A Safety Assessment Methodology for a Digital Reactor Protection System

Dong-Young Lee, Jong-Gyun Choi, and Joon Lyou*

Abstract: The main function of a reactor protection system is to maintain the reactor core integrity and the reactor coolant system pressure boundary. Generally, the reactor protection system adopts the 2-out-of-m redundant architecture to assure a reliable operation. This paper describes the safety 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 such as the random hardware failures, common cause failures, operator errors, and the fault tolerance mechanisms implemented in the reactor protection system. 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 to identify design weak points from a safety point of view.

Keywords: Failure rate, fault tree analysis, failure mode effect analysis, reliability, safety.

1. INTRODUCTION

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. To assure the safe operation of a reactor, the RPS is designed according to the redundancy criteria. The RPS usually adopts the *2*-out-of-*3* or the *2*-out-of-*4* architecture to prevent a single failure [1,2]. The *2*-out-of-*4* RPS system consists of four channels, and each channel is implemented with the same architecture. Fig. 1 shows the *2*-out-of-*4* RPS architecture being developed in Korea, and each channel is implemented with a Programmable Logic Controller (PLC). The adequacy of the RPS architecture is determined according to the safety assessment result performed during the design phase.

Manuscript received January 18, 2005; revised August 2, 2005; accepted October 8, 2005. Recommended by Editorial Board member Jietae Lee under the direction of Editor Keum-Shik Hong. This work was performed under the Mid- and Long-term Nuclear R&D Program sponsored by the Ministry of Science and Technology, Korea.

Dong-Young Lee and Jong-Gyun Choi are with the Instrumentation & Control - Human Factors Div., Korea Atomic Energy Research Institute, 150 Deogjin-dong, Yuseong-gu, Daejeon 305-353, Korea (e-mails: {dylee2, choijg}@kaeri.re.kr).

Joon Lyou is with the Dept. of Electrical and Computer Engineering, Chungnam National University, 220 Gung-dong, Yuseong-gu, Daejeon 305-764, Korea (e-mail: jlyou@cnu.ac.kr).

* Corresponding author.

The safety requirements for a nuclear power plant are a little different from the reliability. The reactor will be in an unsafe state when the RPS does not generate the reactor trip signal on demand. If the RPS is operating correctly, it can shut down the reactor anytime on demand. In this case, the reactor safety requirement is satisfied. If any failure happens in the RPS and it is detected by the system, the RPS automatically generates the channel trip signal according to the fail safe requirement of the RPS [3]. From a reliability point of view, the failed system must be unreliable. But from a safety point of view, the system is safe because it is designed conservatively so that the RPS automatically generates the channel trip signal for the failed channel If any unrecognized failure happens in the RPS, then the RPS can not shut down the reactor on demand. This case will not satisfy the reactor safety requirement, because the undetected failure may disturb the proper RPS operation [4]. As a result, the quantitative safety of a nuclear power plant is defined as the probability that the system operates correctly or fails in a safe manner.

Fault Tree Analysis (FTA) model is used for the safety assessment of the RPS. The FTA model presents the failure events in a deductive manner, and provides a visual display to the designer how the system can generate a malfunction [1,4]. The basic events of the FTA model consist of the random hardware failures, common cause failure mechanisms, operator errors, and so forth. The quantitative safety of the RPS can be evaluated according to the probability of the basic events in the FTA model.

