Journal of the Korean Nuclear Society
Volume 36, Number 2, pp.184~195, April, 2004

ATWS Frequency Quantification Focusing on Digital I&C Failures

Hyun Gook Kang, Seung-Cheol Jang, and Ho-Gon Lim
Korea Atomic Energy Research Institute
150 Deokjin-dong, Yuseong-gu, Daejeon, 305-353, Korea
hgkang@kaeri.re.kr

(Received October 30, 2003)

Abstract

The multi-tasking feature of digital I&C equipment could increase risk concentration because the I&C equipment affects the actuation of the safety functions in several ways. Anticipated Transient without Scram (ATWS) is a typical case of safety function failure in nuclear power plants. In a conventional analysis, mechanical failures are treated as the main contributors of the ATWS. This paper quantitatively presents the probability of the ATWS based on a fault tree analysis of a Korea Standard Nuclear Power Plant is also presented. An analysis of the digital equipment in the digital plant protection system. The results show that the digital system severely affects the ATWS frequency. We also present the results of a sensitivity study, which show the effects of the important factors, and discuss the dependency between human operator failure and digital equipment failure.

Key Words : digital I & C, ATWS, PSA, DPPS

1. Introduction

In a probabilistic safety assessment (PSA) of nuclear power plants, the Anticipated Transient without Scram (ATWS) is considered as one of the most important initiating events. In facts, the ATWS is not an original initiating event, but rather it is a faulted response to an event requiring control element assemblies insertion for reactivity control. However, because of the significant impact that the ATWS has on the plant response, it is included as a separate initiating event category. ATWS is defined as an anticipated operational occurrence coupled with the subsequent failure to scram when the appropriate trip parameters are reached.

In this paper, we address the quantification of ATWS frequency based on a fault tree analysis of a Korea standard nuclear power plant (KSNPP) The effects of the digital equipment in the digital plant protection system (DPPS) and the digital engineered safety feature actuation system (DESFAS) are also addressed. The DESFAS would not affect the function of a reactor trip, and thus only the digital equipment in the DPPS affects the probability of the ATWS. The aim of this study is

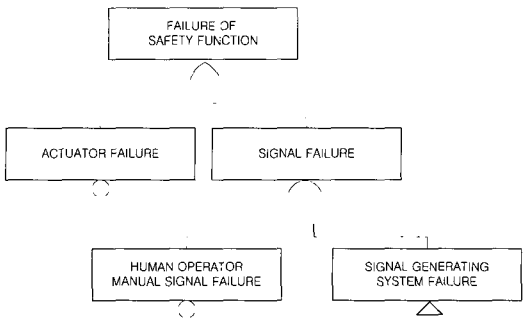

Fig. 1. The Concept of a Safety Function Failure

to investigate the effects of the important features of the digital equipment for a safety function failure, ATWS.

The reasons for a specific safety function failure could be categorized into two groups: mechanical actuator failure and signal generation failure, as shown in Figure 1. In a conventional analysis, mechanical failures are treated as the main contributors of the ATWS, because the conventional analysis treats the signal generation system as independent basic events or as simple fault trees. In the case of an analog signal processing system, every signal maintains a fully independent processing channel.

With digital equipment, however, the situation becomes different. Microprocessors and software technologies make the digital system multi-functional and a system performs several functions sequentially or conditionally. This multi-tasking feature could cause a risk concentration and deteriorate the reliability of the system. The designs of safety-critical systems such as those employed in nuclear power plants have adopted a conservatism approach and have various functional redundancies through separated systems. In the case of digital systems, however, the software programs of these functions are executed by one processor and the redundancy is no longer valid.

Several different functions such as alarm generation, trip signal generation, and safety-function-actuation signal generation are performed by the DPPS. This causes risk concentration. The failure of alarm generation will adversely affect the human operator' s manual action, which could play the role of a backup for automatic signal generation. Regarding the trip signal generation, multiple trip parameters are processed in the DPPS. This also causes the risk concentration. In this study, we will investigate the ATWS only, and as such the results of the study are expected to show only a part of the risk concentration effect.

In sections 2 and 3, we describe the information of the target function and system and a base analysis regarding the initiating events, respectively. In section 4, we explain the fault tree modeling of the ATWS. And in section 5, we show the quantification results and present the results of the sensitivity study, which examines the effects of the important factors of the digital system on the ATWS frequency.

