

KAERI/TR- 2026/2002

디지털 계측제어 계통의 확률론적 안전성 평가를
위한 주요인자 선정 및 민감도 분석

**The PSA of Safety-Critical Digital I&C System:
The Determination of Important Factors and
Sensitivity Analysis**

KAERI

한국원자력연구소

제 출 문

한국원자력연구소장 귀하

본 보고서를 2002년도 “차세대원자로 설계관련 요소기술 개발” 과제의 기술보고서로 제출합니다.

2002. 1. 11.

주 저 자 : 강현국 (종합안전평가팀)

공 저 자 : 성태용 (종합안전평가팀)

엄홍섭 (종합안전평가팀)

정환성 (하나로운영팀)

박진균 (종합안전평가팀)

이기영 (동력로기술개발팀)

박종균 (동력로기술개발팀)

요 약 문

확률론적 안전성평가(Probabilistic Safety Assessment; PSA)의 결과는 계통의 안전성을 증명하는데 매우 중요한 역할을 한다. 따라서 마이크로프로세서를 채용한 디지털 계통에 바로 적용하기에는 아직 PSA 기술개발의 정도가 충분하지 못하여 정확한 분석에 많은 어려움이 있음에도 불구하고 신규 도입되는 디지털 계통의 안전성을 정량적으로 추정하기 위해서 그 적용의 필요성이 높아지고 있다. 이와 관련한 연구 주제들은, 현재의 기술수준에서 보다 정확한 PSA를 수행하기 위한 방법론을 개발하고 절차를 제시하기 위한 연구와 각각의 측면을 보다 정확하게 평가하기 위한 방법론 개발을 위한 연구로 대별할 수 있다. 본 보고서는 첫번째의 범주에 속하며, 가장 보편적으로 사용되고 있는 PSA 방법론인 고장수목(fault tree) 모델링 방법을 기반으로 하여 원전의 안전관련 디지털 계측제어 계통의 안전성평가를 위한 현실적인 방법론을 제시하는데 목적이 있다.

본 보고서의 목적을 요약하면 다음과 같다.

- 1) 디지털 계통에 대한 PSA를 수행할 때 반드시 고려되어야 할 중요한 인자들을 정리
- 2) 인자들 내부에서의 상관관계 및 각 인자와 PSA 결과와의 상관관계를 수학적으로 방법을 이용하여 정량화
- 3) 주요인자들이 최종 PSA결과에 미치는 영향을 보이기 위한 민감도 분석

다양한 문헌분석과 자료수집을 통해 PSA 모델에 반드시 반영되어야 할 인자들을 도출하였는데, 이러한 인자에 대해 잘못된 가정을 적용하여 모델링을 수행할 경우 PSA결과를 크게 왜곡시키게 되므로 주의하여야 한다. 특히 공통원인 고장, 고장내구성 기법, 소프트웨어 오류는 최종 계통의 안전성에 미치는 영향이 매우 커서, 이들 인자에 적용된 값에 따라 PSA 결과치가 수천배까지 변하게 되는 것을 민감도 분석을 통해 확인할 수 있다.

합리적이고 적절한 가정을 바탕으로 한 안전성 분석의 결과는 설계과정에도

중요한 피드백을 줄 수 있으므로 이 연구가 규제자 뿐만 아니라 개발자에게도 도움을 줄 수 있을 것으로 기대된다.

Summary

The result of probabilistic safety assessment (PSA) plays very important role in proving the safety of a designed system. Therefore, even though conventional PSA methods are immature for applying to microprocessor-based digital systems, practical needs force it to be applied. The studies regarding this issue could be categorized into two topics. One is developing the practical PSA methodology and the guide based on currently available technologies. The other is developing more precise and sophisticated evaluation techniques for each factor. This report concentrates on the first topic and is prepared to suggest a practical PSA methodology of safety-critical digital instrumentation and control (I&C) systems which is based on the well-known fault tree methodology.

The aim of this study is: (1) To summarize the factors which should be represented by the model for the PSA and to propose a standpoint of evaluation for digital systems. (2) To quantitatively explain the relationship among the important factors and that between each factor and the PSA result. (3) To show the results of a sensitivity study for some critical factors.

From various documentations such as research reports and journal articles, we list up the factors which should be represented by the model for PSA. Inappropriate considerations on important factors will induce unreasonable assumptions and might severely distort the analysis results. For some critical factors, example models are proposed based on the fault tree method. We demonstrate the effect of these factors by sensitivity study. The result which is quantified using fault tree analysis method shows that some factors remarkably affect the system safety. They are the modeling of common cause failure (CCF), the coverage of fault tolerant mechanisms and software failure probability. Quantitatively, the value of each factor changes the system unavailability up to several thousand times.

We expect that the safety analysis result will provide valuable design feedback if the analysis is performed with careful consideration for avoiding the unrealistic assumptions. And we also expect that this report will provide guidance to both the regulatory body and the utility.

Table of Contents

1. Introduction.....	7
1.1 Background and research objectives.....	7
1.2 Digital applications in nuclear plants.....	8
1.3 PSA methods and digital systems	9
2. Factors in digital system safety assessment.....	12
2.1 Digital equipments in safety-critical systems	12
2.2 Modeling the multi-tasking of digital systems.....	12
2.3 Estimating software failure probability.....	17
2.4 Estimating the effect of software diversity and V&V efforts.....	21
2.5 Estimating the coverage of fault-tolerant features	22
2.6 Estimating the CCF probability in hardware	27
2.7 Modeling the interactions between hardware and software.....	27
2.8 The other factors.....	28
3. Analytic Evaluation in the Context of PSA	30
3.1 Case study layout	30
3.2 The analytic assessment of system unavailability.....	35
3.3 Relationship between the factors and PSA results	39
4. A Sensitivity Study.....	41
4.1 The selection of parameters	41
4.2 Fault tree model.....	43
4.3 The result of PSA	44
4.4 Discussion	51
5. Conclusions.....	53
References.....	56

Table of Figures

Figure 1. Schematic diagram of signal processing using analog circuit and digital processor unit.....	15
Figure 2. Schematic diagram of signal processing using analog circuit and digital processor unit.....	16
Figure 3. Schematic diagram of a typical watchdog timer application.....	24
Figure 4. Fault tree model of the system shown in Figure 3	25
Figure 5. Illustration of system unavailability along the coverage factor $(p = 10^{-3}, w = 10^{-7})$	26
Figure 6. The schematic diagram of a typical four-channel digital PPS.....	32
Figure 7. The functional diagram of each channel of the PPS.....	33
Figure 8. The detailed diagram of a selective 2-out-of-four logic which initiates the interposing relay. (LCL: local-coincidence-logic).....	34
Figure 9. The schematic diagram of grouping the cutsets	38
Figure 10. The master diagram of the fault tree for case study (1).....	46
Figure 11. The master diagram of the fault tree for case study (2).....	47
Figure 12. The graph of system unavailability along fault coverage and software failure probability when the identical input modules and the identical output modules are used	48
Figure 13. The graph of system unavailability along fault coverage and software failure probability when two kinds of input modules and the identical output modules are used	49
Figure 14. The graph of system unavailability along fault coverage and software failure probability when two kinds of input modules and two kinds of output modules are used	50

1. Introduction

1.1 Background and research objectives

Since early 1990s there have been hot arguments about the safety of digital applications to nuclear power plants. The report published in 1997 by National Research Council summarizes these arguable issues [1]. The report states that appropriate methods for assessing safety and reliability are the key to establishing the acceptability of digital I&C systems in nuclear plants.

For the past several decades, PSA techniques are used to assess the relative effects of contributing events on plant-wide safety and system reliability. They provide a unifying means of assessing physical faults, recovery processes, contributing effects, human actions, and other events that have a high degree of uncertainty [1]. Now, PSA is faced with new object of analysis, which is the application of microprocessor-based computer systems. The digital techniques are far from the conventional techniques of analog I&C systems because of some unique features of the digital I&C system. Microprocessors and software technologies make the system more flexible and powerful but more complex. From the viewpoint of PSA, there are many important unresolved issues in digital systems' safety analysis which are complex and correlated.

This study is performed as a part of researches which aim to support the design of next generation nuclear power plants. Design is the art of trade-off. The PSA should fairly evaluate this trade-off by proper modeling and reasonable assumptions. We believe that even though we cannot quantify the safety of digital systems in a very accurate manner, the active design feedback of the insight, which comes from quantitative and qualitative approaches of PSA, should be encouraged.

Even though the objective of this study is to support practical needs from the design of next generation nuclear plants, we deal not only the items specified to the next generation nuclear plants but also the general problems which possibly arise when the digital equipments are applied to the safety-critical functions from the viewpoint of PSA. The objectives of this report are as follows:

- (1) To summarize the factors which should be represented by models for the PSA of microprocessor-based digital systems. Although these factors contain unresolved issues, the sensitivity studies and the reasonable assumptions will result in reasonable assessment accuracy.
- (2) To propose a standpoint of quantitative safety evaluation. We expect that the results of PSA and sensitivity studies will provide a valuable feedback to the designers of digital systems.
- (3) To presents the results of a case study which is conducted with a four-channel digital protection system. We also examine the analysis framework of the safety of digital systems in the context of the PSA and to assess the effect of the factors listed above. We quantitatively explain the relationship between each factor and the PSA result.
- (4) To demonstrate the quantitative effect of these factors.

1.2 Digital applications in nuclear plants

Since the 1980's many utilities have adopted digital technology to cope with the aging of analog I&C equipment. The obsolescence and malfunctions of analog I&C components and systems in conventional nuclear power plants has been one of the most severe problems. Furthermore, next-generation advanced nuclear reactors require more complex and smart functions for control systems, protection systems and operator-supporting systems [2].

The modern technologies which are based on both of digital hardware and advanced software algorithms are being rapidly developed and widely used. By the general progress of I&C technologies for process engineering such as computer technology, control engineering, data processing and transfer technology, and software technology, the modern digital technologies are expected to significantly improve the performance and the safety of nuclear power plants. Digital technology was introduced relatively recently in the nuclear power industry and some utilities adopted modern digital technologies to their I&C systems in recent years.

In France, many of the 900 MWe series and the 1300 MWe series adopted

computers and associated data processing systems. Works on the development and implementation of digital I&C systems for advanced reactors are actively underway in Japan. Several US plants have retrofitted digital systems to replace parts of analog systems [3]. Digital technologies are adopted in the late advanced gas cooled reactors in UK for safety features actuation. Primary Protection System of Sizewell B in the UK also employed microprocessors [4]. Especially, in Korea, UCN 5&6 units are being constructed and Korean Next Generation Reactor (KNGR) is being designed using the digital I&C equipment for the safety functions such as a reactor protection system and an engineered safety feature actuation. Even though the use of digital equipment for safety-related functions provides many advantageous features, there are also many licensing issues which should be solved.

1.3 PSA methods and digital systems

The PSA has been widely used in nuclear industry for licensing and identifying vulnerabilities to plant safety since 1975. PSA techniques are used to assess the relative effects of contributing events on system-level safety or reliability. Currently, the nuclear power industry employs the event tree/fault tree methodology for plant-wide PSA. Therefore, the model of digital I&C system should be compatible with the current static logic-based model structure. Even though the plant-wide analysis is based on a fault tree model, there is no reason that the I&C model must itself be established using the fault tree methodology. However, the fault tree is the most familiar tool for analysis staffs and its logical structure makes system design engineers easy to understand it.

The PSA using the conventional techniques and assumptions cannot adequately evaluate some features of digital systems. It will take considerable time to establish a well-accepted standard on the PSA of digital I&C equipment. Even though the PSA methods are immature for applying to microprocessor-based systems, practical needs force to apply it. Unlike conventional standards, new international standards require quantitative analysis [5]. Because of the prematureness of methodologies, many assumptions are used for quantitative analysis. Unreasonable assumptions cause

unreasonable results of the analysis. Fault-free software and 100% coverage of fault tolerance mechanism are typical ones. In order to obtain more reasonable results, these critical assumptions should be resolved. Appropriate methods for assessing safety and reliability are key to establishing the acceptability of digital I&C systems in nuclear power plants.