A random hardware failure event is one of the basic

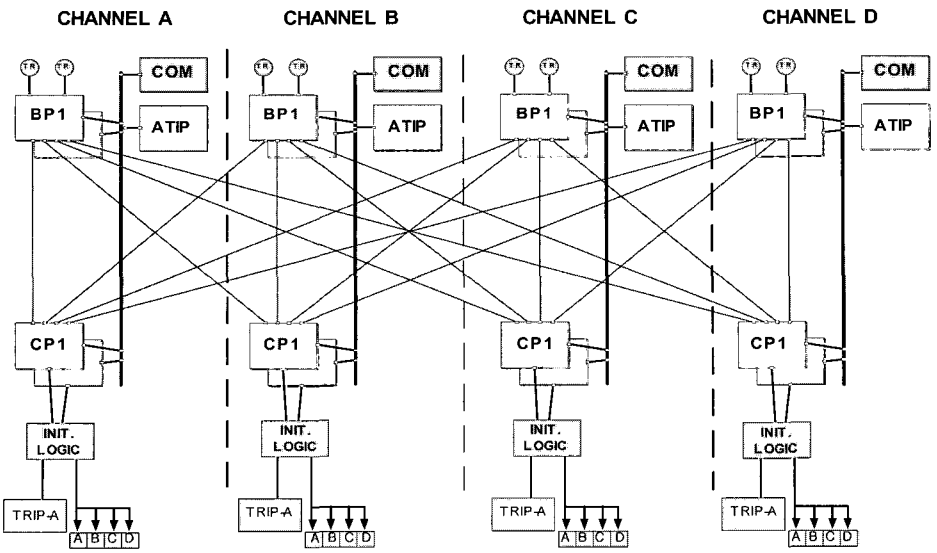


Fig. 1. The configuration of the *2*-out-of-*4* RPS.

events in the FTA model and can be obtained from the generic failure data sources such as a military standard because we have no field failure data based on plant operating experiences. The military handbook MIL-HDBK-217F [5] 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 module. 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 failure 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 new prediction method of the random hardware failure rate is suggested for the PLC having the diagnosis functions. Failure Mode and Effect Analysis (FMEA) [1,3] method is used to categorize the components according to their functions from the all components in the PLC.

In addition to the PLC failure rate, the common cause hardware failures and operator errors are used as the basic events of the FTA model for the safety assessment of the RPS being developed. The common cause failures are defined such that the components within the redundant PLC module are failed simultaneously whenever a fire, electrical overload, sudden environmental changes, improper system operation or maintenance error happen [1]. Also two types of operator errors are included in the FTA model, such as the calibration errors of the trip parameters and a manual trip error by the operator.

The FTA model is the well known safety assessment method in the nuclear power plant. The result of the safety assessment is used as a measure to determine whether the new developed PLC or RPS is applied to the nuclear power plant. So the FTA model must be represented according to the well-established procedures. Also the probability of the basic events for the FTA, such as common cause failure and operator errors, must be determined according to the well-established methodologies.

2. DEVELOPMENT OF THE REACTOR PROTECTION SYSTEM

The RPS being developed in Korea is designed with the *2*-out-of-*4* redundant architecture, and every channel is implemented with the same architecture.

A single channel of the RPS consists of the redundant Bi-stable Processor (BP), the redundant Coincidence Processor (CP), an Automatic Test & Interface Process (ATIP), and a Cabinet Operator Module (COM). The BP module generates a logic-level trip signal by continuously comparing the sensor inputs with the predefined trip set-points. The logic-level trip signals generated in the BP module of any channel are transferred to the CP modules of all the channels via the Safety Data Links (SDL). The CP module monitors the logic-level trip signals transferred from the four BP modules. When two or more logic-level trip signals from the BP channels are activated, the CP modules will activate the output signal for the reactor trip. The ATIP module monitors the operation status of the RPS, and conducts the surveillance test to ensure a reliable operation of the BP and the CP module in the same channel. The test results of the ATIP are transferred to the COM module

