Reliability analysis of digital feedwater regulating valve controller system using semi-Markov process model

Arun Veeramany and Mahesh D. Pandey

Department of Civil and Environmental Engineering, University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
aveerama@uwaterloo.ca

Abstract

A semi-Markov process model is developed for the reliability analysis of main feedwater valve (MFV) controller system used for regulating the water level in a power plant steam generator. This case study demonstrates the general application of semi-Markov process model for digital instrumentation and control systems. The NUREG-CR/6942 technical report proposed a Markov state transition model for the MFV system as part of a Probabilistic Risk Assessment (PRA) of Digital Feedwater Control System (DFWCS). The proposed model extends the Markov model to allow the use of non-exponential distribution in the time to next output of the controller system responsible for maintaining the water level. Through the concept of mission reliability, the paper is able to demonstrate that by assuming a non-exponential profile for transition times, it is possible to take hardware and software aging in to account.

Keywords: Digital Instrumentation and Control, Reliability, Semi-Markov

1. Introduction

Digital control and protection systems are installed in new nuclear power plants (NPP) and as part of upgrades to older plants. There could be random hardware failures in these systems, but random software faults are less likely to occur (Chu et al., 2010a). While hardware failures can be modeled probabilistically, software failures can also be modeled in the same way assuming that the faults caused in software are due to an underlying cause in the digital system. The failure of an I&C system could potentially lead to core damage or release of radioactive substances (Shi et al., 2010).

1.1. Need for reliability analysis of I&C systems

Reliability is a result of features like fault tolerance, fault coverage, fail safe, redundancy, defense-in-depth and diversity of components. Digital system reliability models either account for hardware and software failures separately or take both in to consideration in a single model. Software failures could potentially impact the performance of mitigating systems. Certain failure modes could arise due to software which was not originally considered for analog systems (Chu et al., 2010a). Hence digital system reliability modelling is an area of important research.

1.2. Literature

The technical report by Aldemir et al. (2006) explored various methods available for system reliability evaluation of digital instrumentation and

control (I&C) systems. Static fault tree and event tree approaches were considered obsolete due to the inherent inability of these methods to tackle "dynamic interaction" between digital systems and rest of the plant processes. An example of such an interaction is a competition between two tasks to get hold of a digital controller's resources. Deadlock could be a situation when two threads wait for each other to release resources they are in control of. Starvation is a situation where a low priority thread might have to wait indefinitely for the controller's time slice. Hence temporal interactions could lead to dynamic situations and these can be handled well using state transition methods by branching different situations as distinct states. Despite the provisions for specialized dependency gates, the dynamic fault tree (DFT) method (Rao et al., 2009) has the shortcoming that the generated cutsets might change as the system evolves in time.

The dynamic flowgraph methodology, DFM (Al-Dabbagh and Lu, 2010) is another alternative for modelling reliability of digital I&C systems. It takes the directed graph approach with decision tables for state transitions, edges for failure dependencies and nodes for variables (*.e.g.*, Water level, Valve position). Nodes can have discrete states (*e.g.*, High, Stationary, Low). The decision table construction involves all possible mappings of variables and corresponding states (e.g., Water level high and valve open). The mapping must also account for various switching actions for backup solutions. Yau et al. (1995) demonstrated the use of DFM for a digital flight control system where 9 input variables with 5 states each led to 5^9 rows in the decision table.

The paper worked around the problem by using equations of motion and control laws thus bypassing the construction and lookup of the decision table. Hence decision table construction could potentially encounter a dimensionality problem and modelling would not adhere to a universal solution though it has the ability to model multiple top events. Stochastic petri nets (Kleyner and Volovoi, 2010) is also a graph theoretic approach whose quantification can be done using simulation. These models can be converted to fault trees, but size of the model and simulation speed could severely prohibit its usage for digital I&C systems.

Another technical report by Aldemir et al. (2007) focused exclusively on reliability modelling of digital I&C systems for nuclear reactor probabilistic risk assessments. Markov models were developed for various controllers and computer systems of the DFWCS. These include the main feedwater regulating valve (MFV) controller, the bypass feedwater regulating valve (BFV) controller, the feedwater pump (FP) controller, the pressure drop indicator (PDI) controller, power source of these controllers and finally the main and its backup computers. This report was at large a proof-of-concept for the use of Markov models for digital systems. The state space for the models were elaborately developed and then reduced according to state reduction principles for practical applications. Aldemir et al. (2010) refined and quantified some of these models by generating Markov transition rates using fault injection techniques. Such techniques in software testing widen the scope of test data by introducing deliberate faults in the system.