2. Target Function and System

2.1. Description of the ATWS

An ATWS is potentially a severe event in which the reactor coolant system (RCS) goes through a pressure excursion due to an imbalance between the core heat generation and RCS heat removal.

The ATWS is defined as an anticipated operational occurrence coupled with failure to insert negative reactivity via the control element assemblies, due either to electrical faults within the DPPS and the diverse protection system (DPS) or mechanical binding of the CEAs themselves [1]. Since the primary ATWS concern is the peak RCS pressure, the ATWS initiators may be redefined as only the transients that tend to produce RCS pressure transients. However, all the initiating

events that require a reactor trip are conservatively included in this study.

That is, the ATWS occurs if the CEA insertion fails when an initiating event occurs. The reasons for the CEA insertion failure could be classified as either a signal failure or a mechanical failure. For the signal failure, we consider three signal sources: the DPPS, the DPS, and manual initiation by a human operator.

2.2. Description of the DPPS

The purpose of the DPPS is automatic generation of a trip signal for an emergency. In

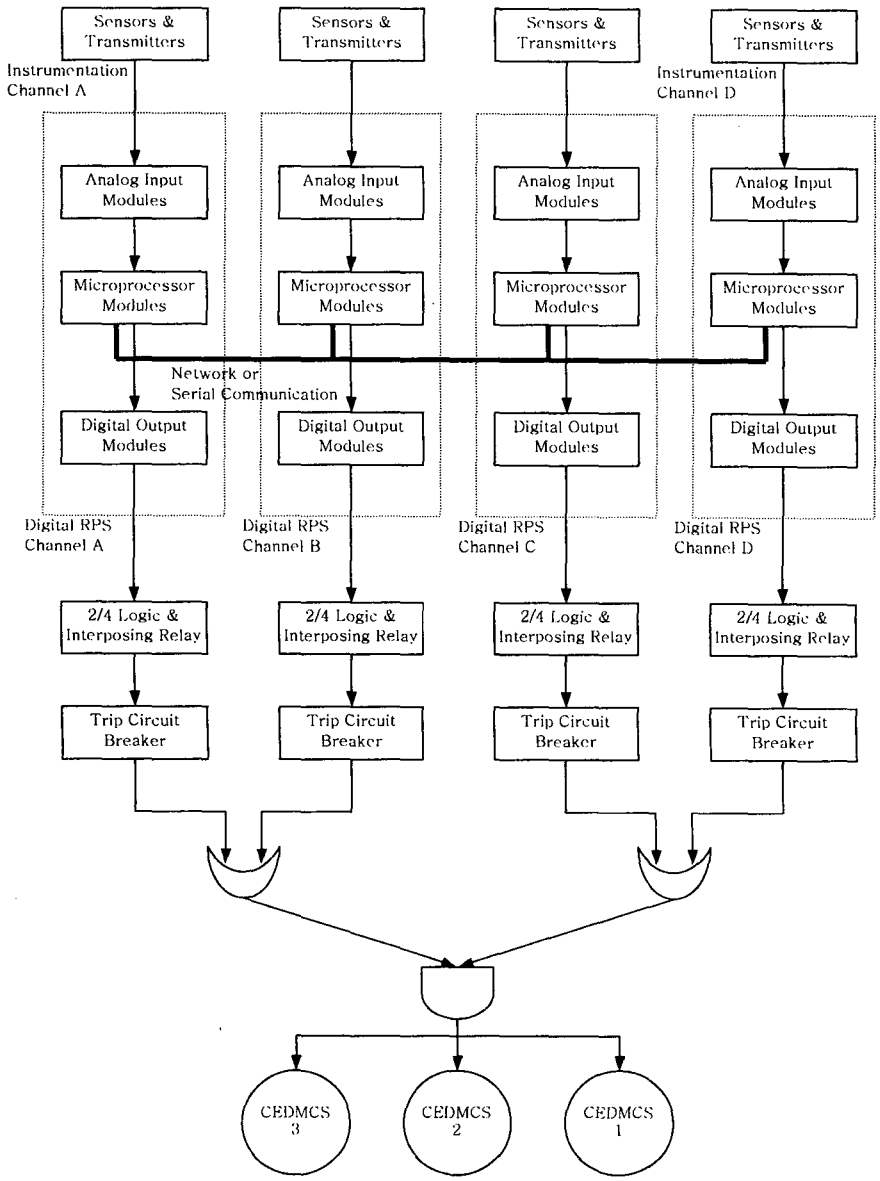

Fig. 2. Schematic Diagram of a Typical Four- Channel DPPS

order to detect an emergency, it monitors various process parameters using independent instrumentation and processing channels. Many protection systems of nuclear power plants adopt a four-channel layout including the DPPS. Figure 2 shows a schematic diagram of a typical four-channel DPPS including a selective two-out-of-four voting logic.