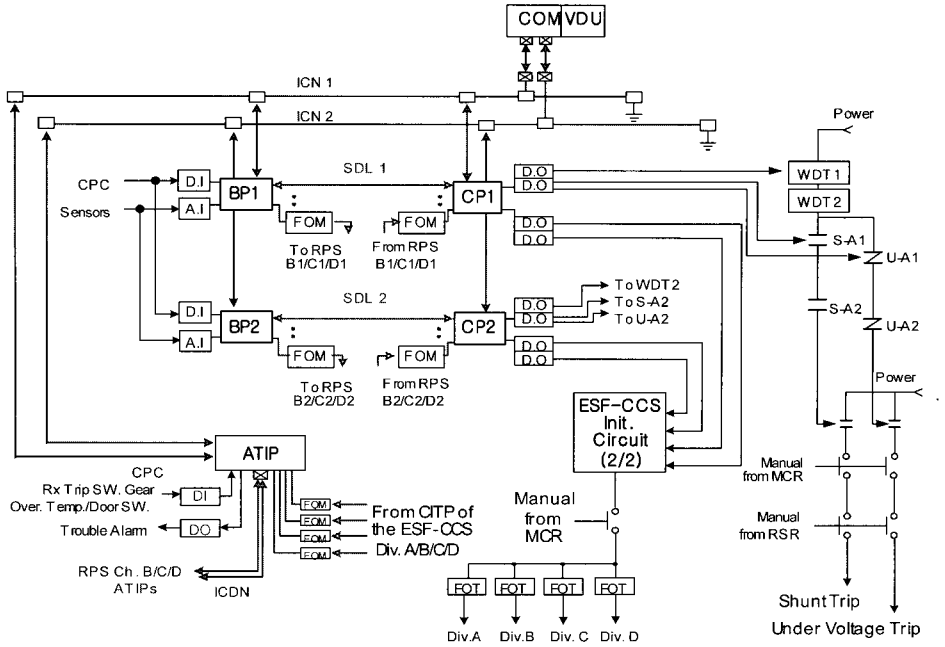


Fig. 2. The architecture of single RPS channel.

which has an operator interface facility implemented with an industrial PC and a flat panel display. The BP, CP, and ATIP modules of the RPS are implemented with the Programmable Logic Controller (PLC).

In addition to the BP, CP, ATIP, and COM, there is the Reactor Trip Switch Gear (RTSG) module in the RPS. The RTSG receives the reactor trip output signal from the CP, then interrupts the holding power of the control rod and causes a reactor shutdown whenever the plant conditions approach the specified safety limits. Fig. 2 shows the single channel architecture of the RPS. This RPS architecture is the most important factor for safety assessment of RPS, and will be used in the FTA model of Fig. 4.

3. SAFETY ASSESSMENT MODELING

The procedure to perform the safety analysis of the digital RPS encompasses the following steps: i) system familiarization, ii) Failure Mode and Effect Analysis, iii) qualitative fault tree modeling, iv) failure rate estimation of the hardware components v) modeling of common cause failures and operator errors, vi) fault tree analysis using a Monte-Carlo simulation [4].

The RPS fault tree model of Fig. 4 is developed for the failure case of the selected trip parameter, Low Steam Generator Level. The FTA includes the input sensor/transmitter, input modules, BP and CP, output modules, RTSG devices. But the failure of the ATIP or COM does not affect to the safe operation of the RPS, so the failure cases of the ATIP or COM are removed from the FTA model. The component failure, common cause failure, and an operator failure are also included in this analysis as basic events. The software failure should be considered in a fault tree model for analyzing a digital system. However, because of insufficient information, a software failure is not considered in this analysis.

The data 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 safety assessment. The failure data of the conventional analog/ mechanical components are provided by references [6]. 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. Because the PLC is under development, the experience failure data for the PLC components are not available. Therefore, the part stress method proposed in the MIL-HDBK-217F is applied to predict the failure rate of each component in the PLC. The common cause hardware failure data is obtained using the beta-factor method [6,7]. Also two types of operator errors are included in the fault tree model [6,8].

3.1. Digital hardware failure rate modeling

3.1.1 The conventional failure model

The hardware failure rate is one of the basic events in the FTA model. The conventional failure rate has been predicted by the sum of the individual failure rates for all the components included in the PLC as follows [1,5] :

$$\lambda_{Conservative} = \sum_{i} \lambda_{i,PLC} \,. \qquad (1)$$

The unavailability of the module is as follows [1,9]:

$$Q_{Conservative} = \lambda_{Conservative} \cdot \frac{T}{2}, \quad (2)$$

where T : the periodic surveillance test interval in hours

3.1.2 The proposed failure model

The conventional failure rate prediction model is a conservative method because the failures which are happened in the PLC modules may not affect the RPS safety if the diagnostic function operates correctly. To consider the effect of the diagnostic function implemented in the PLC, a new failure rate prediction model is proposed.

Fig. 3 shows the functional block diagram of a typical PLC module. The components of the PLC 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 through ***d*** group whenever a deviation happens between these two signals. The external module consists of the output buffer, tri-state, output connector or LED devices.

