BNL-81553-2009-CP

A MARKOV Model for Assessing the Reliability of a Digital Feedwater Control System

Tsong-Lun Chu, Meng Yue, Gerardo Martinez-Guridi, and John Lehner

Presented at the 6th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies Conference
Brookhaven National Laboratory, Upton, NY
April 5-9, 2009

February 2009

Energy Science and Technology Department/

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-AC02-98CH10886 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

This preprint is intended for publication in a journal or proceedings. Since changes may be made before publication, it may not be cited or reproduced without the author's permission.

DISCLAIMER

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

Printed on recycled paper

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)

A MARKOV MODEL FOR ASSESSING THE RELIABILITY OF A DIGITAL FEEDWATER CONTROL SYSTEM[1]

Tsong-Lun Chu, Meng Yue, Gerardo Martinez-Guridi, and John Lehner
Energy Sciences and Technology Department
Brookhaven National Laboratory
Upton, NY 11973
chu@bnl.gov; yuemeng@bnl.gov; martinez@bnl.gov; lehner@bnl.gov

ABSTRACT

A Markov approach has been selected to represent and quantify the reliability model of a digital feedwater control system (DFWCS). The system state, i.e., whether a system fails or not, is determined by the status of the components that can be characterized by component failure modes. Starting from the system state that has no component failure, possible transitions out of it are all failure modes of all components in the system. Each additional component failure mode will formulate a different system state that may or may not be a system failure state. The Markov transition diagram is developed by strictly following the sequences of component failures (i.e., failure sequences) because the different orders of the same set of failures may affect the system in completely different ways. The formulation and quantification of the Markov model, together with the proposed FMEA (Failure Modes and Effects Analysis) approach, and the development of the supporting automated FMEA tool are considered the three major elements of a generic conceptual framework under which the reliability of digital systems can be assessed.

Key Words: Markov model, failure sequences, Laplace transform

1 INTRODUCTION

A system can consist of a number of components, each of which may have multiple failure modes. However, not all failure modes of a component, or subsets of component failures, necessarily fail the system. The system state, i.e., whether the system fails or not, is a function of the states of its components. Each component is either in the success state or in a failed state characterized by one of its failure modes. The actual order in which the component failures occur (i.e., the component failure sequence) can be important, since different orders of the same set of failures may affect the system in completely different ways. Accordingly, we can use a Markov model to assess the system's reliability because sequences containing the same set of component failures but in a different order can be represented by different Markov states.

An FMEA (Failure Modes and Effects Analysis) approach that decomposes a digital system into a level of generic components, such as a microprocessor was proposed in [1], which helps in creating the Markov model of the digital system. Starting from the system state that has no

---

[1] This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the U.S. Nuclear Regulatory Commission.

component failures, possible transitions out of it are all failure modes of all components. Each additional component failure mode will formulate a different system state that may or may not be a system failure state.

Theoretically, the expansion of the Markov transition diagram should be stopped only when all the system states become absorbing states, i.e., the system failure states. The difficulty of doing so is apparent for any relatively complex system, due to the likely huge number of component failure combinations that would need to be included in the Markov model. In addition, each component failure combination would need to be evaluated to determine if it results in system failure. The two major achievements of our proof-of-concept reliability study of a digital feedwater control system (DFWCS) address these difficulties [1-3]. The first achievement is a supporting FMEA tool that automatically evaluates whether the impacts of failure sequences would lead to a system failure [2, 3]. The second achievement, which is presented in this paper, is the derivation of an analytical solution of the Markov model. The Markov model is formulated in a way such that individual failure sequences can be solved separately. This improves the practicality of analytically solving a large Markov model by allowing the use of truncation based on the number of failures in a system state (or failure sequence), i.e., its order. Such truncation is a concept similar to that of cutset truncation typically done in a PRA (Probabilistic Risk Assessment). Thus, the expansion of the Markov transition diagram can be stopped after a certain order of the failure sequences, i.e., double failure or triple failure sequences, once the probability of system failure converges.

