuck3 * LOW-SEQ-8-RUN-1 +
comp-Freeze1 * mfv-Arbitrary_Output2 * bfv-Arbitrary_Output3 * LOW-SEQ-9 +
comp-Freeze1 * mfv-Arbitrary_Output2 * fp-Output_High3 * LOW-SEQ-10 +
comp-Freeze1 * mfv-Arbitrary_Output2 * fp-Output_Low3 * LOW-SEQ-11 +
comp-Freeze1 * mfv-Arbitrary_Output2 * fp-Stuck3 * LOW-SEQ-12 +
comp-Freeze1 * mfv-Arbitrary_Output2 * fp-Arbitrary_Output3 * LOW-SEQ-13 +
comp-Freeze1 * mfv-Arbitrary_Output2 * pdi-Output_Low3 * LOW-SEQ-14 +
comp-Freeze1 * mfv-Arbitrary_Output2 * pdi-Stuck3 * LOW-SEQ-15 +
…

Failure data for basic events must also be imported into the PRA code's project file. Failure data for the 15 cut sets previously described is given below in Table 4.3.2. Note that the algorithm used to generate failure data can only generate conditional failure probabilities. However, typical PRA codes can only handle a single failure probability per basic event and cannot handle conditional probabilities. Therefore, the conditional failure probability for each basic event in a failure sequence was multiplied together, and this probability is reported in the LOW-SEQ-# sequence tag event. This method retains the appropriate failure data for each sequence of events, while still listing the events necessary for failure to occur. Note that each additional event (mfv-Output_Low, comp-Freeze, comp-Arbitrary_Output, etc) described in the DFWCS cut sets must have a failure probability of 1.0 to correctly calculate the results. Therefore, no basic event information for the Markov/CCMT and DFM models should be imported for any basic events other than the sequence tags.

Table 4.3.2: Example Sequence Failure Probabilities

Sequence Event	Failure Probability

LOW-SEQ-0	3.85E-05
LOW-SEQ-1	1.68E-11
LOW-SEQ-2	3.36E-11
LOW-SEQ-3	1.28E-08
LOW-SEQ-4	3.36E-11
LOW-SEQ-5	5.59E-15
LOW-SEQ-6	7.33E-18
LOW-SEQ-7	1.47E-17
LOW-SEQ-8	5.59E-15
LOW-SEQ-9	7.33E-18
LOW-SEQ-10	7.33E-18
LOW-SEQ-11	1.47E-17
LOW-SEQ-12	5.59E-15
LOW-SEQ-13	7.33E-18
LOW-SEQ-14	1.47E-17
LOW-SEQ-15	1.47E-17

When using basic events as sequence tags, it is important to be able to distinguish between sequences. The DFWCS model provided two sets of scenarios: High Failure and Low Failure. Here, *LOW-SEQ-#* identifies the sequence as a low failure sequence, and *HIGH-SEQ-#* identifies a High Failure sequence. This distinction is important since otherwise, failure data from one failure scenario may be overwritten when data from another scenario is imported into the project file.

4.3.2.3 Linking the DFM and Markov/CCMT Results with the PRA Standard Models

In order to generate cut sets for the entire PRA, the newly imported models must be linked to the existing plant PRA. As the new models are in the format of FT cut sets, the system ETs must be edited to include the new FTs. Recall the turbine trip ET presented above in Fig.4.3.4. Fig. 4.3.5, below, incorporates the failure modes of the DFWCS into the turbine trip ET. It should be noted that the DFWCS may fail in such a way as to produce either a High or Low SG state, and the sequence and ET logic may actually vary depending on whether a High or Low Failure of the DFWCS has occurred. If the DFWCS fails in the low state, then there will be a low water level in the steam generators. This state is also reached due to failure of the MFW system as modeled in the static FT depicted in Fig.4.3.4. Therefore, the same ET logic is followed for the new DFWCS Fails Low Top Event as for the MFW Top Event from the existing plant PRA.

For the DFWCS Fails High Top Event, new ET logic is required. A high water level in the steam generator indicates that there is ample water in the steam generator, so the reactor heat sink is not lost in this situation. However, other undesirable events may result from the build up of water, and it may be desirable to model these scenarios in the PRA. In Fig.4.3.5, the occurrence of the DFWCS Fail High Top Event leads to the SG High Level end state, which in turn may transfer the analytical process into a new ET which models the plant and operator response to excessive water in the steam generator.

The ET in Fig.4.3.5 retains all of the information from the existing plant PRA, while incorporating the new information from the DFWCS model. This ET also demonstrates how different failure modes of the DFWCS may be modeled in the tree, as these failure modes can result in drastically different plant states that require different action.

The two additional Top Events, MFW DFWCS LOW and MFW DWFCS HIGH were added to the tree, immediately following the MFW Top Event. After the Top Events were added, the branching from the existing MFW Top Event was copied for the newly inserted Top Events. In the case of the MFW DFWCS HIGH Top Event from Fig.4.3.5, no new branches were added. Instead, a new end state was used in order to identify the high water level in the steam generator and to allow for the logic to transfer to a more appropriate ET.