Four redundant channels are provided to satisfy the single failure criterion and improve the plant availability. Each channel of the DPPS contains six microprocessor-based signal-processing modules, consisting of two bistable processors and four local-coincidence-logic processors. The bistable processor in each channel receives analog inputs from the sensors through analog input modules. A bistable processor compares the input signals to the trip setpoints and transmits the results to local-coincidence-logic (LCL) processors.

A LCL processor performs two-out-of-four voting for each process input using the signals from the four bistable processors. It produces an output signal using a dedicated digital output module. Its stall will result in a loss of its heart beat output signal to a watchdog timer. The watchdog timer will then force the DPPS trip and initiate a trip signal. More detailed description of the DPPS is available in references [2] and [3].

3. ATWS Initiating Events

An initiating event (IE) could be defined as 'any event that perturbs the steady state operation of the plant thereby initiating an abnormal event such as a transient or the loss of coolant accident (LOCA) within a plant'. In the PSA of the KSNPP, about 60 IEs are screened out and categorized into 16 groups by considering their properties. Among these 16 groups, a reactor vessel rupture accident or an interfacing system LOCA directly causes core damage. Therefore, we develop generally risk models for 14 IE groups, including the ATWS. In level 1 PSA, the results of all the IE models are integrated into one safety measure, core damage frequency (CDF). In level 2 PSA, we also calculate another safety measure, large early release frequency (LERF) in consideration of radiation release to containment outside.

As noted in the previous section, the ATWS is not an original IE, but rather it is a faulted response to an event requiring control element assemblies insertion for reactivity control. Therefore, the frequency of the ATWS initiation should be calculated based on the other original IE groups. The large LOCA and the medium LOCA are not concerned with the ATWS initiation frequency calculation because in these two cases reactor trip is not a critical function for the safe shutdown of the KSNPP.

The automatic signals illustrated in Table 1 are different for the IE groups. We must analyze which reactor trip signals from the DPPS correspond to each IE as they happen. As the first step of the development of a possible trip signal list for each IE group, a document survey and expert judgment should be performed. Table 1 shows the results of the surveys. In this phase, we must decide whether the DPS signal corresponds to each IE group. In consideration that the trip signal from the DPS is initiated only by high pressurizer pressure and high containment pressure, the DPS availability could be assumed as in Table 1. Since in the case of LSL, HSL, LSP, and LSF, the trip signals are initiated by sensing the status of cooling loops, we model two cooling loops.

For a more realistic modeling, a simulation of plant behavior for each IE is required. In this study, we simulate the case of small LOCA only (2-inch break on cold leg) as an example case. We ignore the manual actuation of reactor trip or safety function in order to obtain the genuine plant response. Because there are some limitations in

Table 1. ATWS Occurrence Condition

IE Group	DPPS Variables	DPS Availability	Manual Action Failure Prob.
SLOCA	DNB LPP HCP	X	Variable of sensitivity study
SGTR	HSL DNB	X	
LSSB	LSP VOPT LSL LPP DNB	X	
LOFW	LSL HPP	O	
LOCV	HPP	O	
LOCCW	LSF DNB	O	
LOKV	LSF DNB	O	
LODC	HPP DNB HSL	O	
LOOP	DNB LSF	O	
GTRN	HPP DNB	O	

* In the Risk Monitor model, the SBO IE group is modeled internally.

* Abbreviations:

SLOCA	Small Loss of Coolant Accident
SGTR	Steam Generator Tube Rupture
LSSB	Large Secondary Side Break
LOFW	Loss of Feed Water
LOCV	Loss of Condenser Vacuum
LOCCW	Loss of Component Cooling Water
LOKV	Loss of 4.16KV AC bus
LODC	Loss of 125V DC bus
LOOP	Loss of Offsite Power
GTRN	General Transient
VOP	Variable Overpower
HPL	High Logarithmic Power Level
HLD	High Local Power Density
DNB	Low Departure from Nucleate Boiling Ratio
HPP	High Pressurizer Pressure
LPP	Low Pressurizer Pressure
LSL	Low Steam Generator Water Level
HSL	High Steam Generator Water Level
LSP	Low Steam Generator Pressure
LSF	Low Steam Generator Reactor Coolant Flow
HCP	High Containment Pressure

thermo-hydraulic modeling, we assume that the main feedwater is blocked when the accident occurs and the charging pumps in the chemical volume control system are not activated. We do not model the containment pressure.