In this paper, the Markov model approach is applied to represent and quantify the reliability model of the DFWCS system. The top event, i.e., the system failure, of the DFWCS is defined as a loss of automatic control of the main feedwater system. Section 2 describes the Markov model for a fully expanded transition diagram and the analytical solutions of individual Markov states. Section 3 briefly presents the development and quantification of reliability model for the DFWCS system. For comparison, a simplified Markov model using a rare event approximation and a traditional fault tree representation of the DFWCS are also evaluated in Section 3. Section 4 summarizes the paper and presents our conclusions and ideas for possible future work.

2 DEVELOPMENT AND QUANTIFICATION OF A FULLY EXPANDED MARKOV MODEL

2.1 Assumptions

The following considerations significantly affect the development of the Markov model:

1. All components, including those playing a standby role, e.g., the backup central processing unit (CPU), are operating at all times and can fail at any time.
2. Typically, a component can have more than one failure mode with different effects that must be modeled differently. A component is assumed to fail only once in a given failure sequence, i.e., after one failure mode of the component has occurred, other modes cannot occur for the same component.
3. In evaluating the effects of sequences of failure modes, the order in which failures take place is recognized to affect the impact on the system. Therefore, the order must be

accounted for in developing the model, i.e., in defining possible transitions out of a system state and their end states.

4. The components of the system cannot be repaired or replaced while the system is operating.
5. Failures of different components are independent of each other, regardless of how they are physically wired together.

Assumption 1 is generally true for a digital system. Assumption 2 is believed to hold for most of the digital components, because available information on digital component failures seems to suggest so. It may be possible that a certain component fails to an intermediate failure mode before it reaches one of the other failure modes. If recognized, such sequence of failures can be analyzed and modeled using the approach of this study. Assumption 3 reflects one of the major reasons for using the Markov model in such studies as this one. Since the model was developed to assess the frequency of an initiating event with the plant in power operation, it is expected, as stated in Assumption 4, that if some components of the system fail, they will not be repaired because doing so would likely cause or require a reactor trip.

It is recognized that determining the effects of component failure modes in a real digital system could be much more complex than what this study assumes. Assumption 5 is introduced because, otherwise, detailed analyses of the designs at the circuit level, which are unavailable in this study, must be performed for individual components to determine how a specific failure of a component affects the connected components.

2.2 Development of a Markov Transition Diagram

A Markov transition diagram of the system starts from a system state in which every component is in perfect condition. The possible transitions out of this state are all of the failure modes of the system's components. Each such failure mode would lead to a different system state that may or may not be a failed state. If a state is a failed state of the system, then it becomes an absorbing state, i.e., one with no transition out of it. If a state does not correspond to system failure, then additional component failure modes are considered as possible transitions out of the system state that engender additional system states. This process continues and the transition diagram grows to represent a tree wherein all the end states of the tree are absorbing states. The development of the transition diagram is described graphically below.

It is assumed that there are M components and each component, i, has $N_i, i \in [1, M]$ failure modes (component states) that are represented as $C_{(i,j)}, i \in [1, M], j \in [0, N_i]$. It also is supposed that $C_{(i,0)}, i \in [1, M]$ represents the component's normal state, i.e., there is no failure of component i, as illustrated in Fig. 1.

The Markov model starts from a system state with no component failure, i.e., the initial system state is $C_{(1,0)} C_{(2,0)} \cdots C_{(M,0)}$; the transitions to other states that contain component failures are characterized by the Markov model depicted in Fig. 2.

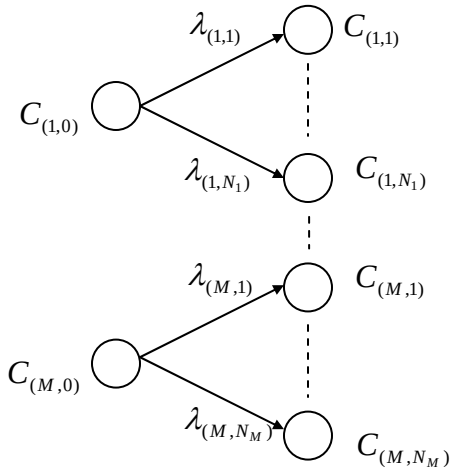

Figure 1. Markov models for *M* independent components.