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. In case of Digital-to-Analog (DA) module, DA conversion is conducted in ***b*** group to give output signal to the external module. The analog signal in the ***b*** sub-function group is transferred to the ***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. In case of DA module, Analog-to-Digital (AD) conversion is conducted in ***c*** group again for comparison in ***a*** group. The original input signal of ***a*** group has the same time stamp with the feed-back signal from the ***c*** group, because the program in the PLC is executed in the same time scan.

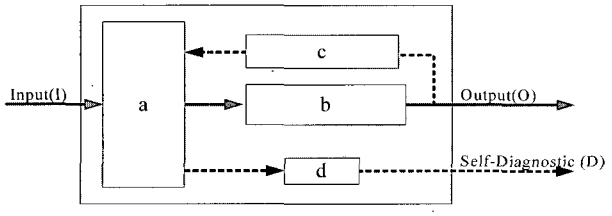


Fig. 3. Functional block diagram of a typical digital hardware module.

iv) The components in ***d*** group transport the error signal to the external module to alert operator that failures are 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 does not 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 does not make the transformed signal for the ***b*** sub-function group. Also the module does not 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 PLC 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

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

columns indicate the output status and the diagnostic status, respectively. 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:

$$\begin{aligned}\text{DF of the module} = {} & \bar{a}bcd + \bar{a}\bar{b}cd + \bar{a}b\bar{c}d + \bar{a}bc\bar{d} \\ & + a\bar{b}\bar{c}d + a\bar{b}c\bar{d} + a\bar{b}\bar{c}\bar{d} + \bar{a}\bar{b}\bar{c}d \\ & + \bar{a}\bar{b}c\bar{d} + \bar{a}b\bar{c}\bar{d} + a\bar{b}\bar{c}\bar{d} \\ = {} & \bar{a}d + \bar{a}\bar{d} + a\bar{b}\bar{c} + \bar{a}bc\bar{d} \\ = {} & \bar{a} + a\bar{b}(\bar{c} + \bar{d}).\end{aligned} \tag{3}$$

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

$$\begin{aligned}P\{\text{DF of the module}\} &= P\left\{\bar{a} + a\bar{b}(\bar{c} + \bar{d})\right\} \\ &= P(\bar{a}) + P(a)P(\bar{b})P(\bar{c}) \\ &\quad + P(a)P(\bar{b})P(\bar{d}) \\ &\approx P(\bar{a}).\end{aligned} \tag{4}$$

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

$$\lambda_m \approx \lambda_a . \tag{5}$$

In addition, the unavailability due to the dangerous failure of the module can be written as follows [1,9]:

$$Q = \lambda_m \cdot \frac{T}{2}, \tag{6}$$

where

Q: the module unavailability due to a dangerous failure,

λ_m: the module failure rate per hour due to a dangerous failure,

T: the periodic surveillance test interval in hours. It depends on the maintenance strategy of the plant. In this paper, 24 hours surveillance test interval is used for the PLC, 1 month test interval (monthly test interval) used for some components, and overhaul test interval also used for other components.

To predict the component failure rate in the PLC, the part stress method of the MIL-HDBK-217F is used. For example, the following equation from the MIL-HDBK-217F is used to estimate the failure rate of the Integrated Microcircuits (Digital Gate/Logic Arrays): [5,6]

$$\lambda_p \approx (C_1\pi_T + C_2\pi_E)\pi_Q\pi_L \quad \text{failures per } 10^6 \text{ hour,} \tag{7}$$

where

C_1 : Die complexity failure rate,

C_2 : Packaging failure rate,

π_T : Temperature Factor,

π_E : Environment Factor,

π_Q : Quality Factor,

π_L : Learning Factor.

The values for the above factors are based on the applicable plant conditions and the configuration details of the microcircuits. Suitable values of the above parameters are chosen for the perceived device specifications and the control room conditions. The ambient temperature of 30 °C is considered for the computation of the components failure rates. In addition, the operating condition is considered as ground benign. The Reliability Workbench environment [10] is used to integrate the failure rates from each component into the PLC module.

3.1.3 Failure rate prediction

The proposed failure model is applied to the PLC modules being developed in Korea. Table 2 shows the failure rates of the digital output (DO) PLC module. From Fig. 3, the functions of the DO module are divided into ***a, b, c,*** and ***d*** sub-function group. The FMEA method is used to categorize the components in the PLC into the sub-function group according to their functions. The failure rates of the sub-function group in Table 2 are determined by the sum of the individual component failure rates included in the each sub-function group. The failure rates of individual component are determined from MIL-HDBK-217F.