Markov models are able to predict future failures while considering failure dependencies and can accommodate both hardware and digital interaction. However, Markov models assume only constant transition rates leading to the assumption that the time spent in any state can follow only the exponential distribution. A system involving complex interactions between hardwired analog and software controlled digital subsystems could be subjected to human, software, electrical, mechanical and electronic failures. Lognormal, Weibull and Gamma distributions to represent time-to-event have been found to be appropriate in different contexts (Vineyard et al., 1999).

1.3. Proposed approach

A water level controller valve could be subject to high failure rates due to surge voltages during startup or shutdown and a fairly constant failure rate at any random running time. With this rationale, the present paper assumes that a Weibull distribution is suitable to model the time to a send a previous valid output to the valve. In order to achieve this ability to consider a non-exponential holding time distribution in the model, the semi-Markov process model is applied for the reliability analysis of digital feedwater regulating valve controller. The idea of applying semi-Markov process model to incorporate the effect of aging related degradation of pipes in the nuclear industry has earlier been explored by Veeramany and Pandey (2011b).

Markov model requires continuous plant state information to generate the transition rates required as inputs. The semi-Markov process model is also

subject to this inhibitive requirement. Further disadvantage is the difficult learning curve for an analyst. This hindrance can be negated to an extent by the use of simple visual interfaces.

1.4. Organization

The paper is organized as follows. Section 2 describes the digital controller system. Section 2.2 describes the Markov model of the system. The semi-Markov process model is reviewed in Section 3. Section 3.3 develops the semi-Markov version of the controller reliability study. Markov results are compared against the semi-Markov results in Section 4 before concluding the paper in Section 5.

2. The digital feedwater regulating valve controller system

2.1. Problem

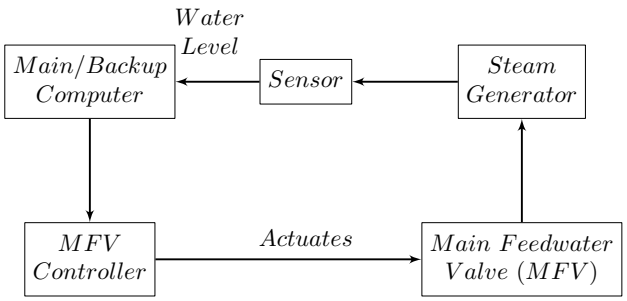

Figure 1: Schematic of the digital feed water control system (DFWCS).

The present paper is a semi-Markov extension of one of the feedwater controller Markov models from Aldemir et al. (2010). The digital feed water control system (DFWCS) shown in Figure 1 is responsible for regulating

water level in the steam generator. A water level sensor outputs level to the computer. The computer then determines the amount by which the valves need to be repositioned so as to adjust the water flow speed. This information is sent in the form of a signal to the controller. Accordingly, the controller actuates the main feedwater regulating valve (MFV) to optimize the water flow. Apart from MFV, there are other controllers and actuating devices as part of the DFWCS. The focus of this paper is to analyze the reliability of the MFV controller system based on its output to the valve. There is a finite probability of the valve getting stuck in its maximum or minimum flow position due to an erroneous output from the controller. It is also possible that the controller sends an arbitrary or random output to the valve. These could be due to a processing error or an internal problem in the computer. In these abnormal cases the controller feeds a valid previous output to the valve. This situation is termed as the failure of the controller system.

2.2. Markov analysis

The model proposed by Aldemir et al. (2010) based on Aldemir et al. (2007) has five states as shown in Figure 2. The system initially begins operation in state 1. In this state, the controller receives correct output from the computer and sends it to the valve. The system moves to state 2,4 or 5 when the output is too low, high or arbitrary respectively. It is assumed that these states do not lead back to the correct output, instead move on to state 3 where a valid previous output is sent to the valve. For modelling purposes,

