Reliability Engineering and System Safety 95 (2010) 1011–1039

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies

T. Aldemir [a,*], S. Guarro [b], D. Mandelli [a], J. Kirschenbaum [c], L.A. Mangan [a], P. Bucci [c], M. Yau [b], E. Ekici [d], D.W. Miller [a], X. Sun [a], S.A. Arndt [e]

[a] The Ohio State University, Nuclear Engineering Program, Columbus, OH 43210, USA
[b] ASCA, Inc., 1720 S. Catalina Avenue, Suite 220, Redondo Beach, CA 90277-5501, USA
[c] The Ohio State University, Department of Computer Science and Engineering, Columbus, OH 43210, USA
[d] The Ohio State University, Department of Electrical and Computer Engineering, Columbus, OH 43210, USA
[e] U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, USA

ARTICLE INFO

Article history:
Received 3 October 2009
Received in revised form
19 April 2010
Accepted 19 April 2010
Available online 13 May 2010

Keywords:
PRA
Digital systems
Dynamic methodologies
Markov
Cell-to-cell-mapping technique
Dynamic flowgraph methodology

ABSTRACT

The Markov/cell-to-cell mapping technique (CCMT) and the dynamic flowgraph methodology (DFM) are two system logic modeling methodologies that have been proposed to address the dynamic characteristics of digital instrumentation and control (I&C) systems and provide risk-analytical capabilities that supplement those provided by traditional probabilistic risk assessment (PRA) techniques for nuclear power plants. Both methodologies utilize a discrete state, multi-valued logic representation of the digital I&C system. For probabilistic quantification purposes, both techniques require the estimation of the probabilities of basic system failure modes, including digital I&C software failure modes, that appear in the prime implicants identified as contributors to a given system event of interest. As in any other system modeling process, the accuracy and predictive value of the models produced by the two techniques, depend not only on the intrinsic features of the modeling paradigm, but also and to a considerable extent on information and knowledge available to the analyst, concerning the system behavior and operation rules under normal and off-nominal conditions, and the associated controlled/monitored process dynamics. The application of the two methodologies is illustrated using a digital feedwater control system (DFWCS) similar to that of an operating pressurized water reactor. This application was carried out to demonstrate how the use of either technique, or both, can facilitate the updating of an existing nuclear power plant PRA model following an upgrade of the instrumentation and control system from analog to digital. Because of scope limitations, the focus of the demonstration of the methodologies was intentionally limited to aspects of digital I&C system behavior for which probabilistic data was on hand or could be generated within the existing project bounds of time and resources. The data used in the probabilistic quantification portion of the process were gathered partially from fault injection experiments with the DFWCS, separately conducted under conservative assumptions, partially from operating experience, and partially from generic data bases. The purpose of the quantification portion of the process was, purely to demonstrate the PRA-updating use and application of the methodologies, without making any particular claim regarding the specific validity and predictive value of the data utilized to illustrate the quantitative risk calculations produced from the qualitative information analytically generated by the models. A comparison of the results obtained from the Markov/CCMT and DFM regarding the event sequences leading to DFWCS failure modes show qualitative and quantitative consistency for the risk scenarios and sequences under consideration. The study also shows that: (a) the risk significance of the timing of system component failures may depend on factors that include the actual variability of initiating conditions of a dynamic transient, even within the nominal control range and (b) the range of dynamic outcomes may also be dependent on the choice of the assumed basic system-component failure modes included in the models, regardless of whether some of these would or would not be considered to have direct safety implications according to the traditional safety/non-safety equipment classifications.

* Corresponding author. Tel.: +1 614 292 4627; fax: +1 614 292 3163.
E-mail address: aldemir.1@osu.edu (T. Aldemir).

0951-8320/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2010.04.011

1. Introduction

In 1995, the U.S. Nuclear Regulatory Commission (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 available data [1]. This policy applies, in part, to 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]. Digital systems are now being installed in operating nuclear power plants in ever increasing numbers and are being used extensively in new nuclear power plants. Presently no universally accepted methods for modeling digital systems are available in current generation PRAs. Debates continue in the PRA technical community regarding the level of detail that any digital system reliability model must have to adequately represent the range of potentially complex system interactions that may contribute to digital systems failures.

While the findings of a recent study [3] indicates that none of the available reliability modeling methodologies for digital systems satisfy all the requirements for ideal utilization in nuclear power plant (NPP) assessments, the study has identified two methodologies capable of modeling some of the essential logic and dynamic characteristics of hardware/software/firmware/process interactions which are otherwise difficult to represent using conventional PRA static/binary logic techniques, such as the standard event-tree (ET)/fault-tree (FT) methodology presently used in essentially all nuclear power plant PRAs. When a digital instrumentation and control (I&C) subsystem model is constructed by the use of these methodologies, the associated logic-probabilistic analytical engines can produce for users important qualitative and quantitative output information of essentially the same nature of, and modularly compatible with, the output of a conventional PRA set of models with which the digital I&C information needs to be integrated. This includes cut-sets, probabilities of occurrence (or frequencies) of specified undesired consequences (Top Events) and uncertainties associated with the results.

Both methodologies use a discrete-state representation of the system under consideration. The dynamic flowgraph methodology (DFM) is a digraph-based technique [4–6], in which a process variable is represented by a node discretized into a finite number of states. The system interactions are represented by cause-and-effect, and time-effects in discrete time step form, mappings between process variable nodes and, more specifically, between the underlying discrete states used to represent the actual discrete or continuous ranges of the process variables. These relationships provide a system model that describes the system behavior (inclusive of both normal and faulted behavior) under both nominal and off-nominal operating conditions. Instead of binary minimal cut-sets for the system, the DFM yields their multi-valued logic equivalents, which in formal terminology are called "prime implicants." A prime implicant is any monomial (conjunction of basic events) that is sufficient to cause the Top (or undesirable) Event but does not contain any shorter conjunction of the same events that is sufficient to cause the Top Event. If probabilistic information concerning the basic events is possible, the DFM deductive analysis provides a complete-base of prime implicants for a given system Top Event. This permits the probabilistic quantification of the Top Event in a fashion completely analogous to how a conventional PRA Top Event is quantified using the set of its associated minimal cut sets and basic event probabilities. Accordingly, the integration of DFM analytical results with the results of standard PRA tools such as SAPHIRE [7], CAFTA [8] or RISKMAN [9] does not present major difficulties, as documented in a range of PRA applications recently completed in both the nuclear and space system industries [10,11].

The Markov/cell-to-cell-mapping technique (CCMT) is based on the representation of system evolution in terms of probability of transitions between computational cells that partition the system state-space as a function of possible system configurations in a user specified time interval [12,13]. These possible transitions are identified by the topology of the underlying user-constructed system model that describes the system behavior under both nominal and off-nominal conditions, and the transition probabilities reflect user-provided data that quantify the likelihood of transition between system configurations and underlying variable and parameter states. The methodology yields the probability of finding the system in a given cell at a given time in a given configuration. This information can be then converted into dynamic event trees [14] for specified initiating events or dynamic fault trees for specified Top Events [14,15] for integration into plant PRAs [16] using the same standard PRA tools mentioned earlier (e.g., SAPHIRE, CAFTA or RISKMAN).

While both Markov/CCMT and DFM have similar capabilities, the practical trade-offs of level of analytical resolution versus computational limits resulting from the possibility of combinatorial state explosion in system models of larger size suggest the use of Markov/CCMT in the inductive analytical mode (i.e. for specified initiating events) and of DFM in the deductive mode (i.e. for specified Top Events) for realistic systems. To permit the logically complete deductive identification of basic event combinations resulting in a given Top Event (i.e., an identification which is complete within the limits of the DFM logic model representation of the actual system), the DFM purportedly limits its probabilistic representation to the probability values assigned to the states of system variables that represent the occurrence or non-occurrence at specific times of the basic system component failure modes, including software-related failure modes. Once these probabilities are identified and assigned, the DFM, as applied in the study documented in this article, does not associate probabilities with the node to node cause-effect and time-effect mapping among states, as this would limit the capability of its analytical engine to analyze a complex model in deductive mode. The Markov/CCMT, on the other hand, uses a more detailed probabilistic representation of system dynamic behavior, by which several alternative next-state outcomes are considered possible starting from the same originating system state and must be assigned separate transition probabilities. This approach reduces the likelihood of missing a risk-significant event sequence originating from specified system initial conditions, while carrying out an analysis in forward-tracing inductive mode.

A complementary DFM-deductive-mode/Markov/CCMT-inductive-mode utilization of the two methodologies formulated to assure more complete coverage of the fault space was illustrated qualitatively in [17,18] and further expanded and supplemented with a quantitative procedure demonstration in [19]. The demonstration was executed for a steam generator (SG) digital feedwater control system (DFWCS) similar to that of an operating pressurized water reactor (PWR), for a turbine trip event under simplifying assumption on system evolution. This paper discusses and summarizes the findings of these two studies using the DFM, Markov/CCMT and the full DFWCS PRA model of [17]. The associated analyses quantitatively address the dynamic conditions associated with a hypothetical transient produced by a plant power maneuver consisting of:

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

Fig. 1 graphically illustrates this power maneuver. The maneuver was chosen as the backdrop for the dynamic PRA analyses discussed

in the rest of the paper, 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 h period in Fig. 1 was arbitrarily chosen because it is a default reference time period considered in conventional PRA analyses when modeling continuously operating systems (e.g. see [7]).

In order to correctly interpret the information presented in the following discussion, some key boundaries imposed by the scope of the study on the focus and extent of the included methodology demonstration must be stated and understood. The principal constraint consisted in having to limit the demonstration to aspects of digital I&C system behavior for which probabilistic data was on hand or could be easily generated within the existing project bounds. In this respect, the full extent of system behavior modeling and failure identification capabilities of the two methodologies could not be fully exploited in the study, and portions of the models that would address

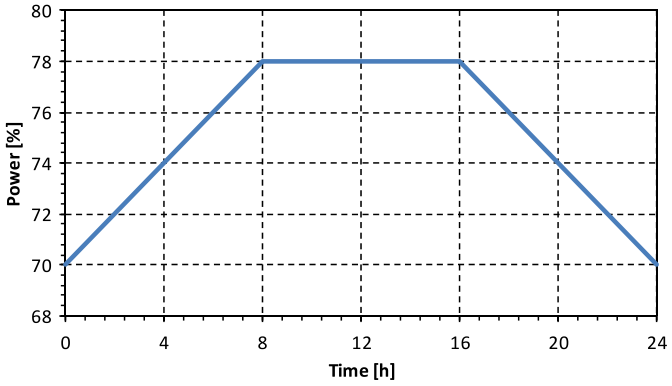


Fig. 1. Reactor power profile for the power excursion scenario.

combinations of component failure modes for which quantification data was not readily available were intentionally left undeveloped in the overall system modeling activities. Notable categories of potential failures not quantified in the models for this reason are failures resulting from software design errors, and common-cause software failures. These two categories in part overlap since the same software running in redundant digital I&C units, if affected by a logic or algorithmic design fault, would contain such fault in all its fielded replications and such fault could result in a simultaneous failure of all redundant units. The difficulty of producing a reasonable and useful risk representation of these types of faults or failures does not lie in the ability or inability of various kinds of PRA logic modeling techniques at hand, including those discussed here, to include them in a system model, but in how the associated risk logic representation may be quantified. Some further discussion on how the methodologies of interest here can represent software design errors is provided in a later section (see Section 3.2).

Section 2 below provides an overview of the DFWCS layout and functional characteristics assumed for the demonstration purposes of Refs. [17,19]. Section 3 describes the demonstrative application of DFM and Markov/CCMT to the DFWCS. Section 4 discusses the results obtained. Observations and conclusions from the study are given in Section 5.

2. The DFWCS [17,18]

The purpose of the DFWCS is to maintain the SG water level within ± 2 in. of an assigned setpoint (designated as 0). The feedwater system serves two SGs with each controlled by its own digital controller as shown in Fig. 2. The controller is considered failed if the SG water becomes too high (over 30 in. above the

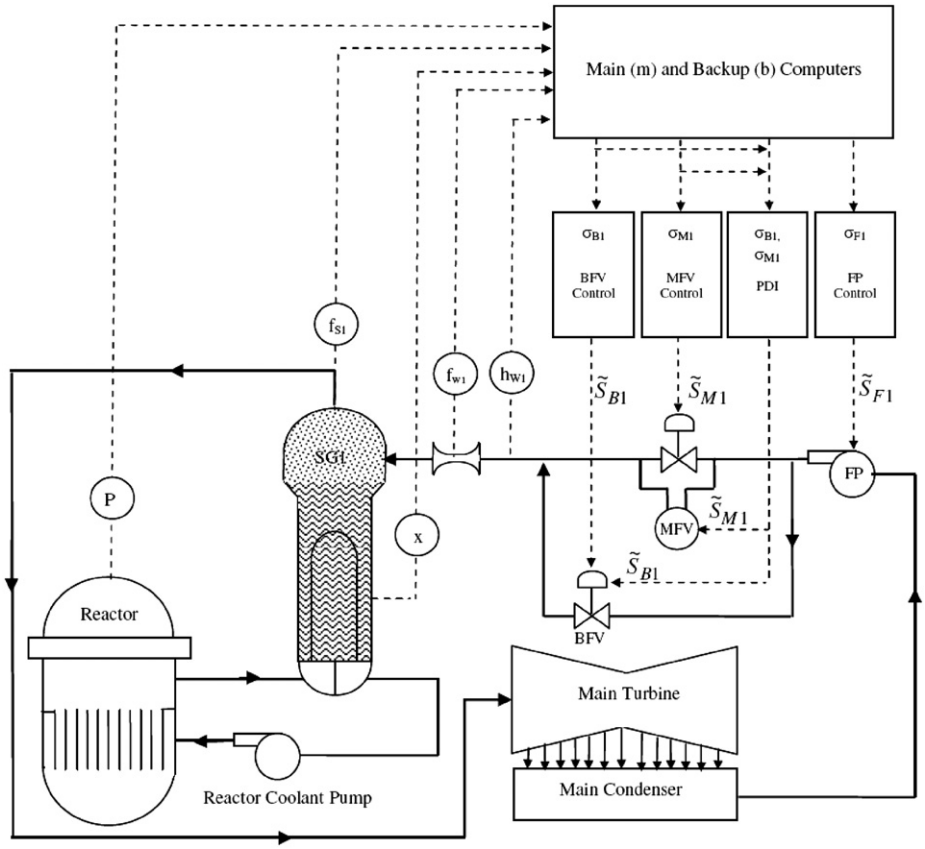


Fig. 2. Detailed view of a single feedwater controller. Solid lines indicate piping. Dashed lines indicate signals.

level setpoint) or if the SG water level falls too low (less than 24 in. below the level 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 study.

A discrete-state representation of the benchmark system was developed in NUREG/CR-6942 [17] as a preliminary step 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 take place among five states (see Fig. 3). 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 and is signaling the controllers to ignore its output. 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 controllers. Transfer of control from the MC to the BC in case of MC failure is represented at this level of modeling in three macro states (MSs) as shown in Fig. 4 to reduce the number of system states since both computers are identical. The transfer of control could be modeled at a lower level if needed. In MS1, both MC and BC are operating normally. In MS2, one computer is down but can be recovered. In MS3 again one computer is down but it is not recoverable. Transitions among the MSs depend upon the state of the controlling computer as shown in Fig. 4. 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:

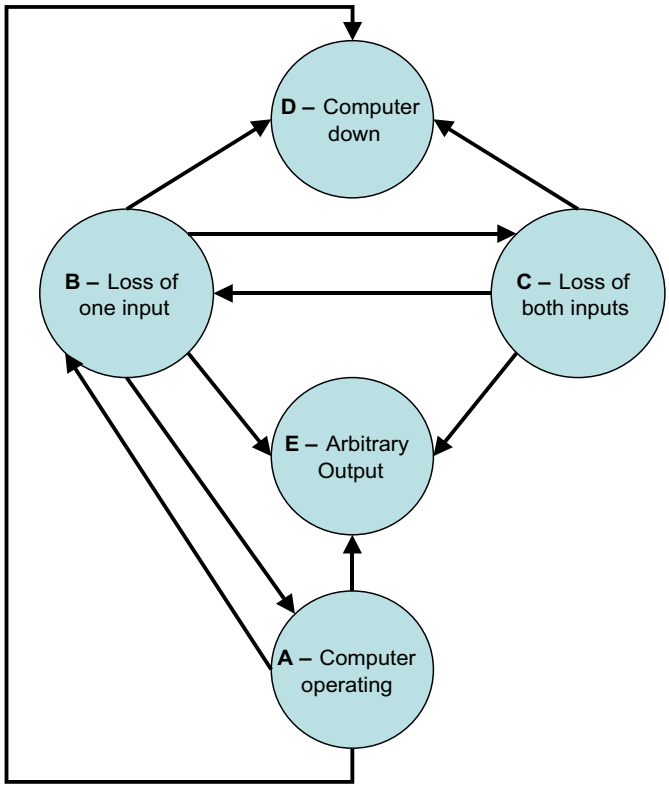


Fig. 3. Intra-computer interactions.