The guide in [6] provides valuable information to the systems design engineers and application engineers about the problems related to the safety-critical computer applications in a detailed manner. The importance of the PSA for digital applications as a demonstration of safety is also pointed out. The PSA demonstrates that a balanced design has been achieved by showing that no particular class of accident of the system makes a disproportionate contribution to the overall risk. That is, the PSA should play the role of decision-making tool and should have sufficient accuracy.

Followings are the characteristics of digital systems from the viewpoint of PSA.

- The function of a system can be changed repeatedly.
- The utilization profiles of hardware components are determined by software.
- Not only software but also digital hardware shows nonlinear characteristics.
- The failure modes of digital systems are not well defined.
- Digital systems are more sensitive to the environmental condition such as ambient temperature than conventional analog systems.
- Software might hide the transient faults of hardware.
- Software fails whenever it executes the faulty part of code.
- The more efforts on the management of software quality may cause the lower expectation of software failure in operation phase.
- Various monitoring and recovery mechanism can be established using microprocessor and software.
- Apparently different components might cause CCF because electronic components consist of a lot of small modules, which are manufactured in globally standardized environment.
- New initiating events induced by digital systems are possible.

In this report, from the practical viewpoint, we summarize these characteristics to several factors and discuss the difficulties on their quantitative assessment. For accurate analysis, the PSA model should represent these factors.

Then, we make more discussions and suggest quantification examples using the fault tree models for some more important factors: The CCF probability estimation of digital system, the coverage of fault-tolerance mechanism and the software failure probability. Generally, when digital equipment is applied to the safety system design, the designer also adopts multi-backup strategy. We don't have enough operating experience and the CCF assessment methodology. In the case of multi-backup system, usually the CCF probability is one of the most critical factors which affect on the result of the system PSA. Digital systems could be programmed to check the integrity of themselves and to monitor the integrity of each other. That is, digital systems have various fault-tolerant mechanisms and the analysis result is very sensitive to their treatment. Software failure in digital safety-critical system induces very severe problems on assessing the system safety. It might remove the redundancy effect if the same software is installed in redundant systems. We also cannot detect the failure of software by hardware-based monitoring mechanism. That is, the software could induce severe CCF problem. The analysis result is also very sensitive to the failure probability of software.

2. Factors in digital system safety assessment

2.1 Digital equipments in safety-critical systems

The digital techniques are far from the conventional techniques of analog I&C systems because of some unique features of the digital I&C system. Microprocessors and software technologies are the basic elements of the digital system. They make the system more flexible and powerful but more complex.

From the viewpoint of PSA, there are some important issues in digital systems' safety analysis which are complex and correlated. In this section, we categorize them into six factors and explain through subsections 2.2 to 2.7 for the information of PSA analysts and design engineers. Some of the factors could be modeled explicitly but the others need to be treated implicitly.

Some of the factors are expected to play more important role in analysis. Especially, as mentioned in Introduction, accepting the concepts of 'imperfectness of fault-tolerant mechanism' and 'possibility of software error' might be inevitable for realistic reliability evaluation. For these two critical factors, the importance of them is demonstrated and intermediate methodology is proposed using a fault tree model. The safety and reliability of a fault-tolerant digital system is quite sensitive to the fault coverage and software failure probability.

2.2 Modeling the multi-tasking of digital systems

Microprocessors and software technologies make the digital system multi-functional. That is, a system performs several functions sequentially or conditionally. This multi-tasking feature should be represented in PSA modeling because it will cause the risk concentration and deteriorate the reliability of the system.

The designers of safety-critical systems such as nuclear power plants have adopted a conservative design strategy and have given 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

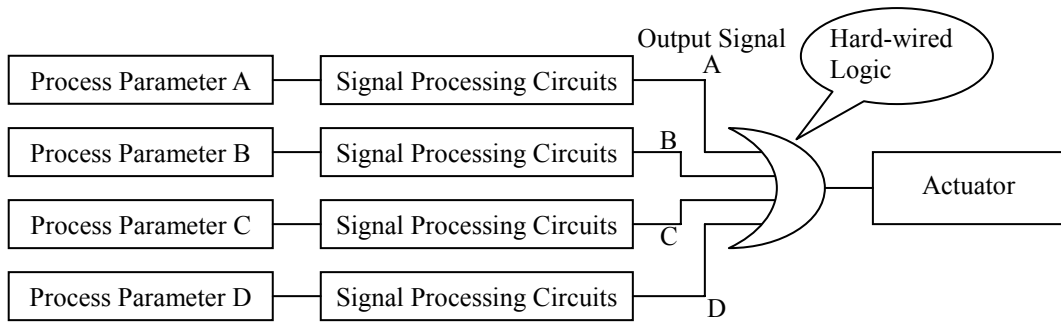
redundancy is no more valid. Especially, in order to compare the developed digital system with the conventional analog system, the effects of multi-tasking on the safety should be carefully modeled and evaluated.

For example, consider two systems shown in Figure 1. As explained above, typical safety critical applications such as a reactor protection system in a nuclear power plant handle diverse process parameters and it provides functional redundancy. Consider the Main Steam Line Break (MSLB) accident. First, 'Low steam generator pressure' parameter (A) triggers the output signal A. As time goes on, the parameters of ' Low pressurizer pressure' (B), ' Low steam generator level' (C), 'Reactor over power' (D) will trigger the output signal B, C and D, respectively. In conventional analog circuit system, as shown in Figure 1 (a), the first triggered output signal, signal A, makes trip circuit breakers open and initiates reactor shutdown. If the signal processing circuits for parameter A fail to generate the proper output signal, the second triggered output signal (B) will trip the reactor. And if the circuits for parameter B also fail, the output signal C, will trip the reactor. However, in the case of digital system, as shown in Figure 1 (b), parameter A, B, C and D use the same equipment for signal processing. If the digital signal-processing unit fails, there is no backup (see Figure 2). Of course, in the safety critical application, there are one or more duplicated trip channels, but conventional analog systems also have fully duplicated channels.

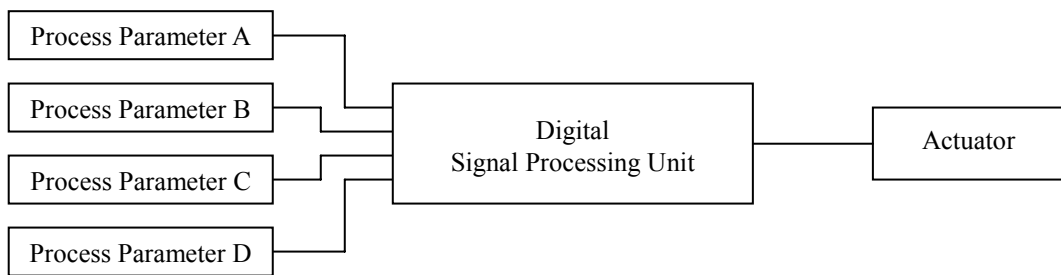
Multi-tasking is generally adopted in microprocessor-based systems, so the signal processing systems in a nuclear power plant tend to have multi-input single-output structure. The multi-tasking of digital systems could result in risk concentration on processing module and output module. It implies that the reliabilities of these components should be analyzed more carefully. From the viewpoint of the designer, it also implies that self-monitoring and fault-tolerant mechanism for these components should be strengthened.

Since the real world is dynamic, the static modeling techniques could not simulate the real world without considerable assumptions. For the comparison between a digital system and an analog system, estimating 'how many parameters will trigger the output signals within the specific time limit for specific kind of accident' is very

important. In this estimation, we need several assumptions, for example, the time limit and the severity of standard accidents. That is, if it is possible, we should define parameters which will be considered for several important standard cases. For example, in the case of MSLB, a reactor protection system should complete its actuation within 30 minutes and it implies that 'Low steam generator pressure', ' Low pressurizer pressure' and ' Low steam generator level' will be considered as the trip parameters.

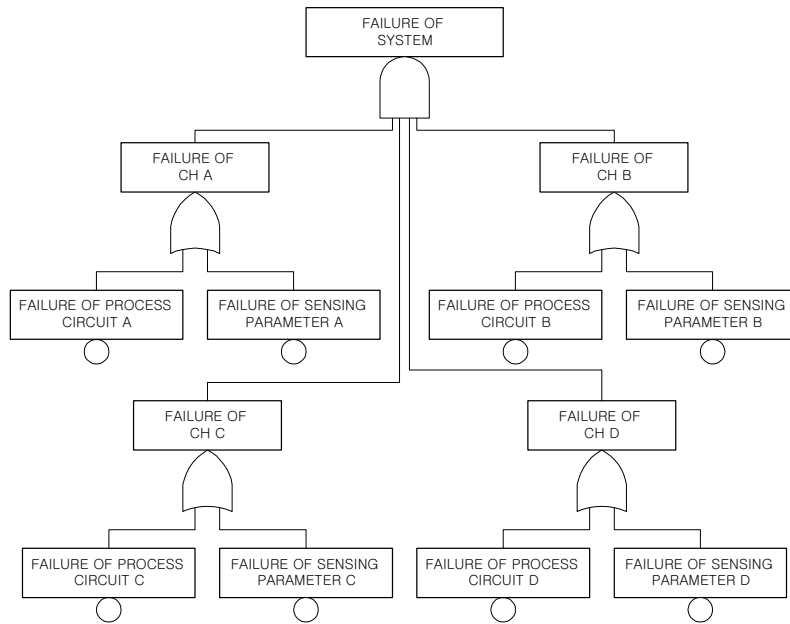


(a) Typical process of signal processing using conventional analog circuits

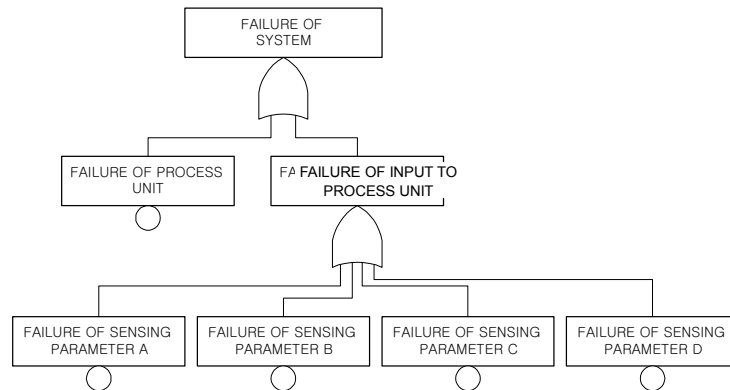


(b) Typical process of signal processing using digital units

Figure 1. Schematic diagram of signal processing using analog circuit and digital processor unit



(a) Fault tree model of the example in Figure 1 (a)



(b) Fault tree model of the example in Figure 1 (b)

Figure 2. Schematic diagram of signal processing using analog circuit and digital processor unit

2.3 Estimating software failure probability

There are ongoing debates among the researchers of software engineering about whether software failure can be treated in a probabilistic manner [4]. Generally, we recognize that software faults are design faults by definition. That is, software is deterministic and its failure cannot be represented by 'failure rate'. When we focus on the software of a specific application, however, the software is no more deterministic because of the randomness of the input sequences. This is the concept of 'error crystals in software,' which is the most common justification for the apparent random nature of software failure. Error crystals are the regions of the input space that cause software to produce errors and a software failure occurs when the input trajectory enters an error crystal.

The position of regulatory bodies including Korea Institute of Nuclear Safety (KINS) can be summarized as 'the reliability of software should be analyzed in a qualitative and quantitative manner and quantitative result will support qualitative result' [7]. However the quantitative software-failure probability is indispensable to the safety assessment of a digital system. Generally, it is considered normal for the microprocessor applications to fail frequently when first installed. They only become reliable after a long sequence of revisions. In safety-critical systems, this approach is known to be inappropriate [8].