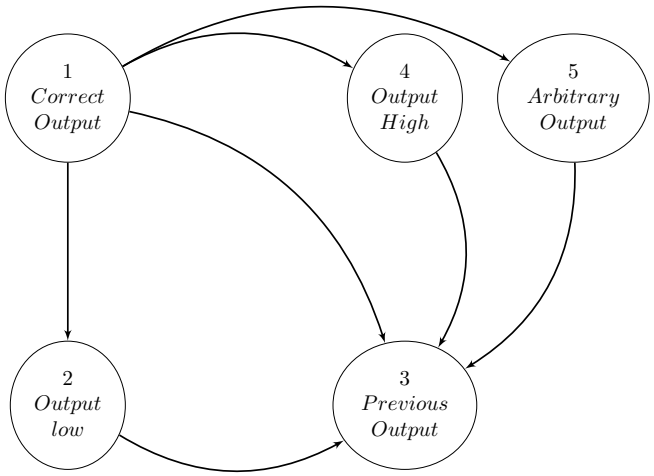

Figure 2: State space for Main Feedwater regulating Valve (MFV)(Aldemir et al., 2010).

state 3 is an absorbing state representing system failure. As per this model, there is a transition from state 1 to state 3 in which case an internal problem with the computer is recognized by the controller and a previous output is sent to the valve. The literature also suggests that there are circumstances when the controller fails to sense the failure of the computer and hence sends arbitrary output to the valve.

Table 1: Sample Markov transition rates for the controller system. (Aldemir et al., 2010)

State Transition				Transition Rate (hr^{-1})
λ_{12}	Correct Output	$\rightarrow$	Output Low	2.55 x 10^{-7}
λ_{13}	Correct Output	$\rightarrow$	Previous Output	4.2 x 10^{-5}
λ_{14}	Correct Output	$\rightarrow$	Output High	5.5 x 10^{-8}
λ_{15}	Correct Output	$\rightarrow$	Arbitrary Output	5.5 x 10^{-8}
λ_{23}	Output Low	$\rightarrow$	Previous Output	4.2 x 10^{-5}
λ_{43}	Output High	$\rightarrow$	Previous Output	4.2 x 10^{-5}
λ_{53}	Arbitrary Output	$\rightarrow$	Previous Output	4.2 x 10^{-5}

Due to lack of field data, Aldemir et al. (2010) assumed failure rates based

on fault injection experiments. The authors claim that these rates listed in Table 1 were for demonstrative use only.

The system of differential equations to solve the Markov model is based on the fact that the rate of change of the probability of being in any state S is negatively proportional to the rate at which the transitions occur outward from S and positively proportional to the rate at which inward transitions occur from other states (Lisnianski and Levitin, 2003).

For example, from Figure 2, it is seen that there are four inward transitions in to state 3 originating from states 1,2,4 and 5 while there is only one transition going out from states 2,4 and 5.

$$
\begin{aligned}
dp_1(t)/dt &= -(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15})p_1(t) \\
dp_2(t)/dt &= \lambda_{12}p_1(t) - \lambda_{23}p_2(t) \\
dp_3(t)/dt &= \lambda_{13}p_1(t) + \lambda_{23}p_2(t) + \lambda_{43}p_4(t) + \lambda_{53}p_5(t) \\
dp_4(t)/dt &= \lambda_{14}p_1(t) - \lambda_{43}p_4(t) \\
dp_5(t)/dt &= \lambda_{15}p_1(t) - \lambda_{53}p_5(t)
\end{aligned} \tag{1}
$$

2.3. Results

Solving system of Equations 1, Figure 3 plots the probability of being in state 3 and it represents the controller system failure probability. Note that the system could land in state 3 either directly from state 1 or through the

