Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies
NPIC&HMIT 2009, Knoxville, Tennessee, April 5-9, 2009, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2009)

DYNAMIC RELIABILITY MODELING OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

T. Aldemir, D. Mandelli, L. A. Mangan, D. W. Miller, M. P. Stovsky and X. Sun
Nuclear Engineering Program
The Ohio State University,
Columbus, OH 43210
aldemir.1@osu.edu

S. Guarro and M. Yau
ASCA, Inc.,
1720 S. Catalina Avenue, Suite 220, Redondo Beach
sergio.guarro@ascainc.com

P. Bucci and J. Kirschenbaum
Department of Computer Science and Engineering
The Ohio State University
Columbus, OH 43210
kirschenbaum.9@osu.edu

B. Johnson and C. Elks
Department of Electrical and Computer Engineering
University of Virginia
Charlottesville, VA 22904
cre4g@virginia.edu

E. Ekici
Department of Electrical and Computer Engineering
The Ohio State University
Columbus, OH 43210
ekici.2@osu.edu

S. A. Arndt
U.S. Nuclear Regulatory Commission,
Washington, DC 20555-0001
saa@nrc.gov

ABSTRACT

Two dynamic methodologies, dynamic flowgraph methodology (DFM) and the Markov/cell-to cell mapping technique (CCMT), are implemented on the benchmark digital feedwater control system (DFWCS) specified in NUREG-6942 (Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments) [1], to demonstrate how an existing nuclear power plant probabilistic risk assessment (PRA) can incorporate a digital upgrade of the instrumentation and control system. The results obtained from the DFM and Markov/CCMT models of the DFWCS failure modes are compared, and the impact of same scenarios directly related to the hypothetical digital upgrade on the core damage frequency (CDF) is assessed on a demonstrative basis, using a plant PRA from NUREG-1150 (Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants) [2]. The study shows that a DFWCS similar to that of an operating plant can be modeled using dynamic methodologies and that the results can be incorporated into an existing PRA to quantify the impact of a digital upgrade on the plant CDF. *Key Words*: digital systems, dynamic PRA, dynamic flowgraph methodology, Markov, cell-to-cell-mapping-technique

1 INTRODUCTION

Nuclear power plants are in the process of replacing and upgrading aging and obsolete instrumentation and control (I&C) systems from analog to digital technology. There are presently no universally accepted methods for modeling digital systems in the current generation probabilistic risk assessments (PRAs). The objective of this paper is to show how dynamic PRA methodologies can be applied to a benchmark digital system that has dynamic interactions among its hardware, firmware and software, as well as the physical properties of controlled process. The system under consideration is the digital feedwater control system (DFWCS) of a generic 2 loops pressurized water reactor (PWR) [3] which is described in Section 2. Two dynamic PRA methods have been chosen in order to analyze this system: dynamic flowgraph methodology (DFM) (see Section 3.1) and the Markov/cell-to-cell-mapping-technique (CCMT) (see Section 3.2). The prime implicants and the cut sets generated respectively by DFM and Markov/CCMT are then analyzed and compared (see Section 3.3). Finally, it is shown how the results from theses dynamic models can be included into the framework of a traditional event tree (ET)/ fault-tree (FT) PRA (see Section 4).

2 THE DFWCS

The purpose of DFWCS [3] is to maintain the steam generator (SG) water level within plus or minus 2 inches of an assigned setpoint (designated as 0). The feedwater system serves two SGs each controlled by its own digital controller. The controller is considered failed if:

- the SG water is over 30 inches above the setpoint level: High SG level
- the SG water level falls under 24 inches below the setpoint: Low SG level.

As described in detail in [3], 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.

Each digital feedwater controller is comprised of several components which provide both control and fault tolerant capabilities. The control algorithms are executed on both a main computer (MC) and backup computer (BC). These computers produce output signals for the MFV, BFV, FP and pressure differential indicator (PDI) controllers. The selection of the appropriate signal to be used (from the MC or BC) is determined by the PDI controller. Each of these controllers can forward the MC or BC's outputs to their respective controlled device (i.e., MFV, BFV or FP), or it can maintain the previous output to that device. If the controllers decide to maintain a previous output value to a controlled device, it is necessary for operators to override the controller.