In Table 2, the dangerous failure rate of the DO module can be approximated by the failure rate of the ***a*** sub-function group from (5), and is 1.39E-06. The conventional failure rate is determined by the sum of the failure rate of all sub-function group, and is 6.35E-06.

Dangerous failure rate considers the effect of the diagnosis function included in the PLC. The dangerous failure rate of the PLC module can be approximated only by the failure rate of the ***a*** sub-function group, and is improved than the conventional

Table 2. Failure rates of the DO PLC modules.

Sub-function Group	Failure Rate ($\times 10^{-6}$ /hr)
a	1.39
b	1.93
c	2.26
d	0.77
Dangerous Failure Rate	1.39
Conventional Failure Rate	6.35

Table 3. Failure rates of the typical PLC modules.

Module Name	Failure rates ($\times 10^{-6}$ /hr)
CPU Module(+Baseboard)	13.076
Power Supply Module	4.43
Digital Input Module	1.25
Digital Output Module	1.39
Relay Output Module	2.2
Analog Input Module	4.72
Analog Output Module	39.2

failure rate. The result of the safety assessment is used as a measure to determine whether the new developed PLC or RPS is applied to the nuclear power plant. If this proposed failure rate model is adopted as a failure rate prediction method by nuclear regulatory body, it can improve the evaluation result for safety assessment without any hazard to the nuclear power plant. Table 3 shows the dangerous failure rates of the typical PLC modules.

3.2. Common cause failures modeling

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 [1]. 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 safety analysis of a nuclear power plant. There are several methods to estimate the common cause failure probabilities. The prevalent modeling techniques for the common cause event are the Beta-factor, Multiple Greek Letters, and Alpha factor methods [7]. In this paper, the Beta-factor model is selected because it is widely using to estimate the common cause failure probability for safety assessment in the nuclear power plant.

The Beta-factor model is a single parameter model. This model assumes that any failure in the PLC module can happen simultaneously in the redundant PLC modules with a constant fraction (β) of the total component failure rate of the module. Table 4 shows the quantitative common cause failures [6]. The beta factor model is written as

$$Q_c = \frac{\beta}{1-\beta} Q_i , \tag{8}$$

where

Q_c: Common cause failure probability,

Q_i: Component independent failure probability and calculated from (6),

Table 4. Common cause failures probability of the RPS.

Event Name	Description	Prob.
MFLTK-LSL1	CCF of Lo SG1 Level transmitters	4.01E-06
RCPSKALL	CCF of Lo SG1 instrument power supply fails	1.33E-06
RPIMWAI	CCF of analog input modules	2.98E-06
RPMWWALL	CCF of manual trip push button switches	1.18E-06
RPOMWDORY	CCF of digital output modules	0.88E-06
RPPMWBP	CCF of bistable processors	8.26E-06
RPPMWCP	CCF of coincidence processors	8.26E-06
RPRBWTCB	CCF of reactor trip circuit breakers	5.37E-06
RPRYWSHIR	CCF of interposing relays to energize	2.78E-06
RPRYWUVIR	CCF of interposing relays to de-energize	2.78E-06
RPSHWST	CCF of Shunt trip devices ST-1, 2, 3 & 4	2.34E-04
RPUVWUV	CCF of UV trip devices UV-1, 2, 3, & 4	3.02E-04
RPWDWALL	CCF of watchdog timers	1.00E-07

Table 5. Human error probability.

Human Error	Description	Probability (Mean)
RPOPHTRIP	Operator fails to manually trip reactor	1.00E-03
RPOPHBI-LSL	Mis-calibration of SG1 Level	0.325E-03

β: Beta factor and assumed to be 0.05.

3.3. Human error modeling

Human errors are also to be 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 [8]. Table 5 shows the human error probability [6].

4. RESULTS

The component failure probabilities, the common cause event, and human error are prepared in Section 3. This failure data will be used as the quantitative probability for the basic events in the FTA model.