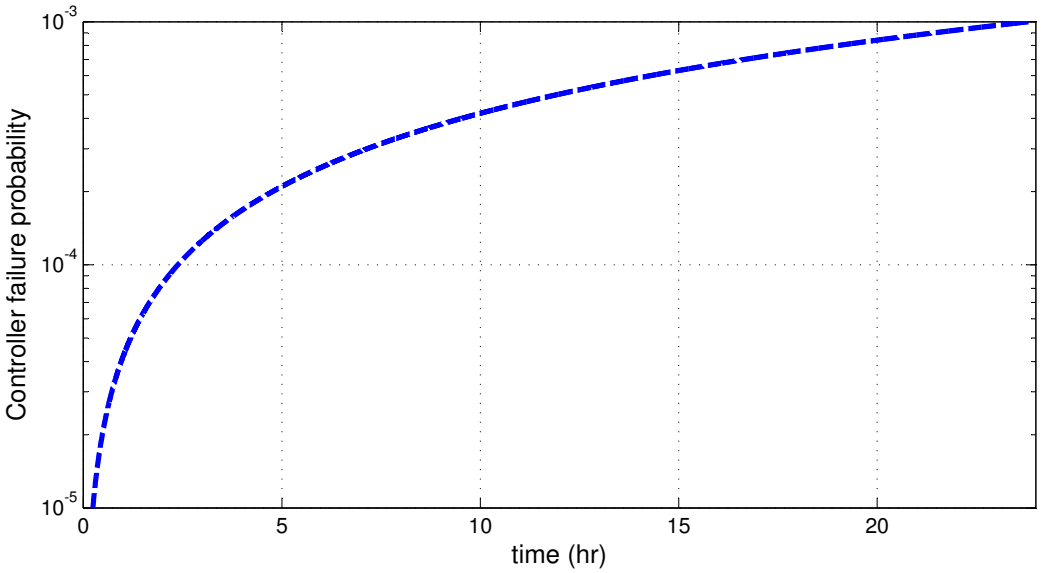

Figure 3: Controller failure probability.

other states. Out of a year, the operational mission time of the DFWCS is assumed to be 11 months allowing for one month of outage time (Aldemir et al., 2007). For PRA purposes, the usual (default) reference time period is 24h (Aldemir et al., 2010). Hence, in this paper, time scale for all the plots is 24h beginning at time zero assuming a system reset.

Figure 4 plots the probability of being in states 2, 4 and 5. The state probability of a high or an arbitrary output is the same owing to the same failure rate shared by the respective transitions from the state of correct output. The failure rate of a low output from correct output is lower than that of a high or an arbitrary output. Correspondingly, the state probabilities reflect the trend. However, comparing Figure 3 and 4 the probability of a controller failure is higher than being in any of the other states. This can be

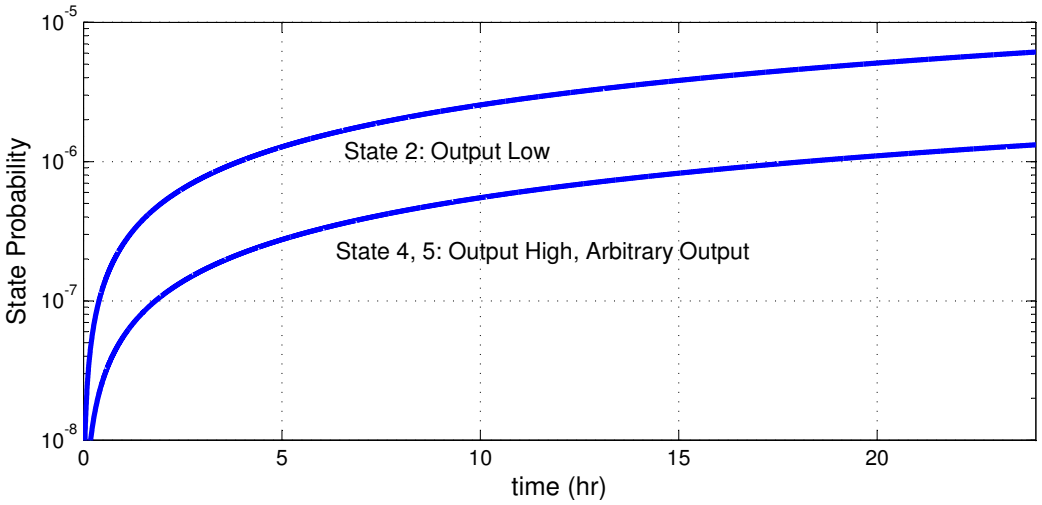

Figure 4: Probability of being in states 2,4 and 5.

attributed to the fact that state of previous output is an absorbing state and hence all transitions eventually end in this state.

A direct transition from correct to previous output has higher influence over the controller failure probability than that due to transiting through intermediate steps and reaching the previous output. This is due to relatively larger failure rate for the transition from correct to previous output when compared to the combined failure rates of the alternate paths.

3. Proposed Semi-Markov Process Model

3.1. Analysis

This paper follows the general formulation of the continuous-time discrete-state semi-Markov process model as developed by Howard (1964, 1971).

Let the model have N states. Let $f_{ij}(t)$ and $F_{ij}(t)$ represent the *pdf* and

cdf respectively of the event corresponding to the transition from state i to state j at time t.