2.1 Benchmark system modeling

The DFWCS is modeled as consisting of three layers of interaction [3]:

- Intra-computer interactions: a layer which describes the status of the single computer (MC or BC)
- Inter-computer interactions: a layer which describes the status of the set of both computers (MC and BC)
- Computer-controller-actuated device interactions: a layer which describes the status of the controllers (MFV, BFV and FP controllers).

The intra-computer interactions layer consists of 5 states. In State A, the computer is operating correctly. In State B, the computer detects loss/invalid output for 1 sensor of any type (e.g., water level). State C represents loss/invalid output for 2 sensors of any one type. In state D the computer has detected an internal problem and is signaling that it has to be ignored. In State E, either the sensor output is invalid or there is an internal processing error in the computer; however, the computer does not detect the fault and is transmitting the wrong information to the controllers. These states capture the possible failures in the failure modes and effects analysis (FMEA) presented in Section 2.2, and that occur within both the MC and BC.

The inter-computer interaction layer displayed in Fig.1 shows the interactions between the two computers (MC and BC), including the transfer of control from the MC to the BC. In this layer, 3 computer macro-states (MSs) are identified. Each of these macro-states indicates the status of both the computers:

1. In State 1 both MC and BC are operating normally.
2. In State 2, one computer is operating correctly and the other is down but can be recovered.
3. In State 3, again one computer is operating correctly and the other is down but it is not recoverable.

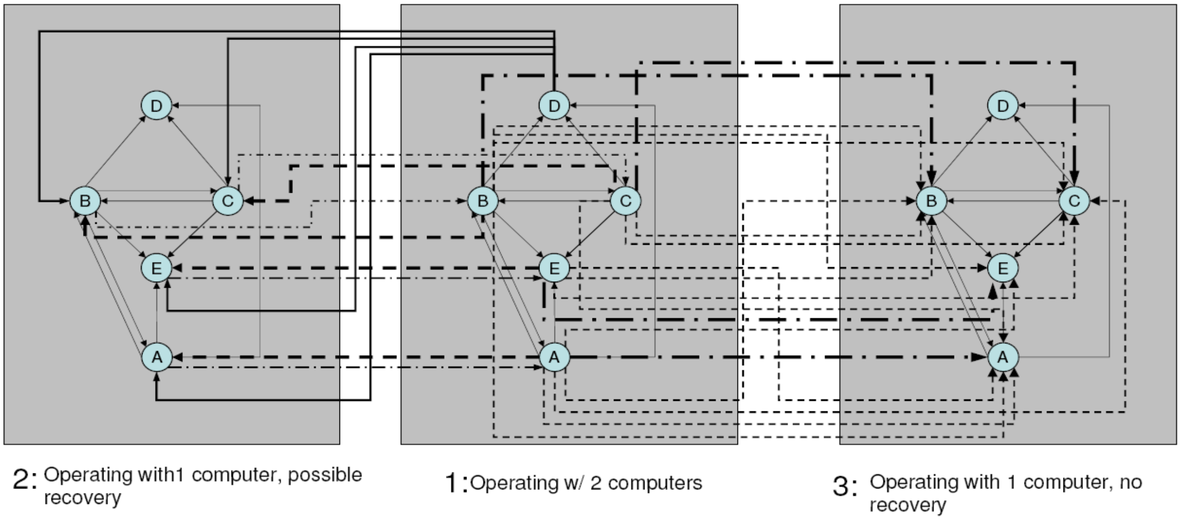
D
B
C
E
A
D
B
C
E
A
D
B
C
E
A
2: Operating with1 computer, possible recovery
1 :Operating w/ 2 computers
3: Operating with 1 computer, no recovery

Figure 1. Representation on the inter-computer interaction layer

Figure 2 shows all the possible controller-computer-actuated device interactions. The shaded circles represent signals to the actuated devices (MFV, BFV and FP) upon computer/controller failure, as well as the mechanical failure of the actuated device (Device Stuck). 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 controller and actuated device are restored.