- 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[1]) or to a loss of output of the computer itself.

The fail-over action from MS1 to MS3 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 MS1 to the respective state in MS3. For example, State A in MS1 would have a transition to State A in MS3. 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 MS3.

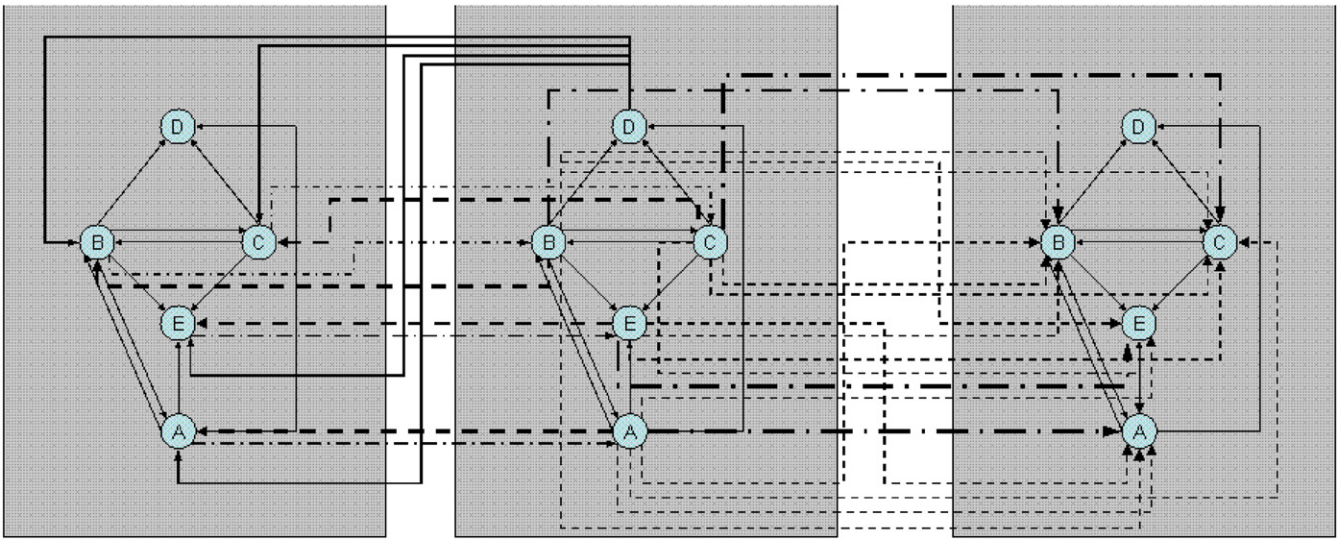
Once valid valve apertures and the pump speed are determined by the computers, those values are passed on to the controllers which check them against independently received data and in turn pass them on the actuated devices themselves.

Fig. 5 shows all the possible controller-computer-actuated device interactions. The 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.

As presented in Fig. 5, the following types of controller failures, including the controller software contribution to these failures, are included in the models:

- 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).

[1] A watchdog timer automatically detects certain classes of software anomalies and resets the processor if any occur.



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 releases 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		

Fig. 4. Inter-computer interactions.

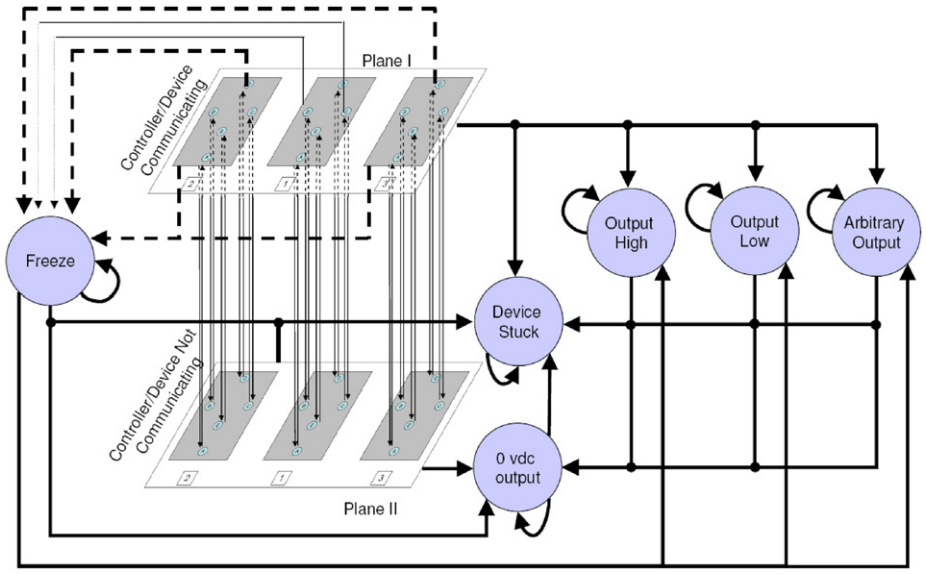


Fig. 5. Computer-controller-actuated device interactions.

- 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.

If both computers fail, the controllers can recognize the failures and send to the actuated devices (i.e. pump or valves) the old valid value (i.e. Freeze). If a controller does not recognize the failure, then it will simply pass on invalid information (Arbitrary

Table 1
Transition rates for MC and BC states [17] (for demonstrative purposes of this study).

Transition $i \rightarrow j$[a]	Statistics of the extreme method		Bernoulli method	
	Un-coverage estimates $(1-C_S)$	Failure rate λ_{ij} (per hour) 3.3E−6 [a] $(1-C_S)$	Un-coverage estimates $(1-C_B)$	Failure rate λ_{ij} (per hour) 3.3E−6 [a] $(1-C_B)$
1→2	0.017	5.61×10^{-8}	6×10^{-3}	1.98×10^{-8}
1→4	0.002	6.6×10^{-9}	8×10^{-4}	2.64×10^{-9}
2→4	0.002	6.6×10^{-9}	8×10^{-4}	2.64×10^{-9}
3→4	0.002	6.6×10^{-9}	8×10^{-4}	2.64×10^{-9}
1→5	0.1	3.3×10^{-7}	0.033	1.089×10^{-7}
2→3	0.021	6.93×10^{-8}	7×10^{-3}	2.31×10^{-8}

[a] $i, j=1$: operating 2: loss of 1 input 3:loss of 2 inputs 4: arbitrary output 5: down.

Output) to the actuated device. Fig. 5 also shows how the computer–computer interactions (presented in Fig. 4) 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 aperture (MFV or BFV) or speed (FP).

The control laws for the DFWCS under both normal and off-normal conditions may be described by a set of algebraic and first order differential equations which have been provided in NUREG/CR-6942. Simulations based on these laws have been used to provide input information for the construction and validation of the DFM and Markov/CCMT DFWCS models discussed in the following sections. The DFWCS definition satisfies the benchmark requirements given in NUREG/CR-6942 [17], and is sufficiently representative of the digital SG feedwater control systems used in operating PWRs to satisfy the demonstration objectives of the study. However, it does not include some digital I&C system features that may be found in non-nuclear applications, although not 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.

Table 1 shows the transition rates for MC and BC states obtained based on the failure modes and effects analysis (FMEA) presented in [17] and using estimation of fault uncoverage via fault injection experiments for the DFWCS [19]. The fault injection experiments were performed to estimate failure rates only for demonstrative use in this study, and a number of assumptions made in their generation limit the general validity of the probabilistic estimates that were produced. The principal limitations are in the fact that fault-injection testing was not carried out according to a necessarily representative operational (input) profile. In addition the following types of originating faults were not considered [19]:

- software requirements and design faults;
- possible non-uniform distribution of hardware faults and fault types;
- common-cause failure effects (whether resulting from design or other causes).

Table 2
Controller, actuated device and power failure rates [17] (for demonstrative purposes of this study).

DFWCS component	Failure rate (per hour)
Main flow valve PID controller	3.3×10^{-7}
Bypass flow valve PID controller	3.3×10^{-7}
Spare PID of the PDI controller	3.3×10^{-7}
Feed-water pump PID	3.3×10^{-7}
Main flow valve	4.2×10^{-5}
Bypass flow valve	4.2×10^{-5}
Feed-water pump	4.2×10^{-5}
Loss of power	4.8×10^{-6}

Table 2 shows the data that were used to represent controller and actuated device failure rates and loss of power [19]. Again, the data are for demonstrative purposes only.

3. Implementation

As indicated in Section 1, while both the DFM and Markov/CCMT have similar capabilities, the DFM uses a more deterministic model of system dynamics to computationally enable the use of an automated deductive procedure for a logically complete (i.e., complete within the boundaries of the DFM model itself) identification of all possible initiating events leading to a specified consequence, whereas Markov/CCMT uses a more detailed probabilistic representation of system dynamics to reduce the likelihood of missing a risk significant event sequence originating from a specified set of initiating events. The computational price paid for this is that, for models with a comparable number of variable nodes, the logic search space of a Markov/CCMT model may become considerably larger than that of a DFM model. This may force the automated analytical search process for system failure scenarios to be carried out in inductive mode only. In these respects, a complementary utilization of the two methodologies is recommended to provide better assurance of proper coverage of

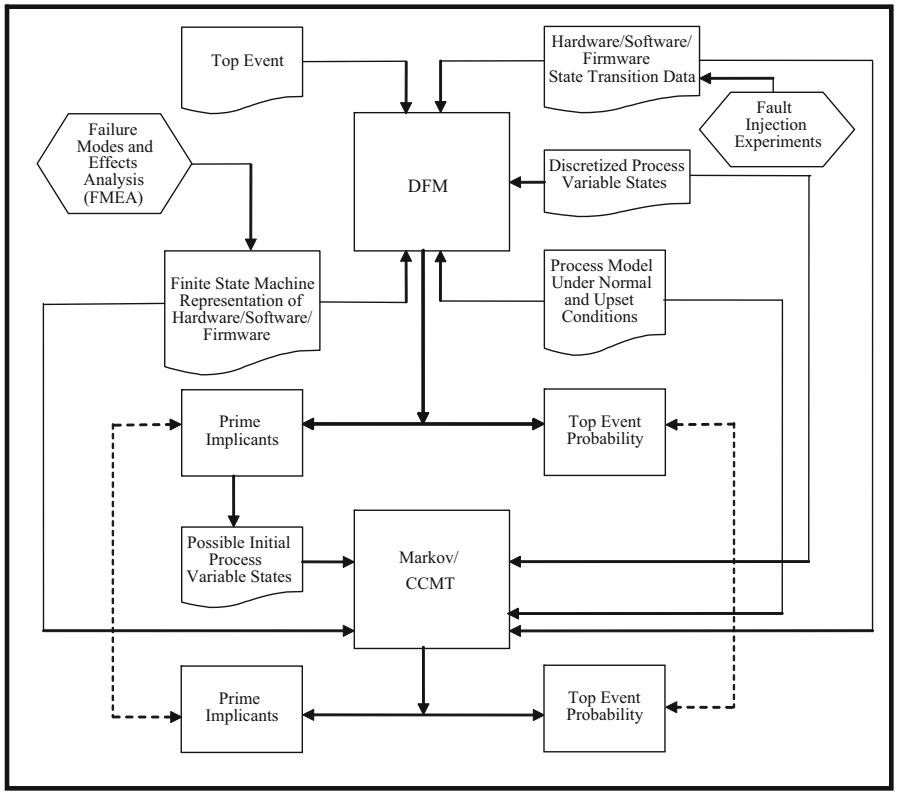


Fig. 6.. A Schematic Representation of the Complementary Utilization of the DFM and Markov/CCMT.

the fault space. Such a utilization of the Markov/CCMT and DFM involves two steps:

1. Identifying the possible initial conditions and prime implicants (or unique event sequences) that lead to specified Top Events (undesirable consequences) using DFM in the deductive mode.
2. Using Markov/CCMT in the inductive mode to validate the prime implicants identified by DFM, as well as to investigate the sensitivity of the prime implicants to finer variations of the initial conditions.

This process is shown schematically in Fig. 6. Both methodologies use a mapping of the discretized system state space onto itself. The mapping is constructed using

- A finite state machine representation of the system of concern, which is used as an initial high level topological model of the system hardware/software/firmware interactions to be modeled in greater detail via DFM and/or Markov/CCMT (this was obtained from an FMEA in this study).
- A discretized representation of the process variables (e.g. pressure, temperature, level) through partitioning the range of interest into intervals (states or cells).
- A process model under nominal and off-nominal or upset conditions where off-nominal conditions correspond to system conditions that may be triggered by the sets of component failure modes, that singly or in combination may cause the system process to deviate from its range of nominal operation.

In the form of modeling applied for this study, the DFM model uses a selection of process variables and associated states (by identifying one state to represent each process variable interval), in a manner that is judged to be representative of the possible nominal, off-nominal and faulted system state space, and then constructs a deterministic mapping among the nodes representing variables and among the underlying states, to represent cause-effects and time-effects within the modeled system. In this form of representation each combination of states of the set of process variables that are causally and time-wise driving another downstream process variable maps into one or more states of the latter, but the mapping itself is not assigned a probability. In its inductive mode, the Markov/CCMT normally uses a subspace consisting of the process variables of interest only (e.g. by excluding variables that may not have physical significance). It then constructs a probabilistic mapping by which a particular combination of states of upstream variables can map with more than one state of a downstream variable, each mapping corresponding to a Markovian state-transition that may occur at each time interval with its own assigned probability. While both methodologies have, in principle, similar mapping capabilities, these modeling choices arise from computational considerations. The mapping processes are described in Sections 3.1 and 3.2, respectively.

In the demonstrative, joint DFM–Markov/CCMT application discussed in this paper, DFM uses the deterministic mapping and a given Top Event definition to trace back in deductive mode the logically complete (as defined in Section 1) set of possible basic-event-combinations/initial-conditions of process variables, which constitute the complete, irredundant base of system prime implicants leading to the Top Event. The Markov/CCMT then uses these possible prime implicant initial conditions deductively determined by DFM and its own probabilistic mapping to inductively search forward in time. This is done to identify whether any additional risk-significant outcomes for the system of interest may be produced from the identified prime implicant

initial conditions. Arguably, such a probabilistic forward search is warranted to give better assurance of completeness in the identification of risk significant event sequences and scenarios for nonlinear systems and/or in the case of component failure modes involving arbitrary outputs (see Section 2), whereby the selection of process variable values (points) to construct the mapping can affect the analytical logic outcomes of the mapping itself.

Both methodologies can quantify the probability of Top Events of concern based on the occurrence probability of the Top Event prime implicants, using the hardware/software/firmware state transition data (in the case of this specific study obtained from fault injection experiments, operational data and data bases). The prime implicants and the Top Event probabilities determined by both methodologies were compared as part of this study.

3.1. The DFM

Fig. 7 shows the DFM model developed to analyze the benchmark DFWCS. This model encompasses the MC, BC, BFV, BFV controller, FP, FP controller, MFV, 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 nodes used to represent the key process parameters (e.g. SG level) or states of key components (e.g. combined MFV/MFV Controller). The node definitions are given in Table 3. The continuous variable nodes are each discretized into a finite number of states. The discretization schemes are shown in Tables 4–11. For continuous variables, the discretization corresponds to a discrete representation of the possible range that the variable can take, such as the one shown for the SG level in Table 6. On the other hand, for component states, the discretization reflects the failure modes that are assumed, such as the one shown for the MFV/MFV Controller in Table 8.