Assume that the process is in state i. From this state, there could be k different states to which the process could transit to in a single step. These states could be completion of a repair, further degradation of the system or a failure mode with an underlying failure mechanism. Also assumed in this model is that all these k possibilities are independent of the occurrence of each other. At a time instant t, the process chooses only one state from these choices such that the time to be spent in the current state i is the minimum before instantaneously jumping to the chosen state. The probability that the next state is j and not any other state k reachable from i is given by:

$$c_{ij}(t) = f_{ij}(t) \prod_{k \neq j} (1 - F_{ik}(t)) \tag{2}$$

For N=2, $c_{ij}(t) = f_{ij}(t)$. The matrix $C(t) = [c_{ij}(t)]$ is called the kernel or core of the semi-Markov process model and

$$w_i(t) = \sum_{j=1}^{N} c_{ij}(t) \tag{3}$$

is called the waiting time distribution for the state i. It represents the probability that the system waits in state i for t time units before making a transition. Hence it is an unconditional probability distribution. It is assumed

that any row i of the kernel $C = [c_{ij}]$ satisfies the condition:

$$\int_0^\infty \sum_j c_{ij}(t)dt \approx 1 \tag{4}$$

This assumption assures that there is unit probability that the system will be in one of the N states of the system at time t, given the initial state as i. The probability that the system does not leave state i by time t is given by:

$$W_i(t) = 1 - \int_0^t w_i(t)dt \tag{5}$$

The objective of the model is to determine the probability $\phi_{ij}(t)$ of being in each state j given that the system initially is in a particular state i. $\phi_{ij}(t)$ can be determined by solving a system of integral equations:

$$\phi_{ij}(t) = \delta_{ij}W_i(t) + \sum_k \int_0^t c_{ik}(\tau)\phi_{kj}(t-\tau)d\tau \tag{6}$$

Where $i = j = k = 0, 1, 2, ...N - 1$.

The right hand side of Equation 6 describes the following probabilities:

1. $i = j$ and second term=0: $W_i(t)$ is the probability that the process does not leave state i by time t.
2. $i = j$ and second term not 0: process leaves state i and returns to i by time t.
3. $i \neq j$ and second term $\neq j$: process leaves state i and reaches state j

by time t.

The system of equations can alternatively be written in a compact form as a matrix:

$$\phi(t) = diag(W(t)) + \int_0^t C(\tau)\phi(t-\tau)d\tau \tag{7}$$

Given that the system started its operation in state i and that state j is the only absorbing state, the failure probability of the system is given by $\phi_{ij}(t)$ and reliability $R(t) = \phi_{ij}(t)$. For the feedwater valve controller system $i = 1$ and $j = 3$.

3.2. Mission Reliability

Let the time to failure T of the system be a random variable. Assume that the system was reliable until its age t_b *i.e.*, $T > t_b$. The probability that the system is able to further complete a mission duration of t_m successfully is conditioned on the present age of the system and is called the mission reliability (Kumar, 2000):

$$MR(t_b, t_m) = \frac{R(t_b + t_m)}{R(t_b)} \tag{8}$$

where $R(t_b) = \phi_{13}(t_b)$ is the reliability function. For plotting, the mission unreliability $1 - MR(t_b, t_m)$ is a convenient choice. Note that if distribution of T is exponential, $MR(t_b, t_m) = R(t_m)$.

3.3. Semi-Markov model for digital feedwater valve controller

The time to any of the events in the model are subject to certain amount of variability. Though hard to determine and establish the variability, this information can be of potential use to study its effect on the controller system's failure probability. In this paper, it is assumed that the time-to-previous output from the state of correct output follows a Weibull distribution. A value between 0 and 1 is assumed for the coefficient of variation (cov). The rest of the transition densities are assumed to follow an exponential distribution with the mean transition rates as listed in Table 1. Let the probability density function of a transition from state i to state j be represented by $f_{ij}(t)$, the distribution function be $F_{ij}(t)$. Let $R_{ij}(t) = 1 - F_{ij}(t)$. Then, the kernel $C(t)$ of the semi-Markov process for the controller system can be written using Equation 2,

$$\begin{bmatrix} 0 & f_{12}(t)\prod_{i=3,4,5} R_{1i}(t) & f_{13}(t)\prod_{i=2,4,5} R_{1i}(t) & f_{14}(t)\prod_{i=2,3,5} R_{1i}(t) & f_{15}(t)\prod_{i=2,3,4} R_{1i}(t) \\ 0 & 0 & f_{23}(t) & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & f_{43}(t) & 0 & 0 \\ 0 & 0 & f_{53}(t) & 0 & 0 \end{bmatrix} \tag{9}$$

The kernel matrix and the matrix $W(t)$ are sufficient to solve for state

probabilities. The probability of being in each of the states is computed by solving the system of integral equations in Equation 7 using the trapezoidal rule (Veeramany and Pandey, 2011b,a).