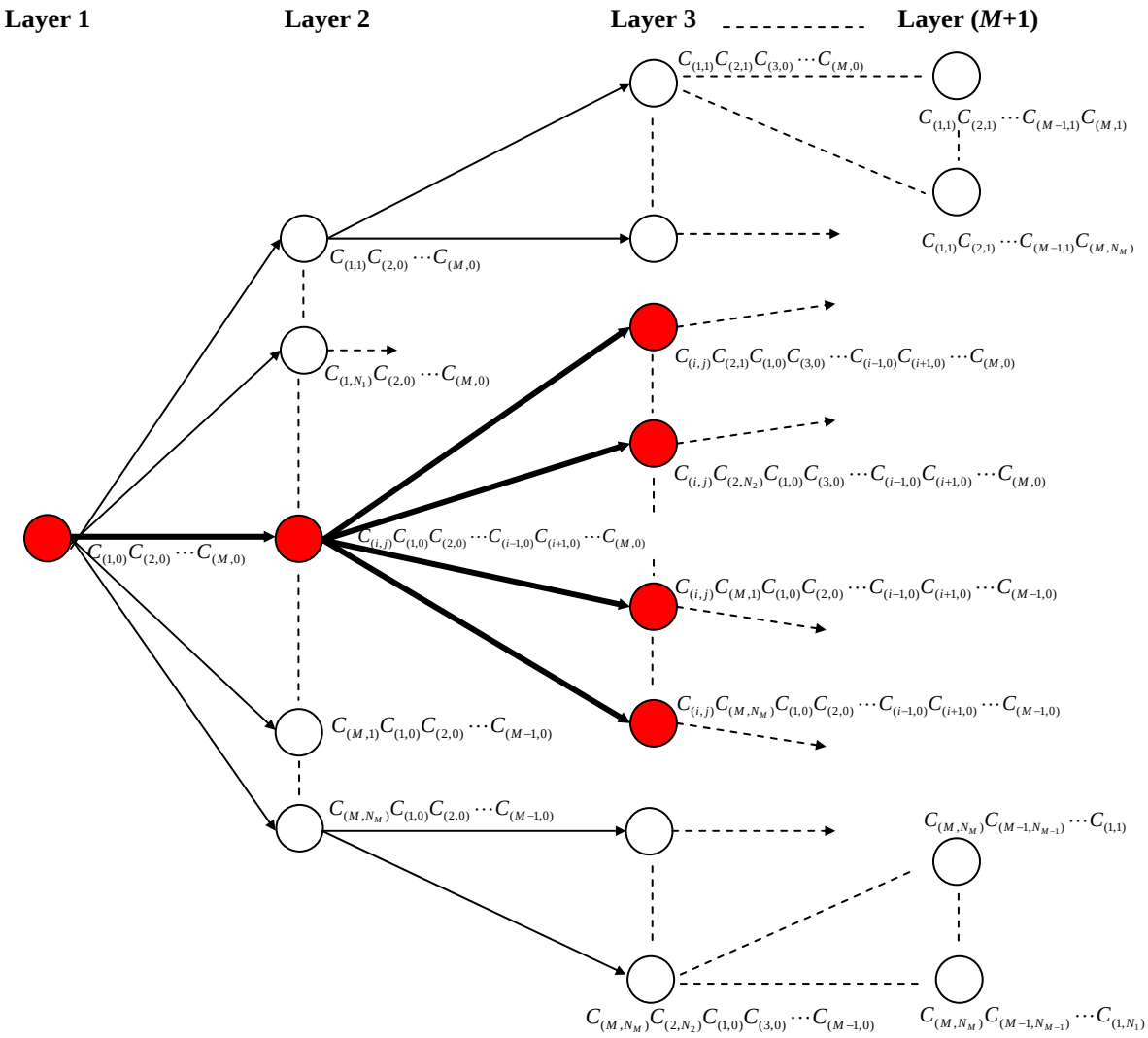

Figure 2. Markov model of a system with *M* components.

Let $\lambda_{(i,j)}$ be the failure rate of failure mode *j* of component *i*. Each additional failure generates a new system state; the order of failures should be strictly followed when generating the transition diagram in this model because differences in their order may produce different results.

Understanding the notations of the system states in Fig. 2 is very important. Components with failures always appear before those without failures, and the failures that appear first are the ones that occur earlier. For example, there are two failures in the system state $C_{(i,j)}C_{(2,N_2)}C_{(1,0)} \cdots C_{(3,0)}C_{(M-1,0)}$ with the *j-th* failure mode of component *i* occurring first, followed by the failure mode N_2 of component 2; no other components are failed in this system state.