Table 3
Node definitions for 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 and 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

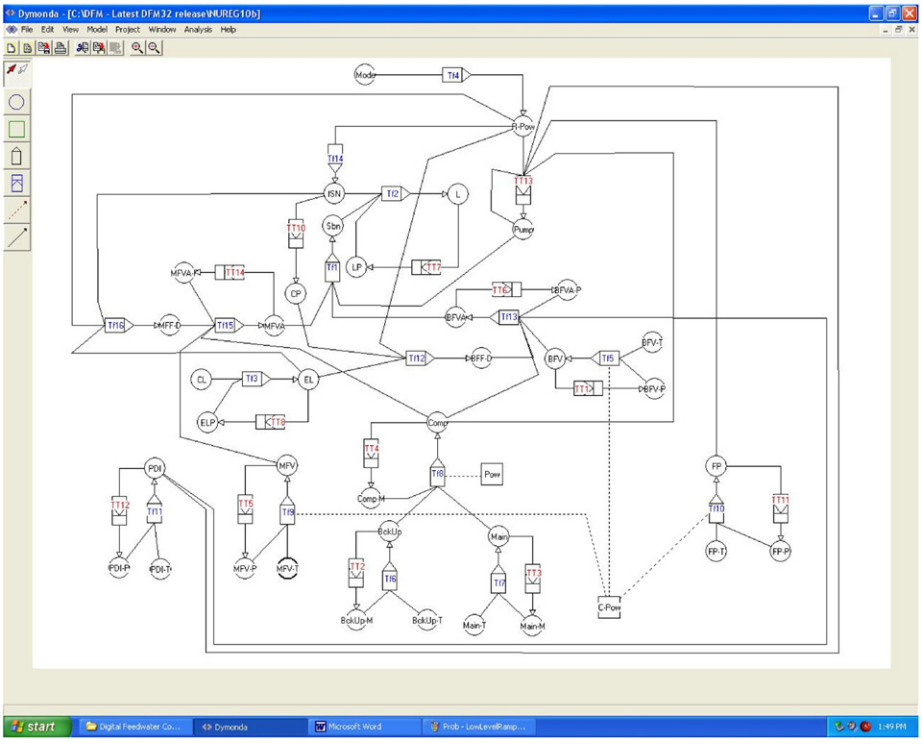


Fig. 7. DFM model of the benchmark system.

Table 4
Discretization of the controller power (node C-Pow).

State	Description
Op	Operating
No	No power

Table 5
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 6
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 7
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 8
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 9
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 10
Discretization of the state transition of the main flow valve/controller (node MFV-T).

State	Description
Comm	Transition to operating and 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 11
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

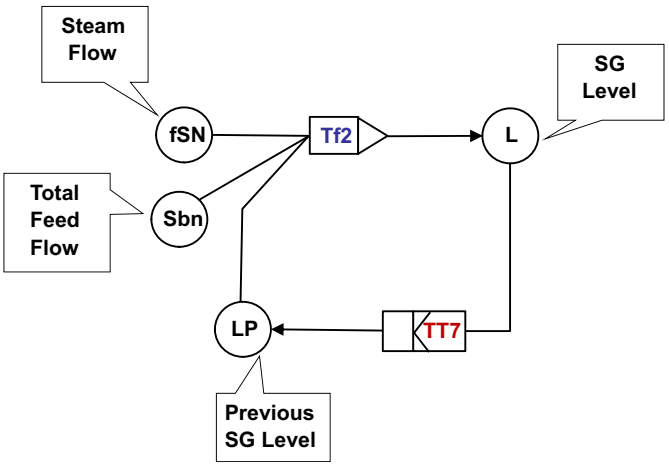


Fig. 8. Zoomed view of transfer box Tf2.

The DFM process variable nodes are graphically linked together to model the relationship between these nodes as shown in Fig. 7. In general, two types of relationships are represented:

1. Physical relationship with or without a timing element.
2. Logical and functional relationship with or without a timing element, including control and safety algorithms and logic incorporated within the system software.

The mapping of discrete logic and time-step states that describes the cause-effect and temporal relationship of process variables is in DFM expressed by decision tables contained in "transfer boxes" that may or may not explicitly include within their logic mapping the representation of time-effects.

An example of a temporal relationship is represented by the transfer box Tf2 in Fig. 7. This transfer box originally appears on the top center portion of the complete model, and a zoomed view is provided in Fig. 8. Transfer box Tf2 shows that the current SG level depends on the steam flow, the total feed flow and the SG level at the preceding time-step. The transfer function between

the nodes is summarized in the associated decision table (Table 12).

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. 7), and a zoomed view is provided in Fig. 9. Transfer box Tf9 shows how the failure modes of the Main Flow Valve/Controller affect the system. In particular, the current state of the MFV/MFV 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). 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. The transfer function between the nodes is summarized in the associated decision table (Table 13). An example of representation of system software functionality is given by the group of variable nodes compensated level (CL), error in level (EL) and error in level at preceding time step (ELP), and the transfer box Tf3 that connects them, expressing the fact that the value of the SG level error software calculated by the software is a function of the compensated level parameter and of the level error at the preceding time step, both of which are also calculated by the software itself. The detailed mapping of how the EL states are in the software calculations determined by the combined values of the CP and ELP states is expressed by a decision table much like those shown in Tables 12 and 13.

With respect to the construction of DFM decision tables, two key observations are in order. The first observations is that the identification of the basic causality and time flow and state mapping expressed by the decision tables can be derived from qualitative information about the system design contained in design descriptions and specifications, or, at a more detailed level, by quantitative information represented by simulator and or test outputs. Section 3.2 goes in some depth in the description of the quantitative aids used in the construction of the Markov/CCMT mappings. This discussion is not repeated here but the information produced by such aids was also used to construct the DFM decision table mappings.

Table 12
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**
:	:	:	:

Table 13
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**

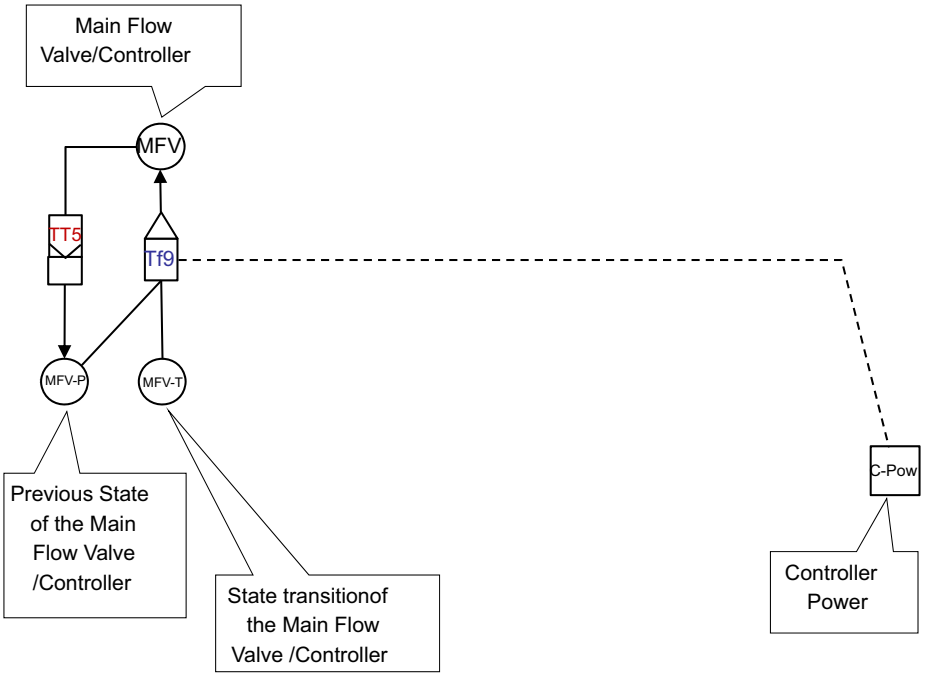


Fig. 9. Zoomed view of transfer box Tf9.

The second observation is that both hardware and software failure modes are expressed in DFM as the intrinsically discrete states of certain system components, which are associated with probability values that can be assigned to them. For example, a valve set of states may be defined as: a) normal, b) stuck open, c) stuck closed, or d) frozen at previous state. Software function failure modes can be defined in similar fashion. For example, a controller algorithm may be characterized as: a) normal, b) overcompensating, c) undercompensating, d) reversed, or e) frozen at preceding output value. The effects of basic component failure modes on the overall system are thus expressed by the logic mapping tabulated in the decision tables that express how the occurrence or non-occurrence of the corresponding process-variable or system-component states, in combination with the states of the other variables on the input side of the corresponding "transfer boxes," affect the state of the process variable on the output side. Thus, if any software algorithm or logic error were hypothesized to be present in the portion of the SG control software represented by transfer box Tf3, an additional node would be added on the input side of it, e.g., to include the set of failure modes (normal, overcompenating, etc.) listed above for illustration purposes. Because no probabilistic information was available for the quantification of such states at the time of the study, the transfer box Tf3 was limited to express only the normal functioning state of the specific portion of the control software functionality there represented. Similar arguments apply to the state transitions used in the Markov/CCMT model.

Although software failures classifiable in the category of design error were for the above reasons not explicitly considered in the DFM model of the DFWCS (the same also being true for the Markov/CCMT version of the model), software failure modes that could be quantified with the information available or generated by the fault injection process discussed in Section 2 were represented in the model. For example, the DFM nodes PDI (Proportional Derivative Integral controller), MFV-T (Main Feed Valve controller), FP-T (Feed Pump controller), and BFV-T (Bypass Feed Valve controller) all include states representing a set of associated software failure modes (and their probabilities), the effects of which on the system are represented in the downstream transfer boxes and decision tables (Tf1, Tf9, Tf10, and Tf5, respectively). In the Markov/CCMT model, such failure modes can be also represented by the appropriate choice of states and transitions to the failure modes are quantified by their respective probabilities.

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. For the benchmark DFWCS, failure and fault analyses using the deductive technique were carried out to derive the prime implicants for the failed states of the DFWCS. 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 Sections 3.1.1 and 3.1.2.

3.1.1. Qualitative and quantitative analysis for low SG level

The Top Event defined here describes failure of the DFWCS by allowing the level in SG to become too low. The assumed reactor power profile is shown graphically in Fig. 1. The analysis concentrated on identifying prime implicants for a SG Low Level failure state occurring in the 8 h 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 Level 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.

Table 14
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

Table 15
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

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.

In this analysis, the time step $t=0$ refers to the 78% power steady-state that follows the end of the initial 8 h ramp-up period, whereas the time step $t=-1$ refers to the initial 8 h 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 14 provides the description of the conditions that are included in the Top Event definition.

The key transition in this Top Event is summarized in the first 2 rows of Table 14. 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 15. 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.

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 as follows: 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 15. 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 16. Table 16 represents an expansion of the original top event, with the lowest SG level column (first column of Table 15) replaced by the possible combinations of steam flow, feed flow, and previous SG level (the first 3 columns of Table 16).

To continue the deductive analysis, the causality shown in the model is further backtracked. For the transition table shown in Table 16, the column corresponding to Sbn at $t=0$ is next expanded with the decision table for transfer box Tf1.

Table 16
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
:	:	:	:	:	:	:

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 h time span. 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 17. 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 bold in Table 17), 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 17 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.

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 [17], 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:

$$\text{Top Event} = \bigcup_{i=1}^{1197} \text{Prime Implicant}_i,$$

where

$$\text{Prime Implicant\#}i \not\subset \text{Prime Implicant\#}j \quad \text{for} \quad i \neq j.$$

Table 17
Top prime implicants for low steam generator level (key failure transition shown in bold, distinguishing boundary condition shown in italics).

#	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@$t=-1$ Mode=1@$t=-1$	3.86E−05

Step 2—Expression of Top Event as set of Mutually Exclusive Implicants (MEIs):

$$\text{Top Event} = \bigcup_{j=1}^{m} \text{Mutually Exclusive Implicant}_j,$$

where

$$\text{Mutually Exclusively Implicant\#}i \cap \text{Mutually Exclusive Implicant\#}j = \emptyset \quad \text{for } i \neq j$$

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

$$\text{Top Event Probability} = \sum_{j=1}^{m} \text{Probability of Mutually Exclusive Implicant}_j.$$

For the low SG level Top Event, the Top Event probability of 4.19E−04 is obtained in this fashion, as shown in Fig. 10.

3.1.2. Qualitative and quantitative analysis for high SG level

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 was used for the analysis discussed in Section 3.1.1 can also be analyzed for a Top Event concerning a high SG level occurring in the 8 h of the ramp-down power maneuver, again assuming that the system starts in a state with

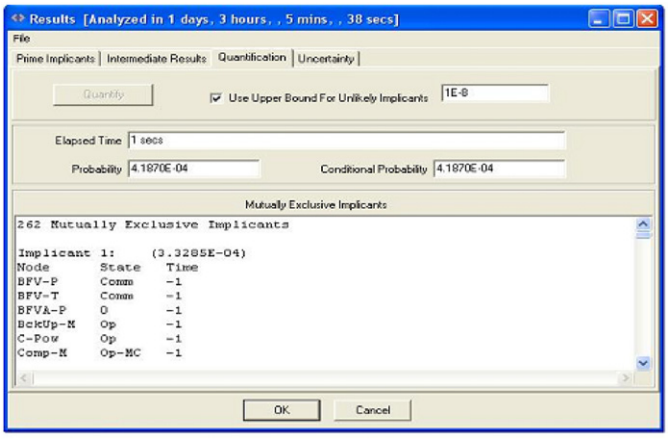


Fig. 10. Quantification for low SG level Top Event.

Table 18
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

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 h ramp-down period, whereas the time step $t=-1$ refers to the 8 h 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 18 provides the description of the conditions that are included in the Top Event definition.

The key transition in this Top Event is summarized in the first 2 rows of Table 18. It corresponds to the progression of the SG level from normal (LP=0) to high ($L=+2$). 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.

Table 19
Top prime implicants for high steam generator level (key failure transition shown in bold, distinguishing boundary condition shown in italics).

#	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@$t=-1$ Mode=1@$t=-1$	4.37E−07

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 19 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 bold in Table 19), 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 italics in Table 19). For example, examination of the prime implicants listed in Table 19 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 19 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

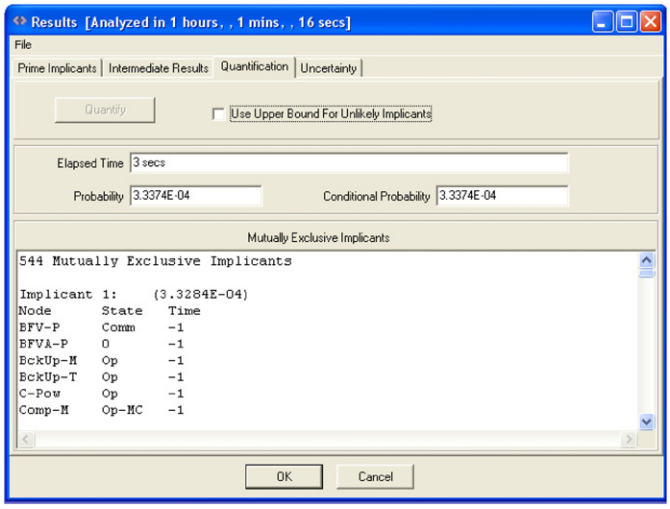


Fig. 11. Quantification for high SG level Top Event.

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.

It should be noted 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.

As shown in Fig. 11, 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.

3.2. The Markov/CCMT

The Markov/CCMT uses the inputs shown in Fig. 6 to determine the transition probabilities between the cells that are defined by the discretized controlled variable states and that partition the system state space. In a full Markov/CCMT model using the complete system state space, these transition probabilities 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 (e.g. Tables 12 and 13). The mapping is constructed by sampling points from each cell as system locations and determining the system arrival cells within a user specified modeling time step. 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 possible range of initial process variables states obtained from the output of DFM. This approach reduces the computational burden of determining the full mapping most of which may not be relevant for the case under study. 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. A more detailed description of Markov/CCMT can be found in [12,13,17].

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 [5]. The modeling time step is chosen as 8 h. 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 SG model is implemented using a C/C++ proprietary code from ASCA Inc. Figs. 12 and 13 show, respectively, the control logic and actuated device Matlab® SIMULINK modules.