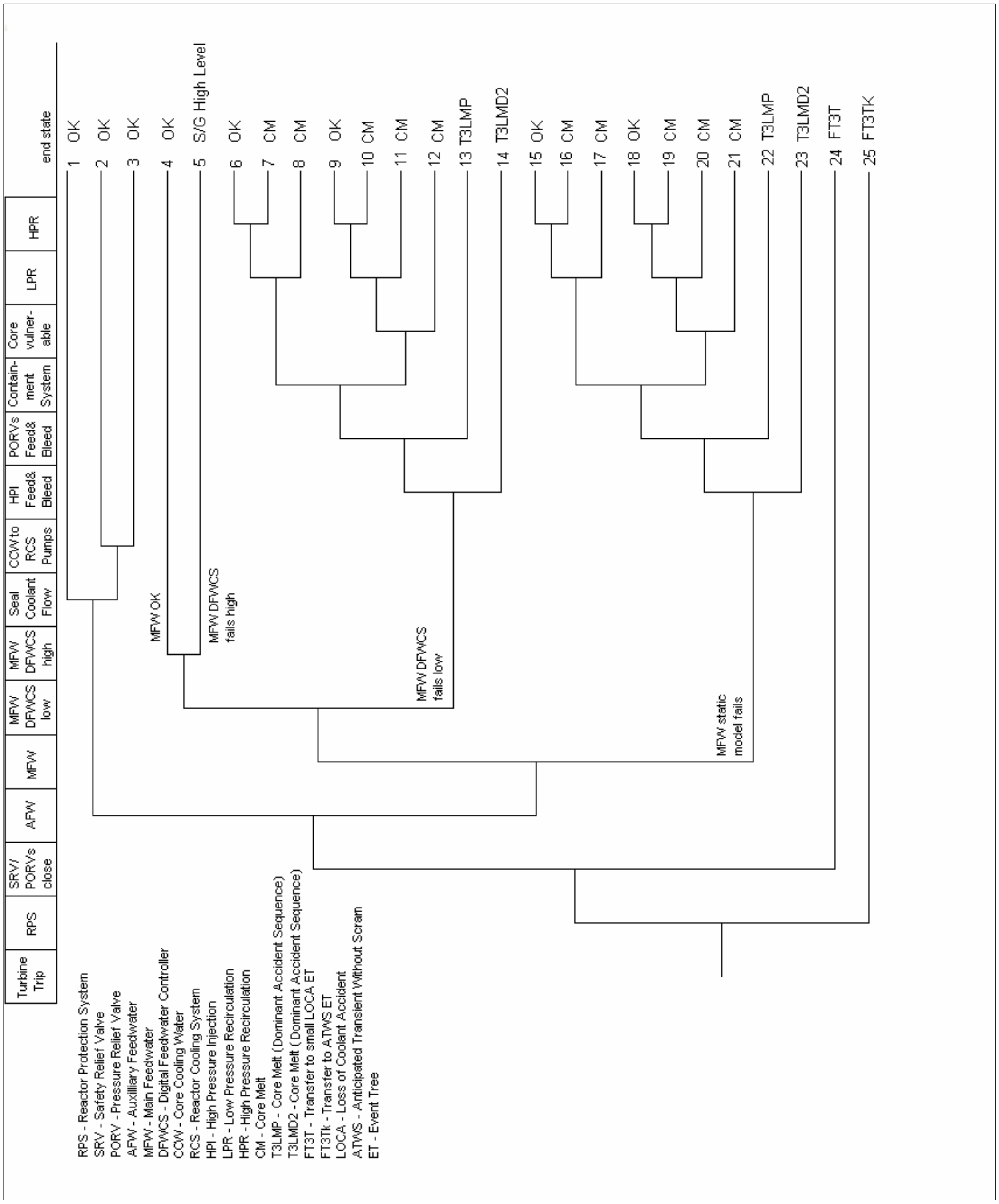

Turbine Trip
RPS
SRV/ PORVs close
AFW
MFW
MFW DFWCS low
MFW DFWCS high
Seal Coolant Flow
CCW to RCS Pumps
HPI Feed& Bleed
PORVs Feed& Bleed
Contain-ment System
Core vulner-able
LPR
HPR
end state
1 OK
2 OK
3 OK
4 OK
5 S/G High Level
6 OK
7 CM
8 CM
9 OK
10 CM
11 CM
12 CM
13 T3LMP
14 T3LMD2
15 OK
16 CM
17 CM
18 OK
19 CM
20 CM
21 CM
22 T3LMP
23 T3LMD2
24 FT3T
25 FT3TK
MFW OK
MFW DFWCS fails high
MFW DFWCS fails low
MFW static model fails
RPS - Reactor Protection System
SRV - Safety Relief Valve
PORV - Pressure Relief Valve
AFW - Auxilliary Feedwater
MFW - Main Feedwater
DFWCS - Digital Feedwater Controller
CCW - Core Cooling Water
RCS - Reactor Cooling System
HPI - High Pressure Injection
LPR - Low Pressure Recirculation
HPR - High Pressure Recirculation
CM - Core Melt
T3LMP - Core Melt (Dominant Accident Sequence)
T3LMD2 - Core Melt (Dominant Accident Sequence)
FT3T - Transfer to small LOCA ET
FT3Tk - Transfer to ATWS ET
LOCA - Loss of Coolant Accident
ATWS - Anticipated Transient Without Scram
ET - Event Tree

Figure 4.3.5: Example Plant Turbine Trip ET with DFWCS

Note that while in a traditional ET all related subsystems would be modeled together under a single Top Event, that approach was not practical here. Failure information pertaining to the DFWCS model has been imported into the PRA in the format of cut sets rather than FT logical information. It is simpler to leave the MFW and MFW DFWCS Top Events separate, rather than modify the MFW FT.

4.3.2.4 Quantification

Once the failure data has been imported and the ET has been expanded to include the DFWCS model, the next step is to generate the sequence cut sets. Cut sets must be generated for each FT called by the ET. However, since the dynamic model information has been imported as fault tree cut set information, it is important that these fault trees are not re-solved as this will lose the imported information. ET Sequences can then be found using the fault tree cut sets.

Ten cut sets for sequence 7 of Fig.4.3.5 are given below in Table 4.3.3. Here the AFW and HPR systems are left as black-box events to better display the results. In these cut sets it is seen how the DFWCS dynamic model results combine with failures from the pre-existing plant PRA to result in core damage. For example, in the first cut set MFW-Stuck-1 refers to the MFV in the stuck state. The time tag, 1, indicates that this event is the first failure (and in this case the only failure) to occur in this sequence generated from the dynamic model. In addition to the MFV-Stuck-1 event indicating the failure of the DFWCS, failures to the AFW and HPR systems combine to result in the Core Melt End State of Sequence 7 from Fig.4.3.5. In total, 199 cut sets were generated for sequence 7 when including full FT logic from the AFW and HPR systems (i.e., not using the black box method) with a probability cutoff of 1.0e-15. Cuts sets for ET end states may then be gathered normally.

Table 4.3.3: Example Sequence Failure Probabilities

Cut Set	Events
1	MFV-STUCK-1 * AFW * HPR
2	POWER-POWER_OFF-1 * AFW * HPR
3	COMP-FREEZE-1 * AFW * HPR
4	COMP-ARBITRARY_OUTPUT-1 * AFW * HPR
5	FP-OUTPUT_LOW-1 * AFW * HPR
6	FP-ARBITRARY_OUTPUT-1 * AFW * HPR
7	MFV-OUTPUT_LOW-1 * AFW * HPR
8	MFV-ARBITRARY_OUTPUT-1 * AFW * HPR
9	FP-STUCK-2 * MFV-STUCK-1 * AFW * HPR
10	BFV-STUCK-2 * MFV-STUCK-1* AFW * HPR

Failure frequencies for each sequence from the turbine trip ET presented in Fig.4.3.5 are given below in Table 4.3.4. Note that sequences not included in Table 4.3.4 are OK states, which are typically not quantified. Failure of the DFWCS leading to a low water level in the SG is modeled in Sequences 7 through 14. Of note in Fig.4.3.5 are Sequences 7, 8, and 10 - 14 which originate from the presence of DFWCS and which lead to core damage. Failure of the static portion of the MFW system as modeled in the existing plant is shown in sequences 16 through 23. Failure of the integrated model (existing MFW plus the DFWCS dynamic model) is then modeled by Sequences 7 through 23.
Sequence 5 includes failure of the DFWCS leading to a high water level in the SG. This sequence may then transfer to a new ET modeling how the plant responds to this scenario (no such information was modeled in the example plant PRA).

The CM end states result in core melt. Sequences 13, 14, 22, and 23 are the dominant core melt sequences (sequences with the T3LMP and T3LMD2 end states from Fig.4.3.5). Finally, sequences 24 and 25 transfer to the small LOCA and ATWS ETs, respectively, which are also modeled in the example plant PRA. These sequences are unaffected by the success or failure of the MFW and DFWCS, but are included here for sake of completeness.

Table 4.3.4: Sequence Failure Frequency for Turbine Trip ET

Sequence	End State	Frequency (per year)
5	S/G High	1.617E-6
7	CM	3.144E-12
8	CM	2.025E-09
10	CM	6.288E-12
11	CM	4.050E-09
12	CM	4.300E-08
13	dominant CM	7.848E-08
14	dominant CM	7.759E-08
16	CM	1.956E-11
17	CM	1.247E-08
19	CM	3.912E-11
20	CM	2.495E-08
21	CM	2.649E-07
22	dominant CM	4.834E-07
23	dominant CM	4.779E-07
24	small LOCA	1.887E-02
25	ATWS	4.380E-04

4.3.2.5 Importance, Uncertainty, and Sensitivity Analysis

Once the model has been quantified, additional analysis may be performed. Since the failure probabilities for events from the dynamic model are tied to the sequence tag basic events, there are some complexities when performing Importance, Uncertainty and Sensitivity analysis.