The scheme shown in Fig. 2 shows the connection between a single controller (e.g., the MFV controller) and the computers (MC and the BC) and its own actuated device (MFV). In particular, the following types of controller failures are under consideration:

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

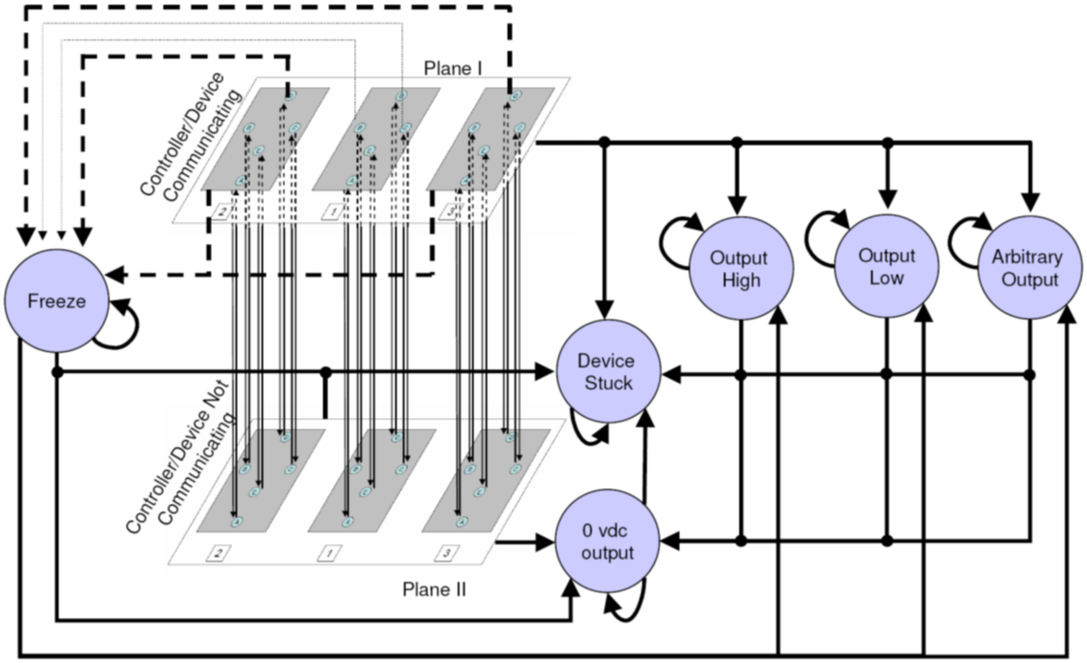

Figure 2 Representation on the computer-controller-actuated device interactions layer

Figure 2 also shows how the computer-computer interactions (see Fig. 1) integrate with computer-controller and controller-actuated device interactions. *Device Stuck* refers to mechanical failures and is independent of the failure modes of the computers and controllers. *Freeze* state represents the situation that both BC and MC recognize an internal failure or invalid data coming from sensors. In this situation, the computers resend their last valid output to the controllers.

2.2 FAILURE MODES AND EFFECTS ANALYSIS OF THE DFWCS

A detailed FMEA for each component of the DFWCS is presented in [3] and includes failure classes such as sensor failures, output failures, input failures and internal failures. Each of the failure classes may contain a large number of faults. For example, sensor failure may be the result of a physical sensor failure, cut wires, loose connections, or hardware (such as analog to digital converters) on the receiver failing. While these failure classes may be general, they capture the necessary information regarding possible failures of the DFWCS. The only mechanical failures that are considered for the DFWCS are the valves getting stuck in their current position. Table I shows the transition rates for DFWCS computers (see Section 2.1) and for the other components obtained using estimation of fault uncoverage via fault injection experiments for the DFWCS [4].