The top event of the FTA model for the RPS safety

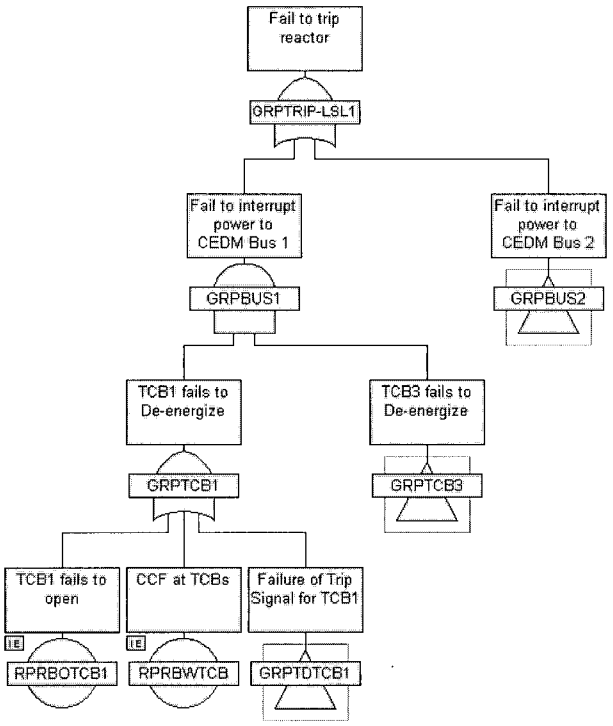


Fig. 4. Fault tree model for the safety analysis of the RPS.

assessment is the 'Fail to Reactor Trip'. The event 'Fail to Reactor Trip' happens when 'Fail to interrupt Power to CEDM Bus 1' or 'Fail to Interrupt Power to CEDM Bus 2' is happened. The event 'Fail to Interrupt Power to CEDM bus 1' happens when 'Fail to De-energize Trip Circuit Breaker TCB 1' and Fail to De-energize Trip Circuit Breaker TCB 3' are simultaneously happened. And the event 'Fail to Interrupt Power from CEDM bus 2' happens when 'Fail to De-energize Trip Circuit Breaker TCB 2' and Fail to De-energize Trip Circuit Breaker TCB 4' are simultaneously happened. This FTA model is determined from RPS architecture of Fig. 1 and 2. This FTA modeling is so big work that it can not present in this paper. Fig. 4 shows a brief example of the FTA model for the RPS.

The FTA model of Fig. 4 will be continued until it reaches to the basic event such as component failure probabilities, the common cause event, or human error. From Fig. 4, the event 'Fail to De-energize Trip Circuit Breaker TCB 1' happens when 'Fail to Open Reactor Trip Circuit Breaker TCB 1', 'Failure of Trip Signal for TCB 1' or 'Common Cause Failure at TCB' is happened. At this point, the events 'Fail to Open Reactor Trip Circuit Breaker TCB 1' and 'Common Cause Failure at TCB' are the basic events, so the extension of the FTA is finished. But the event 'Failure of Trip Signal for TCB 1' is not a basic event and it is caused by the PLC modules failures or communication path failures, so the extension of the FTA model will be continued until the basic events [9].

Table 6. Typical minimal cutsets and unavailability for the RPS.

No	Cutset	Cutset Probability
1	RPRBWTCB	5.37E-06
2	RPUVWUV. RPSHWST	7.0668E-08
3	RPRBOTCB1. RPRBOTCB3	2.3104E-08
4	RPRBOTCB2. RPRBOTCB4	2.3104E-08
5	MFLTK-LSL1. RPOPHTRIP	4.01E-09
6	RPIMWAI. RPOPHTRIP	2.98E-09
7	RPOMWDORY. RPOPHTRIP	1.39E-09

The safety assessment of the RPS is determined by summing the individual probabilities for the basic events in the FTA model. For the selected trip parameter of the Low Steam Generator Level, the safety assessment result of the RPS is as follows [6]:

- Mean Unavailability : 5.51338E-06
- 90 % Upper Bound : 1.7824E-05
- 95% Upper Bound : 2.21437E-05
- 99% Upper Bound : 2.8172E-05

This result is very important factor to decide whether the new developed PLC or RPS is applied to the nuclear power plant.