We use the MARS [4] modeling package developed in KAERI to simulate the KSNPP response. The result shows that the reactor core temperature goes over 2200°F at 2567 seconds. Small LOCA belongs to the plant-condition 4 group, which is categorized by the standard of the 'time response design criteria for safety-related

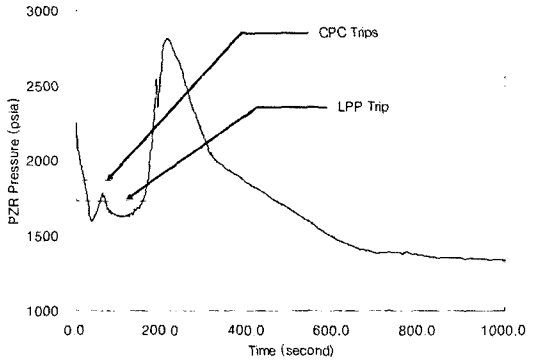

Fig. 3. The Graphical Illustration for the Pressurizer Pressure Response when a Small LOCA Happens

operator actions [5]'. Based on the methodology in the standard, we estimate the time required for an operator action at 25 minutes (1500 seconds), which includes the minimum time for a diagnosis of 20 minutes.

From the simulation result, we find that the core protection calculator trips (DNB and HLD) LPP and LSF will be activated under the 2-inch LOCA condition before the time limit of 1067 (2567-1500) seconds. Figure 3 shows the pressurizer pressure as an example of plant response. Given that the containment pressure is not considered in this simulation and DNB and HLD shares the same signal processing channel, this result agrees well with the survey result in Table 1. However, LSF should be additionally considered. It is recommended to expand the simulation scope and reality in order to verifying the survey results.

The expectation of successful manual actuation by an operator must be calculated based on the available alarms, training, experience, time limitation, and plant situation. That is, the failure probability of manual actuation should be estimated in consideration of the situation of each of the IE groups. In this study, because of a lack of information, we treat this failure probability as a variable of a sensitivity study.

4. Fault Trees for ATWS

4.1. Modeling Assumptions

The Risk Monitor [6], fault trees for the KSNPP developed by the Integrated Safety Assessment team in KAERI, is used to model the general plant risk of the KSNPP. It consists of about 2500 basic events and 3500 logical gates.

The aim of this fault tree modeling is to analyze the effect of digital safety-critical systems on the ATWS frequency. We do not focus on the DPS, which is categorized as a non-safety-critical system. Therefore, the DPS failure is not modeled based on the elementary modules and we treat one DPS processing channel as one basic event.

The DPPS failure is modeled based on the elementary module failure in a detailed manner. The modeling assumptions for the DPPS fault trees are as follows:

- Since we do not have enough information about the failure modes of digital systems, all failure modes are assumed to be hazardous.
- Watchdog timers monitor the status of LCL processors and LCL processors monitor the status of bistable processors. Generally, the coverage of timer-to-processor monitoring is much lower than that of processor-to-processor monitoring because the processor-to-processor monitoring method uses much more sophisticated algorithms. We assume that the fault coverage of the processor-to-processor monitoring is 0.99. The coverage of the timer-to-processor monitoring is treated as a variable of the sensitivity study. And, for simplicity, we also assume that watchdog timers could detect software failures with the same coverage as in the case of hardware failures.
- We assume that every processor contains an identical software program and the software failure induces the common cause failures of the

processors.

- We ignore the fail-to-hazard probability of the network or serial communications.
- We ignore the fail-to-hazard probability of the inter-system data bus and the back plane of the PLC.
- We assume that the components are tested at least once per month. That is, the periodic test interval (T) is 730 hours. Component unavailability (Q) is a half of the product of the failure rate (λ) and periodic test interval: $Q=\lambda T/2$.

4.2. Fault Tree Model

Figure 4 shows the schematic fault tree for the ATWS IE frequency calculation. It consists of all the initiating events listed in Table 1. The system unavailability varies along with the plant situation, because different plant abnormalities initiate different trip parameters.