Table I. Transition rates for the DFWCS components

Component	Failure Rate (/h)
MFV controller	$3.3 \cdot 10^{-7}$
BFV controller	$3.3 \cdot 10^{-7}$
PDI controller	$3.3 \cdot 10^{-7}$
FP controller	$3.3 \cdot 10^{-7}$
MFV, BFV, FP	$4.2 \cdot 10^{-5}$
Loss of power	$4.8 \cdot 10^{-6}$

Transitions Rates δ_{ij} Between Computer States	Failure Rate (/h)
λ_{AB}	$1.98 \cdot 10^{-8}$
λ_{AD}	$2.64 \cdot 10^{-9}$
λ_{BD}	$2.64 \cdot 10^{-9}$
λ_{CD}	$2.64 \cdot 10^{-9}$
λ_{AE}	$1.089 \cdot 10^{-7}$
λ_{BC}	$2.31 \cdot 10^{-8}$

2.3 Example Scenario

The scenario under consideration is a plant transient produced by a power maneuver consisting of:

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

The 24 hour period was chosen because it is the default reference-time period for standard PRA tools when modeling continuously operating systems.

3 IMPLEMENTATION

This section illustrates how DFM (see Section 3.1) and Markov/CCMT (see Section 3.2) analyze the model presented in Section 2 in order to obtain prime implicants (DFM) or cut sets (Markov/CCMT). Section 3.3 compares these two methodologies.

3.1 The DFM

The DFM [5] model developed to analyze the benchmark system is shown in Fig.3. This model encompasses the MC, BC, BFV, BFV controller, FP, FP controller, MFV, MFV controller, PDI controller, the inputs and outputs for the main and backup computers, and the control law and logic for maintaining the SG level. The plant process and hardware, the digital hardware, the digital software, and their interactions are all included and represented in the same model. The process variable nodes are used to represent the key process parameters or states of key components and they each are discretized into a finite number of states.