Importance analysis may be performed for sequence or ET end state cut sets that have been quantified. When performing an Importance analysis, it is important to recall that failure probabilities for individual basic events pertinent to the Markov/CCMT and DFM models have not been generated, and this will affect the results. Importance measures will be correctly generated for all basic events with a known probability. This includes the sequence tag events as well as basic events from the existing PRA. Importance measures for basic events without a given probability may be incorrect.

For example, consider the Birnbaum Importance measure, *B*, which is defined as:

$B = F(1) – F(0)$

where *F(1*) is the minimal cut set upper bound assuming the basic event being investigated will always occur (probability = 1), and *F(0)* is the minimal cut set upper bound assuming the basic event being investigated cannot occur (probability = 0.0). Since the exact unconditional probability for the basic event is unknown, *F(1)* will be calculated incorrectly, and the resulting

Birnbaum importance measure will be incorrect.

However, consider a measure such as Fussell-Vesely, defined as

FV = 1 – F(0)/F(x),

where *F(x)* is the original minimal cut set upper bound and, as before, *F(0)* is the minimal cut set upper bound assuming the basic event being investigated cannot occur (probability = 0). Both *F(x)* and *F(0*) can be calculated for all basic events giving accurate Fussell-Vesely measures for all basic events.

Therefore, it is recommended that Importance measures that are functions of F(0) and F(x) only should be considered for all events in the PRA minimal cut sets. Birnbaum Importance and other measures that are functions of F(1) should be used only for the sequence tag events and existing plant PRA events for which probabilities are known.

Uncertainty analysis may also be performed for sequence or ET end state cut sets. However, this requires accurate uncertainty data for imported basic events. As with the Importance analysis, the unconditional probability (and therefore uncertainty), is unknown for the basic events from the Markov/CCMT and DFM models. Therefore, Uncertainty analysis will also only generate accurate results for the sequence tag events and existing plant PRA events.

Finally, sensitivity analyses may be performed for sequence or ET end state cut sets. When performing a sensitivity analysis, if it is desired to change a probability for basic events from the dynamic models (for which there is no known unconditional probability), the analyst must use caution when investigating a basic event from the dynamic model. Sensitivity analysis on sequence tag events and existing plant PRA events may be performed as normal.

4.3.3 PRA/Dynamic Model Integration through a FT Intermediate Event (Case C)

In this case the dynamic model is developed to represent and quantify the intermediate event of a fault-tree that is part of the existing plant PRA. In this case, the PRA ETs remain unmodified. Instead, one or more fault trees are modified to include the dynamic model. This process was described in detail in NUREG/CR-6942 [14] and is summarized below.

For this case, fault tree logic information must be generated from the DFM or Markov/CCMT model. Since the dynamic model results are given as sequences of events leading to failure, they may be represented as a series of AND events. This series can be described as a large fault tree as shown below in Fig.4.3.6. In this figure there are four sequences which lead to a Low Failure of the dynamic model. Each sequence holds multiple events (Sequnce-1 is shown with three events). By following this example the failure sequences generated from the dynamic model may be described as a fault tree and imported into the plant PRA.

Once imported, the fault tree must be linked to the PRA as appropriate. This can be done simply by adding transfer gates to the existing fault trees as needed. This process was demonstrated in NUREG/CR-6942 [14] using the DFWCS model and an example auxiliary feedwater system fault tree.

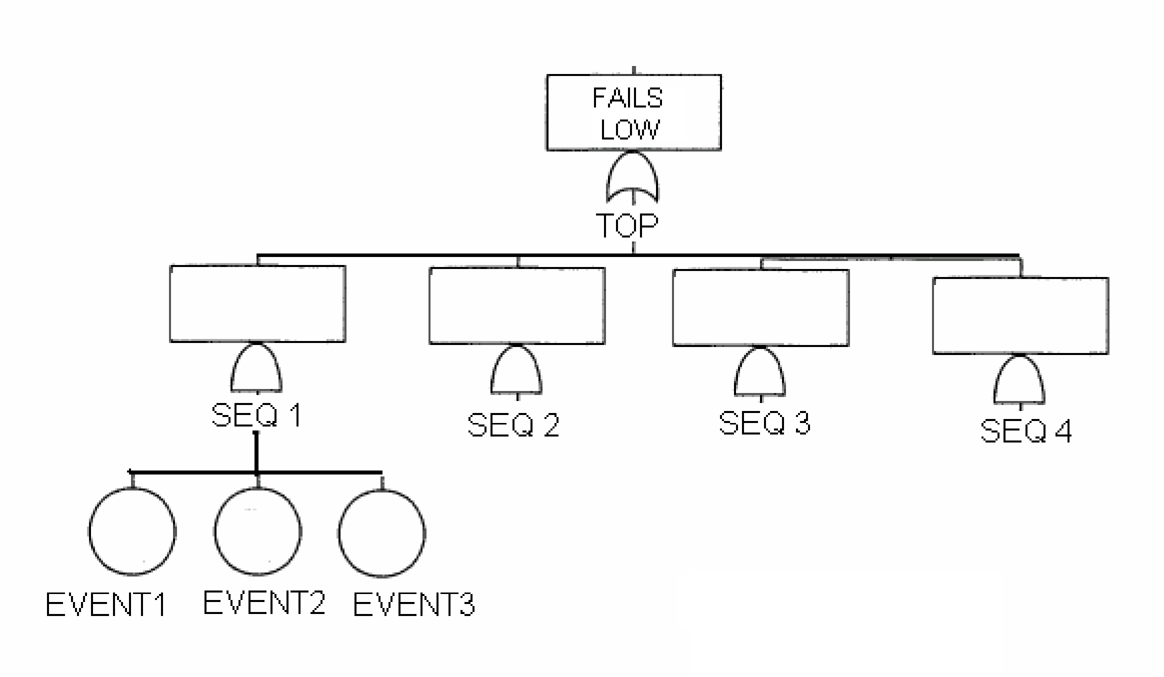


Figure 4.3.6: Fault Tree Describing Several Failure Sequences

4.3.4 PRA/Dynamic Model Integration when Common Basic Events Are Present

The subject of model integration in the presence of common basic events appearing in both conventional PRA minimal cut-sets and dynamic model prime implicants, i.e., across the boundary between standard PRA models and advanced dynamic models deserves specific attention. In this situation certain cut-sets and prime implicants are correlated, and therefore the PRA quantification processes pertaining to uncertainty analysis, importance measures, etc., cannot be carried out without first identifying the common basic events and tagging them (i.e., setting them up in a dedicated list) for proper handling during quantification. For example, in the application of the Monte Carlo or Latin Hypercube techniques that are typical of PRA software quantification schemes, correlated events are sampled differently from independent events.

As mentioned above the correlation issue is important in principle in all situations where the PRA quantification process includes the propagation of uncertainty distributions throughout the integrated models, or the execution of formal importance analysis (e.g., using the Vesely-Fussell and/or Birnbaum importance measures). In a practical sense, it may be less or more important, depending on the magnitude of the contribution to overall system risk metrics provided by the common or correlated events.

It must be noted that the issue mentioned here is not peculiar of situations whereby conventional and dynamic PRA models are to be integrated. The issue actually exists in any situation where different PRA model modules are initially developed in separate modeling environments and have to be subsequently integrated within one single plant PRA model. There are several possible ways in which this situation can be addressed. The specific solution depends on the PRA model environment being used (e.g., SAPHIRE [17], RISKMAN [33], CAFTA [32], etc.) and the degree of integration that is possible to build into the analytical and computational interface between the standard PRA code and the dynamic model software (e.g., the DFM software DYMONDA^{TM}), although a detailed discussion of the analytical and computational approaches that may be applicable to address the situation of interest is beyond the scope of this report.