Unlike the reliability of hardware components, it has been proved that it is much harder to predict software reliability quantitatively using a conventional model. Software reliability growth model is the most mature technique for software dependability assessment. It estimates the increment of reliability as a result of fault removal. It is assumed that when a failure occurs there is an attempt to remove the design fault that caused the failure. The repeated occurrence of failure-free working is the input to probabilistic reliability growth models, which use these data to estimate the current reliability of the program under study, and to predict how the reliability will change in the future. However, it is hard to select a priori for the most suitable model for a particular situation [9]. Furthermore, in the safety critical

systems such as protection systems in nuclear plants, the fixes cannot be assumed effective and we might assume that the last fix has introduced new faults.

In order to apply software failure probability to the fault tree model, we require the basic event probability of software failure. Conservatively estimated lower limit of software-failure probability by testing can be an alternative. Of course, some researchers insist that the quantification of safety-critical software reliability is infeasible using statistical methods because it leads to exorbitant amounts of testing when applied to safety-critical software [10]. However, in order to show the integrity of developed software, the software must undergo test phase even it is not for calculating reliability. We believe that carefully designed random tests and advanced test methodologies can provide an estimate of the lower bound of the reliability that will be experienced in actual use.

For the convenience of explanation, we will show the example of a highly reliable system. The number of observed failures during test is expected to be zero because when we find an error we will debug the responsible code and restart the testing. So the concept of software failure probability implies the degree of expectation of fault due to the software which shows no error in testing phase.

The reliability is assessed to be no worse than the result of this test with a certain confidence. That is, testing provides the lower bound of the reliability of software. Conventional method to calculate the required number of test can be easily derived as follows. Using the random variable T as the number of tests before the first failure and U as the required number of tests, the confidence level C can be expressed as follows:

$$\begin{aligned} C &= \text{prob}(T \leq U) \\ &= \sum_{t=1}^U p(1-p)^{t-1} = p \left[\frac{1-(1-p)^U}{1-(1-p)} \right] \end{aligned} \quad (1)$$

The failure probability is denoted p . We can solve this equation for U as follows:

$$U = \frac{\ln(1-C)}{\ln(1-p)} \quad (2)$$

According to Equation (2), the higher software reliability is required and the higher confidence level is needed, the more test cases are required. Therefore, an impractical number of test cases might be demanded in some ultra-high reliable

systems. Table 1 shows the required number of tests for some failure rates and confidence levels. For example, if we want to show that the required failure rate is lower than 10^{-6} with 90% confidence level, we have to test the software for 2.3×10^6 cases without failure. However, we expect that this problem of large number of test cases can be resolved through fully automated testing and parallel testing. Especially, in the case of sequential processing software which has no feedback interaction with users or other systems, the test automation method will be a strong candidate for reducing the test burden. The validity of test-based evaluation is dependent on the coverage of test cases. The test cases should represent the inputs which will be encountered in actual use [11].

Littlewood and Wright [12] suggested some test stopping rules in consideration of the case of finding some failures in the middle of testing. We also approach with the concept of reliability allocation. If we can establish the target reliability of the total system, the required software reliability (p) which can satisfy the target can be calculated using the fault tree [13].

Table 1. Required number of test cases

$p \backslash C$	50%	90%	99%
10^{-2}	6.90×10	2.29×10^2	4.58×10^2
10^{-3}	6.93×10^2	2.30×10^3	4.60×10^3
10^{-4}	6.93×10^3	2.30×10^4	4.60×10^4
10^{-5}	6.93×10^4	2.30×10^5	4.61×10^5
10^{-6}	6.93×10^5	2.30×10^6	4.61×10^6
10^{-7}	6.93×10^6	2.30×10^7	4.61×10^7
10^{-8}	6.93×10^7	2.30×10^8	4.61×10^8

2.4 Estimating the effect of software diversity and V&V efforts

In order to assess the expected failure rate of software, we also should consider the efforts on the lifecycle of software [14]. Previous experimental researches showed that the application of formal methods to the software development process and the usage of mathematical verification of the software specifications could reduce the possibility of fault due to design failure [15]. As explained in above section, the failure rate of safety-critical software represents the degree of expectation of failure or the possibility of failure. As we expect that the application of software verification and validation (V&V) methodologies could reduce the number of potential faults remained in the software, this effect should be reflected on the probability estimation of basic events. That is, the quantification of the rigidity of software V&V should be performed through PSA process.

Formal methods including formal specification technique are particular examples of software V&V processes. Formal methods use ideas and techniques from mathematical or formal logic to specify and reason about computational systems [16]. The notion of mathematical proof is the most important effect of these methods. Even though the extent of this kind of proofs is limited, they are still one of the strongest aids for developing extremely high reliable software. Welbourne [17] stated that these methods had been widely shown to be feasible in other industries. Besides these formal methods, there are many kinds of approach for improving the quality of software production.

We expect that Bayesian belief network (BBN) can be used for reflecting these quality-improving efforts [18], [19]. Applying BBN to the PSA of digital equipment will be helpful in systemically estimating the completeness of the software engineering and the quality assurance. This estimation should be performed in consideration of various kinds of activities in each stage of software lifecycle.

Diversity of software plays an important role in fault tolerance of digital systems. Diversity can be implemented without modification of hardware components by installing two or more versions of software which are developed by different teams because we expect that faults will tend to be different so failures can be masked by a

suitable voting mechanism. Design diversity does bring an increase in reliability compared with single versions, but this increase is much less than what completely independent failure behavior would imply. Littlewood and Strigini [9] also insist that this independence assumption is often unreasonable in practice. Therefore, the degree of dependence must be estimated for each particular case.

2.5 Estimating the coverage of fault-tolerant features

In the nuclear industry, we should especially concentrate on watchdog timer and duplication technique used in fault-tolerant system. They are the simplest way to establish a fault-tolerant system and already applied to some nuclear applications. When we analyze the duplication, we should carefully consider the CCF among duplicated components.

Microprocessors and software technologies make it possible to implement various fault-tolerant mechanisms which check the integrity of the system itself and to monitor the integrity of each other. The experience shows that these fault-tolerant mechanisms effectively detect the fault on the system but they are not perfect. Digital systems have various kinds of fault and the coverage of the fault-tolerant mechanism is limited.

We expect that this aspect can be expressed using the concept of the coverage factor. In the fault tree, this coverage must be considered. Because the safety systems in nuclear plants adopt 'fail-safe' concept, the coverage factor plays a critical role on assessing the safety of digital systems. The watchdog devices are widely adopted for the fault-tolerance feature of safety systems in nuclear power plants to generate trip signal at the failure of microprocessor-based devices.

For the convenience of explanation, consider the simplest example of a watchdog timer application. It is illustrated in Figure 3. When the watchdog timer detects the failure of processor, it will isolate the power. The fault tree for the system in Figure 3 is shown in Figure 4.

As shown in Figure 4, we categorize watchdog timer failures into two groups: The first is the failure of the watchdog timer itself (recovery failure). The second is that

the watchdog timer cannot detect the failure of microprocessor (functional failure). The symbol p , c and w represent the probability of processor failure, the coverage factor and the probability of watchdog failure (recovery failure), respectively.

For the illustration of the effect of the coverage factor, Figure 5 shows the example system unavailability versus the coverage factor when we assume that p and w are equal to 10^{-3} and 10^{-7} , respectively. The value of p , 10^{-3} failure/demand, is the typical level of failure rate for programmable logic processors. The value of w , 10^{-7} failure/demand, represents the typical failure rate of simple circuit and contact. If the watchdog mechanism is perfect ($c=1$), the reliability of microprocessor-based device will be negligible and the system reliability totally depends on the reliability of the watchdog device. In this case, the system unavailability is 10^{-20} . If the coverage equals zero ($c=0$), the system unavailability is 10^{-6} . Generally, it is well known that the coverage of the watchdog timer is not so high because it is the simplest method among the fault-tolerant mechanisms. The graph in Figure 5 shows the importance of reasonable estimation of the coverage factor of fault-tolerant mechanism.

The remaining problem is to estimate the value of coverage factor. Unfortunately, there is no widely-accepted method except experiment. However, we expect that the simulation using a fault injection method will be promising for estimating the coverage factor. The knowledge of domain experts will be helpful also. Before the credible methodology is developed, even though the exact coverage of the watchdog timer is hard to estimate, we can establish the lower bound of the coverage using similar methods explained in software failure probability.