The choice of the hardware/software/firmware states is based on Figs. 3 and 5. Figs. 14–17 show the Markov transition diagrams for the DFWCS components (MC, BC, BFV controllers, PDI controller, and the controller power source). The Freeze state in Fig. 14 represents the Down state of the computers (see Figs. 4 and 5 for this correspondence). Fig. 14 also assumes that the transition rates out of the two constituent states of MS1, MS2, and MS3 to State 7 are the same for each of the pairs (i.e. λ^{comp}_{MS2-7} for each of the States 2 and 4, λ^{comp}_{MS1-7} for each of the States 1 and 1, and λ^{comp}_{MS3-7} for each of the States 5 and 6). The Markov transition diagrams for MFV and FP controllers are similar to that shown in Fig. 15 for the BFV controller. The Markov transition diagram for the power source of the MFV, BFV, and FP controllers is presented in Fig. 17. The transition rates among BC and MC states are as given in Table 1.

From Table 2, the failure rates for the MFV, BFV, and FP PID controllers are 3.3×10^{-7}/h. Moreover, from Fig. 15, the number of failure modes (i.e. the number of failure states) is 6 (e.g., Output High, Output Low, Arbitrary Output, Loss of Output). Under the assumption that failure modes are equally probable (due to unavailability of mode specific failure data) this implies that for the Markov transition diagram of the BFV controller shown in Fig. 15:

- $\lambda^{BFV}=3.3\times10^{-7}/h/6=5.5\times10^{-8}/h$;
- the transition rates that lead to state 8 (Stuck) of Fig. 15 are $\lambda^{MF}=4.2\times10^{-5}$/h (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. 16. From Table 4, the failure rate for the PDI controller is 3.3×10^{-7}/h. Thus, since the transition rates for the PDI controller are equally like to occur, $\lambda^{PDI}=3.3\times10^{-7}/3/h=1.1\times10^{-7}$/h.

The failure rate of the power source (for the MFV, BFV, and FP controllers) is listed in Table 2, i.e. $\lambda^{POW}=4.8\times10^{-6}$/h (Fig. 17).

Table 20 summarizes the states in Figs. 14 and 17 and indicates that there are 7∗7∗7∗7∗6∗2=28 812 possible state combinations for the overall system. For Markov/CCMT modeling purposes, these states can be reduced as shown in Table 21 by combining states with similar effects on the SG feedwater level evolution. Figs. 18–20 show the corresponding reduced Markov transition diagrams. Fig. 18 accounts for all the interactions shown in Fig. 14 through time dependent failure rates determined from a separate auxiliary Markov model which uses Fig. 14 as a Markov transition diagram as shown in Appendix A.

The two computers (MC and BC) and the three controllers (MFV, BFV, and FP) share the same power sources [17]. 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. 17. A failure in the computer power source causes the failure of both MC and BC and,

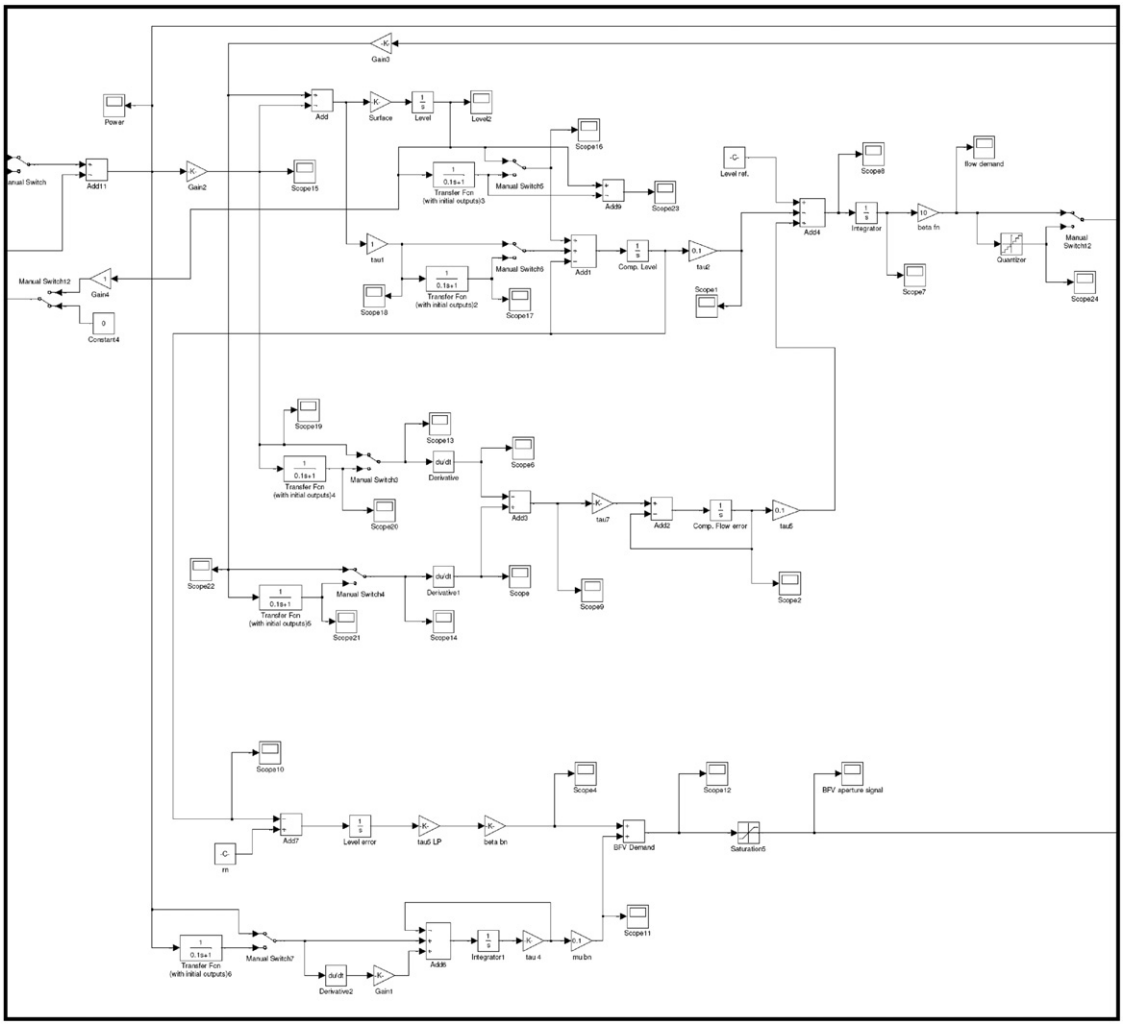


Fig. 12. SIMULINK control logic module.

subsequently, the controllers freeze their own outputs (see Section 2). Since both the computers are modeled in a single Markov transition diagram which accounts for their interaction shown in Fig. 14, the failure of the computer power source can be simply represented with a transition to the Previous Output from every other state of Fig. 18. As indicated in Section 2, once a device failure is detected the last output from that device is used. Table 22 summarizes the number of reduced hardware/software/ firmware states and shows that the reduction leads to $3*5*5*5*4*2=3000$ states.

For the determination of the transition probabilities between the hardware/software/ firmware states, the data presented in Tables 1 and 2 are used along with auxiliary Markov models in Appendix A 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 (with 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.).

3.2.1. *Markov/CCMT analysis for the power excursion scenario*

As indicated in Section 1, the DFWCS behavior is assumed to be represented by the power transient, described in Fig. 1 for this analysis. The reactor power ramps up from 70% at time $t=0$ to 78% at $t=8$ h, remains constant for 8 h, then ramps down from 78% to 70% during $t=16$–24 h.

Fig. 21 shows the Top Events (High and Low level failure) cumulative distribution functions (CDFs) as a function of time. 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.

Tables 23 and 24 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 (order) identifying the order in which the events occur.

As can be seen from Table 23, the top eight sequences (or prime implicants) with the highest probability for Low Level failure are singletons, with MFV in the Stuck state being the dominant event and Power-Off (i.e., failure of the power source of the MFV, BFV, and FP controllers shown in Fig. 17) is the second most dominant event. From Table 24, MFV Stuck 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. From Tables 23 and 24 it is important to note that the same event (i.e. MFV Stuck) can lead to different consequences

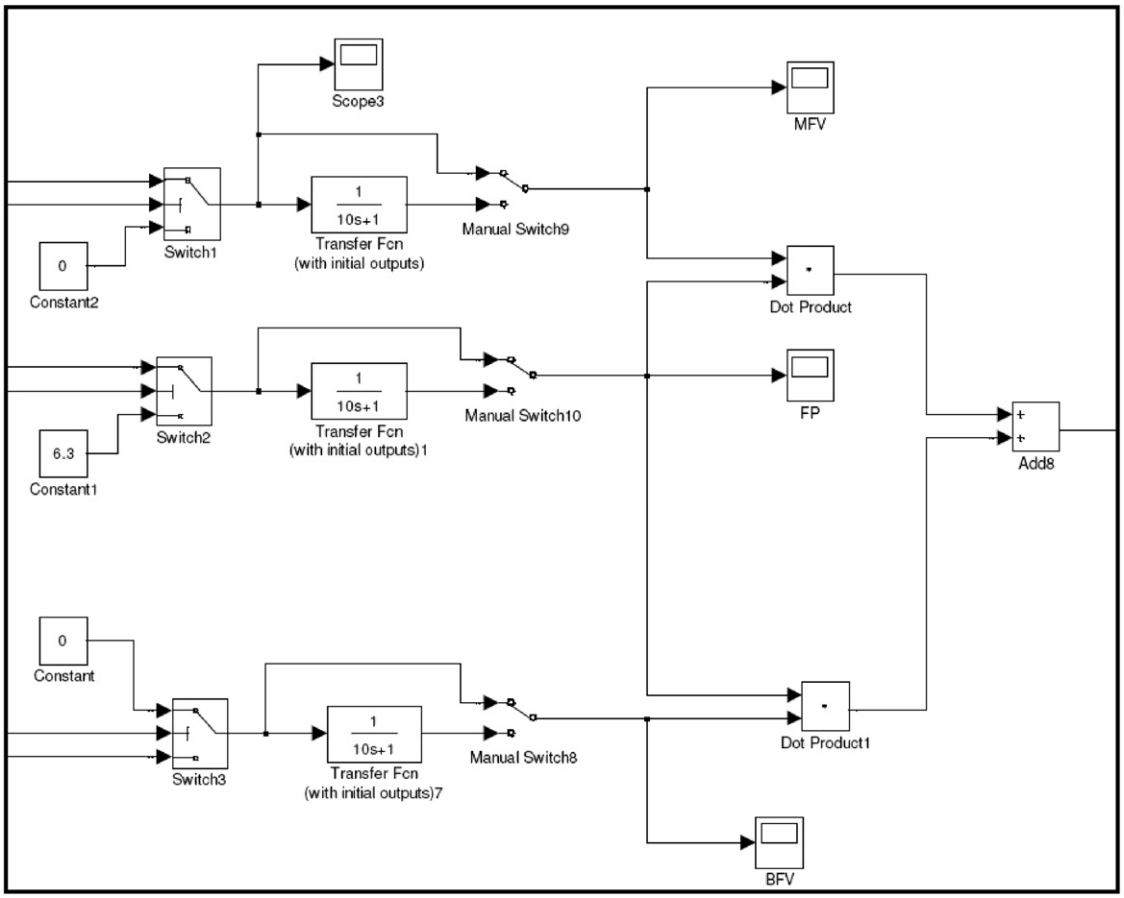


Fig. 13. SIMULINK module for actuated devices of the DFWCS (MFV, BFV, and FP).

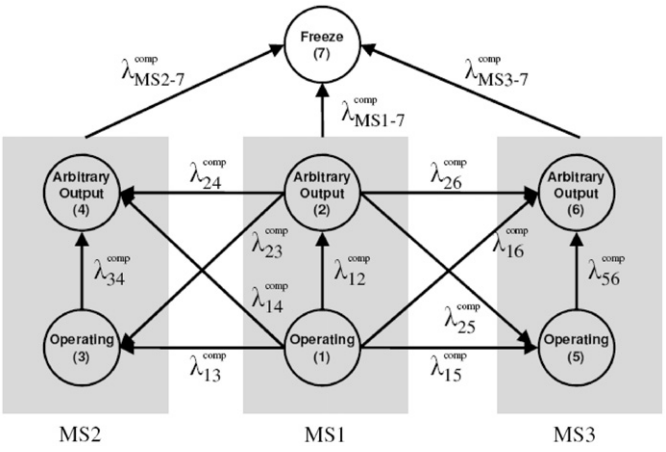


Fig. 14. Markov transition diagram for the MC and BC.

depending its time of occurrence and the system configuration at the time of its occurrence.

Events which occur the most frequently in the failure sequences, without regard to their probability of occurrence, are given in Tables 25 and 26. Tables 25 and 26 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 Off state appears as the third event in 937 sequences or scenarios leading to Low Level failure. Tables 27 and 28 list all events without regard to the order in which events occur in a given sequence.

Table 27 indicates that three most significant component failure modes in descending order that lead to Low Level are the Power Off, PDI Output Low, and PDI Stuck (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). However, Table 25 indicates that PDI failure either in Arbitrary Output mode or the Stuck mode is the initiator rather than Power Off, which becomes the enabling event for system failure by Low Level. Comparison of Tables 25 and 27 also shows that, while PDI failure by low output is the second most frequently encountered event among failures leading to low level (Table 27), it is not among the first three events leading to Low Level (Table 5) and has to be preceded by other failures to cause system failure by Low Level and subsequently is an enabling event. Similarly, comparison of Tables 26 and 28 shows that while computer failure in the Freeze state is the most frequent event encountered among the event sequences leading to High Level (Table 28), it is an enabling but not an initiating event and needs to be preceded either by FP or BFV failure in the Output High mode to cause system failure by High Level. Distinguishing between initiating and enabling events provides useful information to assess the significance of failure events from a defense-in-depth viewpoint. The differences between Tables 25 and 27 and between Tables 26 and 28 also 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.

Finally, the Fussell–Vesely (FV) Importance for Low and High Level failure sequences is presented in Tables 29 and 30 respectively. In both cases, only the top five most significant events are shown. These tables consider both individual events in

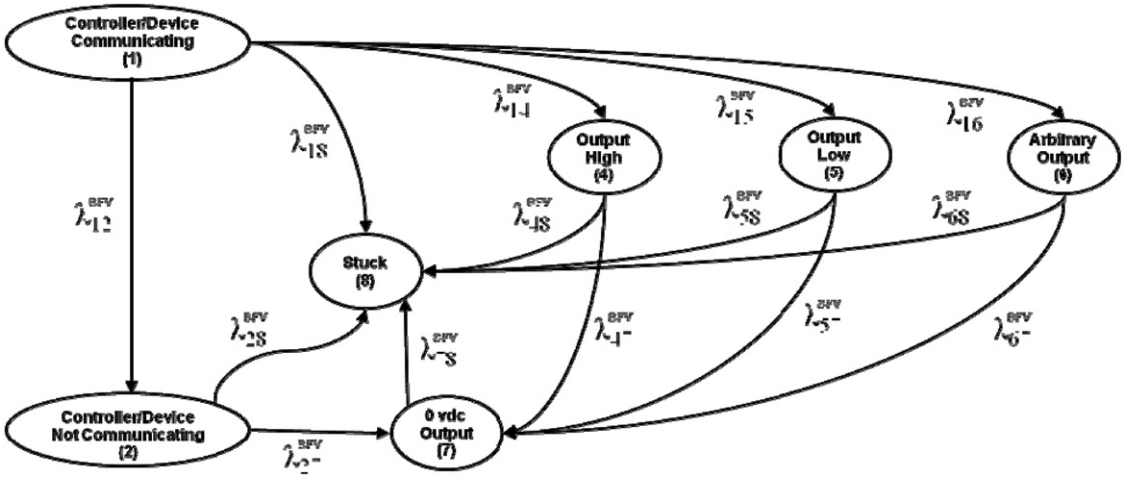


Fig. 15. Markov transition diagram for the BFV controller (the Markov transition diagrams for the MFV and FP controllers are similar).

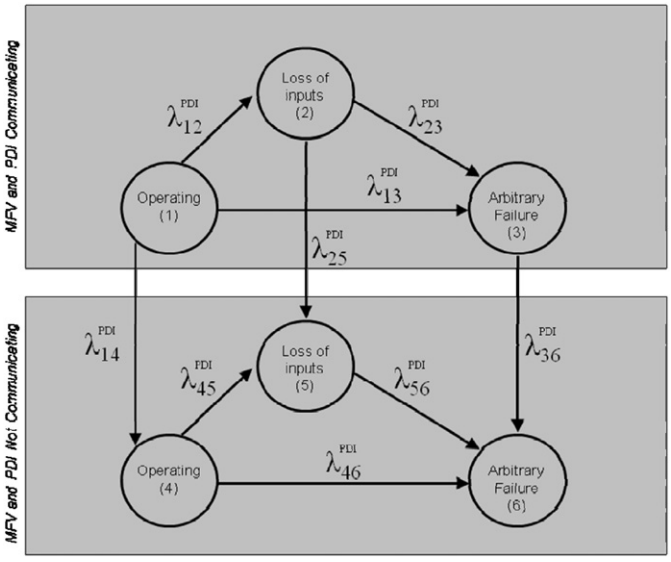


Fig. 16. Markov transition diagram for the PDI controller.