5. SUMMARY AND CONCLUSIONS

This report completes and complements earlier project results documented in NUREG/CR-6942 [1], addressing challenges identified therein and concerns raised in the associated review process (see Section 1.1.2). This chapter summarizes activities (Section 5.1.1) and lists the principal study findings (Section 5.1.2). It also provides observations drawn by the authors from the application of the modeling and analytical techniques applied in the course of the study (Section 5.2.1) and, in closing, some observations on the combined use of deductive and inductive logic-analytical techniques (Section 5.2.2), which are not limited to the use of the DFM or Markov/CCMT paradigms, but may have more general use and applicability.

5.1 Summary of Activities and Results

5.1.1 Project Activities

The project has developed and completed data-gathering, modeling, and analytical activities, as summarized below:

1. Refinement of benchmark Digital Feedwater Control System (DFWCS) definition (Section 1.2).
2. Determination of qualitative and quantitative basic component failure modes and probabilities via FMEA (Failure Modes and Effects Analysis), and fault-injection techniques (Section 1.4).
3. Further development and refinement of the DFM and Markov/CCMT models of the DFWCS originally documented in NUREG/CR-6942 (Chapter 2 and Chapter 3, respectively).
4. DFM analyses and demonstrative risk quantification of selected DFWCS risk scenarios, carried out in both deductive mode (from defined Top Events to their root causes) and inductive mode (from hypothetical faults to Top Events of potential interest) (Chapter 2).
5. Markov/CCMT analyses and demonstrative risk quantification of selected DFWCS risk scenarios, carried out in inductive mode (Chapter 3).
6. Integration, in demonstration mode, of DFM and Markov/CCMT analytical and quantitative results into the framework of the conventional ET/FT PRA of a reference NUREG-1150 [2] plant (Chapter 4).

Regarding the challenge of analyst skill levels needed for the implementation of dynamic methodologies, the report uses the benchmark DFWCS originally defined in NUREG/CR-6942 to show how models developed by different groups of specialists can be utilized within a system-level dynamic PRA modeling framework. After the submodels (e.g., DFM and/or Markov/CCMT) have been produced, the PRA analyst only needs to be familiar with the process of linking and integrating results into the PRA, as has been illustrated and discussed in Chapter 4, rather than with the detailed inner structure of a given dynamic methodology.

In exploring the level of computational power and accuracy needed to model an important NPP control system with inclusion of its basic dynamic characteristics, the study illustrates how a digital reactor control system similar to that of an operating plant can be modeled using dynamic methodologies (i.e., through DFM and/or Markov/CCMT). Furthermore, this study also illustrates how the results can be incorporated into an existing traditional PRA to quantify the impact of the digital update of a control system on the core damage frequency. It should be emphasized that dynamic PRA methodologies have not been developed with the intent of implementing their use at a whole nuclear power plant (NPP) level, but rather only for those systems that, because of their dynamic and complex characteristics, require such capabilities (see Section 1.3.2.1 for a review). Thus the integration of dynamic PRA sub-modules into the conventional framework is an important aspect of the overall PRA analytical process when dynamic modeling is included. A demonstrative example of how such an integration process can be carried out for DFM and/or Markov/CCMT derived qualitative dynamic-PRA results – i.e., prime implicants to be integrated with ET/FT cut-sets – has been presented in NUREG/CR-6942 and is further expanded and quantitatively illustrated in this report.

Regarding the concern related to the risk importance of digital I&C system failures, this study uses the example benchmark system of NUREG/CR-6942 and a 24 hour power maneuver (Section 1.4) to show that, from a qualitative point of view, new risk-significant event sequences, associated with DFWCS failure modes identified by the dynamic analyses, may arise in a hypothetical conversion from an original analog control system to a digital platform. The quantitative contribution of these sequences to a plant-level risk figure-of-merit (e.g., core damage frequency or probability) was estimated to be modest in the context of this study demonstrative exercise. However, it must be noted that the quantitative aspects of the study results are at this time only preliminary and incomplete indications, since the study objectives were demonstrative in nature and did not include obtaining complete and fully vetted quantitative results. The results discussed in Chapter 4 are relative to the update of one control system and some of the related estimations are for scenarios conditioned upon the occurrence of a turbine trip. In these respects, the results are not necessarily representative of the impact of a digital upgrade of the whole reactor and plant protection and control system for all the initiating events under consideration, including possible digital I&C software design errors. As has been stated in Section 1.3, such errors have not been explicitly accounted for in the analyses carried out within this project due to the nature of available failure data. Thus it is premature to draw from this study any conclusions as to whether the overall risk impact from the digital system upgrade of an entire NPP protection and control system may be quantitatively significant in the positive or negative direction.

5.1.2 Key Findings

This study has produced useful indications concerning three basic questions that are, in the authors' view, central to the digital I&C PRA modeling and analysis issue:

Question 1: What modeling techniques are well suited to successfully represent and analyze the risk relevant failure modes of modern NPP digital I&C systems?

Question 2: Can quantitative reliability / risk measures be obtained for assessing the impact of the upgrade of a NPP control or protection system, from analog and relay-based to digital and software-based?

Question 3: Can a formally correct and practically implementable[17] approach be defined, to integrate the results of digital I&C dynamic PRA modeling and analysis techniques into a conventional PRA framework?

The current work has produced the following insights with respect to possible answers to Question 1:

A. The deductive analyses carried out with DFM appear to be well suited to span the search space for the prime-implicants of a given Top Event in logically complete fashion (see Section 1.3.2.2, Footnote 2 for definition of logically complete).

B. The application of the DFM and Markov/CCMT has resulted in the identification of certain risk-relevant event sequences[18] specifically associated with DFWCS failure modes and reflecting the hypothetical conversion of the steam generator feedwater control system, from an original analog system to a digital one[19].

C. Combined application of deductive analysis and inductive analysis in comparative terms shows that different initial conditions and sequencing of events can cause the DFWCS system to fail in different modes, some of which have and some of which do not have safety implications. Because these failure modes depend on timing and logic combinations of underlying conditions, their individual probabilities can be significantly different. The improved qualitative insight capability of a combined deductive / inductive analysis holds whether this is achieved by the use of both types of analysis within DFM, or whether the DFM deductive analyses are complemented with Markov/CCMT inductive ones. However, with the level of modeling detail applied by each methodology in this study, Markov/CCMT inductive analysis may provide better qualitative degree of analytical resolution to validate the quantitative insights for certain types of failures (e.g., Arbitrary Output, see Section 3.4) than DFM inductive analysis.

D. The inductive analyses of both methodologies, which can track dynamic scenarios by identifying associated time-dependent sequences of events may be effective for:

   a. Validating the correctness of the respective models.

[17] "Formally correct" here means that the technical means of execution of the approach preserve the logical integrity and information content of the PRA elements being integrated together. "Practically implementable" means that, given that the respective elements to be integrated have been already defined, the execution of the integration itself can be carried out with existing PRA implements and without adding an inordinate amount of additional effort.

[18] In the context of this discussion, risk-relevant does not necessarily imply quantitative significance. As stated earlier, the quantitative aspects of the risk sequences and of the underlying failure mode data have not been completely addressed in this study, nor validated, even when a quantification has been carried out for demonstrative purposes.

