디지털 원자로보호계통 불가용도 평가

An Unavailability Evaluation for a Digital Reactor Protection System

이동영, 최종균(한국원자력연구소), 김지영, 유준(충남대학교)

Abstract - The Reactor Protection System (RPS) is a very important system in a nuclear power plant because the system shuts down the reactor to maintain the reactor core integrity and the reactor coolant system pressure boundary if the plant conditions approach the specified safety limits. This paper describes the unavailability assessment of a digital reactor protection system using the fault tree analysis technique. The fault tree technique can be expressed in terms of combinations of the basic event failures. In this paper, a prediction method of the hardware failure rate is suggested for a digital reactor protection system, and applied to the reactor protection system being developed in Korea.

Key Words :failure rate, fault tree analysis, failure mode effect analysis, reliability, safety

1. Introduction

The Reactor Protection System (RPS) is designed according to the redundancy criteria to assure the safe operation. The RPS usually adopts the *2*-out-of-*3* or the *2*-out-of-*4* architecture to prevent a single failure. The *2*-out-of-*4* RPS system consists of four channels, and each channel is implemented with the same architecture using Programmable Logic Control (PLC). The adequacy of the RPS architecture is determined according to the unavailability assessment result performed during the design phase. Fault Tree Analysis (FTA) model is used for the unavailability assessment. The FTA model presents the failure events in a deductive manner, and provides a visual display to the designer of how the system can generate malfunction [1]. The basic events of the FTA model consist of the random hardware failures, common cause failure mechanisms, operator errors, and so forth. The quantitative unavailability of the RPS can be evaluated according to the combination probability of the basic events in the FTA model.

A random hardware failure event is one of the basic events in the FTA model and can be obtained from the generic failure data sources such as a military standard. The military handbook MIL-HDBK-217F [2] has been used for the failure rate prediction in the nuclear power industry. The conventional procedure to determine the failure rate in this handbook is to sum of the individually calculated failure rates for each component included in the PLC. This procedure may be adequate for an analog based system, but not for a digital based system such as the PLC. The diagnostic functions implemented in the PLC can detect failures occurrence immediately. Then the RPS automatically generates the channel trip signal according to the fail safe requirement. As a result, the failures which happen in the PLC may not affect the RPS safety if the diagnostic function operates correctly. Therefore, a proper method for predicting the random failure rate of a digital system is required. In this paper, a prediction method of the random hardware failure rate is suggested for the PLC having the diagnosis functions. Failure Mode and Effect Analysis (FMEA) [1] method is used to analyze the diagnosis functions of the PLC and the unsafe failures of the components.

2. Unavailability Assessment

The probability for the conventional analog/mechanical components failure, the digital components failure, the operator errors, and the common cause failure are required to perform a quantitative unavailability assessment. The failure data of the conventional analog/mechanical components are provided by references [3]. This data is derived from the operating experience during the period of 1995 through to 2000 in the Ulchin 3&4 and Yonggwang 3&4 nuclear power plants. The experience failure data for the PLC components are not available because the PLC is under development. Therefore, the part stress method proposed in the MIL-HDBK-217F is applied to predict the failure rate of each component in the PLC.

2.1 Conventional Failure Rate Model

The conventional PLC failure rate has been predicted by the sum of the individual failure rates for all the components included in the PLC as follows [2] :

$$\lambda_{Conventional} = \sum_{i=1}^{n} \lambda_i \ Failures/10^6 Hours \qquad (1)$$

The unavailability of the module is as follows:

$$Q_{Conventional} = \lambda_{Conventional} * \frac{T}{2} \qquad (2)$$

where, T : the periodic test interval in hours.