Fig. 2 shows that there is no component failure in Layer 1, one in Layer 2, and *M* failures in Layer (*M*+1). Generally, a fully expanded Markov model would consist of all possible combinations of component failures in all possible orders, as indicated in this figure. The transition diagram expands very quickly with increasing numbers of components and component failure modes. In practice, a system state that represents system failure can constitute an absorbing state without further expansion. This consideration drastically reduces the size of the transition diagram, such that the model is manageable.

2.3 Analytical Solution of the Markov Model

The structure of the transition diagram in Fig. 2 adopts the form of a tree. Therefore, the associated differential equations can be solved sequentially from left to right. That is, the equation for the node with every component in good condition is solved first, and the solution substituted into the equations for the states immediately to its right, thereby allowing the equations to be solved. The process continues along each branch of the tree until an absorbing state is reached.

Let *P* and $\dot{P}$ respectively represent the probability and its rate of change of a state of the Markov model of Fig. 2. The following differential equations can be written for the first two states of the shaded branch of the transition diagram by inspecting Fig. 2:

$$\dot{P}_{C_{(1,0)}C_{(2,0)}\cdots C_{(M,0)}} = -\sum_{u=1}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)}P_{C_{(1,0)}C_{(2,0)}\cdots C_{(M,0)}} \tag{1}$$

$$\dot{P}_{C_{(i,j)}C_{(1,0)}\cdots C_{(i-1,0)}C_{(i+1,0)}\cdots C_{(M,0)}} = \lambda_{(i,j)}P_{C_{(1,0)}C_{(2,0)}\cdots C_{(M,0)}} - \sum_{\substack{u=1\\u\neq i}}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)}P_{C_{(i,j)}C_{(1,0)}\cdots C_{(i-1,0)}C_{(i+1,0)}\cdots C_{(M,0)}} \tag{2}$$

where the second term on the right side of Equation (2) represents transitions from the state $C_{(i,j)}C_{(1,0)}\cdots C_{(M,0)}$ to all of its associated states in Layer 3.

In general, for a given system state consisting of a sequence of *k* component failures, i.e., $C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_M,j_M)}, i_k \in [1,M], j_k \in [0,N_{i_k}]$ with $k = 1,2,\cdots,M$, and $j_k \neq 0$ and $j_{k+1} = \cdots = j_M = 0$, we have

$$\dot{P}_R = \lambda_{(i_k, j_k)} P_S - \sum_{\substack{u=1 \\ u \neq i_1 \\ \vdots \\ u \neq i_k}}^{M} \sum_{v=1}^{N_u} \lambda_{(u,v)} P_R \,, \tag{3}$$

where P_R is the state $C_{(i_1, j_1)} C_{(i_2, j_2)} \cdots C_{(i_M, j_M)}$ with k failures, and P_S is the state preceding P_R.

Letting $p_0 = \sum_{u=1}^{M} \sum_{v=1}^{N_u} \lambda_{(u,v)}$ and $p_l = \sum_{\substack{u=1 \\ u \neq i_1 \\ u \neq i_2 \\ \vdots \\ u \neq i_l}}^{M} \sum_{v=1}^{N_u} \lambda_{(u,v)}$ for $l = 1, 2, \cdots, k$, Equations (1) to (3) become

$$\dot{P}_{C_{(1,0)} C_{(2,0)} \cdots C_{(M,0)}} = -p_0 P_{C_{(1,0)} C_{(2,0)} \cdots C_{(M,0)}} \,, \tag{4}$$

$$\dot{P}_{C_{(i_1, j_1)} C_{(1,0)} \cdots C_{(i-1,0)} C_{(i+1,0)} \cdots C_{(M,0)}} = \lambda_{(i_1, j_1)} P_{C_{(1,0)} C_{(2,0)} \cdots C_{(M,0)}} - p_1 P_{C_{(i_1, j_1)} C_{(1,0)} \cdots C_{(i-1,0)} C_{(i+1,0)} \cdots C_{(M,0)}} \,, \tag{5}$$