[19] Given the demonstrative intent of the current analyses and associated quantification exercises, no claim is made as to whether the newly identified DFWCS risk scenario sequences constitute a comprehensive set, i.e., whether they characterize the risk associated with the hypothetical upgrade in satisfactory fashion from both a qualitative and quantitative point of view.

   b. Performing sensitivity analyses starting from the baseline failure conditions identified by the prime implicant results of a DFM deductive analysis. Such sensitivity analyses may be carried out by varying initial conditions of certain parameters appearing in the prime implicant definitions, or in associated scenario boundary-condition definitions. For example, in Chapter 3, one such Markov/CCMT analysis has shown how, during a power ramp-up maneuver, the outcome of a frozen controller output or MFV stuck-at condition may change from the predominant Top Event outcome of low SG level to that of high SG level. This may occur if the transient starts at a time when the SG level happens to be 1% below normal, due to some unspecified earlier disturbance.

E. Similar to other modeling activities, there exist trade-offs between level of modeling detail and associated analytical power of resolution on one hand, and modeling and computational level of effort on the other. This is true for both methodologies. The effectiveness and efficiency of a deductive analysis mode has been explored in this study with the DFM methodology, but not with the Markov/CCMT because the Markov/CCMT analytical procedures do not currently include a deductive analysis algorithm that is computationally feasible for system models as complex and detailed as the DFWCS model analyzed in this study. The Markov/CCMT inductive analyses appear to confirm its effectiveness of in providing fine levels of resolution in the time tracking of dynamic sequences when compared to traditional techniques. With respect to the level-of-resolution vs. modeling and computational effort question, DFM offers the advantage of logic completeness at reasonable effort (e.g., within a maximum of three or four time steps) for a system similar to the DFWCS in complexity and dynamic characteristics. Markov/CCMT provides the analyst with the capability of tracking a larger number of time steps, if the analyst can restrict, on the basis of general engineering insight or of insights gained by means of some other type of analysis, the range of initial conditions from which a dynamic inductive analysis can be started.

The above insights are significant. However, there are several reasons why at this time no definitive conclusions can be drawn with regard to what technique, or combination of techniques, is best suited for a specific digital I&C modeling and assessment purpose. One reason is that there are different conceivable contexts, objectives, and levels of depth for PRA analyses of digital I&C systems. Moreover, there has been to date limited experience with the estimation of reliability and risk for these systems by means of any type of analytical models. Furthermore, there has been limited experience with their operation that reliability and risk relevant data against which one may compare model predictions are also not readily available. The reader will find further observation on the effectiveness and practical utility of the investigated methodologies in Section 5.2.1 below.

With regard to Question 2, the study has demonstrated some means of quantification of the analytical results obtained via the application of the modeling techniques being investigated. This demonstration is not fully developed to cover all aspects of digital I&C risk that may be significant. The most important reasons why the study quantitative results should at this time be considered only as first-cut demonstrative values, and not real indicators of the possible risk impact of control system digital upgrades on a typical NPP, are:

A. The possibility of logic design errors, especially with respect to the design of any complex software that governs a digital I&C [3-5] was, by definition of project scope, left unexplored in the analyses carried out for the DFWCS benchmark.

B. The study models the digital update of just one control system and therefore does not cover, even in purely qualitative terms, the full potential extent of a full scale digital upgrade affecting all the elements of both the reactor protection and control systems of a given plant.

C. The quantitative results of the study relative to High and Low SG level probabilities are used in Chapter 4 to quantify turbine-trip / reactor-trip types of traditional PRA scenarios, under the assumption that the values obtained in this study from the analysis of the power maneuver transient are representative of High and Low SG level probabilities for generic plant conditions. This is not necessarily true in all cases, and the probability of Top Events may depend on the plant regime at the time that certain types of component failures are assumed to occur. Thus, in a complete analysis, one would first need to carry out a classification of basic plant regimes, then conduct dynamic analyses like those executed in this study to cover all such regimes and finally use some appropriate averaging of probabilities if values for these probabilities were found to differ significantly from a plant regime to the next. This essentially reflects the same issue discussed below in Section 5.2.1.1 with regard to appropriately treating dynamic scenario sequences and probabilities as being conditional upon the occurrence and probability of the initial plant state at the start of the dynamic sequence.

D. The results of the study do not necessarily reflect, besides the potential effect of system and software logic and/or algorithmic design errors already discussed above: a) possible statistical dependence among failures of different reactor protection and control functions due to common causes (e.g., platform and/or protocol commonality) and b) possible communication issues (e.g., data races, multitasking, multiplexing). Thus the potential probability of failure contributions from these types of failure modes and system interactions are not reflected in the demonstrative estimates documented in the study.

Within the above limitations, the study has provided the following insights with respect to Question 2:

A. Dynamic methods such as DFM and Markov/CCMT provide qualitative results in the form of prime implicants that are the multi-valued logic equivalent of binary cut-sets and can be quantified with data and techniques similar to those used to quantify conventional PRA models.

B. Failure probability and failure rate estimations relative to certain digital I&C components can be utilized, in both DFM and Markov/CCMT transition diagrams and associated analytical failure-mode results, to generate quantitative risk estimations at a level of detail and depth comparable with the standards of practice encountered in traditional PRA. In this study, these estimates were generated primarily via the fault injection technique and combined in the dynamic PRA models with hardware failure mode probabilities and failure rates compiled from open literature sources. Overall digital risk estimates were produced for the DFWCS and were then integrated and incorporated into traditional PRA event sequence estimations.

C. DFM results obtained in deductive or inductive analysis mode for the DFWCS benchmark, and Markov/CCMT inductively-obtained results appear to be consistent with the implemented modeling assumptions and quantification data.

D. Both DFM and Markov/CCMT analyses can be used to identify and rank-order event sequences with respect to their contribution to different DFWCS failure modes, as well as to identify and rank-order the corresponding contribution of individual basic events related to these sequences.

Regarding Question 3, the study has executed a demonstrative integration of the DFM and Markov/CCMT qualitative and quantitative results obtained for the DFWCS benchmark system with the relevant portions of an existing PRA. More specifically, this was done using the PRA framework and data pertaining to one of the NUREG-1150 [2] plants. The results of this integration exercise support the following findings:

A. For point-estimation of risk figures of merit, the integration can be carried without particular difficulties for all three basic cases of interface boundaries – i.e., at the ET initiating event level, at the ET pivotal event level, or at the FT intermediate event level – between the existing PRA structures and dynamic methodologies results cast in the form of prime implicants of a defined Top Event.

B. For the estimation of uncertainty ranges and importance measures, the integration can also be carried in straightforward fashion and without introducing errors, if an assumption of statistical independence of the basic events that appear across the conventional PRA – dynamic PRA model interface holds true in that the contribution of any such correlated basic events to overall plant risk metrics is small.

C. In cases of uncertainty or importance analysis where the limiting assumption stated in B above does not hold true, the integration of results is still possible if one applies the same post-processing techniques that need to be applied when integrating, under the same circumstances of correlated basic events, the model structures and results obtained from separate conventional PRA models and analyses.

5.2 Further Comments and Observations

The observations that follow in this section mostly reflect the report authors' experience and reasoning and, as such, do not represent or portray to represent the positions or technical conclusions of the NRC Staff.

The preceding Section 5.1 has summarized results and findings directly produced by the current study and directly supported by the analyses carried out therein. This section, in addition, presents observations and indications that are suggested by the study analyses but cannot be considered at this stage of development as being directly and fully proven by its results. These indications are nevertheless relevant to the subject of digital I&C risk modeling and analysis and potentially useful to an educated reader who also applies his own experience and judgment towards their practical interpretation and use. Thus these observations are primarily addressed by the authors to peer-researchers in the field, since they also generally reflect a comparative perspective from which further indications may be drawn by the reader with respect to the current state of the art in digital I&C and software-intensive systems modeling and analysis, as well as possible directions for future research and developments in the field.