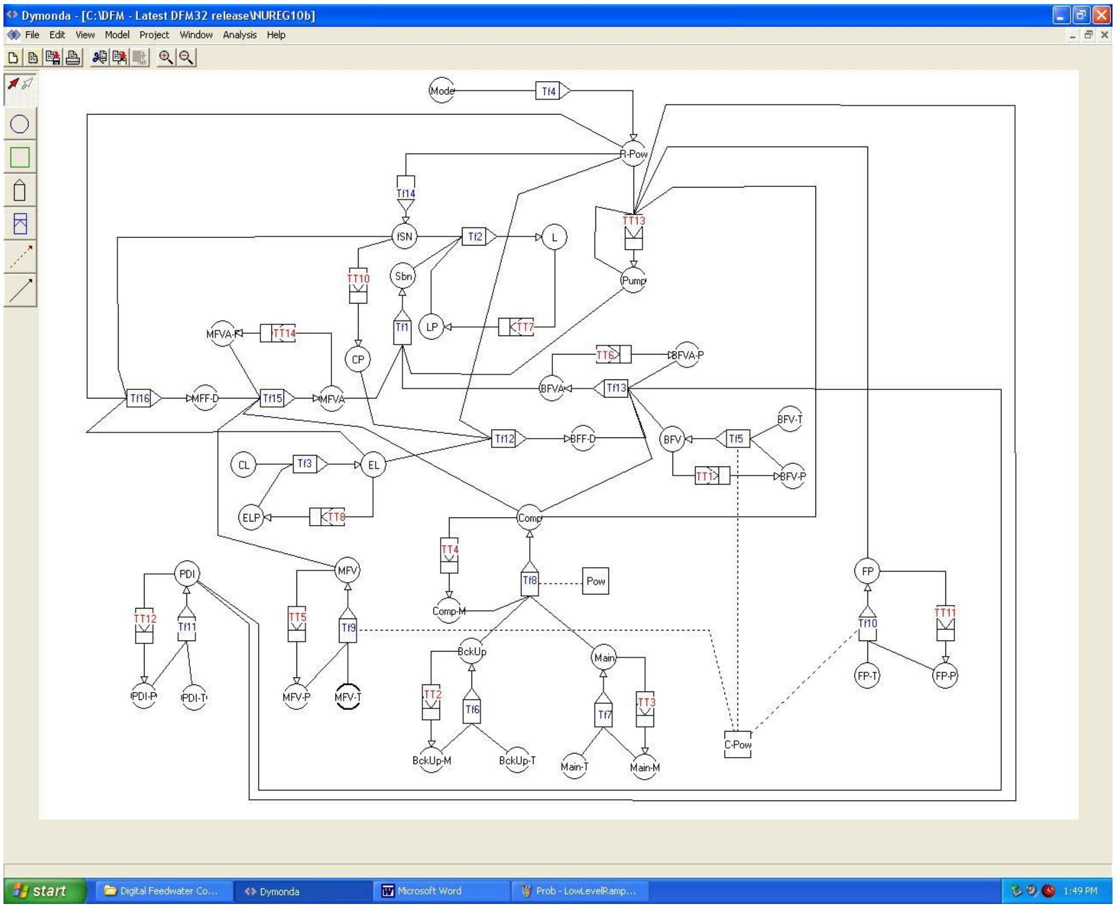

Figure 3. DFM implementation of the DFWCS presented in Section 2

The DFM process variable nodes are graphically linked together to model the relationship between these nodes. Regarding the Low SG Level Top event, the analysis concentrates on identifying prime implicants for a SG low level failure state occurring in the eight hours of the power ramp-up maneuver, given the system starts in a state with no failed components. The focus is on the ramp-up phase because the DFWCS is most vulnerable to the low failure during this phase. Specifically, if the change in feed flow cannot match the increase in steam flow, the SG level can drop and lead to a reactor trip condition. In this analysis, the time step t = 0 refers to the 78% power steady-state that follows the end of the initial 8 hour ramp-up period, whereas the time step t = -1 refers to the initial 8 hour ramp-up period. The 6 Top prime implicants for the Low SG level Top Event are shown in Table II.

For the analysis of the High SG level Top event, the focus is on the ramp-down phase because the DFWCS is most vulnerable to the high failure during this phase. Specifically, if the change in feed flow cannot match the reduction in steam flow, the SG level can rise and lead to a turbine trip condition. The assumption regarding no prior failed components forces the analysis to identify the absolute minimum conditions that would lead to the undesirable high SG level outcome. In this analysis, the time step t = 0 refers to the 70% power steady-state that follows the end of the closing 8 hour ramp-down period, whereas the time step t = -1 refers to the 8 hr window of the power ramp down during the plant maneuver. The 6 Top prime implicants for the High SG level Top event are shown in Table II.

3.2 The Markov/CCMT methodology

Markov/CCMT [4] is an approach that combines the conventional discrete state Markov methodology with CCMT [6] to represent the possible coupling between failure events that can originate from the dynamic (time-dependent) interactions:

1. between the digital I&C system and the controlled/monitored process (modeled through CCMT [6]), and,
2. among the different constituents of the digital I&C system (modeled through Markov transition diagram [7]).

Table II. Top Prime Implicants for High and Low SG Level obtained with DFM

#	Low Level Prime Implicant	Probability
1	MFV Stuck	$3.33 \cdot 10^{-4}$
2	MFV Stuck	$3.33 \cdot 10^{-4}$
3	Controller Power OFF	$3.86 \cdot 10^{-5}$
4	Controller Power OFF	$3.86 \cdot 10^{-5}$
5	Computer Power OFF	$3.86 \cdot 10^{-5}$
6	Computer Power OFF	$3.86 \cdot 10^{-5}$

#	High Level Prime Implicant	Probability
1	MFV Stuck	$3.33 \cdot 10^{-4}$
2	MFV Stuck	$3.33 \cdot 10^{-4}$
3	MFV Controller Arbitrary Output	$4.37 \cdot 10^{-7}$
4	MFV Controller Arbitrary Output	$4.37 \cdot 10^{-7}$
5	MFV Controller Fails High	$4.37 \cdot 10^{-7}$
6	MFV Controller Fails High	$4.37 \cdot 10^{-7}$