For convenience of explanation, we explain only the case of LOFW. Figure 5 shows a fault tree in the case of LOFW. The reasons for reactor trip failure in LOFW are mechanical failure of CEAs and trip signal failure. The trip signal could be generated by the DPPS or the DPS. The DPPS would generate a trip signal based on three trip parameters: HPP, LSL1, and LSL2. In each case of the trip parameters, the system for generating the trip signal is modeled in a separate manner.

Figure 6 shows the fault tree for modeling under-voltage (UV) signal failure for the parameter of LSL1. The reasons for UV signal failure could be the failure of an UV element itself, the failure of a human operator manual initiation, or the failure of the DPPS output. Detailed explanations of the other parts of the DPPS model are available in

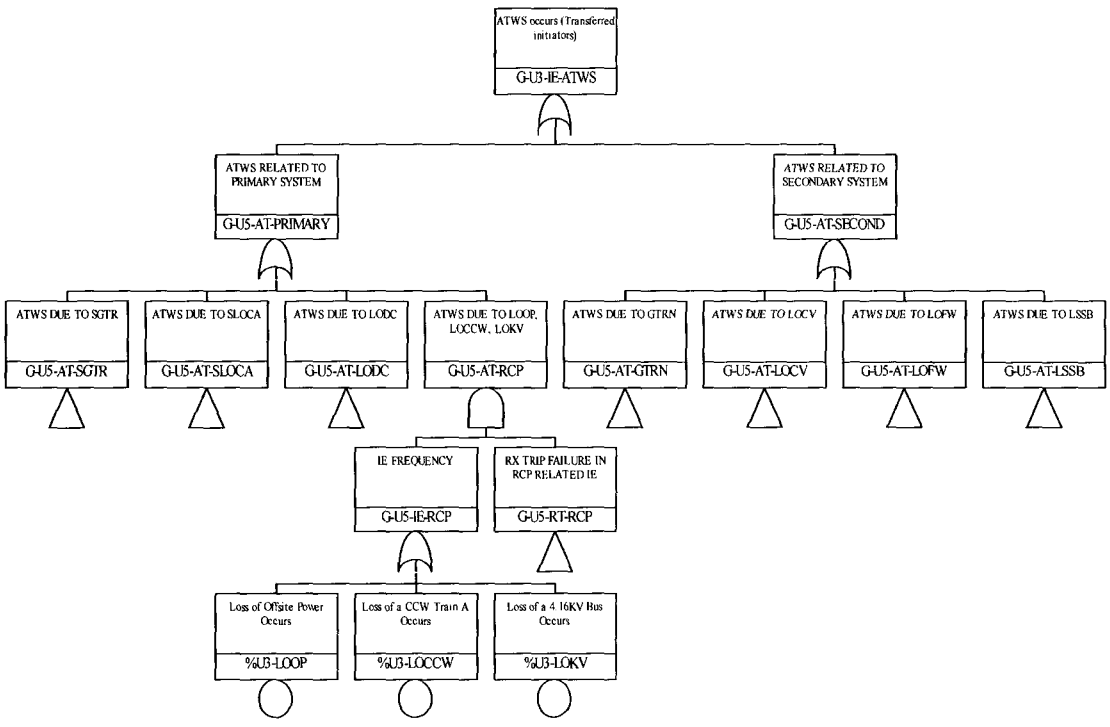

Fig. 4. Schematic Fault Tree for the ATWS

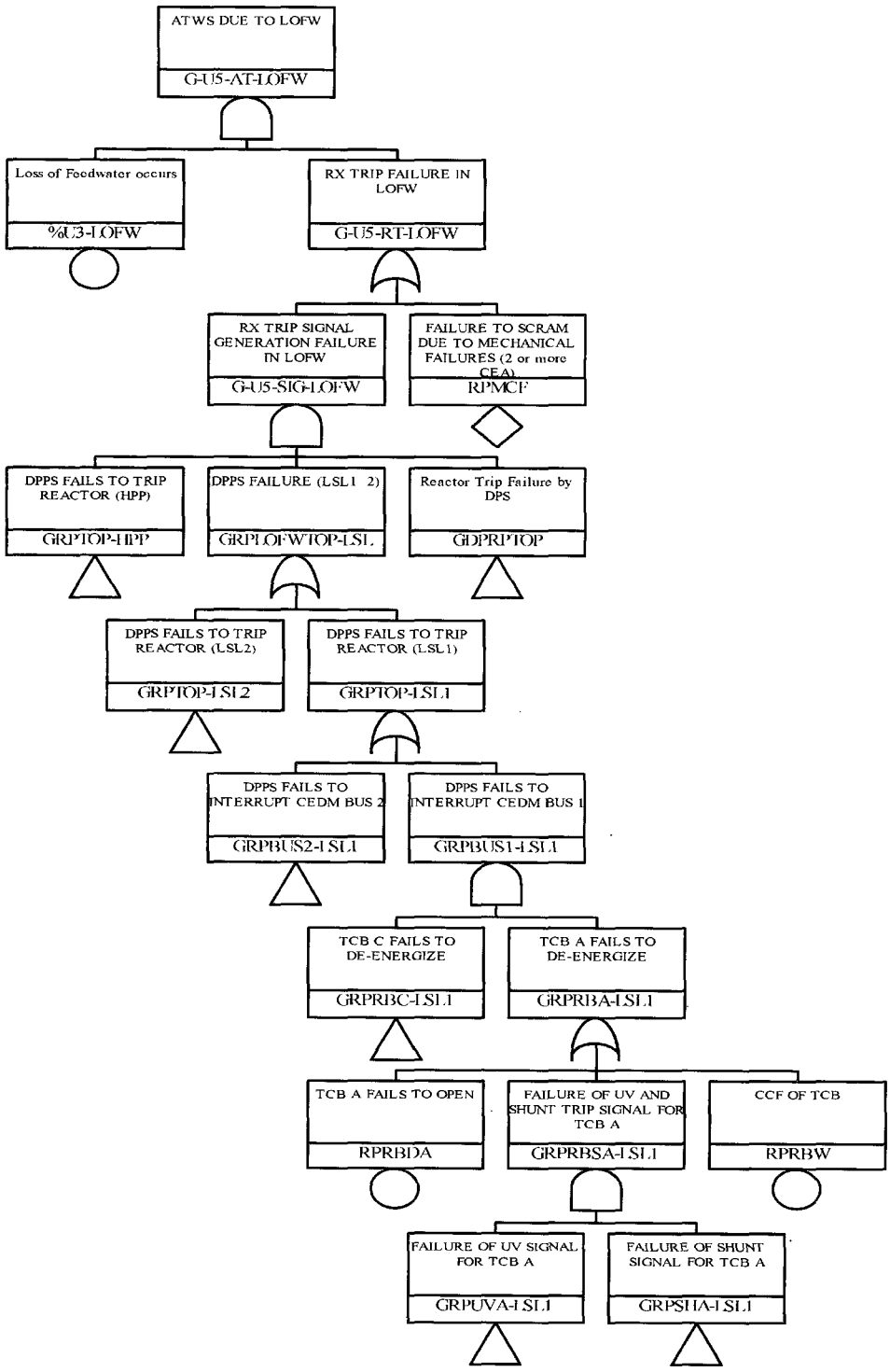

Fig. 5. Fault Tree for Modeling the ATWS in the Case of LOFW

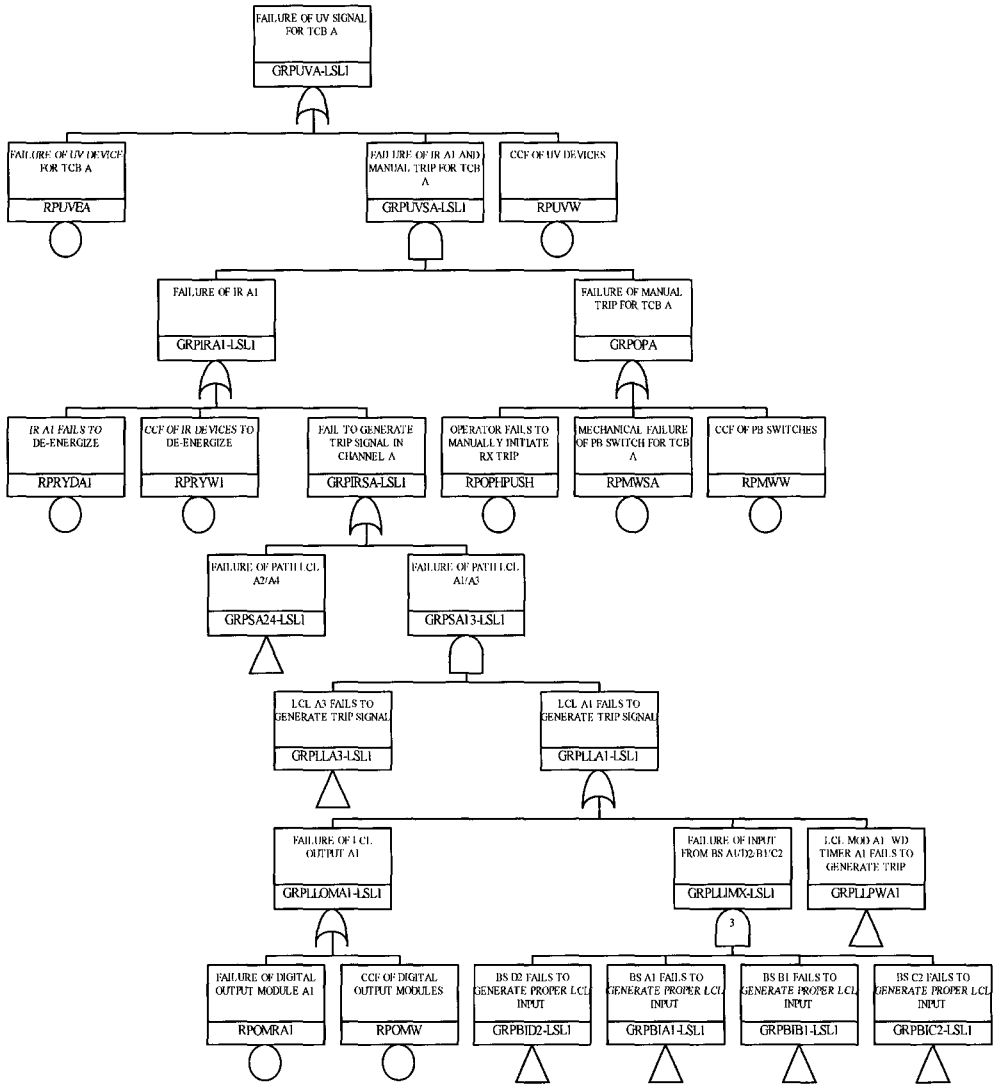

Fig. 6. Fault Tree for Modeling an Under-voltage Signal Failure for the Parameter of LSL1

references [2] and [3].