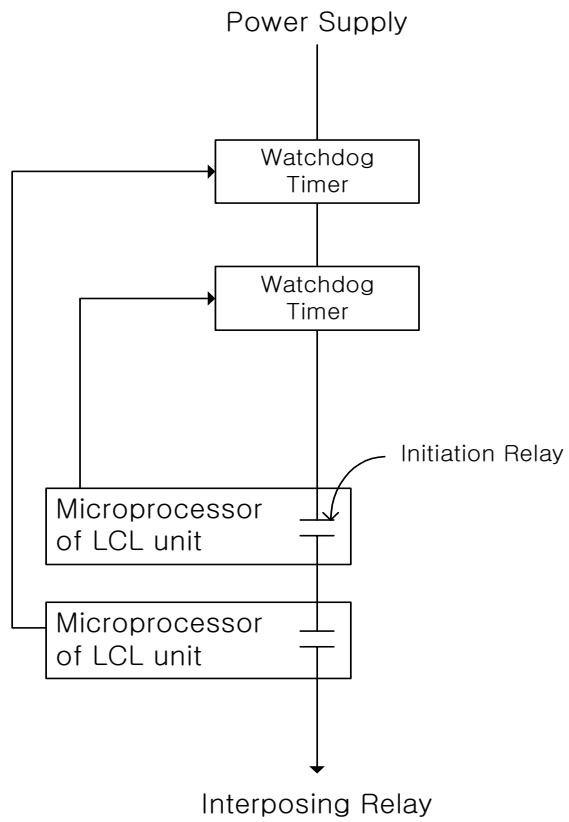


Figure 3. Schematic diagram of a typical watchdog timer application

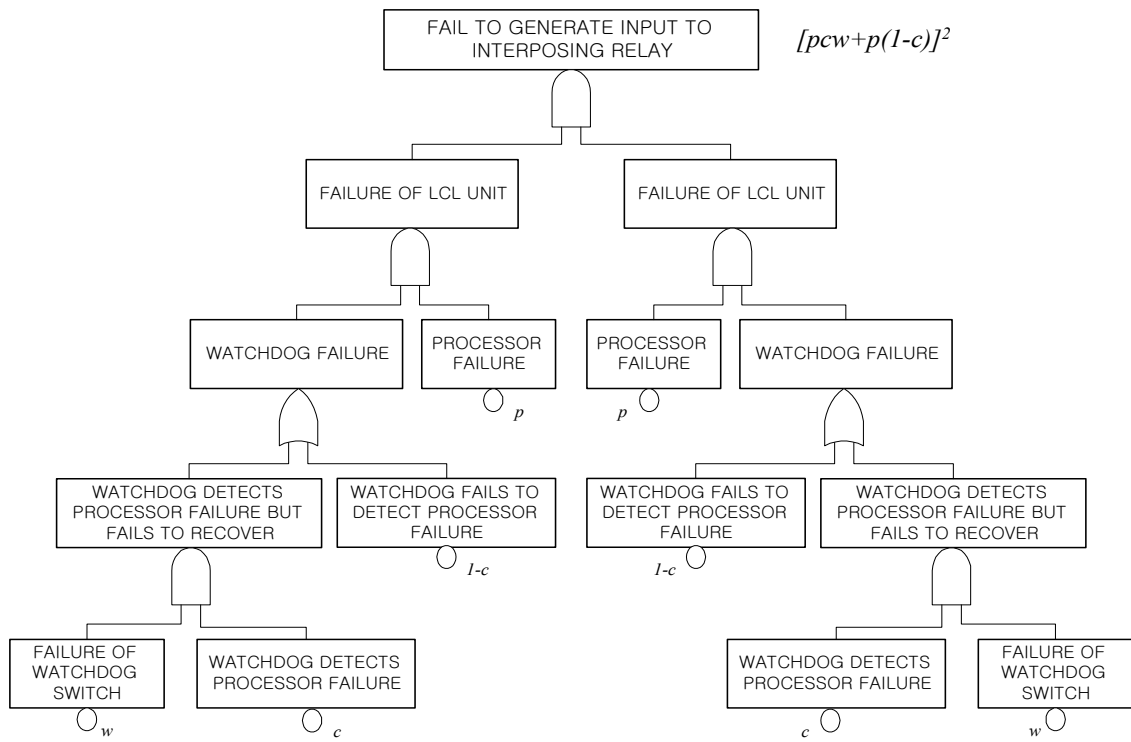


Figure 4. Fault tree model of the system shown in Figure 3

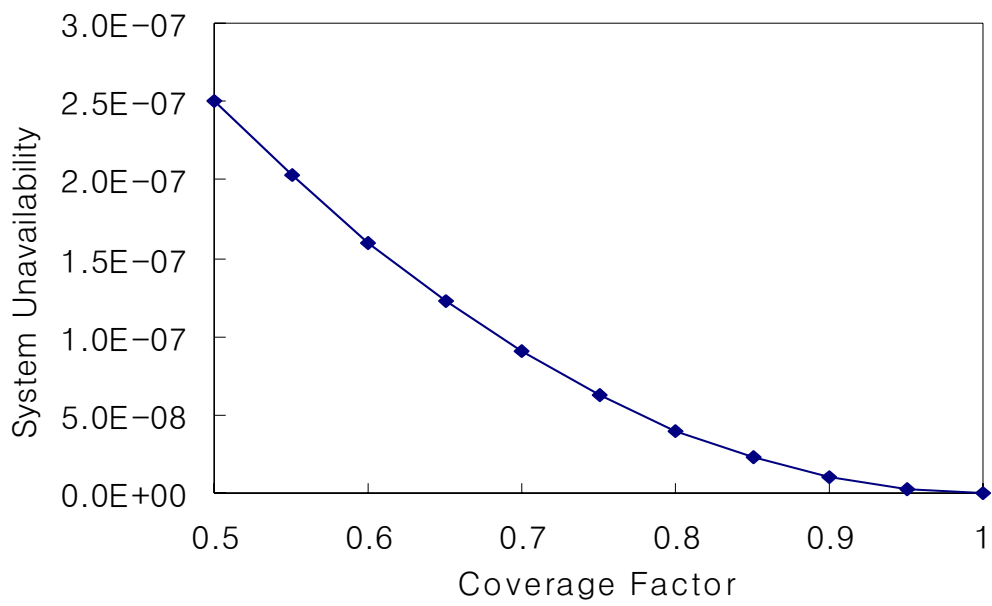


Figure 5. Illustration of system unavailability along the coverage factor
($p = 10^{-3}$, $w = 10^{-7}$)

2.6 Estimating the CCF probability in hardware

The importance of precise estimation of the CCF of digital equipment should be emphasized. As explained above, the application of digital equipment to the safety-critical system will induce more risk concentration. In the case of adopting the same equipment as the redundancy, this concentration will be more critical. Even the products from different vendors do not guarantee the independence of faults. Global standardization and the large manufacturer in electric part market lead to produce similar digital hardware products by different vendors.

In the case that operating experience is enough and generic CCF data is available, we can use the conventional methodologies (β factor approach or Multiple Greek Letter approach). However, in the case of newly designed dedicated systems such as safety-critical calculators in nuclear power plants, generic data is unavailable. Thus, the development of new and precise estimation methodology for the CCF factor of digital hardware is required.

2.7 Modeling the interactions between hardware and software

Conventionally, the research on the hardware reliability and that of software reliability has been independently performed. Therefore, there are some attempts which estimate the reliability of digital system by calculating that of hardware and software separately [20]. In this case, however, we cannot evaluate the effect of interactions between hardware and software.

Most microprocessor-based systems have fault-tolerant mechanisms which are based on hardware and software. They make the system complex but are expected to reduce the number of system failures. Choi [21] also showed that there exists obvious effect of hardware fault masking by software. That is, a substantial number of faults do not affect the program results for several reasons: faults whose errors are neutralized by the next instructions, faults affecting the execution of instructions that do not contribute to the benchmark results, and faults whose errors are tolerated by

the semantic of the benchmark under execution. He insists that these interactions might be very important factors to estimate the dependability of systems. Therefore, the system dependability measurement technique should not consider software and hardware separately and the effect of interaction should be considered properly because even a small change of system fault coverage value could affect the system dependability.

When we consider aging effect on hardware, the problem becomes more complex. The aging effect will induce slight changes on hardware. By some software, the system will make faulty output but by the other software, it will not. Furthermore, we should also consider the correlated effect of hardware design faults and software faults and the correlation between diverse hardware and software. These considerations might result in very complex and impractical models.

Clearly, the modeling of interactions between hardware and software requires much further and extensive investigation. For more realistic results, however, these complex interactions should be considered in a proper manner.

2.8 The other factors

Due to the complexity of microprocessor-based system, there are lots of unsolved problems. In this report, from the practical viewpoint of PSA, we summarize the factors which should be considered in modeling the digital systems as follows:

- Modeling the multi-tasking of digital systems,
- Estimating software failure probability,
- Estimating the effect of software diversity and V&V efforts,
- Estimating the coverage of fault-tolerant features,
- Estimating the CCF probability in hardware, and
- Modeling the interactions between hardware and software.

Major problems which are not mentioned in this study can be listed as follows. Further investigation on these problems is strongly recommended.

- Failure mode of digital system,

- Environmental effects, and
- Digital system induced initiating events including human errors.

3. Analytic Evaluation in the Context of PSA

3.1 Case study layout

The plant protection system (PPS) is one of the most important safety-critical digital systems. In this report, we established a PSA model of the digital PPS with four-channel redundancy. Many PPSs of nuclear power plants including Korean Standard Nuclear Plant (KSNP) adopt four-channel layout. Figure 6 shows the schematic diagram of a typical four-channel PPS including selective two-out-of-four voting logic. The detailed component design and algorithms of the PPS is flexible. Kim, et al. [7] reported the design concept of the digital PPS of KSNP as shown in Figure 7 which shows the components layout. The full system description and design concept of KSNP are not available now because it is under construction. We assumed its layout as shown in Figure 7. So the results shown in this report are based on various assumptions for unknown parts. Although the data of the assumed digital PPS is not complete, we expect that analytic assessment will provide meaningful insights to the designers and the analysts.

Four redundant channels are provided to satisfy single failure criterion and improve plant availability. We assumed that each channel of PPS contains two bistable processors and four local-coincidence-logic processors. The bistable processor in each channel receives analog inputs from sensors through analog input modules. A bistable processor compares the input signals to the trip setpoints and transmits results to local-coincidence-logic processors. A local-coincidence-logic processor performs two-out-of-four voting for each process input using the signals from four bistable processors. It produces the output signal using independent digital output module. Its stall will result in loss of its heart beat signal output to a watchdog timer, then the watchdog timer will force the PPS trip and initiate trip signal. Figure 8 shows the structure of a selective 2-out-of-four logic which initiates the interposing relay.

With this layout, we made several assumptions such as: 1) We use all-mode-failure date, 2) The effect from the other components except PPS is neglected, 3)

Every processor contains the identical software program, 4) We ignore the fail-to-hazard probability of the network or serial communications, the inter-system data bus, and the back plane of PLC. The detailed assumptions will be described in section 4.2.

The aim of this study is to investigate the quantitative relationship between the important factors and the PSA results. So even though the adequacy of these assumptions is not guaranteed and the model requires further refinement, the results of PSA could provide useful insights.