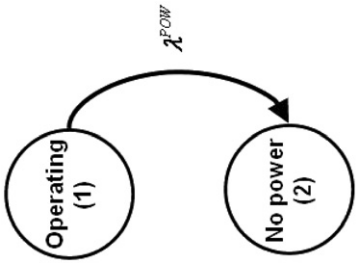


Fig. 17. Markov transition diagram for the power source of the MFV, BFV, and FP controllers.

the sequences as well as their order in the entire sequence. Comparison of Tables 24 and 25, respectively, with Tables 29 and 30 indicates that while ranking by probability of occurrence and FV importance yield similar results for Low Level failure, ranking differs for High Level where the FV importance yields MFV Stuck as the fifth most significant failure and ranking by probability of occurrence yields MFV failure by Arbitrary Output as the fifth most significant failure. However, the order of the top four most significant events is consistent between probability of occurrence and FV importance rankings for High Level failure as well.

Table 20
List of hardware/software/firmware states.

Components	Number of states
Computers	7
MFV Controller	7
BFV Controller	7
FP Controller	7
PDI Controller	6
Controller power	2

Table 21
Reduction of hardware/software/firmware states by combinations.

Component	New State	Combines/renames
Computers	Correct Output	States 1, 3, and 5 of Fig. 14
	Previous Output	State 7 of Fig. 14
	Arbitrary Output	States 2, 4 and 6 of Fig. 14
MFV, BFV, FP Controller	Correct Output	State 1 of Fig. 15
	Previous Output	State 3, 8 of Fig. 15
	Output High	State 4 of Fig. 15
	Output Low	States 2, 5, and 7 of Fig. 15
	Arbitrary Output	State 6 of Fig. 15
PDI Controller	Correct Output	State 1 of Fig. 16
	Previous Output	State 2 of Fig. 16
	Arbitrary Output	State 3 of Fig. 16
	Output Low	States 4, 5, and 6 of Fig. 16

3.3. Sensitivity analysis of the arbitrary output condition

As discussed in Section 1, although both DFM and Markov/CCMT can be used for deductive and inductive reasoning, a computationally more feasible 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 poses a particularly challenging situation since it affects both the 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% and 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

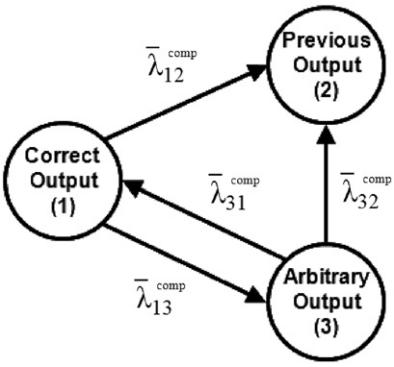


Fig. 18. Reduced Markov transition diagrams for the computers.

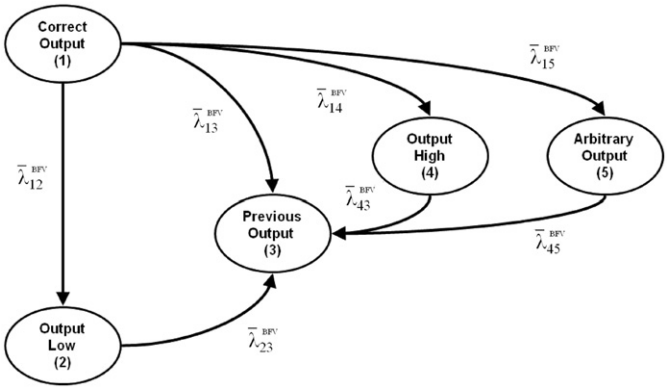


Fig. 19. Reduced Markov transition diagram for the MFV, BFV, and FP controllers.

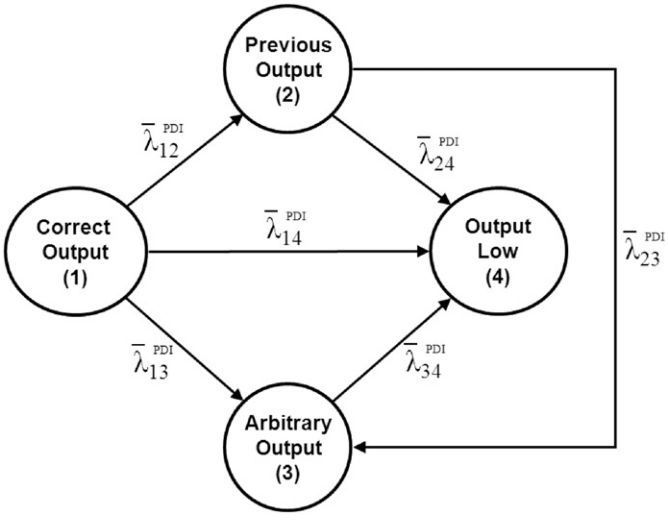


Fig. 20. Reduced Markov transition diagram for the PDI controller.

Table 22
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

Output state valve and pump positions. The samples were averaged together to form 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. A 95%-confidence interval was computed based on the information gathered from each of the analyses. This information is shown in Figs. 22 and 23. For High Level failure, the confidence intervals after 8, 16, and 24 h are 21.64%, 23.25%, and 0.048% of the mean, respectively. For Low Level failure, the confidence intervals after 8, 16, and 24 h are 0.041% 0.066%, and 0.065% of the mean respectively. Table 31 gives the mean probability found for both Low and High failure. These values were found using the total failure probability after 24 h for Low Level and High Level failure from each of the 30 samples. Also reported are the minimum and maximum values. Figs. 24 and 25 show the size of the confidence interval as a function of the number of samples used for Low and High Level failures, respectively, and show that the confidence interval is shrinking as the number of samples used increases, as expected.

Although Figs. 22–25 and Table 31 indicate that the stochastic nature of the modeling of Arbitrary Output does not significantly affect the estimated values of High Level and Low Level probabilities, a more detailed analysis of the results was carried out to investigate other possible impacts of the modeling process on the type and frequency of the sequences leading to system failure.

The post processing of the results was performed by SAPHIRE [7]. From the Low Level failure scenarios, a total of 142,763 event sequences are generated, with 7740 unique sequences. Table 32 lists how many sequences were repeated in a given number of runs, along with the probability contribution from those sequences. The Low Level failure scenarios have a mean probability of occurrence of 4.963E−4 as also shown in Table 31. Out of the 7740 sequences leading to Low Level, 2626 appear in each of the 30 samples and account for over 99% of the total probability (4.962E−4 for the combined 2626 sequences). For certain entries, the probability was too low for SAPHIRE to calculate, and thus only an approximation is given.

Table 33 presents the 10 most dominant sequences leading to Low Level failure. From Table 33, 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. 15) 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 7737 sequences account for the remaining 2% of the total probability.

A comparison of Table 33 with Table 23 shows that stochastic sampling does not produce significant changes on the top 10 most frequently occurring sequences leading to Low Level. The only differences observed are small changes in the sequence probabilities of the relevant sequences (i.e. Sequences 4, 6, and 8 in Table 23 and Sequences 4, 6, and 7 in Table 33) and their contribution for total probability (which leads to reversal of the order of Table 23 Sequences 7 and 8 in Table 33).

From the High Level failure scenarios, a total of 152,070 event sequences were generated, with 7543 unique sequences (Table 32). The High Level scenarios have a mean probability of occurrence of

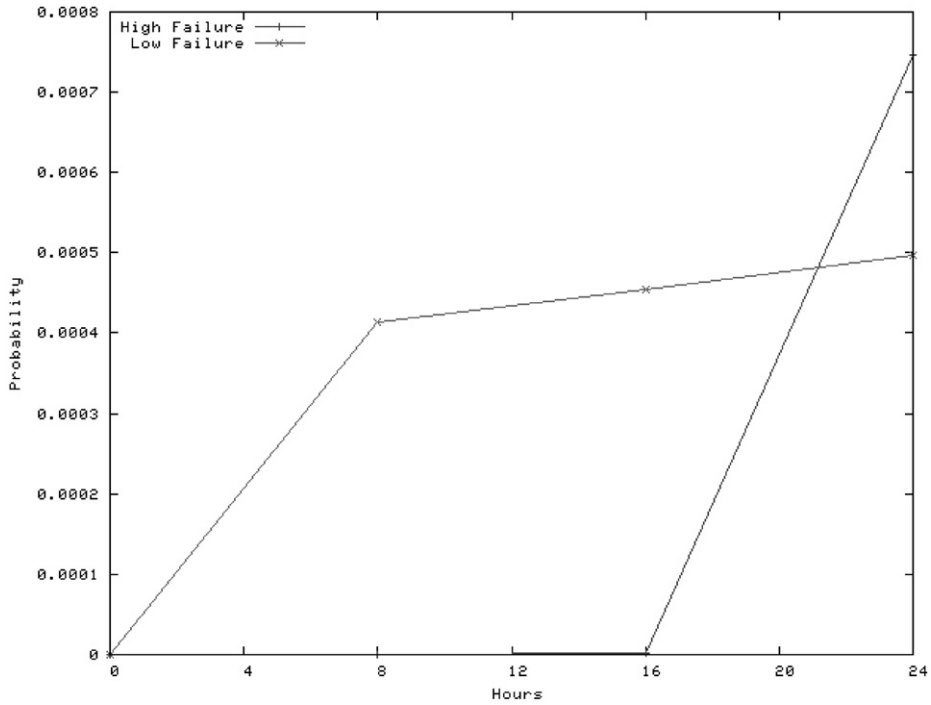


Fig. 21. DFWCS failure probability as a function of time.

Table 23
Low level failure scenarios ranked by probability of occurrence.

Sequence number	Sequence probability	% Total probability	Sequence		Order
			Component	State	
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 24
High level failure scenarios ranked by probability of occurrence.

Sequence number	Sequence probability	% Total probability	Sequence		Order
			Component	State	
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

7.460E−4 (as also shown Table 31). Table 32 shows that 3542 sequences appear in all 30 samples and contribute to 7.454E−04/7.460E−04=99.9% of the total High Failure probability.

Table 34 presents the 10 most dominant sequences leading to High Level failure. Again, most sequences are singletons with MFV Stuck largely dominating. From Table 34, the dominant event sequence for High Level failure is MFV Stuck as the only event, 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. Comparison of Table 34 to Table 24 shows that the nature and probability ranking of the top 9 sequences do not change. While there is about 20% decrease in the probability of Sequence 5, its percent contribution to total probability is about the same (0.06 vs.0.05). On the other hand, Sequence 10 in Table 33 is now replaced with a new sequence in Table 34, which indicates that modeling of Arbitrary Output failure mode may need special consideration regarding its qualitative and quantitative impact on system failure modes.

Frequency of events without regard to their probability of occurrence, are given in Tables 35–38. In comparing Tables 25–38 to Tables 25–28, the following similarities and differences were observed:

- For Low Level failure, Power in the Off state is the most commonly appearing event as the third event in a sequence in Table 35, 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 the first failure. The ranking of the most frequently occurring three

Table 25
Low level failure events ranked by component and number of sequences.

Low failure			
Component	**State**	**Order**	**Number of sequences**
Power	Off	3	937
Computer	Arbitrary Output	3	781
PDI	Arbitrary Output	1	629
PDI	Stuck	1	616
BFV	Output High	1	563

Table 26
High failure events ranked by number of occurrences.

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

Table 27
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
Computer	Arbitrary Output	1228

Table 28
High failure events ranked by number of occurrences (no timing).

High failure		
Component	**State**	**Number of occurrences**
Computer	Freeze	2016
FP	Stuck	1585
MFV	Stuck	1576
FP	Output High	1490
PDI	Arbitrary Output	1373

Table 29
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

events (i.e. Power-Off, Comp-Arbitrary Output, PDI-Arbitrary Output) match those reported in Table 25 for the single run.

- For High Level there is discrepancy between Tables 26 and 36. Table 26 identifies the Computer in the Freeze state as the second failure as the most dominant event, while the PDI in the Arbitrary Output state (top ranking event in Table 36) is much lower in the list. However, both Tables 26 and 36 list FP in the Output High state as the first failure and the Computer in the Freeze state as the third failure in consistent ranking leading to High Level failure.
- Table 37 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. In Table 27, Power-Off and PDI-Output Low are the top ranking events. The rankings of the third and fourth ranking events are different as well.
- Table 38 indicates the PDI in the Arbitrary Output state is the most common event for High Level failure whereas Table 28 lists Computer in the Freeze state as the top ranking failure. While the nature of the events in Tables 28 and 38 are the same their rankings are different.

During the sensitivity analysis it was also observed that a large number of sequences appearing in the relatively small sampling used (i.e. 30 runs) contain an Arbitrary Output failure event. If the sample size is increased, it is expected that Arbitrary Output events will appear increasingly dominant.

Table 30
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

4. Results and discussion

As indicated in Section 1, it is usually preferable to use the DFM in the deductive mode (i.e. for specified Top Events) and Markov/CCMT in the inductive mode (i.e. for specified initiating events) for realistic systems due to computational challenges. In the demonstrative application discussed in this paper the deductive DFM analyses cover potential faults occurring in successive two 8 h long time-steps:

- For Low Level failure, the power ramp-up phase (from 70% to 78% power) and the 8 h 78% power steady state period.
- For the High Level failure Top Event, the ramp-down phase (78–70% power) and the 8 h steady state period immediately following the ramp down.

In the DFM analysis for Low Level failure, the focus is on the ramp-up phase because this is the phase when the DFWCS is most vulnerable to this type of fault condition. If the change in feed flow cannot match the increase in steam flow, the SG level can drop and lead to reactor trip. Similarly, for the High Level failure Top Event the focus is on the ramp-down phase because 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. An extended DFM analysis for High Level failure was carried out for an extra 8 h time step to obtain quantitative results more directly comparable with the Markov/CCMT results. The inductive

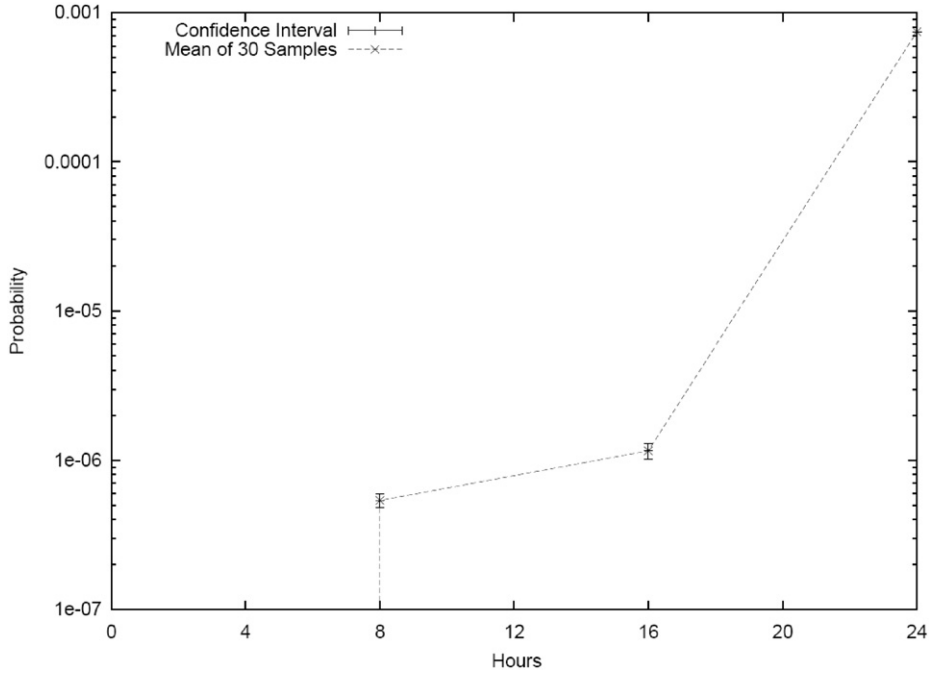


Fig. 22. High failure arbitrary output confidence interval.