The transition rates rates for the Markov model (Aldemir et al., 2010) were a result of reducing the total number of states to five from a seven state model. These effective rates are used in the proposed model as a first hand approximation. Alternatively, state reduction techniques can be applied on a semi-Markov process model to determine the effective distribution parameters as explored by Veeramany and Pandey (2011a).

4. Results of semi-Markov process model

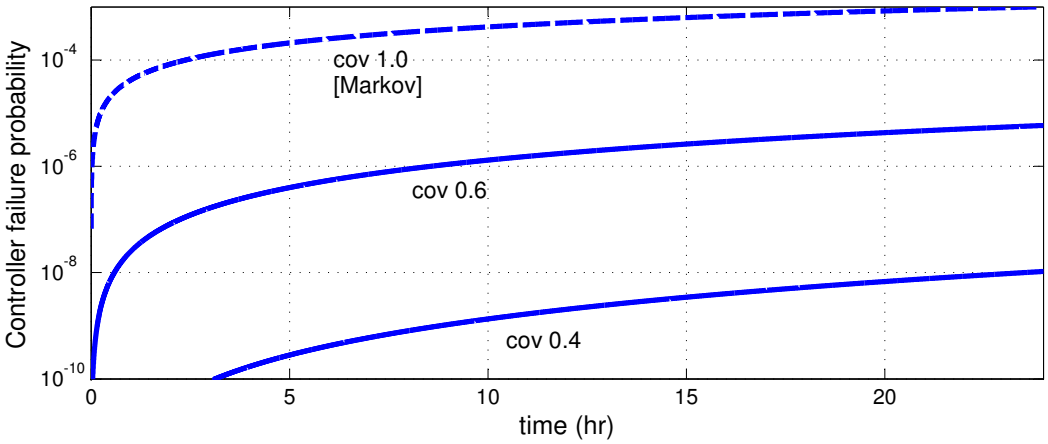

Figure 5: Controller system failure probability comparing variability in time to previous-output.

Figure 5 shows the controller failure probability for three cases of coefficient of variation: 1.0, 0.6 and 0.4. Recall that this variability corresponds to

time to the previous output from the state of correct output. Comparing the Figures 3 and 5, it can be seen that a cov of 1.0 reduces to the Markov case. On the other hand, lower the variability, lesser is the failure probability.

Table 2: Controller failure probability at the end of 24 hrs.

cov	Controller failure probability
1.0	1.0075 x 10^{-3}
0.6	5.88034 x 10^{-6}
0.4	1.05061 x 10^{-8}

The controller failure probabilities at the end of 24 hrs are shown in Table 2 for each of the covs considered. It is seen that the failure probability increases to 1.0075 x 10^{-3} when the time-to-previous output is relaxed to an assumption of exponential distribution, whereas if the actual cov had been 0.4, the probability is seen to be as low as 1.05061 x 10^{-8}.