To facilitate the reading, the following observations are organized in subsections. Section 5.2.1 contains observations concerning the use of the DFM and Markov/CCMT methodologies, with subsections addressing the limitations of the current modeling and quantification processes and issues related to the integration of dynamic modeling with conventional PRA frameworks. Section 5.2.2 contains more general closing comments on digital I&C dynamic modeling and analysis, including some observations on what the authors believe to be remaining open issues in this and other closely related area of research and development.

5.2.1 Considerations on Use of the Methodologies

Two of the most common objections to the use of dynamic models in practical NPP PRA applications are: a) the perceived absence of a "smoking gun", i.e., some definitive proof that dynamic techniques have been able to identify risk-significant sequences that conventional PRA models have missed, and b) the level of effort involved in developing and using dynamic PRA techniques, versus the perceptivity of the derived results.

As previously noted in this report, the first of the two above objections has been discussed in earlier research, including research conducted by the authors [1, 3-5]. This study does not claim in this regard any definitive evidence and findings. However, it has been shown that the application of the DFM or Markov/CCMT techniques has been capable of identifying several risk relevant sequences that were not included in conventional PRA models. It may be argued that these sequences may not be significant in quantitative terms, and that this in turn may mean that they are not truly relevant. However, the lack of current validated means for quantifying risk relevant sequences that include digital system contributions makes it difficult to decide which risk scenarios may be significant or not on the basis of quantitative considerations only. This is especially true when the potential contribution of software design and specification is not included in the quantification process.

The second objection to the use of dynamic methods has also been addressed in other parts of this report (see Chapters 2 and 4) and in the literature [1, 6-8]. This subject is not independent of the other issue just discussed, in the sense that a greater level of effort may be accepted by potential users if important results and insights can be provided by the use of a specific methodology that simpler means of analysis cannot produce.

Beyond the above general consideration, however, two more specific observations can be presented to address the model-complexity and level of effort objection. The first one pertains to a characteristic intrinsic to the nature of the DFM and Markov/CCMT methodologies, and as such available to any user. Unlike ET and FT models, DFM and Markov/CCMT models are models of a system, not of a specific event or sequence of events. Thus, for example, once the effort of producing a DFM system model has been completed, the analysis of a large number of Top Events relative to that system can be carried out via the automated deductive software algorithms. This has been discussed and illustrated in several DFM-related reports and publications [6-8], but is also reflected in the analyses discussed in this report. In fact, in the course of this study, the same DFWCS model was analyzed in deductive mode by means of the DFM Dymonda^{TM} software tool, in relation to two distinct Top Events of interest (Low and High

SG level). In addition, the High SG level Top Event was re-analyzed for one additional back-tracking time-step to verify consistency of DFM results with Markov/CCMT results (Section 4.2); an inductively-executed validation analysis, using as initial conditions the deductively-obtained prime implicant events identified for the above two Top Events, was also carried out using the DFM software. Parallel inductive analyses, more detailed in time-resolution aspects, were also carried out on the DFWCS Markov/CCMT model for both of the above mentioned system Top Events of interest.

The second consideration is that system models such as DFM and Markov/CCMT are re-usable, by similarity, across different specific applications and analyses. This is true if the models are modularized to represent sets of standardized plant subsystems and components. The possibility of creating re-usable DFM model templates and modular building-blocks has been discussed and illustrated in the literature [6, 8, 9]. In principle, it would appear that the same could be done with Markov/CCMT model constructs. After an initial effort-intensive model build-up period during the earlier applications of the methodologies, the implication is that successive applications would take advantage of the existence of such system model templates and building blocks. This should considerably reduce the level of effort and resources required to set up and execute dynamic PRA analyses with either methodology.

5.2.1.1 Understanding Results Obtained via DFM and Markov/CCMT

From a methods perspective, the results in the study were obtained via DFM deductive analysis and via inductive analyses carried out both in Markov/CCMT and in DFM. As pointed out in Chapters 2 and 4, the basic trade off between deductive and inductive logic model analysis is in terms of level of model detail that can be analytically handled versus formal logic completeness of the analytical process. The deductive approach can provide the guarantee of logic completeness of the analysis results, provided the model to be analyzed is defined in coarse discrete terms to permit the analytical algorithms to be successfully executed within the limits of the current computational power. Inductive analysis, on the other hand, can be carried out successfully on a model that is defined in greater level of detail and therefore may represent more closely the system being modeled. However, this is obtained at the expense of the guarantee of logic completeness, and also places squarely on the analyst the burden of defining realistic initial conditions from which the inductive analysis may proceed, i.e., the system conditions assumed to exist at the start of the risk sequence that is inductively tracked and analyzed.

With respect to the proper definition of initial conditions, it must be noted that a key characteristic of any inductively obtained risk scenario is that the scenario sequence is conditional upon the occurrence of the initial conditions assumed for the start of the inductive analysis or simulation. This has both qualitative and quantitative implications, as the identified sequence may have or not have any practical relevance, depending on the likelihood of occurrence of the assumed initial conditions.

To better understand the above point, one may consider the Markov/CCMT simulations carried out in the study. The baseline simulations assumed nominal and balanced conditions of the DFWCS followed by possible failures of each of the DFWCS constituents at the end of a Markov/CCMT modeling time step. Balanced means here that the feedwater flow was assumed at the beginning of the simulation to match the demand associated with the particular power level and SG level at that time. However, sensitivity analysis simulations were also intentionally run starting from off-balance initial conditions (e.g., a condition of temporary mismatch between feedwater and steam flow in the SG) to explore the associated effects on the ultimate outcome. This was a very useful experiment, since the results have shown that, even in the presence of the same set of failure events, the ultimate outcome can be quite different, depending on the transient conditions that may exist in the plant at the time when the failures occur. In one of the cases explored, for example, a stuck feedwater valve condition during the power ramp-up maneuver was found to lead to a High SG Level outcome when a 1% excess feedwater flow was assumed to exist at the start of the ramp-up, whereas the same failure is found leads to a Low SG Level condition when the feedwater is assumed to be initially in balance. From a risk assessment point of view, one has to decide if both sets of conditions and sequences are significant and relevant. In this regard, qualitatively speaking, although both situations start from nominal conditions (e.g., in both cases the feedwater flow and the SG level are within ranges that do not trigger any trips or alternative system activations, such as auxiliary feedwater), the condition that leads to a Low SG Level is, by assumption, one of feedwater flow imbalance, presumably because of some preceding unspecified plant disturbance.

To address the question of risk relevance for all the nominal range situations in quantitative terms, an inductive analysis would have to cover and probabilistically assess the various initial conditions that are possible within such a range. This may be possible, for example, by examining the plant parameter records over a full cycle of continuous operation and determining what fraction of the time the plant was within certain subranges of the entire nominal range, while at a given power level. Such fractions of time could then be used as the weighting probabilities for sequences developed inductively with initial feedwater conditions starting from each of the said subranges.

The above discussion underscores that the use of simulation-based techniques in risk assessment can be very useful and insightful, but needs also to be carried out with great attention to assumptions and details, lest the analyst be mislead into possible oversights or misinterpretations of the results.

5.2.1.2 Integration of Dynamic PRA with Conventional PRA Results

The subject of dynamic-PRA / conventional-PRA models and results integration is addressed in Chapter 4, with specific focus on illustrating the integration of DFM and Markov/CCMT results into a NUREG-1150 type of conventional PRA framework. Here the subject is discussed from a more general point of view, i.e., by briefly discussing issues that are generally applicable to broader classes of models and situations and have to be adequately addressed, regardless of the specific techniques whose results are to be integrated.