and,

$$\dot{P}_R = \lambda_{(i_k, j_k)} P_S - p_k P_R \,. \tag{6}$$

As discussed, the equations are solved sequentially, i.e., solving Equation (1), substituting the solution into Equation (2), and then solving Equation (2), and so on. This process continues along each branch of the transition diagram until attaining an absorbing state. For an absorbing state with k failures, the second term on the right-hand side of Equation (3) becomes zero. It is demonstrated that the solutions of absorbing states with one, two, and three failures are

$$P_{C_{(i_1, j_1)} C_{(2,0)} \cdots C_{(M,0)}} = \frac{\lambda_{(i_1, j_1)}}{p_0} [1 - e^{-p_0 t}] \,, \tag{7}$$

$$P_{C_{(i\ \ , j_1)} C_{(i_2, j_2)} C_{(3,0)} \cdots C_{(M,0)}} = \frac{\lambda_{(i_1, j_1)} \lambda_{(i_2, j_2)}}{p_0 p_1} [1 - \frac{p_1}{p_1 - p_0} e^{-p_0 t} - \frac{p_0}{p_0 - p_1} e^{-p_1 t}] \text{ , and} \tag{8}$$

$$P_{C_{(i_1, j_1)} C_{(i_2, j_2)} C_{(i_3, j_3)} C_{(4,0)} \cdots C_{(M,0)}} = \frac{\lambda_{(i_1, j_1)} \lambda_{(i_2, j_2)} \lambda_{(i_3, j_3)}}{p_0 p_1 p_2} [1 - \frac{p_1 p_2}{(p_1 - p_0)(p_2 - p_0)} e^{-p_0 t} - \frac{p_0 p_2}{(p_0 - p_1)(p_2 - p_1)} e^{-p_1 t} - \frac{p_0 p_1}{(p_0 - p_2)(p_1 - p_2)} e^{-p_2 t}] \,. \tag{9}$$

Equivalently, the solution of the differential equations in the frequency domain can be obtained using Laplace transforms. The induction method, described in Appendix C of [2] proves that, in general, for a system state consisting of a sequence of k component failures, the solution of Equation (3) in the Laplace transformed space is

$$P_{C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_M,j_M)}}(s)\Bigg|_{\substack{j_k\neq 0\\ j_{k+1}=0\\ \vdots\\ j_M=0}} = \frac{\lambda_{(i_1,j_1)}\lambda_{(i_2,j_2)}\cdots\lambda_{(i_k,j_k)}}{(s+\sum_{u=1}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})(s+\sum_{\substack{u=1\\ u\neq i_1}}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})\cdots(s+\sum_{\substack{u=1\\ u\neq i_1\\ u\neq i_2\\ \vdots\\ u\neq i_k}}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})} \tag{10}$$

Undoubtedly, if $j_M \neq 0$, i.e., all components of the system are failed in a certain way, Equation (10) becomes

$$P_{C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_M,j_M)}}(s)\Big|_{j_M\neq 0} = \frac{\lambda_{(i_1,j_1)}\lambda_{(i_2,j_2)}\cdots\lambda_{(i_M,j_M)}}{(s+\sum_{u=1}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})(s+\sum_{\substack{u=1\\ u\neq i_1}}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})\cdots(s+\sum_{v=1}^{N_{i_M}}\lambda_{(i_M,v)})s} \tag{11}$$

Furthermore, stopping the expansion of the Markov model in such a way that the number of failures contained in end states is k, the probability of system state $C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_k,j_k)}$ $C_{(1,0)}\cdots C_{(i_{k+1},0)}\cdots C_{(i_M,0)}$ for $j_k \neq 0$ and $j_{k+1}=0$, which then becomes an end state, is given by

$$P_{C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_k,j_k)}C_{(i_{k+1},j_{k+1})}\cdots C_{(i_M,j_M)}}\Bigg|_{\substack{j_k\neq 0\\ j_{k+1}=0\\ \vdots\\ j_M=0}} = \frac{\lambda_{(i_1,j_1)}\lambda_{(i_2,j_2)}\cdots\lambda_{(i_k,j_k)}}{(s+\sum_{u=1}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})(s+\sum_{\substack{u=1\\ u\neq i_1}}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})\cdots(s+\sum_{\substack{u=1\\ u\neq i_1\\ u\neq i_2\\ \vdots\\ u\neq i_{k-1}}}^{M}\sum_{v=1}^{N_u}\lambda_{(u,v)})s} \tag{12}$$