2.2 Proposed Failure Rate Model

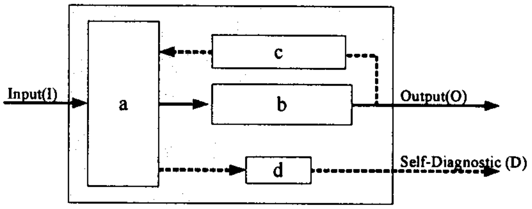

Fig. 1. Functional block diagram of a typical digital hardware module.

Fig. 1 shows the functional block diagram of a typical digital hardware module. The components of the hardware module can be categorized into 4 sub-function groups according to their functions as follows:

i) The components in ***a*** group receive input signals and transform them adequately, and transfer the transformed signal to ***b*** group. This group also compares the transformed signal with the feedback signal from the external module. The comparison between these two signals is used for the loop-back test, and generates an error signal to the external module and the operator through ***d*** group whenever a deviation happens between these two signals.

ii) The transmitted signal from ***a*** group is processed in ***b*** group. The components in this group provide the final output to the external module and also provide the feedback signal to ***c*** group.

iii) The components in ***c*** group transform the final output for the loop-back test. The transformed final output is given to ***a*** group for a comparison.

iv) The components in ***d*** group transport the error signal to the external module or operator to alert them that failures happened in the module.

If there is no failure in the module, all the sub-function groups perform their allotted functions correctly. The PLC module performs its mission successfully, and the module is in the success state. If the ***b*** sub-function group is failed and the other sub-function groups operate properly, the module doesn't make the final output to the external module and the module comes to a failure state. But the module immediately generates the error alarm signal to the external module because the self-diagnostic function operates correctly by a loop-back test in the ***a*** sub-function group. After an error alarm signal, the operator changes the RPS operation mode from the *2*-out-of-*4* to the *2*-out-of-*3*, and starts the maintenance activities immediately. Therefore, the failure case of only the ***b*** sub-function group is in a so-called safe failure state. If the ***a*** sub-function group is failed, the module doesn't make the transformed signal for the ***b*** sub-function group. Also the module doesn't conduct the loop-back test. As a result, the module comes to a failure status. Therefore the failure case of the ***a*** sub-function group is in a so-called dangerous failure state. If all the groups are failed, the module is in a dangerous failure state.

Table 1 shows the failure status of a typical digital hardware module. The first column of the table represents the failure combination for each sub-function group. '0' indicates the failure status of the allotted sub-function group and '1' indicates the successful operation status of the given sub-function group. The second and third columns indicate the output status and the diagnostic status, respectively.

Table 1. Failure status of a typical digital hardware module.

Failure Combination (abcd)	Output Status	Diagnostic Status	Module Failure
1111	1	1	S
0111	0	0	DF
1011	0	1	SF
1101	1	0	S
1110	1	0	S
0011	0	0	DF
0101	0	0	DF
0110	0	0	DF
1001	0	0	DF
1010	0	0	DF
1100	1	0	S
0001	0	0	DF
0010	0	0	DF
0100	0	0	DF
1000	0	0	DF
0000	0	0	DF

The fourth column represents the failure status of the module according to the combination of each sub-function group failure. The S, DF, and SF represent the Success, Dangerous Failure, and Safe Failure state, respectively. Only the Dangerous Failure state affects the RPS safety directly. As shown in Table 1, the dangerous failures of the module can be summed as follows:

$$\begin{aligned}\text{DF State} &= \bar{A}BCD + \bar{A}\bar{B}CD + \bar{A}B\bar{C}D + \bar{A}BC\bar{D} + A\bar{B}\bar{C}D \\ &\quad + A\bar{B}C\bar{D} + \bar{A}\bar{B}\bar{C}D + \bar{A}\bar{B}C\bar{D} + \bar{A}B\bar{C}\bar{D} + A\bar{B}\bar{C}\bar{D} + \bar{A}\bar{B}\bar{C}\bar{D} \\ &= \bar{A}CD(B+\bar{B}) + \bar{A}\bar{C}D(B+\bar{B}) + \bar{A}C\bar{D}(B+\bar{B}) \\ &\quad + A\bar{B}\bar{C}(D+\bar{D}) + \bar{A}\bar{C}\bar{D}(B+\bar{B}) + A\bar{B}C\bar{D} \\ &= \bar{A}CD + \bar{A}\bar{C}D + \bar{A}C\bar{D} + A\bar{B}\bar{C} + \bar{A}\bar{C}\bar{D} + A\bar{B}C\bar{D} \\ &= \bar{A}D(C+\bar{C}) + \bar{A}\bar{D}(C+\bar{C}) + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\ &= \bar{A}D + \bar{A}\bar{D} + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\ &= \bar{A}(D+\bar{D}) + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\ &= \bar{A} + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\ &= \bar{A} + A\bar{B}(\bar{C}+\bar{D})\end{aligned} \tag{3}$$

The dangerous failure probability of the module can be written as:

$$\begin{aligned}P\{DF\ State\} &= P\{\bar{A} + A\bar{B}(\bar{C}+\bar{D})\} \\ &= P(\bar{A}) + P(A)P(\bar{B})P(\bar{C}) + P(A)P(\bar{B})P(\bar{D}) \approx P(\bar{A})\end{aligned} \tag{4}$$

Therefore, the dangerous failure rate of the module can be approximated by the failure rate of the ***a*** sub-function group as follows:

$$\lambda_m = \lambda_a \tag{5}$$

3. Result

The parameters for the component failure rate calculation are based on the applicable plant conditions. Suitable values of the above parameters are chosen for the perceived device specifications and the control room conditions. The ambient temperature of 40℃ is considered for the computation of the components failure rates. In addition, the operating condition is considered as ground benign. The Reliability Workbench environment is used to integrate the failure rates from each component into the PLC module. Table 2 shows the failure rates of the typical PLC modules.

Table 2. Failure rates for the PLC modules

Module Name	Failure rates (10^{-6} /hr)
CPU (+ Baseboard)	21.78
DC 24V Digital Input Module	1.33
Analog Input Module	13.6
DC 24V Digital Output Module	11.14
AC250V Relay Output Module	2.7

The components within the redundant PLC module are to be failed simultaneously on account of the common cause events such as a fire, electrical overload, sudden environmental changes, improper system operation or maintenance error. A common cause failure happening in the RPS prevents the proper safety action of the RPS when the plant conditions approach the specified safety limits. Therefore, a common cause failure of the RPS has a severe influence on the risk analysis of a nuclear power plant. The Beta-factor method is used for the common cause event [4].

Human errors are also an important factor for a safety analysis in a nuclear power plant particularly after the TMI accident. Two kinds of human errors are analyzed as basic events of the fault tree model. These errors are i) manual reactor trip error by an operator, ii) calibration errors of the trip parameters by the maintenance staff. In order to quantify the human error for a manual reactor trip, we should consider these factors, i) mission time to complete a task, ii) expected operator stress level, iii) the type of human-machine interface, etc. The human error related to a test and calibration can be quantified using the THERP methodology [5].

The unavailability assessment of the RPS is determined by combination of the individual failure probabilities for the basic events in the FTA model. For the selected trip parameter of the Low Steam Generator Level, the unavailabilityassessment result of the RPS is as follows:

• Mean Unavailability :	5.818794E-06
• 90 % Upper Bound :	1.8829E-05
• 95% Upper Bound :	2.26232E-05
• 99% Upper Bound :	2.9692E-05

참 고 문 헌

[1] ANSI/IEEE Std. 352, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, 1987.

[2] MIL-HDBK-217F, *Reliability Prediction of Electric Equipment*, 1991.

[3] KAERI/TR-2164/2002, *Reliability Study: KSNPP Reactor Protection System*, Korea Atomic Energy Research Institute, 2002.

[4] NUREG/CR-4780, Volume 1, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples*, NRC, 1988.

[5] NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application*, NRC, 1983.