The CCMT is a systematic procedure to describe the dynamics of both linear and non-linear systems in discrete time and in system state space previously partitioned into V_j ($j=1,\ldots, J$) cells. The evolution of the system in discrete time is modeled and described through the probability $p_{n,j}(k)$ that the controlled variables are in a predefined region or cell V_j in the state space at time $t=k\Delta t$ (k=0, 1,…) with the system components (such as pumps, valves, or controllers) having a components states combination $n=1,\ldots,N$. Each component is modeled through a Markov transition diagram [7] where states and transition among them are defined according to the modeling presented in Section 2 and to the FMEA analysis presented in [4]. The interaction between the controlled/monitored process and the hardware/software/firmware states is represented in terms of probability of transition between the cells within $k\Delta t\ t\leq(k+1)\Delta t$ (k=0, 1,…). The resulting model can be converted to dynamic ETs or dynamic FTs [8] for incorporation in an existing PRA. The dynamic ETs can be also interpreted as prime implicants.

In this application, the process variable state space is represented by three cells: Nominal Range, Low Level and High Level. The Table III shows the first 6 prime implicants (all singletons) in descending order of likelihood for both High and Low SG Level Top events.

3.3 Comparison

In general, the results obtained from the DFM and Markov/CCMT analyses exhibit close consistency. The qualitative and quantitative comparison of the results for the Low SG Level and High SG Level Top events are summarized in Tables IV and V, respectively. The DFM analyses leading to these results and considered in this discussion are the deductive analyses presented in Sections 3.1. These analyses cover potential faults occurring in successive 8 hour long time-steps.

More specifically, for the Low SG Level failure scenario, the DFM deductive analysis covers two time steps, identifying those basic fault conditions that may occur during the power ramp-up phase (from 70% to 78% power) and cause the low SG level Top Event to occur during the 8 hour ramp up or the 8 hour 78% power steady state period. For the High SG Level Top Event, the initial DFM baseline analysis identified basic fault conditions to occur during the ramp-down phase (78% to 70% power) which would lead to the High SG Level Top Event to occur during the 8 hour ramp down or the 8 hour steady state period immediately following the ramp down.

Table III. Cut set for High and Low SG Level obtained with Markov/CCMT

#	Low Level Prime Implicant Probability	Low Level Prime Implicant
1	$3.33 \cdot 10^{-4}$	MFV Stuck
2	$1.15 \cdot 10^{-4}$	Power Off
3	$3.85 \cdot 10^{-5}$	Freeze
4	$3.70 \cdot 10^{-6}$	Computer Arbitrary Output
5	$2.61 \cdot 10^{-6}$	FP Output Low
6	$1.31 \cdot 10^{-6}$	FP Arbitrary Output

#	High Level Prime Implicant Probability	High Level Prime Implicant
1	$6.64 \cdot 10^{-4}$	MFV Stuck
2	$7.69 \cdot 10^{-5}$	Freeze
3	$1.74 \cdot 10^{-6}$	MFV Controller Fails Low
4	$1.31 \cdot 10^{-6}$	MFV Output High
5	$4.36 \cdot 10^{-7}$	MFV Arbitrary Output
6	$3.32 \cdot 10^{-7}$	FP Stuck MFV Stuck

Table IV. Comparison of Low SG Level Results

	DFM	Markov/CCMT
Probability (low level manifestation during 8 hr ramp-up only)	$4.19 \cdot 10^{-4}$	$4.15 \cdot 10^{-4}$
Highest Contributor	MFV stuck	MFV stuck
Second Contributor	Computer & Controller Power Off	Freeze
Time of Basic Failure Event Covered by Analysis	8 hour ramp-up period	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)
Time interval for Top Event to occur	8 hour ramp up (70% to 78%), or 8 hour steady state (78%)	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)