It should be noted that the poles of Equations (10) to (12) always are distinct (the poles are the roots of denominators in these equations). Therefore, the corresponding time-domain solution of the equations can be expressed in terms of the poles of Equation (10). The probability of state $C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_M,j_M)}$ with $j_k \neq 0$ and $j_{k+1}=\cdots=j_M=0$ is given by

$$P_{C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_M,j_M)}}(t)\Bigg|_{\substack{j_k\neq 0\\ j_{k+1}=0\\ \vdots\\ j_M=0}} = \sum_{l=0}^{k}[(s+p_l)P_{C_{(i_1,j_1)}C_{(i_2,j_2)}\cdots C_{(i_M,j_M)}}(s)\Big|_{s=-p_l}e^{-p_l t}] \tag{13}$$

It can be readily shown that Equation (13) leads to Equations (4) to (6) if *k* is set to 1, 2, and 3, respectively. Section 3 describes using the solution in quantifying the top event of interest, i.e., loss of automatic control of the DFWCS.

For a system of many components, with each component having a few failure modes (i.e., component states), it is impractical to consider all system-level states that can be defined in terms of component-level states, i.e., the possible system-level states are too numerous. This issue of state explosion is addressed by considering the dominant contributors or sequences of the

system, using a concept similar to that of cutset truncation typically done in a probabilistic risk assessment (PRA). That is, those system states with a larger number of component failures tend to have a lower probability of occurrence than system states with fewer component failures. The system states are quantified to calculate the probability of system failure during the expansion of the transition diagram; this expansion is terminated when the calculated system-failure probability converges, as described in Section 3.

3 QUANTIFICATION OF THE RELIABILITY OF THE DFWCS SYSTEM

The procedure for employing the proposed reliability method for a digital system is summarized here; more details are given in [1, 2].

An approach for supporting a Failure Modes and Effects Analysis (FMEA) to develop the reliability model of a digital system was proposed in [1, 2]. By decomposing a digital system to the levels of modules, and eventually, generic digital components, such as an analog/digital converter and a multiplexer, failure modes of individual components can be postulated and the impact on the system of a specific component failure mode can be determined by propagating it based on knowledge of how the system functions and malfunctions.

To address the underlying difficulties in implementing such an approach, which are mainly related to complexity of current digital systems and interactions between digital systems and plants, an automated tool has been developed in [2, 3] to support the FMEA of the DFWCS. The nature of the automated FMEA tool is a simulation platform formulated using the original source code of the DFWCS CPU (Central Processing Unit) modules, and recreating the controller software interfaced by input- and output-variables representing physical signals exchanged between modules, the system, and the controlled process. For any given component failure mode(s), its effects on associated signals are determined first and then the variables corresponding to these signals are modified accordingly. Criteria are developed as part of the automated tool, based on the definition of the system's failure (i.e., a loss of automatic control of the main feedwater system) and the status of both CPUs and controllers, such that the system's state, i.e., its response, can be determined automatically. More details are given of the DFWCS system, the proposed FMEA approach, and the automated FMEA tool in [1-3].

As discussed in Section 2, the states in the transition diagram in Fig. 2 are component failure sequences, developed as follows: An individual failure that does not fail the system constitutes the first failure in a double-failure sequence. The second failure can be any individual failure mode of a different component. Similarly, triple sequences arise from adding one of the individual failure modes of a different component as the third failure of a double combination that does not fail the system. It is not necessary to consider additional component failure modes for single failures or double sequences that fail the system. Whether the system is failed by the sequences is determined by using the proposed FMEA approach and the automated FMEA tool [2, 3]. Sequences containing a higher number of failures can be obtained by following this process.

The role of common cause failures (CCFs) is important in the reliability assessment. In the reliability model of the DFWCS system, a CCF is treated as a failure of a "pseudo-component" that contains all of the associated components, e.g., the CCF of two CPU modules covers all failures of the major components that a CPU module contains. In this study, the failure rate of a

CCF was modeled by adding the failure rates of the failure modes of all components contained in a "pseudo-component" and using a beta factor.