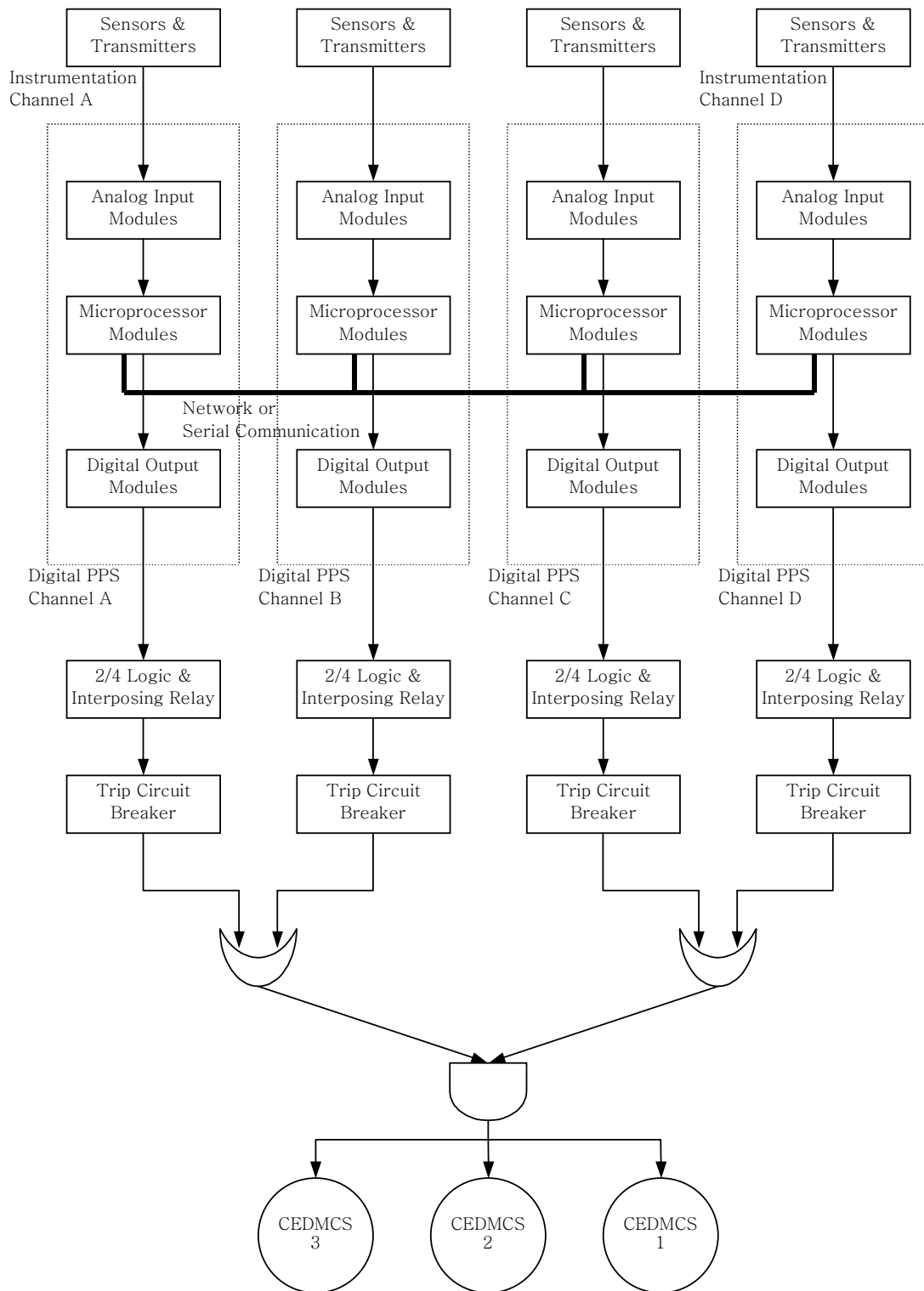


Figure 6. The schematic diagram of a typical four-channel digital PPS

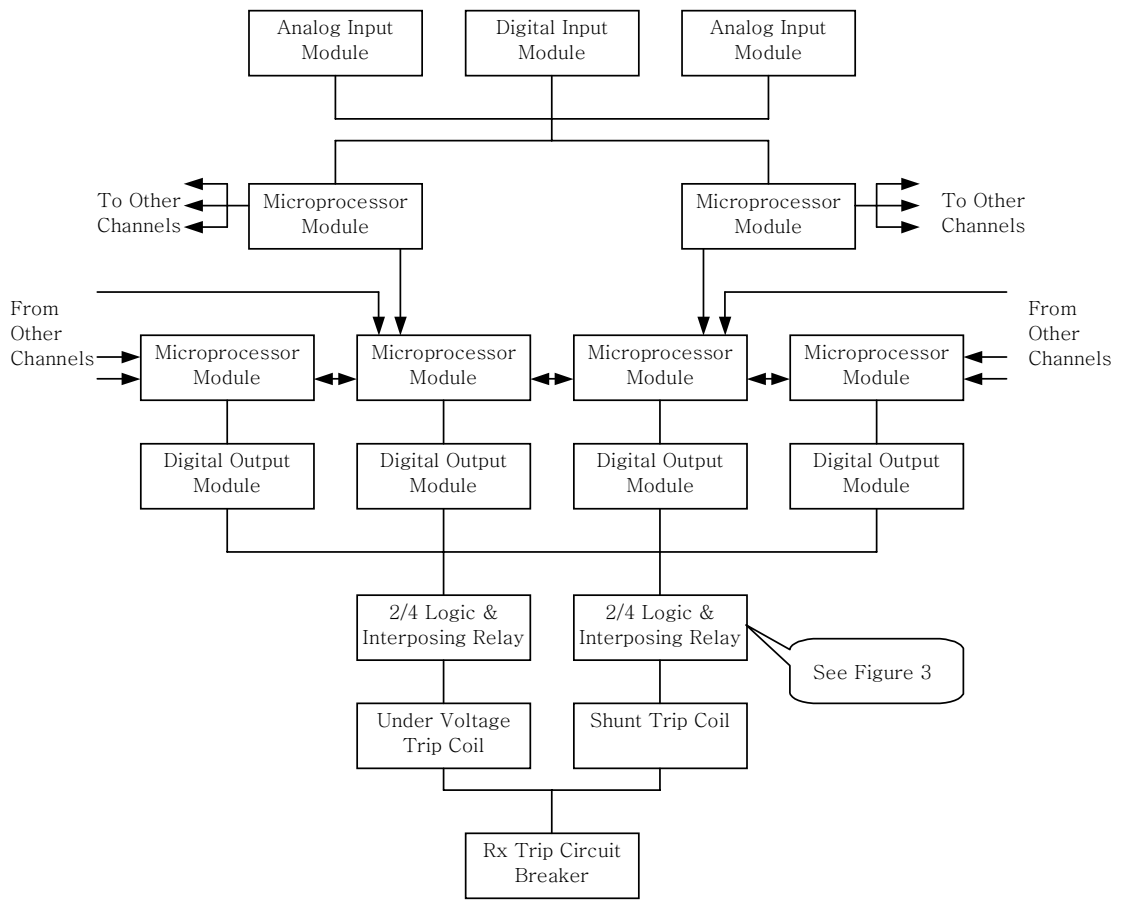


Figure 7. The functional diagram of each channel of the PPS

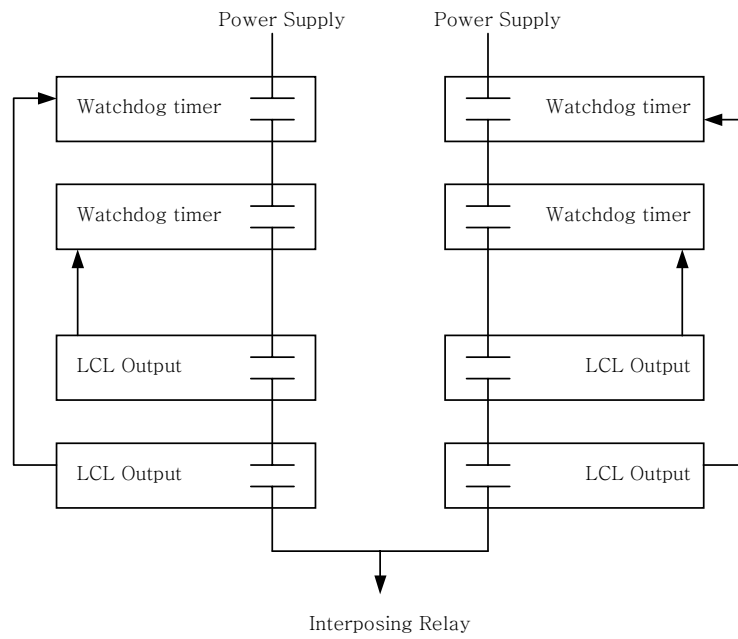


Figure 8. The detailed diagram of a selective 2-out-of-four logic which initiates the interposing relay. (LCL: local-coincidence-logic)

3.2 The analytic assessment of system unavailability

Generally, the result of the fault-tree calculation is expressed in the form of a probability sum as follows:

$$\text{System Unavailability} = q_1 + q_2 + \dots + q_i + \dots + q_n \quad (1)$$

$$q_i = p_1 \times p_2 \times \dots \times p_j \times \dots \times p_m \quad (2)$$

where q_i is the probability of cutset i and p_j is the probability of basic event j . The probability of a basic event in the fault tree is the failure probability of a corresponding component. Cutset can be defined as a set of system events that, if they all occur, will cause system failure [22].

Generally, we can categorize the cutsets of multi-channel protection systems into four groups: 1) Cutsets which disturb collecting input signals, 2) Cutsets which disturb generating proper output signals, 3) Cutsets which cause the distortion of processing results, and 4) Cutsets of the possible combinations of events which make all channel unavailable. Schematically we can draw a diagram for the explanation of this grouping as shown in Figure 9.

In the case of the example PSA, we can easily expect that the four-channel redundancy makes the probabilities of almost whole ‘possible combinations of basic events’ negligible because the order of the failure probabilities of digital modules are less than 10^{-3} per demand. That is, the cutsets in group 4) will be negligible. Then the cutsets which contain CCF events become the main contributors to system unavailability. The CCF is the failure of multiple components at the same time. And in the case of the example system, the probability of CCF is much higher than the probability of the combinations of different basic events.

By the analyses of several possible design alternatives, we ascertain this expectation. The details of the analysis result depend upon the design concept of the system, but every dominant cutset of the four-channel digital protection system consists of the CCF probabilities of digital modules and the error probability of a human operator. Conceptually, the dominant cutsets of a multi-channel digital

protection system can be expressed mathematically as follows:

$$\begin{aligned}
 q_1 &= \Pr(\text{OP}) \times \Pr(\text{AI CCF}) \\
 q_2 &= \Pr(\text{OP}) \times \Pr(\text{DO CCF}) \\
 q_3 &= \Pr(\text{OP}) \times \Pr(\text{PM CCF}) \times \Pr(\text{WDT CCF}) \\
 q_4 &= \Pr(\text{OP}) \times \Pr(\text{PM CCF}) \times \{ \Pr(\text{WDT } \alpha_1) \times \Pr(\text{WDT } \alpha_3) \dots \} \\
 q_5 &= \Pr(\text{OP}) \times \Pr(\text{PM CCF}) \times \{ \Pr(\text{WDT } \alpha_1) \times \Pr(\text{DO } \beta_3) \dots \} \\
 &\dots
 \end{aligned}
 \tag{3}$$

where

- $\Pr(\text{OP})$ the probability that a human operator will fail to manually initiate the reactor trip
- $\Pr(\text{AI CCF})$ the probability of the CCF of analog input modules
- $\Pr(\text{DO CCF})$ the probability of the CCF of digital output modules
- $\Pr(\text{PM CCF})$ the probability of the CCF of processor modules
- $\Pr(\text{WDT CCF})$ the probability of the CCF of watchdog timers
- $\Pr(\text{WDT } \alpha)$ the probability that the watchdog timer α will fail to initiate the reactor trip
- $\Pr(\text{DO } \beta)$ the probability that the digital output module β will fail to initiate the reactor trip.

The first and the second cutsets (denoted by q_1 and q_2) of equation (3) correspond to the probability of simultaneous failures of a human operator and all input/output modules. The third cutset, q_3 , implies the probability of simultaneous failures of a human operator, all processor modules and all watchdog timers. The fourth and fifth cutsets, q_4 and q_5 , of equation (3) correspond to the probability of simultaneous failures of a human operator and all processor modules and the combined failures of watchdog timers and digital output modules. The cutsets of q_3 , q_4 and q_5 are related to the processor module.

The processor module is the most complex part of a digital system and the

reliability of this module is relatively lower than input/output modules. Furthermore, it contains the software. In this analysis, we assume that the software failure probability is included in the failure rate of the processor module. Installation of the same software in redundant systems might remove the redundancy effect. Therefore, the CCF of processor modules will be a major obstruction to the proper working of digital protection systems. However, most safety-critical applications such as protection systems of nuclear plants will reduce the risk by adopting fault-tolerant mechanisms. If the fault-tolerant mechanisms are effective enough, the safety of the system will not be severely affected by the failure probability of processor modules. They might be effective but not perfect. In the case of watchdog timer applications, we expect relatively low fault detection probability. The failure probability of a watchdog timer should include the detection probability of a processor module's fault.

$\Pr(OP)$ in the equation (3) is not directly correlated to the digital system. And the effect of $\Pr(WDT \alpha)$ and $\Pr(DO \beta)$ on the system safety is relatively small. Then, from the equation (3), we find critical variables: $\Pr(AI \text{ CCF})$, $\Pr(DO \text{ CCF})$, $\Pr(PM \text{ CCF})$, and $\Pr(WDT \text{ CCF})$.

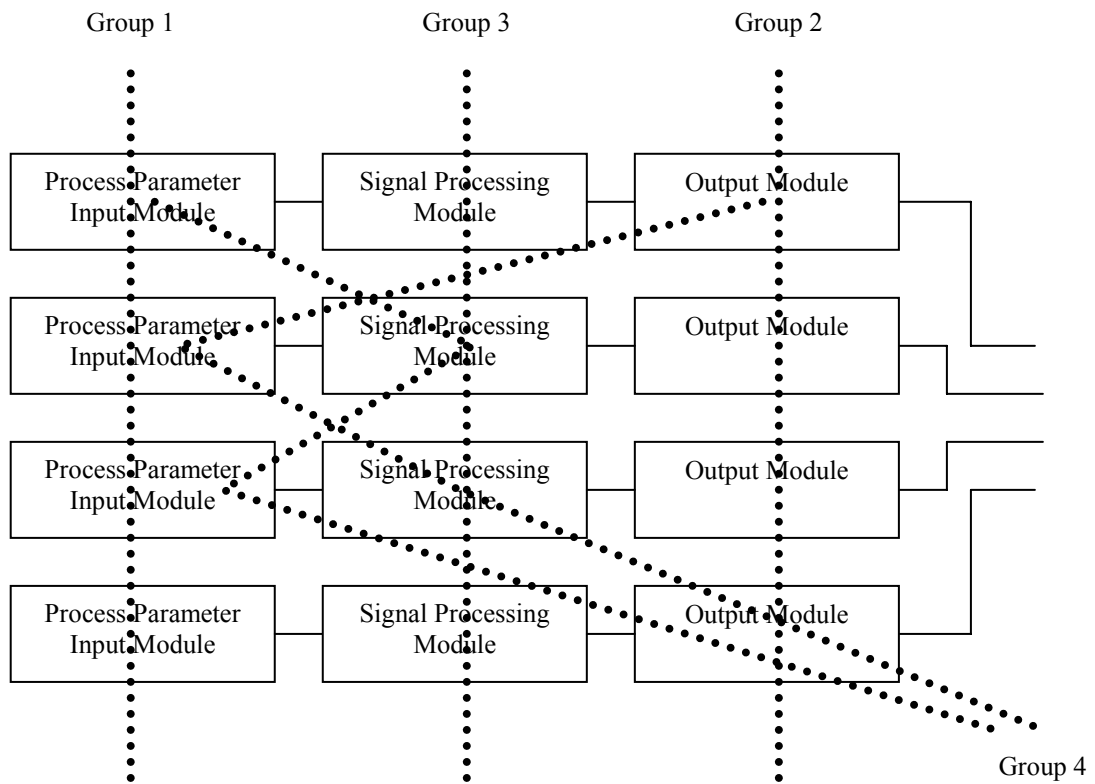


Figure 9. The schematic diagram of grouping the cutsets

3.3 Relationship between the factors and PSA results

We can also summarize the effect of each factor listed in section 2.8 to the result of the PSA shown in the equation (3) as follows:

- Modeling the multi-tasking of digital systems: Not available
This factor is related to the ‘function of system’, so it should be explicitly modeled in the fault tree.
- Estimating software failure probability: q_3
We consider the failure probability of software as one of the processor-failure causes. Especially, if the same software is installed to several redundant processors, it will possibly induce a CCF of processor modules.
- Estimating the effect of software diversity and V&V efforts: q_3
Software is related to the function of processor module, so it should be explicitly modeled in the basic event for processor failure. Well-verified/validated software implies relatively small failure number of processor function.
- Estimating the coverage of fault-tolerant features: q_4 and q_5
Failure of fault detection affects the safety of system more critically than the failure of watchdog timer itself does. The successful fault detection directly implies successful fault removal because safety-critical applications usually adopt ‘fail safe’ concept. So the coverage of fault-tolerant features should be reflected in watchdog timer failure probability.
- Estimating the CCF probability in hardware: All (q_1 , q_2 , q_3 , q_4 and q_5)
CCF is the critical factor of the system failure in the case of multi-channel safety system. Precise estimation of CCF probability will improve the reality of the overall safety evaluation.
- Modeling the interactions between hardware and software: q_3
Software and processor hardware is related to the function of processor module, so it should be explicitly modeled in the basic event for processor failure.
- Failure mode of digital system: All

The failure modes of digital systems are not well defined yet. Usually analysts utilize all-mode-failure data that contains both 'fail to safe' and 'fail to hazard' cases because the more precise data is not available. If the failure modes can be defined and adequate data is available, the result of safety evaluation will be more realistic.

– Environmental effects: All

It is well known that generally the digital system is sensitive the environmental condition.

– Digital system induced initiating events including human errors: N/A

This factor should be inspected from the plant-wide viewpoint.

4. A Sensitivity Study

4.1 The selection of parameters

In this chapter, we will show the sensitivity of the PSA result along the critical variables mentioned in chapter 3. Equation (3) is derived using static methodology, the fault tree method, so the complex and dynamic features of digital systems are not fully reflected. The lack of failure data is another weak point of analysis. However, although the data and modeling methodology of the digital protection system is not yet complete, we expect that the intuition from equation (3) will be helpful in designing a safer system. Especially, a systematic analysis and a quantitative comparison between the design alternatives are expected to support decision-making for design improvement [23].

The CCF probabilities of input/output modules, $\Pr(\text{AI CCF})$ and $\Pr(\text{DO CCF})$, depend on the system design because the variation of the failure probability of the safety-critical-grade hardware is limited. So we assume three design alternatives: 1) a system which uses identical input modules and identical output modules, 2) a system which uses two kinds of input modules and identical output modules, and 3) a system which uses two kinds of input modules and two kinds of output modules. For each design alternative, we establish a separate fault tree model to perform sensitivity studies.

The CCF probability of processor modules, $\Pr(\text{PM CCF})$, depends on the hardware failure probability of processor module itself, the software failure probability, the diversity of processor modules, and the interaction effect between hardware and software. For the simplicity of sensitivity study, we assume that identical processor modules are used and ignore the interaction effect between hardware and software. So $\Pr(\text{PM CCF})$ depends on the software failure probability. There are ongoing debates among the software engineering researchers about whether software failure can be treated in a probabilistic manner [4]. Generally, from the deterministic viewpoint, software is deterministic and its failure cannot be represented by a 'failure rate'. When we focus on the software of a specific

application, however, the software is no more deterministic because of the randomness of the input sequences. This is based on the concept of 'error crystals in software,' which is the most common justification for the apparent random nature of software failure [1]. Error crystals are the regions of the input space that cause software to produce errors and a software failure occurs when the input trajectory enters an error crystal. As explained in chapter 2, the software failure probability of 1.0×10^{-6} with 90% confidence level implies 2.30×10^6 tests, so we think that proving less than 10^{-6} failure probability by testing method is impractical. And the software which has more than 10^{-4} failure probability cannot be expected to be applied to safety-critical system such as the PPS of nuclear power plants. In this study, we adopt the 'error crystal' concept, and use 0.0, 1.0×10^{-6} , 1.0×10^{-5} , and 1.0×10^{-4} for the value of software failure probability. The value 0.0 for software failure probability implies the perfect software.

And $\text{Pr}(\text{WDT CCF})$ depends on the failure probability of contained relay and the fault coverage of watchdog timers. Because we assume that the variation of the failure probability of the safety-critical-grade hardware is limited, $\text{Pr}(\text{WDT CCF})$ mainly depends on the fault coverage of a watchdog timer. The reliability of a watchdog device is extremely higher than that of a microprocessor-based device because of its simplicity. If we assume that the watchdog mechanism is perfect, the failure rate of microprocessor-based device will be negligible and the system unavailability totally depends on the failure rate of the watchdog device and non-monitored devices. In order to avoid such an unrealistic analysis, the concept of coverage factor should be applied. A survey on the error detection [24] shows an experimental result that the 73% of injected faults were detected by various mechanisms using watchdog processors in the case of Z-80 microprocessor. It is well known that the watchdog microprocessors-based fault detection methods using are superior to the watchdog timer-based methods. Therefore, we assume that the 70% is the maximum of fault-detection coverage of watchdog timer-based methods and that 30% to 70% is the range of watchdog timers' fault coverage. Practically, we think that 40% to 60% is the reasonable range of watchdog timers' fault coverage. Finally, we use the discrete values of 0.3, 0.4, 0.6, 0.7, and 1.0 for the value of the coverage

factor. The value 1.0 for the coverage of watchdog timer implies the perfect detection of faults in a processor module.

We performed a total of 60 ($3 \times 5 \times 4$) calculations. In this study, we consider only two trip parameters (steam generator level and pressurizer pressure) and ignore the CCF probability between different kinds of hardware devices even if they are used for the same purpose.

4.2 Fault tree model

The scope of fault tree model is from process sensors and transducers to trip circuit breakers (TCB). Using KwTree, which is the fault-tree analysis software package produced by Korea Atomic Energy Research Institute, we establish the fault tree model. The assumptions used in the model can be summarized as follows:

- The probabilities of basic events are assumed to be the value of the programmable logic controller (PLC) modules which are expected to be used in nuclear industry. Since we don't have enough information, all failure modes assumed to be hazardous.
- Since this analysis is concentrating on the digital system itself, the effect from the other components such as trip circuit breakers, interposing relays, sensors and transducers is out of scope even though they are modeled in fault tree. For the simplicity of analysis, we assumed zero failure rates to these non-PPS components.
- Watchdog timers monitor the status of local-coincidence-logic processors and local-coincidence-logic processors monitor the status of bistable processors. Since the coverage of timer-to-processor monitoring is much lower than that of processor-to-processor monitoring, we cannot assume the coverage of timer-to-processor monitoring as unity. As mentioned in section 4.2, the coverage of watchdog timers is treated as a variable.
- We assume that every processor contains the identical software program and the software failure induces the CCF of processors. As mentioned in section

4.2, the failure probability of software is treated as a variable.

- 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 PLC.
- We assume that the components are tested at least one per month.

Figures 10 and 11 shows the master diagram of established fault tree. The top event of this fault tree is the event of ‘Fails to trip the reactor’. This top event will happen when one of control-element-driving mechanism (CEDM) buses is not interrupted. CDEM bus interruption failure is caused by the failure of successful functioning of TCBs. It implies the failure of the TCB component itself or the failure of signal which initiates the actuation of the TCB. The signal to the TCB is generated by two components of an undervoltage (UV) trip coil and a shunt trip coil. Similarly, they are caused by the failure of the components themselves or by the failure of activating signals. The signals to trip coils are generated by interposing relays (IR) or by a manual trip switch. IR failures are also caused by the failure of the components themselves or by the activating signal failure from the PPS channel A.

PPS channel consists two paths for generating trip signal and each path consists two local-coincidence-logic modules. The failure of local-coincidence-logic module is caused by three reasons: 1) The failure of output module, 2) The failure of processor module and watchdog timer, and 3) The failure of input to local-coincidence-logic module. The failure of output module implies the failure of component itself. The failure mechanism of the processor module and the watchdog timer is explained in chapter 2. The failure of input to local-coincidence-logic module is caused by the failure of bistable processors, the failure of the input modules of bistable processor, and the failure of sensors.

4.3 The result of PSA

The results of this sensitivity study are graphically illustrated in Figures 12 to 14.

Of course, the best unavailability of 4.80×10^{-9} is obtained from the system which has diverse input/output modules, perfect software and 100% fault coverage while the system which has identical input/output modules, poor software and poor fault coverage shows the worst result of 1.60×10^{-5} . From this result, we find that the CCF treatment is the most important factor among the factors which affects the PSA result of the digital system. And the fault coverage of watchdog timer and the software failure probability also affect the PSA result severely.

And we can check the order of magnitude of the conventional PPS design. Practically, as explained in section 4.1, it is very hard to show the software failure probability is under 1×10^{-5} and the fault coverage of a watchdog timer is over 0.7. If we use the identical input/output modules and processor modules, the four-channel redundant digital PPS will have the system unavailability around 3.7×10^{-6} as shown in Table 2. However if we adopt the design of diverse input/output modules, it will have the system unavailability around 4.6×10^{-7} as shown in Table 4.

Even though the human error is not in the scope of sensitivity study, we consider 5% as the human error probability in order to get the realistic numerical scale of results. If the human error probability is excluded, the quantitative values of unavailability become 20 times as large as the results shown in Figures 12 to 14.

The result of quantitative assessment shows that these factors remarkably affect the system safety. Quantitatively, the value of each factor changes the system unavailability up to several thousand times. That is, inappropriate considerations of these three important factors will induce unreasonable assumptions and severely distort the analysis results.