5. Quantification Result

Using KwTree [7], which is a fault-tree analysis software package produced by Korea Atomic Energy Research Institute, the ATWS fault tree is analyzed. A previous study [3] revealed that there are three important factors in digital system safety analysis: human failure probability, software failure probability, and the watchdog timer coverage. In order to quantify the effects of the three important factors listed above, we perform a sensitivity study.

Regarding the human failure probability, we use 1E-10, 0.05, 0.5, and 1.0. The first and the last case represent the case of almost perfect human action and no human action, respectively. Regarding the software failure probability, in this

Table 2. ATWS Frequency in the Case of the Watchdog Timer Coverage of 0.3

Pr(OP) \ Pr(SW)	1.00E-03	1.00E-04	0
1.00E-10	8.433E-06	8.433E-06	8.433E-06
0.05	1.435E-05	9.722E-06	9.208E-06
0.5	6.764E-05	2.139E-05	1.625E-05
1	1.269E-04	3.436E-05	2.408E-05

Table 3. ATWS Frequency in the Case of the Watchdog Timer Coverage of 0.7

Pr(OP) \ Pr(SW)	1.00E-03	1.00E-04	0
1.00E-10	8.433E-06	8.433E-06	8.433E-06
0.05	1.133E-05	9.350E-06	9.130E-06
0.5	3.749E-05	1.767E-05	1.547E-05
1	6.657E-05	2.693E-05	2.252E-05

Table 4. ATWS Frequency in the Case of the Watchdog Timer Coverage of 0.9

Pr(OP) \ Pr(SW)	1.00E-03	1.00E-04	0
1.00E-10	8.433E-06	8.433E-06	8.433E-06
0.05	9.825E-06	9.164E-06	9.091E-06
0.5	2.242E-05	1.581E-05	1.508E-05
1	3.642E-05	2.321E-05	2.174E-05

analysis, we examine the effect of the software of LCL processor modules only. We use 0, 1E-4, and 1E-3 as the software probability. We roughly assume that the watchdog timer could detect the failure of software with the same coverage as in the case of the hardware failure. Regarding the watchdog timer coverage, we use 0.3, 0.7, and 0.9.

The results are shown in Tables 2 to 4. Figure 7 shows a graphical illustration of the results in Table 3. In the case of a zero software failure and a highly credible operator backup, the effect of the watchdog timer is negligible. However, in the other cases, the coverage of the watchdog timer plays a critical role. This result agrees well with that shown in references [3], [8] and [9], i.e., the watchdog timer coverage plays a critical role in deciding the system unavailability when we consider realistic values for software failure and human failure.