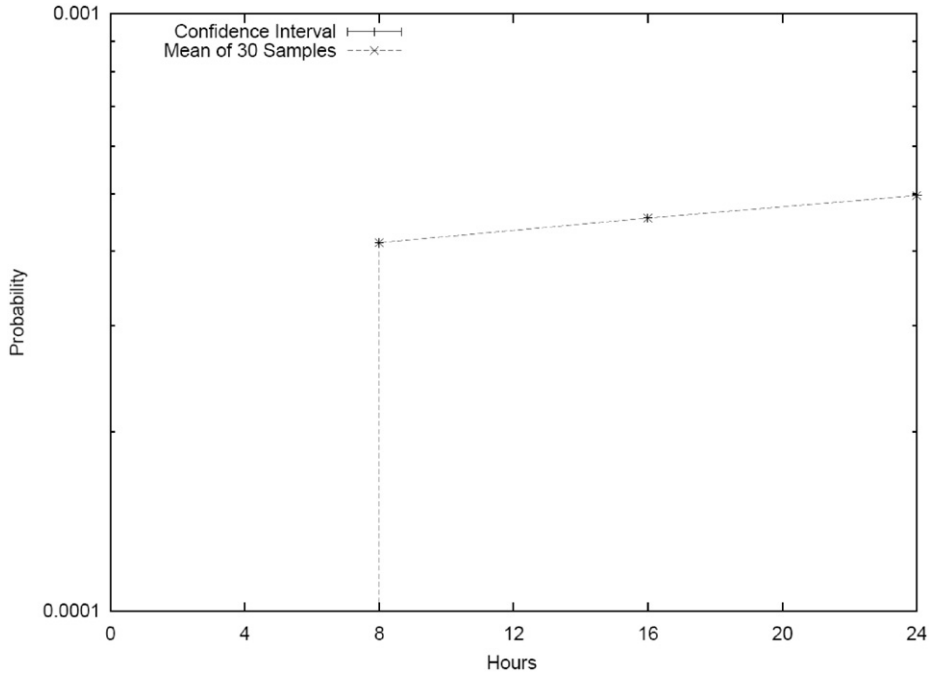


Fig. 23. Low failure arbitrary output confidence interval.

Table 31
Probability data from 30 samples.

	Low Level	High Level
Mean	4.96E−04	7.46E−04
Max	4.97E−04	7.47E−04
Min	4.95E−04	7.46E−04
Std Dev	2.77E−19	7.52E−19

Markov/CCMT analyses started from steady-state operation at 70% power and covered all the three 8 h periods shown in Fig. 1.

Tables 39 and 40 summarize the results. The tables show that:

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

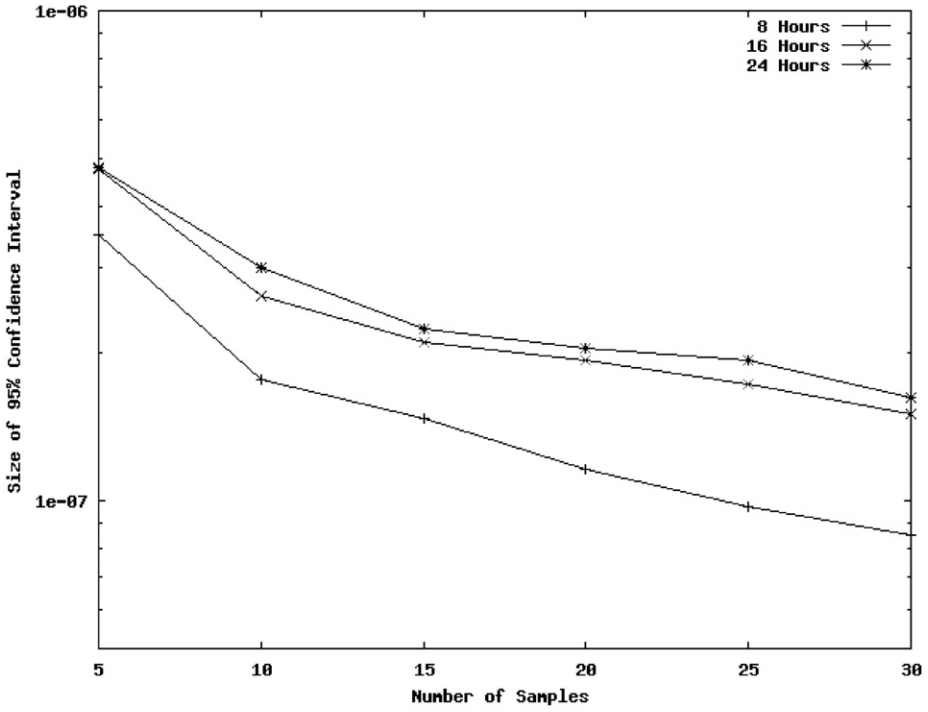


Fig. 24. Size of the 95% confidence interval for low failure.

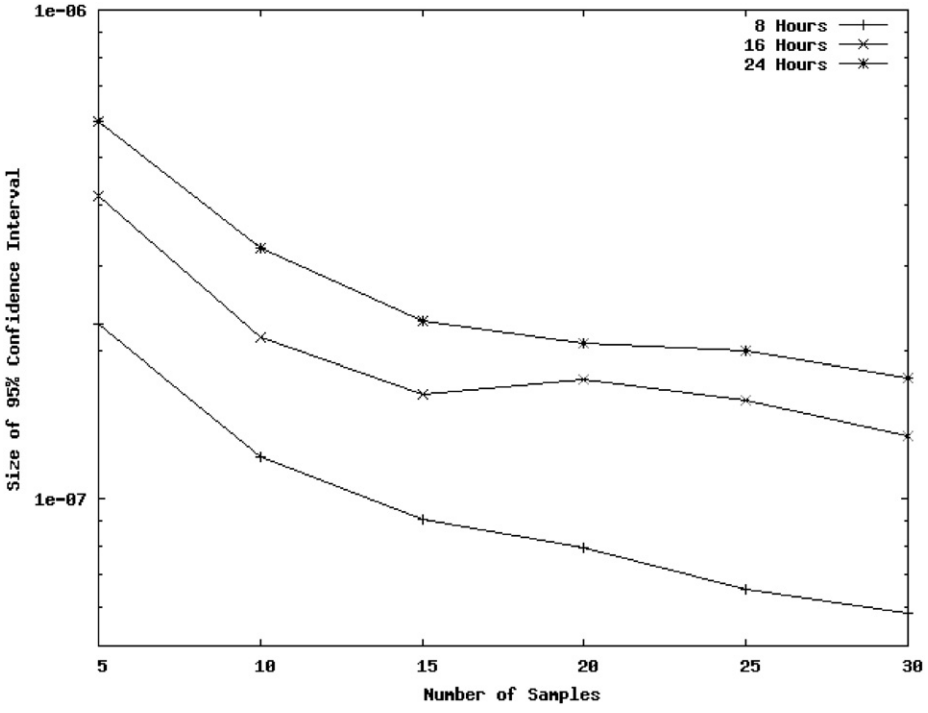


Fig. 25. Size of the 95% confidence interval for high failure.

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. 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. One finding of the comparative evaluation of results points out at how the dynamic representation capabilities of the two methodologies can uncover risk sequence features that cannot be uncovered by the execution of conventional binary/static logic analysis

Table 32
Sequence information from stochastic sampling.

Number of occurrences	Low failure		High failure	
	Number of sequences	Mean probability	Number of sequences	Mean probability
30	2626	4.96E−04	3542	7.45E−04
29	211	3.36E−10	90	2.02E−12
28	120	7.40E−10	13	1.0E−17[a]
27	87	3.24E−13	62	5.99E−11
26	104	5.84E−13	77	5.68E−13
25	196	1.51E−14	66	2.44E−13
24	193	2.45E−10	119	7.31E−10
23	224	2.56E−11	118	2.59E−11
22	95	1.24E−14	128	9.44E−15
21	152	7.59E−14	59	8.33E−15
20	118	3.32E−14	170	3.63E−07
19	121	3.30E−13	57	3.81E−13
18	219	7.77E−16	87	8.24E−13
17	100	2.22E−16	106	1.11E−10
16	76	3.11E−15	147	1.02E−10
15	74	2.32E−10	77	2.44E−17
14	139	2.24E−11	112	2.15E−13
13	70	4.20E−14	132	3.33E−16
12	192	1.37E−13	243	5.55E−16
11	136	5.66E−14	101	1.0E−16[a]
10	195	1.36E−13	128	2.090E−14
9	114	3.23E−14	141	8.730E−11
8	191	1.11E−16	116	3.74E−13
7	172	2.390E−14	201	1.30E−14
6	110	1.95E−14	181	2.70E−13
5	59	1.89E−15	204	6.78E−11
4	202	1.44E−15	214	1.64E−07
3	419	1.0E−18*	148	8.69E−08
2	449	1.0E−18*	222	2.53E−14
1	576	1.0E−17*	482	5.90E−13
Unique sequences	**7740**	**–**	**7543**	**–**
Total	**142763**	**4.963E−04**	**152070**	**7.460E−04**

[a] Approximation, the probability is too low for SAPHIRE to calculate.

Table 33
Low level failure scenarios from stochastic sampling.

Sequence number	Sequence probability	% Total probability	Number of occurrences	Sequence		Order
				Component	State	
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	Stuck	1
				FP	Stuck	2
10	1.11E−07	0.02	30	MFV	Stuck	1
				BFV	Stuck	2

techniques. This concerns the combined deductive/inductive analysis of the Comp Freeze scenario in the ramp-up portion of the power transient, which, under perfectly nominal initial conditions of the system (i.e., with all process variables exactly at set-point levels) is determined by the DFM and Markov/CCMT inductive analyses to result in a SG Low Level outcome. This finding was also already in the results of an earlier completed deductive DFM analysis, where the Comp Freeze basic event is in fact found to be among the prime implicants for the SG Low Level Top Event, under the condition of a power ramp-up maneuver. The finding is easy to understand intuitively, as a computer/software freeze condition would also result in a "freeze" of the feedwater flow injected into the steam generators, which, in the presence of an increased level of thermal power being transferred from the primary circuit, would result in a negative imbalance between the feedwater inflow and the steam outflow and ultimately in a low SG level, if no other corrective action were meanwhile applied. However, a further inductive analysis conducted in sensitivity analysis mode assuming that the freeze condition occurred when the feedwater flow was at the upper limit of its $\pm 10\%$ nominal control range, revealed that this particular variation of the scenario, in which the actual fault was accompanied by a different type of nominal condition than the "perfectly nominal" one mentioned above, would produce the opposite system outcome of "SG High Level" plant trip condition. This could also be intuitively understood, since the control system

Table 34
High level failure scenarios from stochastic sampling.

Sequence number	Sequence probability	% Total probability	Number of occurrences	Sequence		Order
				Component	State	
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

Table 35
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 36
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

Table 37
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

would be frozen into pumping a steady 10% excess of feedwater while the power was being ramped up at the relatively slow rate of 1% per hour, so that for practically the entire duration of the ramp-up the net effect would be now a positive imbalance between feedwater inflow and steam outflow.

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, and also confirm that the dynamic analysis techniques can provide system risk scenario insights that go beyond what provided by the execution of traditional binary event-tree/fault-tree analyses. Event sequences from both DFM and Markov/CCMT results can, however, be imported into an existing PRA based on the traditional event-tree/fault-tree methodology by representing them as dynamic event trees, [16,20], or as cut-set contributors to a conventional fault-tree.

Table 38
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

Table 39
Comparison of low SG level results.

Method	**DFM**	**Markov/ CCMT**
Probability (8 h ramp-up only)	4.19E−04	4.15E−04
Highest Contributor	Main feed valve stuck	Main feed valve stuck
2nd Contributor	Computer and Controller Power	Computer Power
Time of Basic Failure Event Covered by Analysis	8 h ramp-up period	Full 24 h interval
Time interval for Top Event to occur	8 h ramp up (70–78%), or 8 h steady state (78%)	Full 24 h interval

5. Conclusion

This study investigates the suitability of two dynamic methodologies to represent and analyze risk relevant failure modes of modern NPP digital I&C systems, and the resulting event sequence scenarios, using as their test-bed a DFWCS similar in general characteristics to that of an operating nuclear power plant. The study illustrates the capability of dynamic PRA methodologies such as DFM and Markov/CCMT to capture key aspects of dynamic control system behavior, including dynamic

Table 40
Comparison of high SG level results.

	DFM baseline analysis	DFM extended analysis	Markov/CCMT
Probability (8 h 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 and high) pos)	Main feed valve controller (arbitrary pos and high) pos)	Comp Freeze
Time of Basic Failure Event covered by analysis	8 h ramp down (78–70%)	8 hour steady state (78%) or 8 h ramp down (78–70%)	Full 24 h interval
Time interval for Top Event to occur	8 hour ramp down (78–70%) or 8 h steady state (70%)	8 h steady state (78%), 8 h ramp down (78–70%), or final steady state (70%)	Full 24 h interval

interactions and resulting effect that traditional PRA binary logic models cannot represent, unless such models are expressing in binary synthesis more detailed and complex results obtained via the application of other supplementing techniques, such as continuous-time or discrete-time full system simulation.

The findings of the study can be summarized as follows:

1. The deductive analyses carried out with DFM appear to be well suited to span the search space for the prime-implicants of a given DFWCS failure mode in logically complete fashion.[2]
2. The application of the DFM and Markov/CCMT has resulted in the identification of potentially risk-relevant event sequences specifically associated with the assumed DFWCS failure modes.
3. The study shows that different initial conditions and sequencing of events can cause the DFWCS system to fail in different modes, which may have different safety implications (refer for example to the case discussed at the end of Section 4). The study also shows that the failure probabilities associated with these modes can be significantly different.
4. The inductive Markov/CCMT analyses can track dynamic scenarios by identifying ranges of variations of associated time-dependent sequences of events, with associated probabilities, and may be effective for:
   4.1. Validating the correctness of the results obtained from deductive DFM analyses.
   4.2. Performing sensitivity analyses starting from the baseline failure conditions identified by the prime implicant results of a DFM deductive analysis.
5. Dynamic methods such as DFM and Markov/CCMT provide qualitative results in the form of prime implicants that are the timed multi-valued logic equivalent of binary cut sets. The information contained in dynamic prime-implicants (e.g., the relative timing of failure events resulting in a given type of system failure) cannot be directly obtained with static binary logic methods, but is presented in a format that is compatible with the format of traditional PRA cut-set information and combined with the latter in seamless fashion.
6. Failure probability and failure rate estimations of digital I&C components, if available, can be utilized in both DFM and Markov/CCMT models to generate quantitative risk estimations at a level of detail and depth comparable with the standards of practice encountered in traditional PRA.
7. Both DFM and Markov/CCMT analyses can be used to identify and rank-order event sequences with respect to their contribution to different assumed DFWCS failure modes, as well as to identify and rank-order the corresponding contribution of individual basic events related to these sequences.

It should be mentioned, however, that this demonstration has not covered all aspects of digital I&C risk that may be significant. The most important reasons why the study quantitative results should be presently considered to represent only first-cut demonstrative values, and not real indicators of the possible risk impact of control system digital upgrades on a typical NPP, are the following:

1. The possibility of logic design errors, especially with respect to the design of any complex software that governs a digital I&C was, by definition of project scope, left unexplored in the analyses carried out for the DFWCS benchmark.
2. 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.
3. 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 initiating conditions in traditional PRA scenarios, using the values obtained in this study from the analysis of the power maneuver transients as extrapolated proxies for High and Low SG level plant-trip probabilities for generic plant conditions. No claim is made concerning the validity of this extrapolation across the range of possibilities, as the probability of the trip-events quantified via the study demonstrative results may depend on the plant regime at the time that underlying 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, and then conduct dynamic analyses like those executed in this study to cover the basic regimes of potential interest and finally use some appropriate averaging of probabilities, e.g., using as relative weights the fractions of time that the plant would be in a specific regime versus another, 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.
4. 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, software

[2] 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/cannot identify.

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.

Acknowledgment

The research presented in this paper was sponsored by the U.S. Nuclear Regulatory Commission (US NRC). The information and conclusions presented here in are those of the authors and do not necessary represent the views or positions of the US NRC. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assume any legal liability or responsibility for any third party's use of this information.