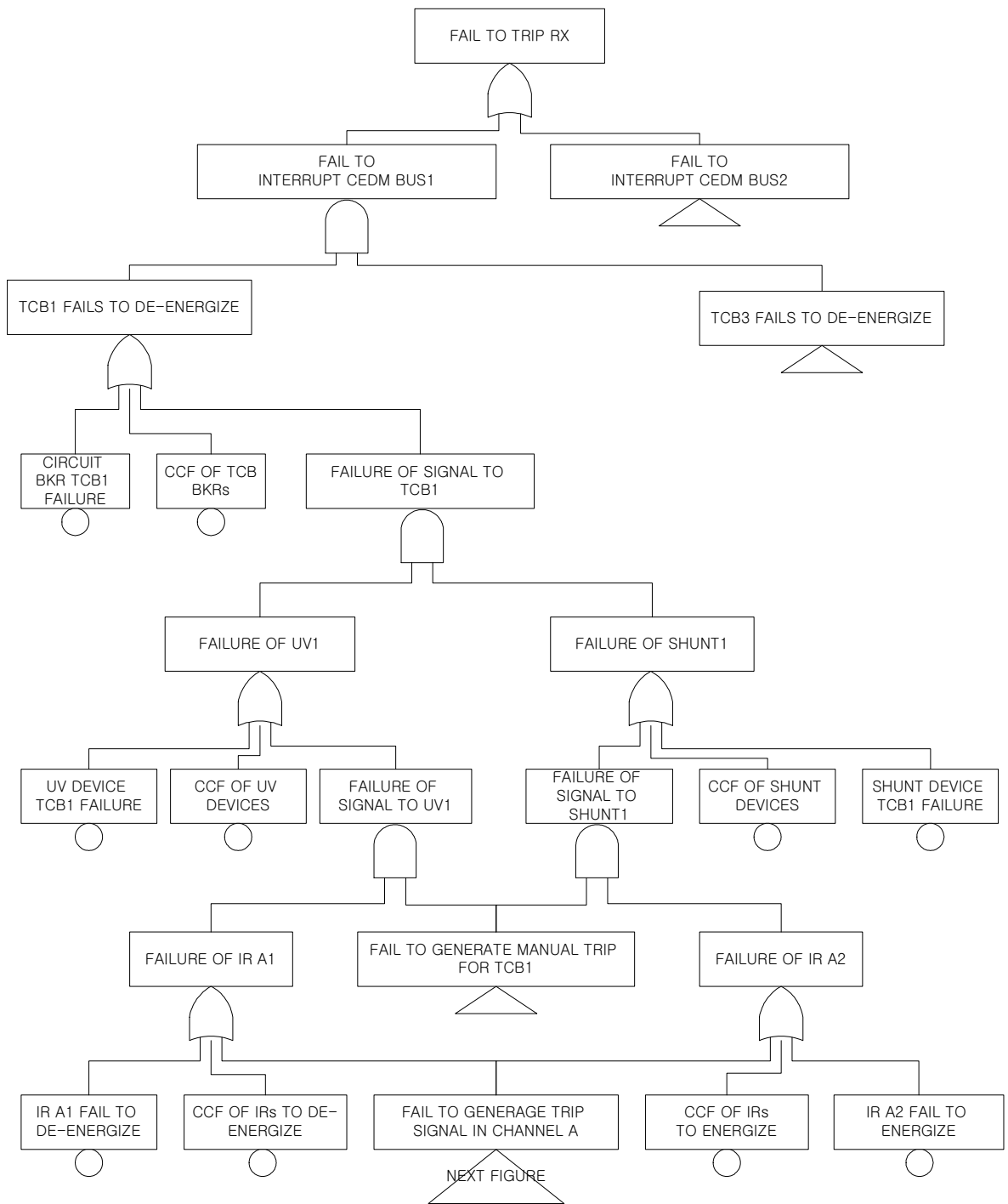


Figure 10. The master diagram of the fault tree for case study (1)

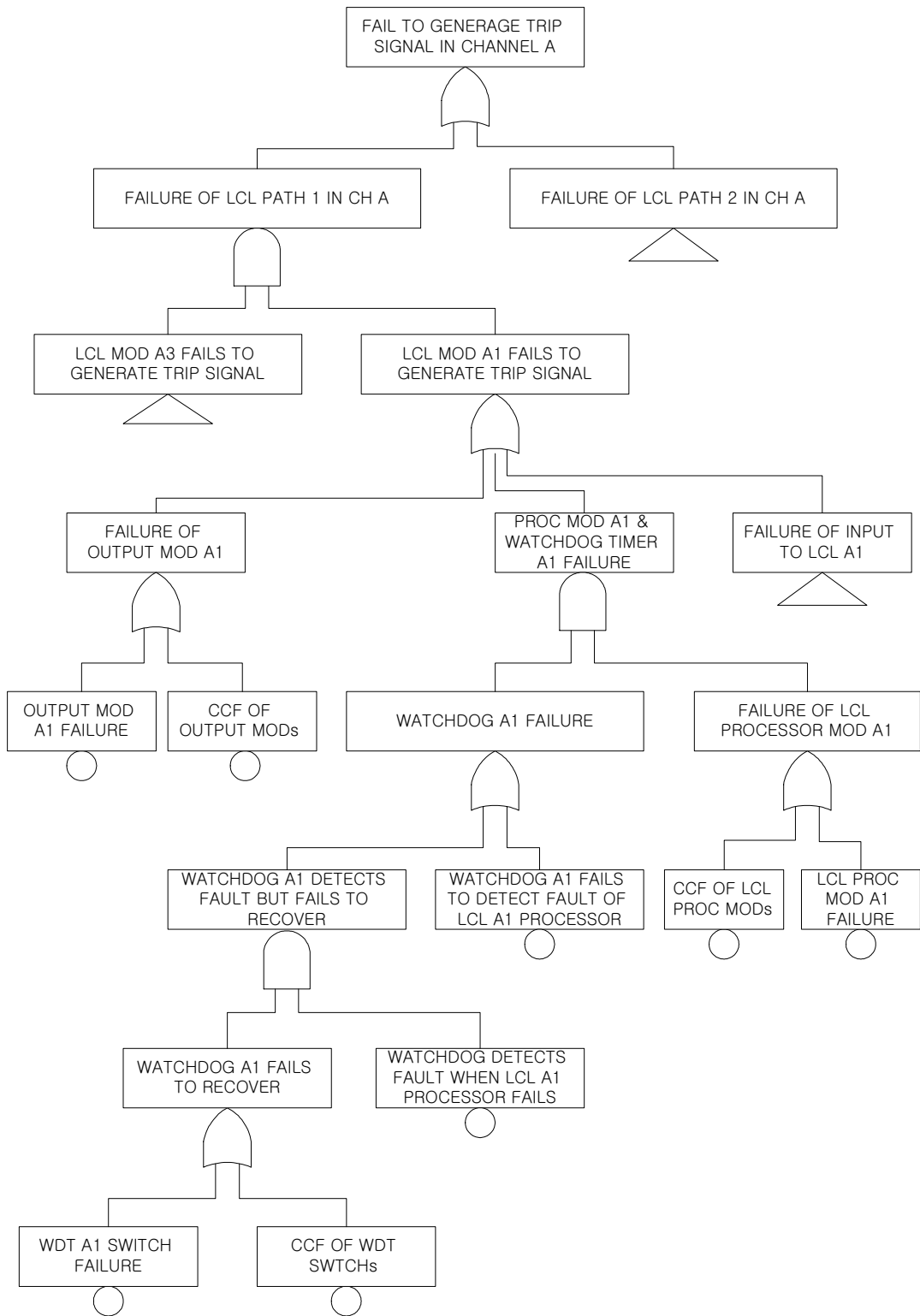


Figure 11. The master diagram of the fault tree for case study (2)

Table 2. System unavailability when the identical input modules and the identical output modules are used

System Unavailability		Software Failure Probability			
		0.00E+00	1.00E-06	1.00E-05	1.00E-04
Fault Coverage	0.3	6.06E-06	6.16E-06	7.06E-06	1.60E-05
	0.4	4.83E-06	4.88E-06	5.38E-06	1.03E-05
	0.6	3.65E-06	3.66E-06	3.77E-06	4.88E-06
	0.7	3.44E-06	3.45E-06	3.49E-06	3.92E-06
	1.0	3.31E-06	3.31E-06	3.31E-06	3.31E-06

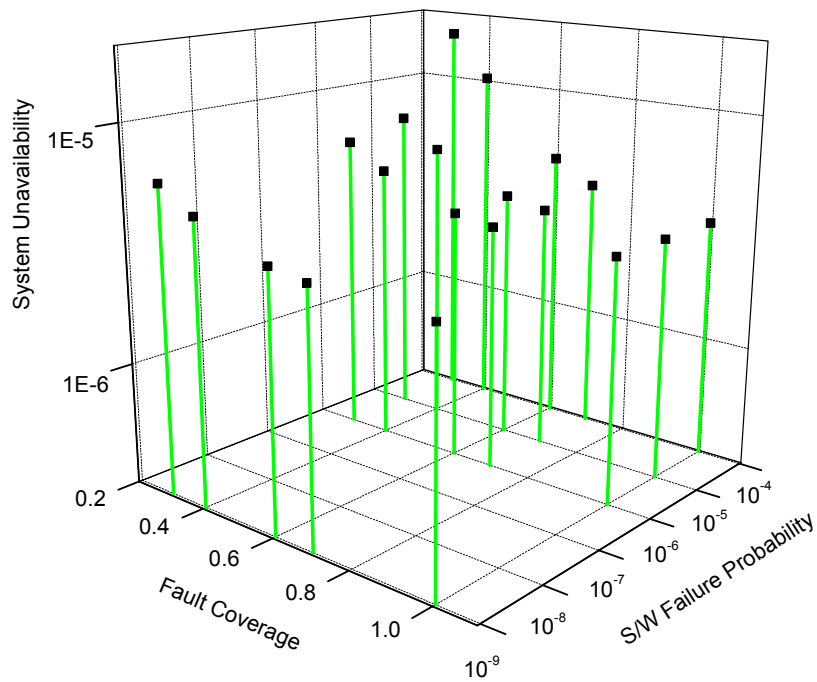


Figure 12. The graph of system unavailability along fault coverage and software failure probability when the identical input modules and the identical output modules are used

Table 3. System unavailability when two kinds of input modules and the identical output modules are used

System Unavailability		Software Failure Probability			
		0.00E+00	1.00E-06	1.00E-05	1.00E-04
Fault Coverage	0.3	3.11E-06	3.21E-06	4.10E-06	1.31E-05
	0.4	1.87E-06	1.93E-06	2.42E-06	7.37E-06
	0.6	6.93E-07	7.05E-07	8.16E-07	1.92E-06
	0.7	4.86E-07	4.90E-07	5.33E-07	9.61E-07
	1.0	3.54E-07	3.54E-07	3.54E-07	3.54E-07

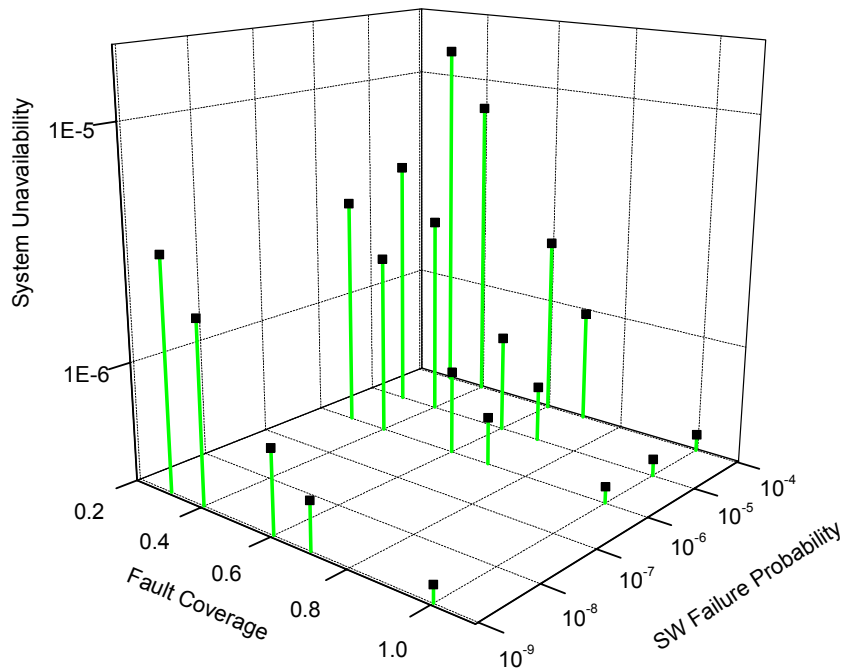


Figure 13. The graph of system unavailability along fault coverage and software failure probability when two kinds of input modules and the identical output modules are used

Table 4. System unavailability when two kinds of input modules and two kinds of output modules are used

System Unavailability		Software Failure Probability			
		0.00E+00	1.00E-06	1.00E-05	1.00E-04
Fault Coverage	0.3	2.76E-06	2.86E-06	3.75E-06	1.27E-05
	0.4	1.52E-06	1.58E-06	2.07E-06	7.02E-06
	0.6	3.44E-07	3.56E-07	4.66E-07	1.57E-06
	0.7	1.36E-07	1.41E-07	1.84E-07	6.11E-07
	1.0	4.80E-09	4.80E-09	4.80E-09	4.85E-09