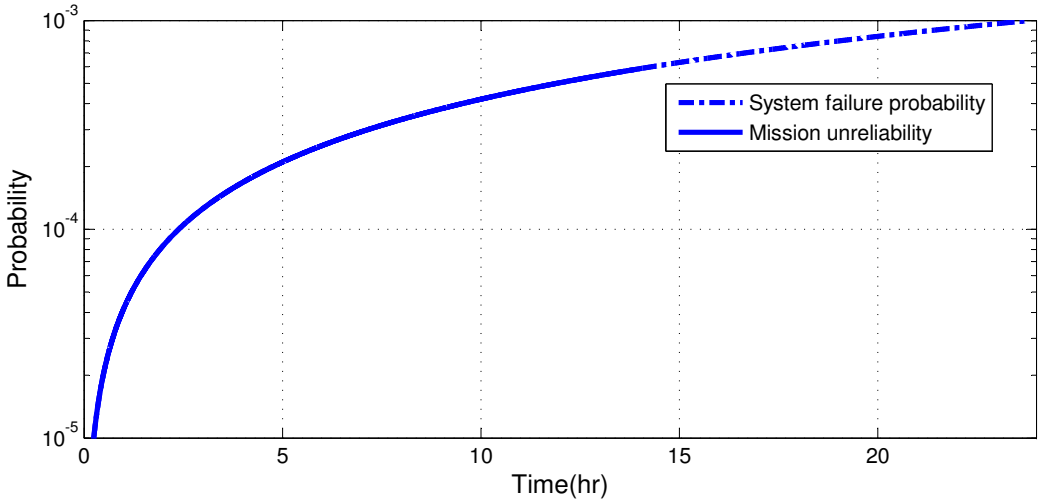

Figure 6: Controller system mission unreliability for additional 14 hrs given that the system was reliable for the initial 10 hrs [*cov*=1].

Since a digital I&C system is a combination of hardware and software systems, it is prone to aging. Nuclear power plant systems are so highly sophisticated that certain maintenance activities could be carried out even without planned outages. Under these circumstances, continuous execution of software embedded in hardware (firmware) could exhibit software aging due to performance degradation, numerical error accumulation and unexpected crashes (Laird and Brennan, 2006). Moreover, mechanical movement of the feedwater valve in response to controller commands could go out of control.

In an intuitive sense, the failure probability of an aging system at the present moment is very low given that the system was reliable until now. Overtime, failure probability of such a system is likely to be larger than that of a newly installed system due to increased risks of wear and tear. However both these quantities remain the same if the failure time of a system is assumed to follow an exponential distribution. This inability to take aging in to account is a result of the memoryless property of the exponential distribution as seen by comparing the system failure probability and the mission unreliability of the MFV controller with $cov = 1$ in Figure 6.

Assuming a $cov = 0.6$ for the variability in the time to previous output, Figure 7 shows that mission unreliability of a system that survived 10 hrs is indeed larger than the system failure probability of a newly installed system.

Apart from the main feedwater regulating valve (MFV) controller, the digital feedwater controller system (DFWCS) is connected to a feedwater

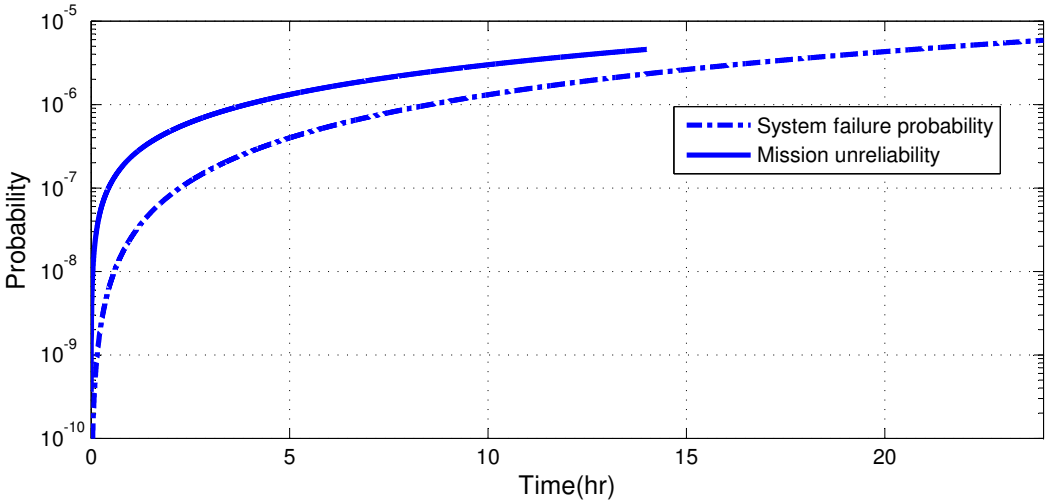

Figure 7: Controller system mission unreliability for additional 14 hrs given that the system was reliable for the initial 10 hrs [cov=0.6].

pump (FP) and its controller, a bypass feedwater valve (BFV) and its controller, a main computer and its backup and a pressure drop indicator (PDI) controller. A critical application in the nuclear plant reliability analysis is the probabilistic assessment of the entire digital controller system. NUREG-CR/6942 proposed Markov models for each of MFV, computer and the PDI systems. The MFV, BFV and the FP share the same model used in this paper. Hence, a larger application of semi-Markov process model would be to integrate the reliability models of the above said systems in to a single model for the digital feedwater controller system.