Table III. Comparison of High SG Level Results

	DFM	Markov/CCMT
Probability (high level manifestation during 8 hr ramp-down only)	$6.68 \cdot 10^{-4}$	$7.40 \cdot 10^{-4}$
Highest Contributor	MFV stuck	MFV stuck
Second Contributor	MFV Controller Fails High	Freeze
Time of Basic Failure Event Covered by Analysis	8 hour steady state (78%) and 8 hour ramp down (78% to 70%)	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)
Time interval for Top Event to occur	8 hour steady state (78%), 8 hour ramp down (78% to 70%), or final steady state (70%)	8 hour ramp up (70 to 78%), 8 hour steady state (78%), or 8 hour ramp down (78% to 70%)

The DFM and Markov/CCMT probability values and qualitative results produced for the Low SG Level events are in good agreement. The qualitative difference that appears to exist in the second highest contributor to the High SG Level Top Event is the result of a Markov/CCMT modeling choice. In fact the 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 (see Section 2.1). This super-state groups together a set of contributors (e.g. computer power off, controller power off, loss of input from the sensor), 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.

4 INTEGRATION OF RESULTS WITH TRADITIONAL PRA MODELS

Once the prime implicants for an initiating event have been generated, they can be incorporated into an existing PRA through standard features of PRA tools, such as SAPHIRE [9]. In importing FT logical information, it must be ensured that:

- the events in the dynamic event tree are appropriately named so that the PRA tool is able to recognize the identical events in the dynamic tree as the same events in the rest of the tree, and
- the timing of the events is not lost when the dynamic event tree is incorporated into the existing model, so that timing information can be included in the resulting analysis.

In the integration into the PRA tool, these objectives are achieved, respectively, by following a specific, consistent naming scheme when naming events and by time tagging the events to maintain sequence ordering information [9]. Post-processing of the cut sets resulting from the analysis may be necessary to eliminate outputs that violate the timing constraints. Again, minimal cut sets/prime implicants may be exported into text files for post-processing using standard features of the PRA tools [4].

5 CONCLUSION

This paper shows how it is possible construct PRA models of digital instrumentation and control system using the DFM and Markov/CCMT as two example dynamic methodologies. The digital feedwater control system of a PWR has been used as an example system to illustrate the process. The prime implicants and their probabilities generated by these two methodologies have been compared. The comparison shows a very close consistency between the DFM and Markov/CCMT results. The paper also shows how it is possible to incorporate these analyses into an existing PRA.

6 REFERENCES

1. T. Aldemir, M. P. Stovsky, J. Kirschenbaum D. Mandelli, P. Bucci, L. A. Mangan, D. W. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. W. Johnson, C. Elks, and S. A. Arndt, Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, NUREG/CR-6942, U.S. Nuclear Regulatory Commission, Washington, D.C. (2007).

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

3. J. Kirschenbaum, P. Bucci, M. Stovsky, D. Mandelli, T. Aldemir, M. Yau, S. Guarro, E. Ekici, S.A. Arndt, “A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems”, Nuclear Technology, Vol. 165 Jan. 2009.

4. U. S. Nuclear Regulatory Commission, Reliability Modeling of Digital Instrumentation and Control Systems for nuclear Reactor Probabilistic Risk Assessments, NUREG/CR-6942, Washington, D.C. (2006).

5. S. Guarro, M. Yau, and M. Motamed, Development of Tools for Safety Analysis of Control Software in Advanced Reactors, NUREG/CR-6465, U.S. Nuclear Regulator Commission, Washington, D.C. (1996)

6. C.S. Hsu, “Cell-to-Cell Mapping: a Method of Global Analysis for Nonlinear Systems”, Springer-Verlag, New York, 1987.

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

8. P. Bucci, J. Kirschenbaum, L. A. Mangan, T. Aldemir, C. Smith, T. Wood, “Construction of Event-Tree/Fault-Tree Models From a Markov Approach to Dynamic System Reliability”, Reliab. Engng & System Safety, 93, 1616-1627 (2008)

9. C. L. Smith, J. Knudsen, M. Calley, S. Beck, K. Kvarfordt and S. T. Wood, “SAPHIRE Basics: An Introduction to Probability Risk Assessment Via the Systems Analysis Program for Hands-on Integrated Reliability Evaluations” SAPHIRE Software, Idaho National Laboratory, Idaho Falls, ID (2005).