Table 6 shows the most important minimal cutsets to affect the RPS unavailability [9]. In this evaluation, the cutsets represent the combination of the basic event failures that prevent the reactor trip when demanded. The most dominant minimal cutset is a common cause failure of the reactor trip circuit breakers (RPRBWTCB). The second dominant minimal cutset is a combination of the common cause failures of the UV trip devices (RPUVWUV) and the Shunt trip devices (RPSHWST). The third and fourth dominant minimal cutest relate with the combination events of the 'Reactor trip circuit breaker TCB fails to open' (RPRBOTCB). The sixth dominant minimal cutset is a combination of the common cause failures of the analog input modules (RPIMWAI) and the manual trip failure by an operator (RPOPHTRIP). In the Table 6, the event, RPOMWDORY, represents the common cause failure of the relay output module. From this minimal cutest analysis, the analog input and the relay output module are related with the PLC.

From Table 6, many kinds of common cause failures are dominant contributors to the RPS unavailability. To improve the RPS unavailability, the diversity functions to minimize the effect of the common cause failure should be considered during plant level design phase.

5. CONCLUSION

The conventional failure rate prediction model is a very conservative method. To consider the effect of

the diagnostic function implemented in the PLC, a new failure rate prediction model is proposed in this paper. The dangerous failure rate which considers the effect of the diagnosis function included in the PLC is improved than the conventional failure rate. So, if this proposed failure rate model is adopted as a new failure rate prediction method by nuclear regulation body, it will improve the evaluation result for safety assessment without any hazard to the nuclear power plant.

In addition to the failure rate prediction of the hardware component, the safety assessment was accomplished to determine the unavailability of the RPS. For this purpose, the FTA model is implemented with the well-established procedure in the nuclear power, and the probability of the common cause failures and operator errors are determined with well-established method.

Also the minimum cutest analysis is performed to identify the design weak points during the design phase. The dominant cutsets related with the PLC are RPIMWAI & RPOPHTRIP and RPOMWDORY & RPOPHTRIP as shown in Table 6. According to this analysis, some diverse functions are recommended to reduce the effects of the common cause failures during the plant level design phase.

REFERENCES

[1] Krishna B. Misra, *Reliability Analysis and Prediction*, Elsevier, 1992.

[2] D. Y. Lee, J. B. Han, and J. Lyou, "Reliability analysis of the reactor protection system with fault diagnosis," *Key Engineering Materials, Advances in Nondestructive Evaluation,* Part 2, pp. 1749-1754, November 2003.

[3] IEEE Std. 603, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,* 1998.

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

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

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

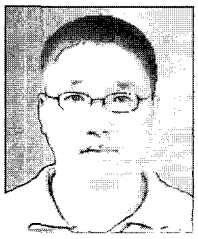
[7] NUREG/CR-4780, Volume 1, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples*, NRC, 1988.

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

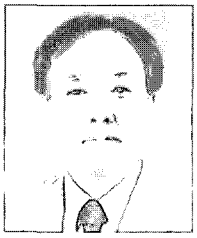
[9] KNICS-RPS-AR103, Rev.00, *Unavailability Analysis for Reactor Protection System*, Korea Atomic Energy Research Institute, 2003.

[10] Computer Program, Version 10.0 by ISOGRAPH, *Reliability Workbench for Windows 95/98/NT/2000/ Me*, 2002.

Dong-Young Lee received the B.S. and M.S. degree in Electrical Engineering from Kyungpook National University in 1984 and 1987. He has been a Researcher of the Korea Atomic Energy Research Institute since 1987. His research interests include instrumentation and control system, reliability analysis, and safety assessment.



Jong-Gyun Choi received the B.S. degree in Nuclear Engineering from Hanyang University in 1994, M.S. and Ph.D. from KAIST in 1996 and 2001. He has been a Researcher of the Korea Atomic Energy Research Institute since 2001. His research interests include instrumentation and control system, reliability analysis, and safety assessment.



Joon Lyou received the B.S. degree in electronics engineering from the Seoul National University, and M.S. and Ph.D. from the KAIST. He has been a Professor of the department of electrical and computer engineering of the Chungnam National University, since 1984. His research interests are industrial control and sensor signal processing, IT based robotics, and navigation systems.