Appendix A. Auxiliary Markov models

The purpose of this appendix is to show how auxiliary Markov models can be generated from the original Markov transition diagrams presented in Section 3.2 to reduce state space. The main idea is to merge states that have similar impacts on the dynamics of the overall system and, hence, the states that generate the same output. Note that transitions between states of the auxiliary Markov transition diagram must reflect those pictured in the original transition diagram. It has been possible to determine the new transition rates by simply using the well known Bayes and conditional probability relations.

Sections A.1–A.3 present how it is possible to perform this state reduction procedure for the set of computers (MC and BC), the MFV, BFV, FP controllers and the PDI controller.

A.1. Computer auxiliary Markov models.

The starting point is Fig. 14 which represents the Markov transition diagram for the set of computers. If we consider the states that generate the same output, we can identify the following three new states for the computer auxiliary Markov transition diagram (see Fig. 18):

1. *Correct output*: the computers send to the controllers the correct value of flow demand. This state includes State 1, 3, and 5 of Fig. 14.
2. *Previous output*: the computers send to the controllers the oldest valid value of flow demand. This state includes State 7 of Fig. 14.
3. *Arbitrary output*: the computers send to the controllers an arbitrary generated value of flow demand. This state includes State 2, 4, and 6 of Fig. 14.

From the original Markov transition diagram shown in Fig. 14 the following relationships are observed:

$$\frac{dP_1^{comp}(t)}{dt} = -\lambda_{12}^{comp}P_1^{comp}(t)-\lambda_{13}^{comp}P_1^{comp}(t)-\lambda_{14}^{comp}P_1^{comp}(t) -\lambda_{15}^{comp}P_1^{comp}(t)-\lambda_{16}^{comp}P_1^{comp}(t)-\lambda_{MS1-7}^{comp}P_1^{comp}(t) \quad (A.1)$$

$$\frac{dP_2^{comp}(t)}{dt} = -\lambda_{23}^{comp}P_2^{comp}(t)-\lambda_{24}^{comp}P_2^{comp}(t)-\lambda_{25}^{comp}P_2^{comp}(t) -\lambda_{26}^{comp}P_2^{comp}(t)-\lambda_{MS1-7}^{comp}P_2^{comp}(t)+\lambda_{12}^{comp}P_1^{comp}(t), \quad (A.2)$$

$$\frac{dP_3^{comp}(t)}{dt} = -\lambda_{34}^{comp}P_3^{comp}(t)-\lambda_{MS2-7}^{comp}P_3^{comp}(t)+\lambda_{13}^{comp}P_1^{comp}+\lambda_{23}^{comp}P_2^{comp}(t), \quad (A.3)$$

$$\frac{dP_4^{comp}(t)}{dt} = -\lambda_{MS2-7}^{comp}P_4^{comp}(t)+\lambda_{14}^{comp}P_1(t)+\lambda_{24}^{comp}P_2^{comp}(t)+\lambda_{34}^{comp}P_3^{comp}(t)), \quad (A.4)$$

$$\frac{dP_5^{comp}(t)}{dt} = -\lambda_{56}^{comp}P_5^{comp}(t)-\lambda_{MS3-7}^{comp}P_5^{comp}(t)+\lambda_{15}^{comp}P_1^{comp}(t)+\lambda_{25}^{comp}P_2^{comp}(t), \quad (A.5)$$

$$\frac{dP_6^{comp}(t)}{dt} = -\lambda_{MS3-7}^{comp}P_6^{comp}(t)+\lambda_{16}^{comp}P_1^{comp}(t)+\lambda_{26}^{comp}P_2^{comp}(t)+\lambda_{56}^{comp}P_5^{comp}(t), \quad (A.6)$$

$$\frac{dP_7^{comp}(t)}{dt} = \lambda_{MS1-7}^{comp}P_1^{comp}(t)+\lambda_{MS1-7}^{comp}P_2^{comp}(t)+\lambda_{MS2-7}^{comp}P_3^{comp}(t) +\lambda_{MS2-7}^{comp}P_4^{comp}(t)+\lambda_{MS3-7}^{comp}P_5^{comp}(t)+\lambda_{MS3-7}^{comp}P_6^{comp}(t). \quad (A.7)$$

In Eqs. (A.1)–(A.7), $P_i^{comp}(t)$ indicates the probability of State i of the Markov transition diagram shown in Fig. 14 at time t. As indicated in Section 3.2, the Freeze state in Fig. 14 represents the Down state of the computers (see Figs. 4 and 5 for this correspondence). Fig. 14 also assumes that the transition rates out of the two constituent states of MS1, MS2, and MS3 to State 7 are the same for each of the pairs (i.e. λ_{MS2-7}^{comp} for each of the States 2 and 4, λ_{MS1-7}^{comp} for each of the State 1 and 1, and λ_{MS3-7}^{comp} for each State 5 and 6).

Solution of the system of Eqs. (A.1)–(A.7) with data from Table 1 yields:

$$P_1^{comp}(t) = e^{-5.55368\times10^{-9}t}e^{-5.55368\times10^{-9}t}(e^{4.12869\times10^{-9}t} -6.0315\times10^{-14}e^{4.12949\times10^{-9}t}-2.19434 \times10^{-17}e^{4.20103\times10^{-9}t}+1.42254\times10^{-15}e^{4.20184\times10^{-9}t} -5.46703\times10^{-30}e^{5.55368\times10^{-9}t},. \quad (A.8)$$

$$P_2^{comp}(t) = e^{-5.55368\times10^{-9}t}(-e^{4.12869\times10^{-9}t}+e^{4.12949\times10^{-9}t} +1.04518\times10^{-17}e^{4.20103\times10^{-9}t} -1.2081\times10^{-19}e^{4.20184\times10^{-9}t}+9.33776 \times10^{-17}e^{5.55368\times10^{-9}t}), \quad (A.9)$$

$$P_3^{comp}(t) = e^{-5.55368\times10^{-9}t}(-7.95154\times10^{-14}e^{4.12869\times10^{-9}t} -0.165573e^{4.12949\times10^{-9}t}+0.165573e^{4.20103\times10^{-9}t} +7.95454\times10^{-16}e^{4.20184\times10^{-9}t} -1.76583\times10^{-17}e^{5.55368\times10^{-9}t}), \quad (A.10)$$

$$P_4^{comp}(t) = e^{-5.55368\times10^{-9}t}(-7.91\times10^{-14}e^{4.12869\times10^{-9}t} -0.162e^{4.12949\times10^{-9}t}-0.165573e^{4.20103\times10^{-9}t} +0.327463e^{4.20184\times10^{-9}t}-2.56181\times10^{-18}e^{5.55368\times10^{-9}t}), \quad (A.11)$$

$$P_5^{comp}(t) = e^{-5.55368\times10^{-9}t}(-2.03035\times10^{-13}e^{4.12869\times10^{-9}t} -0.422838e^{4.12949\times10^{-9}t}+0.422838e^{4.20103\times10^{-9}t} +3.36192\times10^{-15}e^{4.20184\times10^{-9}t} -2.73152\times10^{-17}e^{5.55368\times10^{-9}t}), \quad (A.12)$$

$$P_6^{comp}(t) = e^{-5.55368\times10^{-9}t}(-2.0189\times10^{-13}e^{4.12869\times10^{-9}t} -0.413e^{4.12949\times10^{-9}t}-0.423e^{4.20103\times10^{-9}t} +0.836e^{4.20184\times10^{-9}t}+5.48\times10^{-17}e^{5.55368\times10^{-9}t}), \quad (A.13)$$

$$P_7^{comp}(t) = e^{-5.55368\times10^{-9}t}(8.00432\times10^{-14}e^{4.12869\times10^{-9}t} +0.163731e^{4.12949\times10^{-9}t} +1.144\times10^{-13}e^{4.20103\times10^{-9}t}-1.16e^{4.20184\times10^{-9}t} +e^{5.55368\times10^{-9}t}). \quad (A.14)$$

The state probabilities of the auxiliary model Markov transition diagram in Fig. 18 can be determined by observing that

$$\overline{P}_1^{comp}(t) = P_1^{comp}(t)+P_3^{comp}(t)+P_5^{comp}(t), \quad (A.15)$$

$$\overline{P}_2^{comp}(t) = P_7^{comp}(t), \quad (A.16)$$

$$\overline{P}_3^{comp}(t) = P_2^{comp}(t)+P_4^{comp}(t)+P_6^{comp}(t), \quad (A.17)$$

where $\overline{P}_i^{comp}(t)$ indicates the probability of the state i of the auxiliary Markov transition diagram shown in Fig. 18 at time t.

The transitions rates for the auxiliary Markov models states can be found from the relations:

$$\overline{\lambda}_{12}^{comp}(t) = \frac{\lambda_{MS1-7}^{comp}P_1^{comp}(t)+\lambda_{MS2-7}^{comp}P_3^{comp}(t)+\lambda_{MS3-7}^{comp}P_5^{comp}(t)}{P_1^{comp}(t)+P_3^{comp}(t)+P_5^{comp}(t)}$$
$$= (1.34\times10^{-9}e^{4.12869\times10^{-9}t}-7.95441\times10^{-10}e^{4.12949\times10^{-9}t} +7.95441\times10^{-10}e^{4.20103\times10^{-9}t} +7.52634\times10^{-24}e^{4.20184\times10^{-9}t} -6.07971\times10^{-26}e^{5.55368\times10^{-9}t})/(e^{4.12869\times10^{-9}t} -0.588412e^{4.12949\times10^{-9}t}+0.588412e^{4.20103\times10^{-9}t} +5.57992\times10^{-15}e^{4.20184\times10^{-9}t}-4.49734\times10^{-17}), \quad (A.18)$$

$$\overline{\lambda}_{13}^{comp}(t) = \frac{(\lambda_{12}^{comp}+\lambda_{14}^{comp}+\lambda_{16}^{comp})P_1^{comp}(t)+\lambda_{34}^{comp}P_3^{comp}(t)+\lambda_{56}^{comp}P_5^{comp}(t)}{P_1^{comp}(t)+P_3^{comp}(t)+P_5^{comp}(t)}$$
$$= (4.29\times10^{-11}e^{4.12869\times10^{-9}t}-4.73573\times10^{-13}e^{4.12949\times10^{-9}t} +4.73573\times10^{-13}e^{4.20103\times10^{-9}t}+6.4373\times10^{-26}e^{4.20184\times10^{-9}t} -3.61961\times10^{-29}e^{5.55368\times10^{-9}t})/(e^{4.12869\times10^{-9}t} -0.588412e^{4.12949\times10^{-9}t}+0.588412e^{4.20103\times10^{-9}t} +5.57992\times10^{-15}e^{4.20184\times10^{-9}t}-4.49734 \times10^{-17}e^{5.55368\times10^{-9}t}), \quad (A.19)$$

$$\overline{\lambda}_{32}^{comp}(t) = \frac{\lambda_{MS1-7}^{comp}P_2^{comp}(t)+\lambda_{MS2-7}^{comp}P_4^{comp}(t)+\lambda_{MS3-7}^{comp}P_6^{comp}(t)}{P_2^{comp}(t)+P_4^{comp}(t)+P_6^{comp}(t)}$$
$$= (1.34\times10^{-9}e^{4.12869\times10^{-9}t}-5.62257\times10^{-10}e^{4.12949\times10^{-9}t} +7.95441\times10^{-10}e^{4.20103\times10^{-9}t}-1.57318 \times10^{-9}e^{4.20184\times10^{-9}t}-1.95775 \times10^{-25}e^{5.55368\times10^{-9}t})/(e^{4.12869\times10^{-9}t}-0.42468e^{4.12949\times10^{-9}t} +0.588412e^{4.20103\times10^{-9}t}-1.16373e^{4.20184\times10^{-9}t}-1.45639 \times10^{-16}e^{5.55368\times10^{-9}t}), \quad (A.20)$$

$$\overline{\lambda}_{32}^{comp}(t) = \frac{\lambda_{23}P_2^{comp}(t)+\lambda_{25}P_2^{comp}(t)}{P_2^{comp}(t)+P_4^{comp}(t)+P_6^{comp}(t)}$$
$$= (4.20952\times10^{-11}e^{4.12869\times10^{-9}t}-4.20952 \times10^{-11}e^{4.12949\times10^{-9}t}-4.39971\times10^{-28}e^{4.20103\times10^{-9}t} +5.08554\times10^{-30}e^{4.20184\times10^{-9}t}-3.93074\times10^{-27} \times e^{5.55368\times10^{-9}t})/(e^{4.12869\times10^{-9}t}-0.42468e^{4.12949\times10^{-9}t} +0.588412e^{4.20103\times10^{-9}t}-1.16373e^{4.20184\times10^{-9}t}-1.45639 \times10^{-16}e^{5.55368\times10^{-9}t}). \quad (A.21)$$

A.2. MFV, BFV, FP controller auxiliary Markov models

The starting point for is Fig. 15 which represents the Markov transition diagram for the BFV controller. The transition diagrams for the MFV and FP controllers are similar.

From Fig. 15, it is possible to write the following equations for this Markov transition diagram:

$$\frac{dP_1^{BFV}(t)}{dt} = -\lambda_{12}^{BFV}P_1^{BFV}(t)-\lambda_{14}^{BFV}P_1^{BFV}(t)-\lambda_{15}^{BFV}P_1^{BFV}(t) -\lambda_{16}^{BFV}P_1^{BFV}(t)-\lambda_{18}^{BFV}P_1^{BFV}(t), \quad (A.22)$$

$$\frac{dP_2^{BFV}(t)}{dt} = -\lambda_{27}^{BFV}P_2^{BFV}(t)-\lambda_{28}^{BFV}P_2^{BFV}(t)+\lambda_{12}^{BFV}P_1^{BFV}(t), \quad (A.23)$$

$$\frac{dP_4^{BFV}(t)}{dt} = -\lambda_{47}^{BFV}P_4^{BFV}(t)-\lambda_{48}^{BFV}P_4^{BFV}(t)+\lambda_{14}^{BFV}P_1^{BFV}(t), \quad (A.24)$$

$$\frac{dP_5^{BFV}(t)}{dt} = -\lambda_{57}^{BFV}P_5^{BFV}(t)-\lambda_{58}^{BFV}P_5^{BFV}(t)+\lambda_{15}^{BFV}P_1^{BFV}(t), \quad (A.25)$$

$$\frac{dP_6^{BFV}(t)}{dt} = -\lambda_{67}^{BFV}P_6^{BFV}(t)-\lambda_{68}^{BFV}P_6^{BFV}(t)+\lambda_{16}^{BFV}P_1^{BFV}(t), \quad (A.26)$$

$$\frac{dP_7^{BFV}(t)}{dt} = -\lambda_{78}^{BFV}P_7^{BFV}(t)+\lambda_{27}^{BFV}P_2^{BFV}(t)+\lambda_{47}^{BFV}P_4^{BFV}(t) +\lambda_{57}^{BFV}P_5^{BFV}(t)+\lambda_{67}^{BFV}P_6^{BFV}(t), \quad (A.27)$$

$$\frac{dP_8^{BFV}}{dt} = \lambda_{18}^{BFV}P_1^{BFV}(t)+\lambda_{28}^{BFV}P_2^{BFV}(t)+\lambda_{48}^{BFV}P_4^{BFV}(t)+\lambda_{58}^{BFV}P_5^{BFV}(t) +\lambda_{68}^{BFV}P_6^{BFV}(t)+\lambda_{78}^{BFV}P_7^{BFV}(t). \quad (A.28)$$

Note that here $P_i^{BFV}(t)$ indicates the probability of the ith state of the Markov transition diagram shown in Fig. 15 at time t.