5. Conclusion

The main feedwater valve controller system used to regulate water level in a nuclear power plant steam generator is a critical digital instrumenta-

tion and control system of interest. A Markov model developed based on NUREG-CR/6942 was extended to a semi-Markov model so that Weibull distribution could be assumed for the time-to-previous output from a correct output instead of an exponential distribution. The advantage of this approach is the ability to incorporate software and hardware aging in to the reliability model. The benefits have been demonstrated in this paper through time dependent system failure probability and mission unreliability results of the feedwater valve controller system. Better predictability of controller system reliability has a direct impact on probabilistic risk analysis of the entire Digital Feedwater Controller System (DFWCS).

References

Al-Dabbagh, A. W., Lu, L., 2010. Reliability modeling of networked control systems using dynamic flowgraph methodology. Reliability Engineering & System Safety 95 (11), 1202 – 1209.

Aldemir, T., Guarro, S., Mandelli, D., Kirschenbaum, J., Mangan, L., Bucci, P., Yau, M., Ekici, E., Miller, D., Sun, X., Arndt, S., 2010. Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. Reliability Engineering & System Safety 95 (10), 1011 – 1039.

Aldemir, T., Miller, D., Stovsky, M., Kirschenbaum, J., Bucci, P., Fentiman, A. W., Mangan, L., 2006. NUREG/CR-6901: Current state of reliability

modeling methodologies for digital Systems and their acceptance criteria for Nuclear power plant assessments. Tech. rep., Washington, DC, US Nuclear Regulatory Commission.

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

Chu, T., Martinez-Gurdi, G., Kuritzky, A., Amri, A., 2010a. International experience with modeling digital systems in psas. In: Proc. of the 10th International Probabilistic Safety Assessment & Management Conference. Seattle, Washington, USA.

Howard, R. A., 1964. System analysis of semi-markov processes(systems analysis of semimarkov processes, expressing results in form of matrix flow graph). IEEE transactions on military electronics 8, 114.

Howard, R. A., 1971. Dynamic Probabilistic Systems, vol. 1: Markov Models. John Wiley and Sons, Inc., New York, USA.

Kleyner, A., Volovoi, V., 2010. Application of petri nets to reliability prediction of occupant safety systems with partial detection and repair. Reliability Engineering & System Safety 95 (6), 606 – 613.

Kumar, D., 2000. Reliability maintenance and logistic support: a life cycle approach. Springer, New York, U.S.A.

Laird, L. M., Brennan, M. C., 2006. Software measurement and estimation: a practical approach. John Wiley and Sons, NJ, U.S.A.

Lisnianski, A., Levitin, G., 2003. Multi-state System Reliability: Assessment, Optimization and Applications. World Scientific, Singapore.

Rao, K. D., Gopika, V., Rao, V. S., Kushwaha, H., Verma, A., Srividya, A., 2009. Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment. Reliability Engineering & System Safety 94 (4), 872 – 883.

Shi, L., Enzinna, R., Yang, S., Blodgett, S., 2010. Probabilistic risk assessments of digital i&c in nuclear power plant. In: Proc. of the 10th International Probabilistic Safety Assessment & Management Conference. Seattle, Washington, USA.

Veeramany, A., Pandey, M. D., 2011a. Reliability analysis of nuclear component cooling water system using semi-markov process model. Nuclear Engineering and Design. To appear, DOI: 10.1016/j.nucengdes.2011.01.040.

Veeramany, A., Pandey, M. D., 2011b. Reliability analysis of nuclear piping system using semi-markov process model. Annals of Nuclear Energy. In Press, Corrected Proof, DOI: 10.1016/j.anucene.2010.12.012.

Vineyard, M., Amoako-Gyampah, K., Meredith, J. R., 1999. Failure rate distributions for flexible manufacturing systems: An empirical study. European Journal of Operational Research 116 (1), 139 – 155.

Yau, M., Guarro, S., Apostolakis, G., 1995. Demonstration of the dynamic flowgraph methodology using the titan ii space launch vehicle digital flight control system. Reliability Engineering & System Safety 49 (3), 335–353.