The top event of interest is the failure of a DFWCS to control feedwater automatically while the plant is operating at full power during one year; this is considered an initiating event (IE) for the PRA of the plant. An initiating event frequency, f , is the expected number of system failures per unit time that is related to the reliability of the system $R(T)$, i.e., the probability that the system is operating successfully in time period (0, T), by

$$f = -\frac{\ln[R(T)]}{T} \tag{14}$$

Equation (14) can be used to evaluate the initiating event frequency via the $R(T)$ assessed over one year, employing the Markov model of the DFWCS.

The defined top event does not consider the possibility of manually controlling the system. For some system-failure modes, manual control is possible using the DFWCS. However, modeling manual control is beyond the scope of the study.

3.1 Quantification of Markov Model

The Markov model is quantified using the data provided in Reference [2]. As indicated therein, the failure parameters used in this study have very large uncertainties, and the failure mode distributions of components might be incomplete. The failure data are not appropriate for quantifying models that will support decision-making (e.g., regulatory decisions or design changes). They are used only to demonstrate the reliability methods, and exercise the reliability models proposed in this proof-of-concept study for digital systems.

Equations (7) to (9) are used to quantify the sequences of failure modes that cause system failure. Table I summarizes this quantification. There are 112 single failures; 39,497 double-failure sequences; and, 11,972,960 triple-failure sequences. Considering that each of these sequences must be quantified, and that the number of individual, double, and triple sequences that must be evaluated to determine whether they fail the system is much larger, the computational effort is significant. The last column shows the cumulative probabilities of system failure obtained by successively adding the contributions of the single failure modes, double sequences, and triple sequences. The contribution of single failures is the highest, followed by that of double failure sequences; that from the triple failure sequences is only a small fraction of the total probability, i.e., approximately 6%. The cumulative probabilities in the last column of Table I indicate that the total system failure probability is converging and should be fairly close to the actual system failure probability.

Using the total system failure probability (0.079) in $f = -\ln[R(T)]/T$, the frequency of loss of automatic control of the DFWCS is calculated to be 0.083 per year.

Table I. Quantification of system failure probability and frequency

	Number of sequences that cause system failure	Probability of sequences with system failure	Total system failure probability (frequency per year)
Individual failure modes	112	0.051	0.051 (0.052)
Sequences of two failure modes	39,497	0.023	0.074 (0.077)
Sequences of three failure modes	11,972,960	0.0052	0.079 (0.083)

3.2 Approximate Quantification of Markov Model

The failure sequences of the DFWCS also are quantified using two approximate quantification methods, viz, the rare event approximation, and typical fault-tree cutset quantification.

1. Rare event approximation (Simplified Markov model). In this simplifying assumption, competition among the failure modes is ignored, i.e., when quantifying a system failure sequence, only those failure modes that take place in the sequence are retained in the transition diagram and all others are assumed non-existent. Fig. 3, below, represents the Markov model of such a sequence.

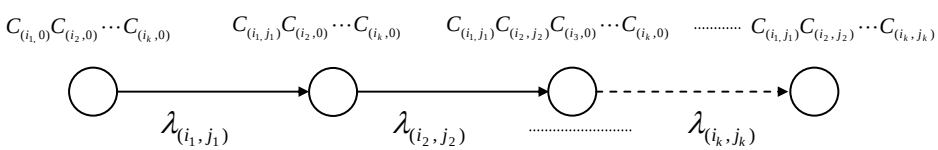

Figure 3. A simplified Markov model.

If the failure rates are distinct, then the simplified Markov model can be easily solved from the solution of the full Markov model, i.e., by setting the poles in Equations (7) to (9) to the individual failure rates, e.g., $p_0 = \lambda_{(i_1,j_1)}$. If the failure rates are identical, as expected in some cases, then a numerical method is used to solve the inverse Laplace transform of the Markov states to obtain the time domain solutions; Appendix C in [1] gives details.

This approximate method should generate a reasonable result, provided the top event of interest is a rare event, as is expected to be the case for a reactor protection system. For the DFWCS whose failure is not very rare, the results may be unsatisfactory.

