Modeling of Communications in the Safety Assessment of Nuclear Power Plants

D. Mandelli*, J. Kirschenbaum+, L. A. Mangan*, E. Ekici#, T. Aldemir*

*Nuclear Engineering Graduate Program
+Department of Computer Science and Engineering
#Department of Electrical and Computer Engineering
The Ohio State University, Columbus, OH 43210

INTRODUCTION

Nuclear power plants (NPPs) are in the process of replacing and upgrading aging and obsolete instrumentation and control (I&C) systems with digital ones. Moreover, the next generation of NPPs will rely on digital systems for monitoring and control purposes.

Communication between controller components is an important characteristic of digital I&C systems. Clearly, permanent or temporary failures in the communication components of an I&C system may induce unexpected consequences for NPP. Several of these failures have been observed in the nuclear industry so far [1, 2]. In particular, [1] shows how an overload of the communication network due to the malfunction of a non safety related system can induce malfunctions on a safety related system that is sharing the same network.

In this paper, the importance of communication systems in the safety assessment of NPPs that rely on digital I&C is illustrated. The following sections introduce the dominant key factors in the modeling of digital communication systems and how they can affect the dynamics of digital I&C using a digital feedwater control system of a pressurized water reactor (PWR) as an example.

DIGITAL COMMUNICATION MODELING

Communication systems (CS) consist of transmission lines, transceiver hardware, and protocol stacks. Error-free operation of individual parts is not a sufficient condition for the error-free operation of the system. While some errors during transmission can be masked and recovered by protocols, excessive load on CS can incur large delays and render sent messages useless for applications using the CS.

Success of a CS can be measured in delay, error rate, and throughput metrics. In addition to errors, traffic load offered to CS plays an important role on timely delivery of messages. Modeling a CS does not only involve the reliability modeling of hardware components, but also modeling of protocols and their behavior under different load and error conditions.

The process of modeling a CS involves the identification of information paths, the characterization of information generators and their relations, and an understanding of selected metrics. Protocol modeling for different CS types is an active field of research for communication and networking community [3, 4, 5]. Less attention is paid to modeling of systems with non-uniform traffic load sources and incorporation of hardware/ software (HW/SW) failures. Safety assessments of NPPs will undoubtedly benefit from existing work in this area while motivating further research to incorporate constraints of real-life systems.

SYSTEM DESCRIPTION

The system under consideration is based on the digital feedwater control system (DFWCS) for an operating PWR [6] (see Fig.1).

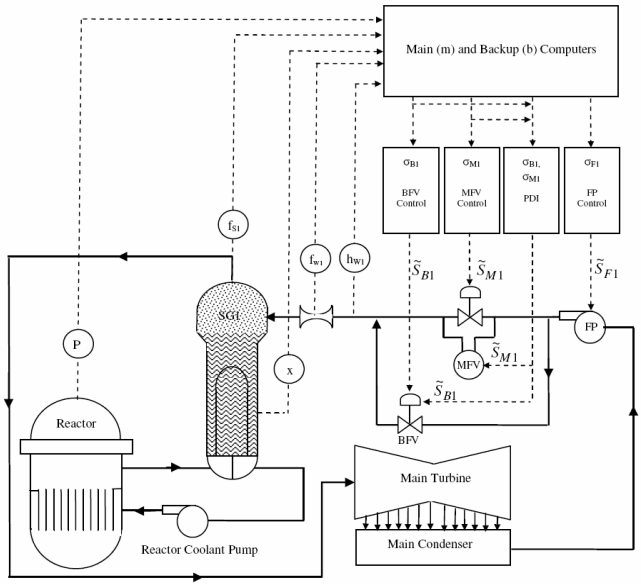

Fig.1. Connection scheme of the DFWCS components from [6]

The purpose of the DFWCS is to maintain the water level inside the steam generator (SG) optimally within ± 2 inches of the setpoint level (defined at 0 inches). The DFWCS fails low if the water level is less than -24 in and fails high if the level is higher than +30 in. As shown in Fig.1, the DFWCS 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 SG to maintain a constant water level in the SG.

The DFWCS is comprised of several components (see Fig.1) 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 controllers. Each of these controllers forward the MC or BC's outputs to their respective controlled device (MFV, BFV or FP), or it can maintain the previous output to that device if the computers fail.

SYSTEM ANALYSIS

Our analysis focuses on the effect of communication load on a simple, dedicated CS between the MFV controller and the MFV consisting of one transmitter, one receiver, and a communication link. For the sake of illustration, we assume that the delay is only a function of the queuing at the controller side and ignore propagation and processing delays. We also ignore all transmission errors to solely focus on the effect of communication load on reliability of the entire DFWCS.

This simple communication system can be modeled as a single server infinite capacity queue system [7]. As the average load offered to the CS increases, the average packet delay increases as 1/(C-L) under M/M/1 queuing model [7], where L is the offered load in packets/sec and C is the capacity of the communication link in packets/sec Under M/M/1 model, packet arrivals follow a Poisson process and the service times are independently and identically distributed following an exponential distribution. Since packets are buffered until all packets ahead of them are transmitted, packets may suffer long delays that render them unusable due to old age. Therefore, packet delay exhibits a probabilistic behavior rather than a deterministic one.

We utilize a transfer function that maps the normalized offered load to the probability of packets being discarded due to excessive delay. This function is generated based on the cutoff delay threshold to decide packet dropping events. Under this model, each packet is discarded (or lost) independently with a given probability, which is a function of the offered load. Such a sample function is depicted in Fig. 2. In this figure, the normalized offered load L/C is shown on the x axis.