By solving the system of equations (A.22)–(A.28) it is possible to get

$$P_1^{BFV}(t) = e^{-3.47858\times10^{-8}t}(e^{2.31552\times10^{-8}t}-1.09716e^{2.32006\times10^{-8}t} -3.01431\times10^{-15}e^{2.32158\times10^{-8}t} -7.87262\times10^{-31}e^{3.47858\times10^{-8}t}), \quad (A.29)$$

$$P_2^{BFV}(t) = e^{-3.47858\times10^{-8}t}(-0.333333e^{2.31552\times10^{-8}t}+0.333333e^{2.32006\times10^{-8}t} -1.61713\times10^{-14}e^{2.32158\times10^{-8}t}+2.23617\times10^{-17}e^{3.47858\times10^{-8}t}), \quad (A.30)$$

$$P_4^{BFV}(t) = e^{-3.47858\times10^{-8}t}(-0.333333e^{2.31552\times10^{-8}t} +0.333333e^{2.32006\times10^{-8}t}-1.63932 \times10^{-14}e^{2.32158\times10^{-8}t}+1.89993\times10^{-17}e^{3.47858\times10^{-8}t}), \quad (A.31)$$

$$P_5^{BFV}(t) = e^{-3.47858\times10^{-8}t}(-0.333333e^{2.31552\times10^{-8}t} +0.333333e^{2.32006\times10^{-8}t}-1.62341 \times10^{-14}e^{2.32158\times10^{-8}t}+1.88127\times10^{-17}\times e^{3.47858\times10^{-8}t}), \quad (A.32)$$

$$P_6^{BFV}(t) = e^{-3.47858\times10^{-8}t}(-0.333333e^{2.31552\times10^{-8}t} + 0.333333e^{2.32006\times10^{-8}t} - 1.62301 \times10^{-14}e^{2.32158\times10^{-8}t} + 1.88115\times10^{-17}e^{3.47858\times10^{-8}t}), \quad (A.33)$$

$$P_7^{BFV}(t) = e^{-3.47858\times10^{-8}t}(0.333333e^{2.31552\times10^{-8}t} - 1.33333e^{2.32006\times10^{-8}t} + e^{2.32158\times10^{-8}t} - 3.34393 \times10^{-17}e^{3.47858\times10^{-8}t}), \quad (A.34)$$

$$P_8^{BFV}(t) = e^{-3.47858\times10^{-8}t}(-2.82722\times10^{-14}e^{2.31552\times10^{-8}t} - 1.44958 \times10^{-13}e^{2.32006\times10^{-8}t} - e^{2.32158\times10^{-8}t} + e^{3.47858\times10^{-8}t}). \quad (A.35)$$

If we consider the states that generate the same output in Fig. 15, we can identify the following five new states for the controller auxiliary Markov transition diagram (see Fig. 19):

1. *Correct Output*: the controller sends to its own actuated device the correct output generated by the set of computers. This state includes State 1 of Fig. 15.
2. *Output Low*: the controller sends to its own actuated device the lowest possible output. This state includes States 2, 5, and 7 of Fig. 15.
3. *Previous Output*: the controller sends to its own actuated device the previous valid output. This state includes State 8 of Fig. 15.
4. *Output High*: the controller sends to its own actuated device the highest possible output. This state includes State 4 of Fig. 15.
5. *Arbitrary Output*: the controller sends to its own actuated device a random generated output. This state includes State 6 of Fig. 15.

Then it is possible to determine the state probabilities of the auxiliary Markov transition diagram $\overline{P}_i^{BFV}(t)$ simply by observing that

$$\overline{P}_1^{BFV}(t) = P_1^{BFV}(t), \quad (A.36)$$

$$\overline{P}_2^{BFV}(t) = P_2^{BFV}(t) + P_5^{BFV}(t) + P_7^{BFV}(t), \quad (A.37)$$

$$\overline{P}_3^{BFV}(t) = P_8^{BFV}(t), \quad (A.38)$$

$$\overline{P}_4^{BFV}(t) = P_4^{BFV}(t), \quad (A.39)$$

$$\overline{P}_5^{BFV}(t) = P_6^{BFV}(t). \quad (A.40)$$

In Eq.(A.36)–(A.40), $\overline{P}_i^{BFV}(t)$ indicates the probability for the state i of the auxiliary Markov transition diagram shown in Fig. 19 at time t. Hence, it is possible to determine the transitions rates between the auxiliary Markov models states as the following:

$$\overline{\lambda}_{12}^{BFV} = \frac{\lambda_{12}^{BFV}P_1^{BFV}(t) + \lambda_{15}^{BFV}P_1^{BFV}(t)}{P_1^{BFV}(t) + P_1^{BFV}(t)} = 25.5\times10^{-8}/h, \quad (A.41)$$

$$\overline{\lambda}_{23}^{BFV} = \frac{\lambda_{28}^{BFV}P_2^{BFV}(t) + \lambda_{58}^{BFV}P_5^{BFV}(t) + \lambda_{78}^{BFV}P_7^{BFV}(t)}{P_2^{BFV}(t) + P_5^{BFV}(t) + P_7^{BFV}(t)} = (3.8566\times10^{-9}e^{2.31552\times10^{-10}t} + 7.71333\times10^{-9}e^{2.32006\times10^{-8}t} - 1.157\times10^{-8}e^{2.32158\times10^{-8}t} - 8.94953 \times10^{-26}e^{3.47858\times10^{-8}t})/(0.333333e^{2.31552\times10^{-10}t} + 0.666667e^{2.32006\times10^{-8}t} - e^{2.32158\times10^{-8}t} - 7.73511 \times10^{-18}e^{3.47858\times10^{-8}t}). \quad (A.42)$$

The remaining transition rate values are identical to the one presented for the original Markov model for the MFV, BFV, and FP controller:

$$\overline{\lambda}_{13}^{BFV} = \lambda_{18}^{BFV} = 4.2\times10^{-5}/h, \quad (A.43)$$

$$\overline{\lambda}_{14}^{BFV} = \lambda_{14}^{BFV} = 5.5\times10^{-8}/h, \quad (A.44)$$

$$\overline{\lambda}_{15}^{BFV} = \lambda_{16}^{BFV} = 5.5\times10^{-8}/h, \quad (A.45)$$

$$\overline{\lambda}_{43}^{BFV} = \lambda_{48}^{BFV} = 4.2\times10^{-5}/h, \quad (A.46)$$

$$\overline{\lambda}_{53}^{BFV} = \lambda_{68}^{BFV} = 4.2\times10^{-5}/\mathrm{h}. \quad (A.47)$$

A.3. PDI controller auxiliary Markov models

The starting point is Fig. 16 which represents the Markov transition diagram for the PDI controller. If we consider the states that generate the same output we can identify the following five new states for the controller auxiliary Markov transition diagram (see Fig. 21):

1. *Correct Output*: the controller sends to its own actuated device the correct output generated by the set of computers. This state includes State 1 of Fig. 16.
2. *Previous Output*: the controller sends to its own actuated device the previous valid output. This state includes State 2 of Fig. 16.
3. *Arbitrary Output*: the controller sends to its own actuated device a random generated output. This state includes State 3 of Fig. 16.
4. *Output Low*: the controller sends to its own actuated device the lowest possible output. This state includes States 4, 5, and 6 of Fig. 16.

From the original Markov transition diagram shown in Fig. 16 we have

$$\frac{dP_1^{PDI}(t)}{dt} = -\lambda_{12}^{PDI}P_1^{PDI}(t) - \lambda_{13}^{PDI}P_1^{PDI}(t) - \lambda_{14}^{PDI}P_1^{PDI}(t), \quad (A.48)$$

$$\frac{dP_2^{PDI}(t)}{dt} = -\lambda_{23}^{PDI}P_2^{PDI}(t) - \lambda_{25}^{PDI}P_2^{PDI}(t) + \lambda_{12}^{PDI}P_1^{PDI}(t), \quad (A.49)$$

$$\frac{dP_3^{PDI}(t)}{dt} = -\lambda_{36}^{PDI}P_3^{PDI}(t) + \lambda_{13}^{PDI}P_1^{PDI}(t) + \lambda_{23}^{PDI}P_2^{PDI}(t) \quad (A.50)$$

$$\frac{dP_4^{PDI}(t)}{dt} = -\lambda_{45}^{PDI}P_4^{PDI}(t) - \lambda_{46}^{PDI}P_4^{PDI}(t) + \lambda_{14}^{PDI}P_1^{PDI}(t), \quad (A.51)$$

$$\frac{dP_5^{PDI}(t)}{dt} = -\lambda_{56}^{PDI}P_6^{PDI}(t) + \lambda_{25}^{PDI}P_2^{PDI}(t) + \lambda_{45}^{PDI}P_4^{PDI}(t), \quad (A.52)$$

$$\frac{dP_6^{PDI}(t)}{dt} = \lambda_{36}^{PDI}P_3^{PDI}(t) + \lambda_{46}^{PDI}P_4^{PDI}(t) + \lambda_{56}^{PDI}P_6^{PDI}(t). \quad (A.53)$$

In the system of Eqs. (A.48)–(A.53), $P_i^{PDI}(t)$ indicates the probability of the ith state of the Markov transition diagram shown in Fig. 16 at time t.

By solving the system of equations (A.48)–(A.53), we get

$$P_1^{PDI}(t) = e^{-1.8192\times10^{-10}t}(2.71948 \times10^{-16}e^{9.096\times10^{-11}t} + e^{1.2128\times10^{-10}t} - 2e^{1.1516\times10^{-10}t} + e^{1.8192\times10^{-10}t}), \quad (A.54)$$

$$P_2^{PDI}(t) = e^{-1.8192\times10^{-10}t}(-e^{9.096\times10^{-11}t} + e^{1.2128\times10^{-10}t} - 3.62313 \times10^{-16}1e^{1.1516\times10^{-10}t} + 2.37831\times10^{-16}e^{1.8192\times10^{-10}t}), \quad (A.55)$$

$$P_3^{PDI}(t) = e^{-1.8192\times10^{-10}t}(-6.66134 \times10^{-16}e^{9.096\times10^{-11}t} - e^{1.2128\times10^{-10}t} + e^{1.1516\times10^{-10t}} - 1.35692 \times10^{-16}e^{1.8192\times10^{-10t}}), \quad (A.56)$$

$$P_4^{PDI}(t) = e^{-1.8192\times10^{-10}t}(-e^{9.096\times10^{-11}t} + e^{1.2128\times10^{-10}t} - 1.1437\times10^{-16}e^{1.1516\times10^{-10}t} + 7.5437\times10^{-17}e^{1.8192\times10^{-10}t}), \quad (A.57)$$

$$P_5^{PDI}(t) = e^{-1.8192\times10^{-10}t}(e^{9.096\times10^{-11}t} - 2e^{1.2128\times10^{-10}t} + e^{1.1516\times10^{-10}t} - 2.25378\times10^{-16}e^{1.8192\times10^{-10}t}), \quad (A.58)$$

$$P_6^{PDI}(t) = e^{-1.8192\times10^{-10}t}(1.63169\times10^{-15}e^{9.096\times10^{-11}t} + e^{1.2128\times10^{-10}t} - 2e^{1.1516\times10^{-10}t} + e^{1.8192\times10^{-10}t}). \quad (A.59)$$

The state probabilities for the auxiliary Markov transition diagrams are obtained by observing that

$$\overline{P}_1^{PDI}(t) = P_1^{PDI}(t), \quad (A.60)$$

$$\overline{P}_2^{PDI}(t) = P_2^{PDI}(t), \quad (A.61)$$

$$\overline{P}_3^{PDI}(t) = P_3^{PDI}(t), \quad (A.62)$$

$$\overline{P}_4^{PDI}(t) = P_4^{PDI}(t) + P_5^{PDI}(t) + P_6^{PDI}(t). \quad (A.63)$$

In Eq.(A.60)–(A.63), $\overline{P}_i^{PDI}(t)$ indicates the probability of the ith state of the auxiliary Markov transition diagram shown in Fig. 19 at time t. Hence, it is possible to determine the transition rates between the auxiliary Markov models states as

$$\overline{\lambda}_{12}^{PDI}(t) = \lambda_{12}^{PDI} = 1.09\times10^{-7}/h, \quad (A.64)$$

$$\overline{\lambda}_{13}^{PDI}(t) = \lambda_{13}^{PDI} = 1.09\times10^{-7}/h, \quad (A.65)$$

$$\overline{\lambda}_{23}^{PDI}(t) = \lambda_{23}^{PDI} = 1.09\times10^{-7}/h, \quad (A.66)$$

$$\overline{\lambda}_{14}^{PDI}(t) = \frac{\lambda_{14}^{PDI}P_1(t)}{P_1(t)} = 1.09\times10^{-7}/h, \quad (A.67)$$

$$\overline{\lambda}_{24}^{PDI}(t) = \frac{\lambda_{24}^{PDI}P_2(t)}{P_2(t)} = 1.09\times10^{-7}/h, \quad (A.68)$$

$$\overline{\lambda}_{34}^{PDI}(t) = \frac{\lambda_{34}^{PDI}P_3(t)}{P_3(t)} = 1.09\times10^{-7}/\mathrm{h}. \quad (A.69)$$

References

[1] U.S. Nuclear Regulatory Commission. Final Policy Statement. Federal Register 1995;60:43622.
[2] Guideline for performing defense-in-depth and diversity assessments for digital I&C upgrades—applying risk-informed and deterministic methods. 1002835. Palo Alto, CA: EPRI; 2004.
[3] Aldemir T, Miller DW, Stovsky M, Kirschenbaum J, Bucci P, Fentiman AW, et al. Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments. Nureg/Cr-6901. Washington, DC: U. S. Nuclear Regulatory Commission; 2006.
[4] Shields EJ, Apostolakis G, Guarro SB. Determining the prime implicants for multi-state embedded systems. In: Apostolakis G, Wu JS, editors. Proceedings of PSAM-II. San Diego, CA: International Association for Probabilistic Assessment and Management; 1994. p. 7–12.
[5] Guarro S, Yau M, Motamed M. Development of tools for safety analysis of control software in advanced reactors. Nureg/Cr-6465. Washington, DC: U.S. Nuclear Regulatory Commission; 1996.
[6] Yau M, Motamed M, Guarro S. Nuclear power plant digital system PRA pilot study with the dynamic flowgraph methodology. Npic&Hmit 2006. La Grange Park, IL: American Nuclear Society; 2006.
[7] C.L. Smith, J. Knudsen, M. Calley, S. Beck, K. Kvarfordt, 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).
[8] CAFTA For Windows, Version 3.0c. Los Altos, CA: SAIC; 1995.
[9] Riskman 7.1 For Windows. Irvine, CA: ABS Consulting; 2003.
[10] S. Dixon, M. Yau, Modeling of dynamic and time-dependent nuclear power plant risk scenarios. EPRI Risk And Reliability User Group Meeting, West Palm Beach, January 12, 2010.
[11] Instruction guide for integration of the context-based software risk model (CSRM) with a Cx probabilistic risk assessment (PRA). ASCA Report AR 09-03. Prepared for NASA Johnson Space Center, July 2009.
[12] Aldemir T. Computer-assisted Markov failure modeling of process control systems. IEEE Transactions on Reliability 1987;R-36:133–44.
[13] Belhadj M, Aldemir T. Some computational improvements in process system reliability and safety analysis using dynamic methodologies. Reliab Eng System Saf 1996;52:339–47.
[14] P. Bucci, J. Kirschenbaum, T. Aldemir, C.L. Smith R.T. Wood, Constructing dynamic event trees from Markov models. In: Stamataletos M, Blackman HS, editors. PSAM8: Proceedings of the eighth international conference on probabilistic safety assessment and management, CD-ROM version, Paper #369. ASME Press, Inc.; 2006.
[15] Bucci P, Kirschenbaum J, Aldemir T, Smith CL, Wood RT. Generating dynamic fault trees from Markov models. Trans Am Nucl Soc 2006;95.
[16] Bucci P, Mangan LA, Kirschenbaum J, Mandelli D, Aldemir T, Arndt SA. Incorporation of Markov reliability models for digital instrumentation and control systems into existing PRAs. Proceedings of NPIC&HMIT 2006. La Grange, IL: American Nuclear Society; 2006.
[17] Aldemir T, Stovsky MP, Kirschenbaum J, Mandelli D, Bucci P, Mangan LA, et al. Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments. Nureg/Cr-6942. Washington, DC: U.S. Nuclear Regulatory Commission; 2007.
[18] Kirschenbaum J, Bucci P, Stovsky M, Mandelli D, Aldemir T, Yau M, et al. A benchmark system for comparing reliability modeling approaches for digital instrumentation and control systems. Nucl Technol 2009;165:53–95.
[19] Aldemir T, Guarro S, Kirschenbaum J, Mandelli D, Mangan LA, Bucci P, et al. A benchmark implementation of two dynamic methodologies for the reliability modeling of digital instrumentation and control systems. Nureg/Cr-6985. Washington, DC: U.S. Nuclear Regulatory Commission; 2009.
[20] Bucci P, Kirschenbaum J, Mangan LA, Aldemir T, Smith CL, Wood RT. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. Reliab Eng System Saf 2008;93:1616–27.