2. Typical fault tree cutset quantification. In this simplification, in addition to the rare event approximation described above, the order in which failures occurs is ignored, and the full mission time for each failure event is used. This is the typical way in which the fault-tree method quantifies a minimal cutset, i.e., each failure is quantified using the expression $1-e^{-\lambda t}$, or its simplification, λt.

For a single failure of the system, this method is the same as the rare-event approximation. However, the outcomes expectedly will be significantly different for double and triple failures. Since single failures dominate the frequency of failure for the DFWCS, the deviation from the exact result may not be as large as anticipated for a system with greater redundancy, e.g., a reactor protection system. Table II summarizes the frequency of loss of automatic control calculated using the three methods described above.

Table II. Frequency of loss of automatic control

	Exact Method	Simplified Markov	Fault Tree Cutset Method
Frequency of Loss of Automatic Control (per year)	0.083	0.12	0.21

The results in the table show that the frequency of loss of automatic control has a point-estimate frequency of 0.083 per year, denoting that such an initiating event is not very rare. Using the simplified Markov method does not consider the competition between different failure modes, and accordingly, only provides a rough estimate of the frequency. In addition, the FT cutset method ignores the fact that sequences with the same component failure modes but different orders of occurrence may affect the system differently. For these reasons, this method gives a less accurate result, i.e., more than a factor of 2 higher than the exact result.

4 CONCLUSIONS

A Markov approach is proposed and applied to assess the reliability of the DFWCS system. Under the assumptions given in Section 2, the Markov transition diagram can be developed and analytical solutions derived for any given states, i.e., the component failure sequences of the DFWCS system.

Compared to the fault tree quantification method, the full and the simplified Markov quantification methods consider the order of component failures. The former offers an exact solution to the model, while the simplified Markov model does not account for competition among the failure modes.

The Markov approach is one of the three major elements of the methodology for assessing digital system reliability proposed in the proof-of-concept reliability study [1, 2]. The other two elements of the methodology are (1) the novel FMEA approach that decomposes the system into the level of generic components, and (2) the conceptual development of the automated tool that supports the FMEAs of digital systems. The Markov model, together with the FMEA approach and the supporting automated FMEA tool are considered a generic conceptual framework under which the reliability assessment of digital systems can be performed.

Even with the automated tool supporting the FMEAs and the analytical solutions to individual Markov states, the required computational effort is not trivial, as mentioned in Section 3. However, it should be highlighted that the proposed approach inherently can support parallel processing because the sequences can be analyzed, i.e., determining effects and quantifying the sequences, independently. Therefore, a linear scalability for performing FMEA and quantifying the failure sequences can be achieved by distributing the sequences onto

multiple computers, from which the results can be combined. This approach offers a practical solution for overcoming the complexity and scale of digital systems.

According to Assumption 4 in Section 2.1, repair is not modeled for failures of the major components because the repair is not possible. For a system whose components can be repaired online, the Markov model approach remains valid but the Markov model will be modified by adding repair to the transition diagram. The solution of the Markov model using Laplace transform becomes much more difficult. The simplified Markov model based on the rare event approximation can still be solved easily. Assumption 5 is considered a limitation of the proposed FMEA approach. An idea similar to the software-based fault-injection method [4] can be used to study the reliability of components by modeling the physics of the electronic components. This method might suffice to refine the component FMEAs and address the limitation introduced by Assumption 5.

It should be pointed out that purpose of the quantification is only to exercise the reliability assessment methodology proposed in this proof-of-concept study. Better data are needed before the conclusion regarding the reliability of the DFWCS can be drawn.

5 REFERENCES

1. T.-L. Chu, et al., “Traditional Probabilistic Risk Assessment Methods for Digital Systems,” NUREG/CR-6962 (2008).
2. T.-L. Chu, et al., “Modeling a Digital Feedwater Control System Using Traditional Methods,” NUREG/CR-YYYY, available at: http://www.nrc.gov/about-nrc/regulatory/research/digital/tech-reference.html (2008).
3. M. Yue, et al., “An Automated Tool for Supporting FMEAs of Digital Systems,” *Proceedings of ANS PSA* (2008).
4. C. Elks, et al., “Quantitative Dependability Assessment of the Benchmark Digital Feed-Water Control System: Final Report,” University of Virginia, Technical Report UVA-CSCS 2007-003 (2008).