We analyze the effect of the load on the CS on the DFWCS failure probability (failing either high or low). As the network load increases, packets that control the operation of MFV are dropped with increasing probabilities. It is assumed that no other failures occur in any part of the system throughout the simulation time.

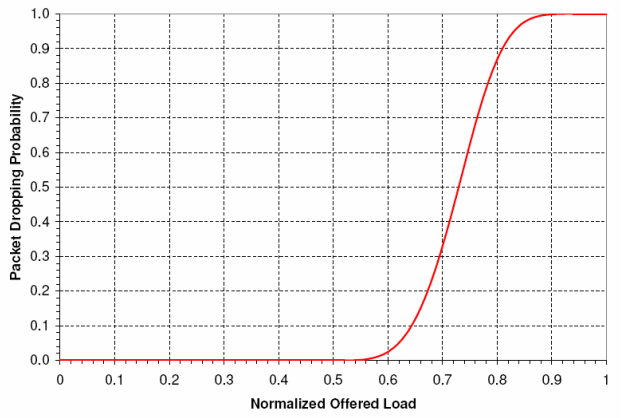

Fig. 2 Function that maps normalized load to packet dropping probability due to excessive delay

Figure 3 depicts the average DFWCS failure probability as a function of normalized load on CS, where each data point is the average of 100 independent simulations. A clear transition in failure state is observed around 0.819 normalized load. While loads below this point are well-tolerated and almost no failures occur, almost any load beyond this transition point results in failure. Note that this transition occurs at roughly 0.93 packet dropping probability, indicating that the control system is resilient to packet losses in general. This behavior is achieved by maintaining the previous set point if no feedback is received. However, it cannot completely prevent system failures if the majority of the packets are dropped due to excessive delay.

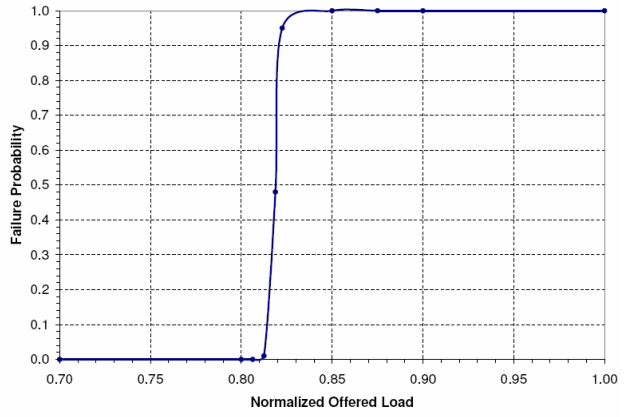

Fig. 3 Failure probability of DFWCS as a function of normalized load on CS

DISCUSSION AND CONCLUSION

The illustrative example presented in this paper serves as a motivation for further research on modeling of CS and incorporation of such models into safety

assessment of digital I&C systems. We have illustrated that it is possible for a digital I&C system to fail without any failure of components, simply due to load offered to a CS. We emphasize that even dedicated communication systems are not immune to this type of failures.

In shared CS, such as the one used in [1], such events are anticipated to occur even more frequently: loads offered by other devices connected to the CS would increase packet latency and reduce packet delivery probability due to collisions in the network. It is clear that detailed CS models encompassing hardware and protocol issues must be developed.

Incorporation of these models into safety assessment models also present unique challenges. Existing CS models are rather complex in nature, and do not lend themselves well to being used as part of larger models. Development of scalable models for systems more complex than the one presented here is an open research problem and an outstanding challenge.

To the best of our knowledge, detailed CS modeling has not been considered in any of the existing literature on safety assessment. Furthermore, the fact that CS systems and models provide non-deterministic performance measures by nature bolsters our argument for dynamic reliability modeling for digital I&C systems [6]. Development of general and system-specific communication models, complexity reduction methods, and automated analysis of digital I&C systems are among our future research directions.

REFERENCES

1. NRC INFORMATION NOTICE: 2007-15: “Effects of Ethernet-Based, non-safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations”, April 17, 2007.
2. NRC INFORMATION NOTICE 92-33: Increased Instrument Response Time When Pressure Dampening Devices are Installed, April 30, 1992.
3. G. BIANCHI, “Performance Analysis of the IEEE 802.11 Distributed Coordination Function”, IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, pp. 535-547 (2000)
4. J.W. ROBINSON, and T.S. RANDHAWA, “Saturation Throughput Analysis of IEEE 802.11e Enhanced Distributed Coordination Function”, IEEE Journal on Selected Areas in Communications, vol. 22, no. 5, pp. 917-928 (2004)
5. G. KORKMAZ, E. EKICI, and F. OZGUNER, “A Cross-Layer Multi-hop Data Delivery Protocol with Fairness Guarantees for Vehicular Networks”, IEEE Transactions on Vehicular Technology, vol. 55, no. 3, pp. 865-875 (2006)
6. T. ALDEMIR, P. BUCCI, M. P. STOVSKY, J. KIRSCHENBAUM, X. SUN, D. MANDELLI, L. A. MANGAN, D. W. MILLER, 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. NRC, Washington, D.C. (2007)
7. L. KLEINROCK: “Queuing Systems: Volume I – Theory”, Wiley Interscience, New York (1975)