In general, given a conventional ET/FT PRA framework, a dynamic PRA analyst will typically have at his/her disposal results obtained by either:

a) a deductive process that guarantees logic completeness and may or may not be complemented by inductive validations; or
b) inductively obtained results (e.g., Monte Carlo based discrete simulations, dynamic event trees, Markov models resolved inductively, etc.).

If the analyst is dealing with Case (a) and is using the dynamic model results to resolve and quantify an event that appears in a conventional PRA ET or FT, he/she may treat that event as if it were the Top Event of a conventional PRA fault-tree or sub-tree. That is, he/she can obtain cut-sets or prime-implicants via the dynamic model deductive process and then integrate those results in the same fashion as one would import binary cut-sets from an external fault-tree model into a conventional, self contained PRA. Most conventional PRA software packages have utilities to allow externally obtained cut sets to be imported and integrated with an existing model. This is essentially what was done to integrate DFM prime implicants into the NUREG-1150-style models and discussed in Chapter 4. In essence, logically complete deductive results are fully compatible with conventional PRA models. Caution should be applied when integrating such models is in the presence of correlation, i.e., common events, across the interface between the two types of models.

Inductively obtained results, on the other hand, are not automatically compatible with conventional PRA models. This is because inductively obtained results are conditional upon the initial conditions assumed as the start-point of the inductive simulation or analysis. When these conditions are fault-events, it is clear that the rest of the event sequence is conditional upon the occurrence of such faults and the associated probability (or frequency). However, there are also cases when some of the conditions are not faults, but specific plant or subsystem states that, although within the normal range, are not states in which one can expect the plant to be most of the time. In such cases, the resulting sequences cannot be folded into a conventional model without first determining the likelihood (i.e., probability or frequency) of the conditioning states in terms that are quantitatively comparable with the probabilities of other events in the PRA.

The last important issue to be kept in mind with respect to the integration of dynamic and conventional models is the already mentioned issue of the possible existence of identical, or correlated, events across the interface between the two sets of models. It is important to note that this problem exists, when two sets of conventional PRA models are individually constructed to be integrated at a later point in time. A full discussion of the possible solution to this issue is beyond the scope of this report. However, the issue is fully solvable in practical terms if a conventional PRA software tool provides an open interface by which a user can review the binary model cut sets and execute certain logic manipulations upon them.

5.2.2 Remaining Open Issues and Concluding General Observations

Before closing this chapter with some of the most general observations that can be drawn, from both the work carried out in this study and from the awareness of what the study could not address, it is appropriate to underscore one more time that the nature of this project was essentially demonstrative. Thus, some of the key findings of this study, and especially those involving the identification of possible PRA application procedures that have been documented in the report, should be further validated and organized into repeatable processes, perhaps with the aid of suitable supplemental implementation tools (i.e., software tools) in order to make them accessible and acceptable to users in industrial and/or regulatory application environments.

A full answer to the question of adequate risk identification and quantification for digital systems cannot be produced without covering ground that was beyond the scope of the work documented in this report. A key aspect of the problem that remains open at the present time is that the identification of potential software-related digital system failure modes has not been yet addressed in an organized and systematic form, so that a comprehensive classification be derived with sufficient cross-validation and level of confidence to make possible a selection of the most appropriate modeling and quantification means for risk assessment purposes. The authors believe that this study and the associated insights, by identifying some of the gaps in more specific ways, have indirectly confirmed that a more systematic digital I&C failure-mode modeling activity may eventually be necessary in order to provide a substantive baseline in this regard, specifically addressing the more risk-relevant subsystems of a NPP.

By limitation of scope, one issue that the study was not able to explicitly address was the possibility of digital I&C systems failures due to design errors in the associated software. This issue is one that, in the authors' view, certainly deserves special attention. Findings in this respect have been documented in studies focused on other types of digital system applications, mostly in the space arena [3,4,5]. Recent research sponsored by NASA and conducted with the joint application of conventional and dynamic PRA methods has also shown that such a hybrid modeling approach (i.e., conventional and dynamic models in tailored combination) can be effective in permitting the identification of potential design weaknesses in software-intensive systems, as well as of software testing strategies that can address these weaknesses and produce realistic risk estimates for such systems [4,5]. However, since the issue has not specifically investigated in the NPP application context, it is currently not possible to confirm whether or not such findings are transferable with the same validity and relevance onto the nuclear plant arena. Thus, if any future, systematic NPP digital I&C failure mode identification and modeling efforts are undertaken, these should not leave this issue unaddressed, so that its relevance in the context of NPP digital system applications may be better understood and dealt with accordingly.

The closing comment of this chapter addresses one last time the question of deductive versus inductive modeling. In the course of the study the authors have successfully applied both techniques, more specifically, the deductive analysis approach to span and systematically cover, within the level of approximation afforded by the DFM methodology applied in such a mode, the range of possible prime implicants for a given Top Event of interest. Inductive analyses, both in the DFM and the Markov/CCMT environments, were then used to validate the deductive results and explore variations of the scenarios, in the case of the use of the Markov/CCMT analyses, in greater detail with respect to timing effects. The authors believe that these applications of the methodologies have resulted in some degree of confidence that the two methods, in a broad modeling and analytical perspective, are complementary. This observation should not be surprising to PRA experts and practitioners, as the use of deductive and inductive techniques in complementary fashion is actually routine in conventional PRA, as way of balancing the need to cover in logically complete fashion a search space with that of following the sequential progression of risk scenario sequences in intuitively understandable representations and with as much detail as deemed necessary by the analyst. Thus, in a conventional PRA, the search space for sequence initiating events is parsed and organized by means of deductively derived master logic diagrams (MLDs), then scenario sequences are inductively identified and produced in the form of event trees (ETs), and finally significant ET events are further developed deductively with fault trees (FT) to identify their root causes in the form of minimal cut sets.

It is therefore consistent with the PRA practice and experience to suggest, also on the basis of the technical observations obtained from the DFM and Markov/CCMT applications in this study, that the two methodologies can be viewed as being potentially complementary in logic-analytical characteristics and flexibility of application, at least in the context of the complex digital I&C modeling problem at hand and for large scale uses where portions of the a system to be modeled will be exhibiting different levels of dynamic characteristics and time-driven interdependencies. In practical terms, the preference of an analyst for the use of modeling techniques, singly or in combination, may depend greatly on the nature and scope of the particular PRA model to be developed, as well as on the availability in production mode of software support tools for the development of models and the execution of analytical procedures. As stated earlier, the modeling and analytical burden to be faced for the use of any evolved PRA process that may include dynamic methods of any kind will be less severe after the initial necessary learning-curve resource penalty, as it should become possible then to modularize and standardize significant portions of the needed plant and/or system models, so that it will be possible and practical to use these repeatedly over a wide range of plant applications and analyses.

6. REFERENCES

. 1. U.S.NUCLEAR REGULATORY COMMISSION, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities; Final Policy Statement", *Federal Register*, **60**, 43622 (1995).

2. Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades - Applying Risk-Informed and Deterministic Methods, 1002835, EPRI, Palo Alto, CA (2004)

3. T. ALDEMIR, D. W. MILLER, M. STOVSKY, J. KIRSCHENBAUM, P. BUCCI, A. W. FENTIMAN, and L. M. MANGAN, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, U. S. Nuclear Regulatory Commission, Washington, D.C. (2006)

4. S. GUARRO, M. YAU, and M. MOTAMED, Development of Tools for Safety Analysis of Control Software in Advanced Reactors, NUREG/CR-6465, U.S. Nuclear Regulatory Commission, Washington, D.C. (1996)

5. S. GUARRO, A. MILICI, and R. MULVEHILL, Extending the Dynamic Flowgraph Methodology (DFM) to Model Human Performance and Team Effects, NUREG-CR/6710, U.S. Nuclear Regulatory Commission, Washington, D.C. (2001)

6. S. DIXON, M. YAU and S. GUARRO, "Demonstration of the Context-Based Software Risk Model Method for Risk Informed Assurance and Test of Software-Intensive Space Systems", *Proceedings of the 9th International Conference on Probabilisitc Safety Assessment and Management,* Hong Kong, China (2008).

7. S. GUARRO, S. DIXON, and M. YAU, Risk-Informed Safety Assurance and Probabilistic Risk Assessment of Mission-Critical Software-Intensive Systems, AR07-01, ASCA, Inc., Redondo Beach, California (6-15-2007)

8. S. GUARRO and G. EWELL, "Integrating MEMS Quality and Reliability Goals With the Use of Multi-Valued Logic Analysis,", *Proceedings of the 2nd International Conference on Integrated Micro/Nanotechnology for Space Applications (MNT99)*, Aerospace Corporation, Pasedena, California (1999).

9. M. YAU, G. APOSTOLAKIS and S. GUARRO, "The Use of Prime Implicants in Dependability Analysis of Software Controlled Systems", *Reliability Engineering and System Safety*, **62**, 23-32 (1998).

10. M. YAU, S. GUARRO, A. MILICI, and R. MULVEHILL, The Use of Prime Implicants in Dependability Analysis of Software Controlled Systems, AR-97-02, ASCA, Inc., \Redondo Beach, California (1997)

11. M. HASSAN and T. ALDEMIR, "A Data Base Oriented Dynamic Methodology for the Failure Analysis of Closed Loop Control Systems in Process Plants", *Reliability*

Engineering & System Safety, **27**, 275-322 (1990).

12. B. TOMBUYES and T. ALDEMIR, "Dynamic PSA of Process Control-Systems Via Continuous Cell-To-Cell-Mapping", 1541-1546, Elsevier, New York (1996).

13. T. ALDEMIR, "Quantifying Setpoint Drift Effects in the Failure Analysis of Process Control Systems", *Reliability Engineering & System Safety*, **24**, 33-50 (1989).

14. T. ALDEMIR, M. P. STOVSKY, J. KIRSCHENBAUM, D. MANDELLI, P. BUCCI, L. A. MANGAN, D. W. MILLER, X. SUN, E. EKICI, S. GUARRO, M. YAU, B. W. JOHNSON, C. ELKS, and S. A. ARNDT, Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, NUREG/CR-6942, U.S. Nuclear Regulatory Commission, Washington, D.C. (2007)

15. U.S.NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, U.S. Nuclear Regulatory Commission, Washington, D.C. (1990)

16. G. A. APOSTOLAKIS and C. GARRET, *Context in the Risk Assessment of Digital Systems*, pp 23-32 (1999).

17. C. L. SMITH, J. KNUDSEN, M. CALLEY, S. BECK, K. KVARFORDT and S. T. WOOD, *SAPHIRE Basics: An Introduction to Probability Risk Assessment Via the Systems Analysis Program for Hands-on Integrated Reliability Evaluations (SAPHIRE) Software*, Idaho National Laboratory, Idaho Falls,ID (2005).

18. E. CASTILLO, *Extreme Value Theory in Engineering*, Academic Press, Inc (1988).

19. J. ARLAT, A. COSTES, Y. CROUZET, J.-C. LAPRIE and D. POWELL, "Fault Injection and Dependability Evaluation of Fault-Tolerant Systems", *IEEE Transactions on Computers*, **42**, 913-923 (1993).

20. C. R. YOUNT and D. P. SIEWIOREK, *A Methodology for the Rapid Injection of Transient Hardware Errors*, pp 881-91 (1996).

21. C. ELKS, Y. Y. YU, M. REYNOLDS, and B. W. JOHNSON, Quantitative Dependability Assessment of a Digital Feed Water Control System: Preliminary Results, UVA-CCS-QDA-001, Ver. 7, University of Virginia, Charlottesville, VA (2006)

22. T. D. SMITH and B. W. JOHNSON, *A Variance Reduction Technique Via Fault Expansion for Fault Coverage Estimation*, pp 366-76 (1997).

23. M. YAU, M. WETHERHOLT and S. GUARRO, "Safety Analysis and Testing of Critical Space Systems Software", *Proceedings, 4th International Conference on Probabilistic Safety Assessment and Management (PSAM-4)*, Paper # September 13-18, New York, NY (1998).

24. S. SWAMINATHAN and C. SMIDTS, "The Mathematical Formulation of the Event Sequence Diagram Framework", *Reliab.Engng & System Safety*, **65**, 103-118 (1999).

25. S. GUARRO, "PROLGRAFB: A Knowledge Based System for the Automated Construction of Nuclear Plant Diagnostic Models" (1987).

26. SAPHIRE/DFM Software Integration Project, Task 1 Work Accomplished - Final Report to NASA HQ/ OSMA, ASCA, Inc, Redondo Beach, California (2008)

27. T. ALDEMIR, "Computer-Assisted Markov Failure Modeling of Process Control Systems", *IEEE Transactions on Reliability*, **R-36**, 133-144 (1987).

28. T. ALDEMIR, "Utilization of the Cell-To-Cell Mapping Technique to Construct Markov Failure Models for Process Control Systems", G. APOSTOLAKIS (Ed.), *Probabilistic Safety Assessment and Management: PSAM1*, 1431-1436, Elsevier, New York (1991).

29. C. S. HSU, *Cell-to-cell Mapping: A Method of Global Analysis for Nonlinear Systems*, Springer-Verlag, New York, NY (1987).

30. P. BUCCI, J. KIRSCHENBAUM, T. ALDEMIR, C. L. SMITH and R. T. WOOD, "Constructing Dynamic Event Trees From Markov Models", M. STAMATALETOS and H. S. BLACKMAN (Eds.), *PSAM8: Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, CD-ROM Version*, Paper # 369, ASME Press, Inc. (2006).

31. P. BUCCI, J. KIRSCHENBAUM, T. ALDEMIR, C. L. SMITH and R. T. WOOD, "Generating Dynamic Fault Trees From Markov Models", *Trans.Am.Nucl.Soc.*, **95** (2006).

32. CAFTA For Windows, Version 3.0c, SAIC, Los Altos, California (1995)

33. RISKMAN 7.1 for Windows, ABS Consulting, Irvine, California (2003)

34. P. BUCCI, L. A. MANGAN, J. KIRSCHENBAUM, D. MANDELLI, T. ALDEMIR and S. A. ARNDT, "Incorporation of Markov Reliability Models for Digital Instrumentation and Control Systems into Existing PRAs", *Proceedings of NPIC&HMIT 2006*, American Nuclear Society, La Grange, IL (2006).

35. P. BUCCI, J. KIRSCHENBAUM, T. ALDEMIR, C. L. SMITH and T. S. WOOD, "Constructing Dynamic Event Trees From Markov Models", M. STAMATALETOS and H. S. BLACKMAN (Eds.), *PSAM8: Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, CD-ROM Version*, Paper # 369, ASME Press, Inc. (2006).

36. I. ASCA, Risk-Informed Safety Assurance and Probabilistic Risk Assessment of Mission-Critical Software-Intensive Systems, AR07-01, prepared for the NASA Johnson Space Center, (6-15-2007)