The result of the quantification shows that the ATWS initiating event probability varies between 8.43E-6 and 1.27E-4, which is a higher value than that of the analog-protection-system-based plant 8.40E-6 [10]. The worst result, 1.27E-4, is from the case of poor software quality, poor watchdog timer coverage, and no human operator backup.

It is notable that an optimistic result, 8.43E-6, could be obtained from the case of the almost perfect human operator having a failure probability of 1E-12. This means that for ultra-high reliable systems, we have to carefully consider the situation of the human operator. The current

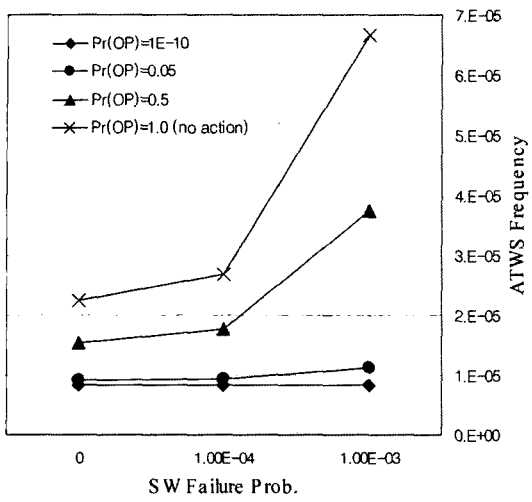

Fig. 7. Graphical Illustration of the ATWS Frequency Calculation Shown in Table 3 (WDT Coverage = 0.7)

situation makes it hard to give a high credit to the human operator action because the DPPS generates not only the automatic trip signals but also the key alarms.

6. Concluding Remarks

The aim of this study was the quantification of the probability of the ATWS and an examination of the effects of the important factors of the DPPS modeling. In order to establish the ATWS fault-tree model, we investigated reactor-trip-failure cases for each IE. Based on an analysis for a combined model of the established DPPS models and the Risk Monitor, we performed a sensitivity study on three important factors and discussed the results.

The sensitivity study shows that the ATWS frequency of the digital protection system-based KSNPP could be between 8.43E-6 and 1.27E-4. These results are higher than those of the analog protection system-based plant $8.40E^{-6}$.

The study suggests that it is necessary to address the effects of a risk concentration induced by digital equipment. In this study, we investigated the ATWS only, and hence the results of the study shows only a part of the risk concentration effect. A further study to investigate core damage frequency based on further researches regarding human failure probability and input dependencies is strongly recommended in order to obtain the total risk concentration effect.

Acknowledgement

This work has been carried out under the Nuclear R&D Program supported by MOST.

Reference

1. KEPCO, Full scope level 2 PSA for Ulchin unit 3&4: Internal event analysis, (1998).
2. Kang, H.G., et al., Reliability Study: Digital Reactor Protection System of Korean Standard Nuclear Power Plant, KAERI/TR-2419/2003, Korea Atomic Energy Research Institute, (2003).
3. Kang, H.G. and Sung, T., "An analysis of safety-critical digital systems for risk-informed design," Reliability Engineering and Systems Safety, Vol. 78, (2002).
4. K.D. Kim, J.J. Jeong, S.Y. Mo, Y.G. Lee and C.B. Lee, "A visual environment for system analysis codes," Progress in Nuclear Energy, Vol. 39, (2001).
5. ANS, Time response design criteria for safety-related operator actions, ANSI/ANS-58.8, (1994).
6. Seung-Cheol Jang, et al., Development of risk model for the Korean standard nuclear power plant, KAERI/TR, To be published, (2004).
7. Sang Hoon Han, et al., "User's Manual for KIRAP (KAERI Integrated Reliability Analysis code Package) Release 2.0," KAERI/TR-

361/93, (1993).

8. Kang, H.G., Jang, S.C. and Ha, J.J., "Evaluation of the Impact of the Digital Safety-Critical I&C Systems on the Plant Risk," Proceeding of ISOFIC 2002, Seoul, Korea.
9. Kang, H.G. and Sung, T., "A Quantitative Study on Important Factors of the PSA of Safety-Critical Digital Systems," Journal of KNS, Vol. 33, No. 6, (2001).
10. Min, K.R. et al., "Reliability Study: KSNPP Reactor Protection System, KAERI/TR-2164/2002, Korea Atomic Energy Research Institute, (2002).