Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 25-26, 2012

An Approach to Evaluate the Network Communication Reliability

Hee Eun Kim, Bo Gyung Kim, Hyun Gook Kang*
Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology,
373-1 Guseong-dong,Yuseong-gu, Daejeon 305-701, South Korea
*Corresponding author: hyungook@kaist.ac.kr

1. Introduction

Digital I&C systems usually generate a large amount of data which need to be transmitted to other systems. The use of signal transmission components can be reduced by using network communications. Nowadays, nuclear power plants (NPPs) extensively depend on networked communications to transmit data within and among various control and safety systems [1]. However, errors in communications might lead to unsafe state or hazardous state of system. Kang et al. [2] also pointed out issues related to modeling the network communication failure. In this study, only the networked communications between safety-related equipment will be considered.

2. Safety network communications in NPP

A safety critical network is highly reliable network which aims to be used in the safety critical system. In this section, brief description and general model of network communications in NPP will be provided.

2.1. Communication networking abstractions

Network communications functions are decomposed to several groups, and implemented separately. The Open Systems Interconnection (OSI) reference model standardizes the functions in terms of abstraction layers. In this model, many communication protocols are used as layered protocols where each layer gives a service to the protocol of the layers above and requires service from layers below. With the data at the application layer, headers are added as the data is passed down the stack. In the end, the packet is packaged as a frame at the data link layer and then transmitted to the media when access is available. At the peer end, the headers are stripped until the data reaches the application layer, assuming there are no errors along the way [3].

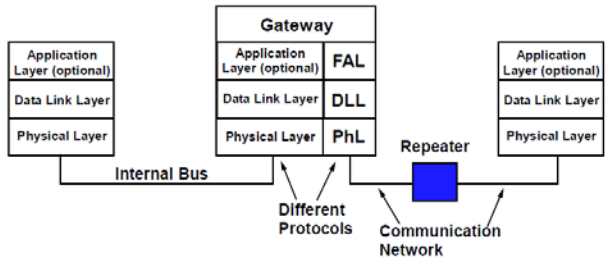

Fig. 1. Example of three-layer model applied to a safety system network.

However, it is typical that only layers one, two, and seven are utilized in safety critical, high integrity communications because these features may lower communication reliability and introduce unpredictable delays in sending messages between nodes [1]. The reduced layer model is shown in. Fig. 1.

2.2. Network failure

Communication networks are made up of nodes and links that connect the nodes by hardware as well as the software components that allow for the functionality to communicate through such networks [4]. Therefore, network failure is caused by defects in the hardware of the network modules or a fault in the network protocol, which is the basis of network software [2]. Fig. 2. shows common problems classified by OSI layer.

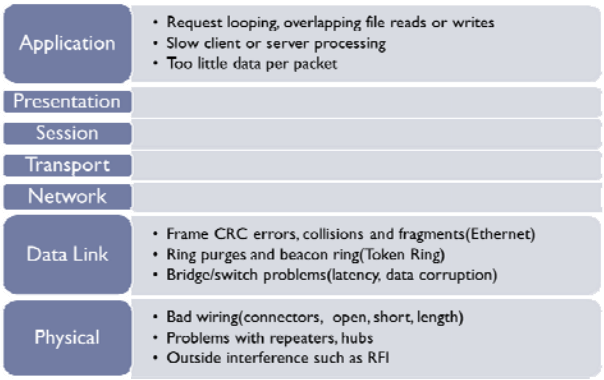

Fig. 2. Examples of networking problems classified by OSI layer [3].

3. Considerations on network failures

In general, the two main failure modes in communications are the loss of communication and the creation of erroneous information. Those failure modes can be divided further by the mechanisms of the communication errors and, the severity of the failure. In this study, the concept of severity includes the duration of the fault and the number of the influenced devices.

3.1. Failure types

The errors are divided into three categories according to whether the error is predominantly communication channel related, associated more with the transceiver (transmitter and receiver), or a result of network segmentation. The nonexhaustive list of communication error types for those categories has been compiled from

several sources [1]. If we assume that all those errors are hazardous that the signal couldn't be transmitted properly, the outturn of the system will be the same regardless of the error mechanism. However, transient faults and permanent faults need to be treated as different failure types, because some of the transient fault might be disappeared or have little effect on the system.

3.2. Failure path

It can be assumed that the function of each layer is independent of status of other layers, because each protocol layer solves distinct class of communication problems. Moreover, we can assume that if there is a hazardous and non-recoverable error, another fault in that layer does not have to be considered since the system is already on hazardous state. Then we can identify individual functional failure paths and model each functional process as a serial sequence.

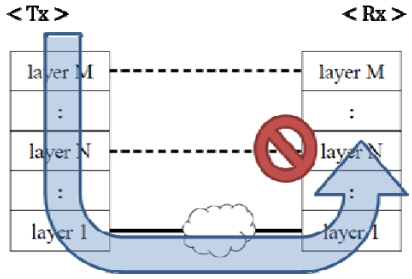

Fig. 3. Identification of specific failure path.

3.3. Consideration of common cause failure

One of the main concerns in analyzing the communication failure is a common cause failure mechanism. Typical sources of common cause failures are power supply, electromagnetic field, physical catastrophe, design errors, human training, and operating procedures [1]. If we assume that all the errors are hazardous mentioned as above, faults can be treated in the same way even though fault mechanisms are different. Then we can categorize the common cause failures according to the number of the influenced devices.

4. Reliability evaluation method

4.1. Evaluation of failure path

If individual functional failure paths are identified, each probability of fault should be provided. Then the probability of each path can be calculated as

$$1-q_i=(1-p_1)\times(1-p_2)\times\cdots\times(1-p_j)\times\cdots\times(1-p_m) \quad (1)$$

where q_i is the probability that the specific failure path i will not be occurred and p_j is the probability that there is no specific fault in jth layer. It is desirable that the probability that dependent failures caused by CCF is included in the p_j.

4.2. Further considerations

Other aspects which can affect the reliability of the system should be considered to establish realistic model. For example, a safety system's network topology can increase reliability of the network, because it can include redundant, even diverse links to provide fault tolerance, fault detection, and fault removal features. Furthermore, it is desirable that the propagation of failures through communication devices and their effects on the related components or systems are evaluated [5] with regard to the message data types relevant to safety applications.

5. Conclusions

To assess the probability that a system becomes unsafe due to a network failure, network errors should be analyzed first. In this study, some criteria to categorize the errors were suggested. If we can identify the failure path, each path could be modeled in connection with other network aspects, so the reliability of the system can be quantitatively evaluated.

REFERENCES

[1] R. Kisner et al., Design Practices for Communications and Workstations in Highly Integrated Control Rooms, NUREG/CR-6991, 2009.
[2] H.G. Kang et al., An Overview of Risk Quantification Issues for Digitalized Nuclear Power Plants using a Static Fault Tree, Nuclear Engineering and Technology, Vol. 41, No. 6, pp. 849-858, 2009.
[3] J.S. Haugdahl, Network Analysis and Trouble shooting, Addison Wesley, 2000.
[4] Medhi, D. "Network Reliability and Fault-Tolerance", Wiley Encyclopedia of Computer Science and Engineering, 2007.
[5] T.L. Chu et al., Traditional Probabilistic Risk Assessment Methods for Digital Systems, NUREG/CR-6962, 2008.
[6] G.G. Preckshot, Data Communications, NUREG/CR-6082, 1993.
[7] Authen et al., Reliability Analysis of Digital Systems in a Probabilistic Risk Analysis for Nuclear Power Plants, Nuclear Engineering and Technology, Vol. 44, No. 5, pp. 471-482, 2012.