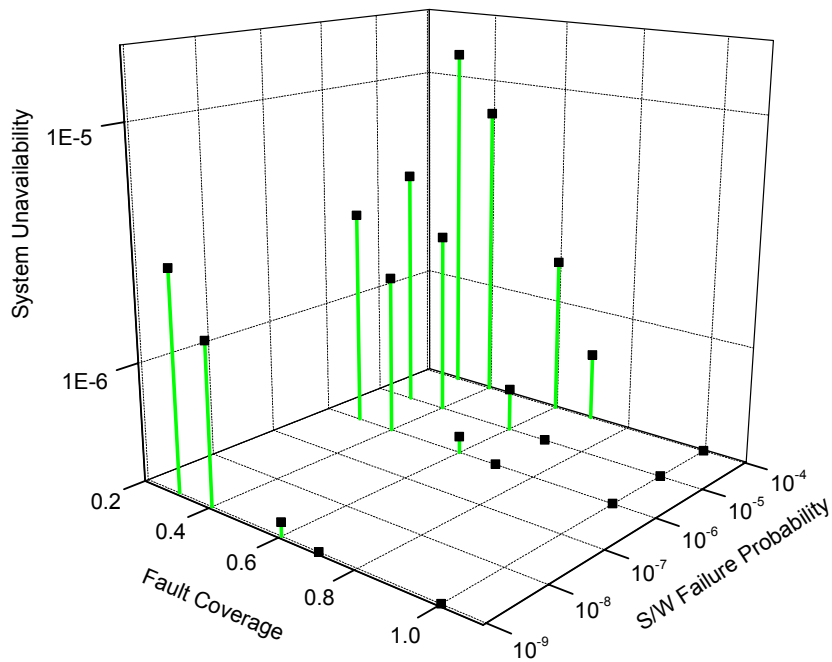


Figure 14. The graph of system unavailability along fault coverage and software failure probability when two kinds of input modules and two kinds of output modules are used

4.4 Discussion

As shown in analytic results in chapter 3 and quantitative results of sensitivity study in chapter 4, CCF is the one of the main contributors of multi-channel system's unavailability because CCF implies the concurrent failure of redundant backups. Unsystematic treatment of CCF is responsible for much of the uncertainty about the risks from operating nuclear power plants [25]. Therefore, the importance of precise CCF modeling of digital equipment should be especially emphasized because the designers have given various functional redundancies through separated systems. For example, in the PPS of the Korean Standard Nuclear Plant, there are 16 processors and 16 digital output modules which do the identical function of local coincidence logic. However, if the CCF probabilities of processors and digital output modules are high, these huge redundant systems might simultaneously lose their function. This sensitivity study also shows the effect of the CCF treatment. When we change the system design to adopt the diverse input/output modules as redundancy, we will get drastically improved system safety.

However it should be noted that even the products from different vendors do not guarantee the independence of faults. For the full diversity of digital equipment, we should be very careful to avoid CCF. The analysts also should be careful to make assumption of independence.

This sensitivity study also shows that the fault coverage of watchdog timer plays important role in assessing system safety. In this study, we simply assume that the watchdog timer covers the faults caused by both software and hardware with the same coverage. For more realistic evaluation, however, the separate application of the hardware fault coverage and the software fault coverage is suggestible for the further study. It is notable that the efforts to improve the coverage of a watchdog timer will critically improve the system safety and the importance of the system (hardware and software) design which enhances the coverage of fault-detection should be emphasized.

Software failures in digital safety-critical system induce very severe problems on assessing the system safety. It might remove the redundancy effect if the same

software is installed in redundant systems. We also cannot detect the failure of software by pure hardware-based monitoring mechanism. In order to get the reasonable result of safety assessment, the software failure probability should not be ignored even though the its quantitative estimation is a hard job. This sensitivity study shows the effect of software failure quantitatively. It is also notable that, from the viewpoint of unavailability of total system, we can compensate for the effort on proving complete software with a large coverage of a sophisticated monitoring mechanism. We quantitatively show this trade off in this study.

5. Conclusions

We are now faced with urgent need for digital systems' safety analysis but there exist some important unresolved problems which are complex and correlated. In this report, we show a practical PSA framework and a case study based on well-known fault tree method and classified important factors. It is clear that there are many important unresolved issues in digital systems' safety analysis. Because the safety of a digital system depends on the factors listed in this report, the quantification of the sensitivity of these factors is inevitable. After the analysis on the relationship among the factors and that between each factor and the PSA result, we select three most important factors: the modeling of CCF, the coverage of fault tolerant mechanisms and software failure probability. We also show the result of the sensitivity study on these three factors. Quantitatively, the value of each factor changes the system unavailability up to several thousand times.

In this study, from the practical viewpoint of PSA, we summarize the factors which should be considered in modeling the digital systems as follows. We explained about these important factors for the information of PSA analysts and design engineers and expect that the proper consideration of these factors will make PSA result more realistic.

- Modeling the multi-tasking of digital systems,
- Estimating software failure probability,
- Estimating the effect of software diversity and V&V efforts,
- Estimating the coverage of fault-tolerant features,
- Estimating the CCF probability in hardware, and
- Modeling the interactions between hardware and software.

Major problems which are not mentioned in this study can be listed as follows. Further investigation on these problems is strongly recommended.

- Failure mode of digital system,
- Environmental effects, and

– Digital system induced initiating events including human errors.

Especially, accepting the concepts of 'imperfectness of fault-tolerant mechanism' and 'possibility of software error' might be inevitable for realistic reliability modeling. The estimation of the CCF probability is also expected to play an important role.

We tried to analytically show the correlation among these factors and the safety assessment result. In order to quantify the effect of these factors to the system unavailability, we also show the results of a case study. The best unavailability of 4.80×10^{-9} is obtained from the system which has diverse input/output modules, perfect software and 100% fault coverage while the system which has identical input/output modules, poor software and poor fault coverage shows the worst result of 1.60×10^{-5} . And we can check the order of magnitude of the conventional PPS design. If we use the identical input/output modules and processor modules, the four-channel redundant digital PPS will have the system unavailability around 3.7×10^{-6} . However if we adopt the design of diverse input/output modules, it will have the system unavailability around 4.6×10^{-7} .

Regarding the modeling of CCF, when we apply the conventional methodologies such as the beta factor method and the Multi-Greek Letter method, we must be careful on component grouping and parameter estimation because the CCF dominate the system failure probability. Regarding the coverage of watchdog timer, mentioned in the previous chapter, we assume that the 70% is the maximum of fault-detection coverage of watchdog timer-based methods. It is notable that the perfectness of fault-tolerant mechanism (100% coverage) is impossible to achieve in practical cases. Regarding the software failure, we have to consider its probability as the possibility of one of the most important potential failure mechanisms. Especially, in the case that the same version of software is installed in several backup systems, the software failure acts like the CCF.

Last but not least, even though we cannot quantify the safety of digital systems in a very accurate manner, the active design feedback of the insight, which comes from

quantitative and qualitative approaches of PSA, should be encouraged. For example, the improved design by which the coverage of watchdog mechanism is enlarged to the extent of input/output modules will contribute toward reducing the probability of system failure. Properly designed on-line testing and monitoring mechanism will also improve the system integrity by reducing the inspection interval.

References

- [1] National research council, Digital Instrumentation and Control Systems in Nuclear Power Plants, National Academy Press, Washington, D.C., 1997.
- [2] J.L. Mourlenvat, A. Parry, J.F. Petetrot and J.F. Aschenbrenner, "Instrumentation and Control Revamping," Nuclear Technology, Vol. 92, pp. 300-308, December 1990.
- [3] G. Ives, "Digital Systems: Review of safety critical applications," Nuclear Engineering International, pp. 37-40, April 1994.
- [4] R. M. White and D. B. Boettcher, "Putting Sizewell B digital protection in context," Nuclear Engineering International, pp. 41-43, April 1994.
- [5] J.L. Rouvroye & A.C. Brombacher, "New quantitative safety standards: different techniques, different results?" Reliability Engineering in System Safety, Vol. 66, pp. 121-125, 1999.
- [6] HSE, The use of computers in safety-critical applications, London, HSE books, 1998.
- [7] I.S. Kim, et. al., Suitability Review of FMEA and Reliability Analysis for Digital Plant Protection System and Digital Engineered Safety Features Actuation System, KINS/HR-327.
- [8] D.L. Parnas, G.J.K. Asmis and J. Madey, "Assessment of Safety-critical Software in Nuclear Power Plants," Nuclear Safety, Vol. 32, No. 2, 1991.
- [9] B. Littlewood and L. Strigini, "Validation of ultrahigh dependability for software based systems," Communications of ACM, Vol. 36, No. 11, 1993.
- [10] R.W. Butler and G.B. Finelli, "The infeasibility of quantifying the reliability of life-critical real-time software," IEEE Transactions on software engineering, Vol. 19. No. 1, 1993.
- [11] J.K. Park et al., "A study on the quantitative evaluation for the software included in digital systems of nuclear power plants," KAERI/TR-2091/2002, 2002.
- [12] B. Littlewood and D. Wright, "Some conservative stopping rules for the operational testing of safety-critical software," IEEE Trans. Software Engineering, Vol. 23, No. 11, pp. 673-685, 1997.

- [13] H.G. Kang, T. Sung et al., "Determination of the Number of Software Tests Using Probabilistic Safety Assessment KNS conference," Proceeding of Korean Nuclear Society, Taejon, Korea, October 2000.
- [14] H.G. Kang, T. Sung et al., A Technical Survey on Issues of the PSA of digital I&C systems, KAERI/AR-560/2000, 2000.
- [15] H. Saiedian, "An Invitation to Formal Methods," Computer, April 1996.
- [16] J. Rushby, Formal methods and the certification of critical systems, SRI-CSL-93-07, Computer Science Laboratory, SRI International, Menlo Park, 1993.
- [17] D. Welbourne, "Safety Critical Software in Nuclear Power," The GEC Journal of Technology, Vol. 14, No. 1, 1997.
- [18] G. Dahll, The use of Bayesian Belief Nets in Safety Assessment of Software based System, HWP-527, Halden Project, 1998.
- [19] H.S. Eom, et. al., Survey of Bayesian Belief Nets for Quantitative Reliability Assessment of Safety Critical Software Used in Nuclear Power Plants, KAERI/AR-594-2001, 2001.
- [20] W. Bastl and H.W. Bock, "German qualification and assessment of Digital I&C systems important to safety," Reliability Engineering and System Safety, Vol. 59, pp. 163-170, 1998.
- [21] J.G. Choi and P.H. Seong, "Dependability estimation of a digital system with consideration of software masking effects on hardware faults," Reliability Engineering and System Safety, Vol. 71, pp. 45-55, 2001.
- [22] Norman J. McCormick, Reliability and risk analysis, Academic Press, Inc. New York, 1981.
- [23] Hyun Gook Kang and Taeyong Sung, "A Quantitative Study on Important Factors of the PSA of Safety-Critical Digital Systems," Journal of Korea Nuclear Society, Vol. 33, No. 6, 2001.
- [24] A. Mahmood and E.J. McCluskey, "Concurrent Error Detection Using Watchdog Processors – A Survey," IEEE Trans. On Computers, Vol. 37, No. 2, February 1988.
- [25] NUREG/CR-4780, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, February 1988.

서 지 정 보 양 식

수행기관보고서번호	위탁기관보고서번호	표준보고서번호	INIS 주제코드
KAERI/TR-2026/2002			
제목 / 부제	디지털 계측제어 계통의 확률론적 안전성 평가를 위한 주요인자 선정 및 민감도 분석		
연구책임자 및 부서명 (주저자)	강현국 (종합안전평가팀)		
연구자 및 부서명	성태용 (종합안전평가팀), 엄홍섭 (종합안전평가팀), 정환성 (하나로운영팀), 박진균 (종합안전평가팀), 이기영 (동력로기술개발팀), 박종균 (동력로기술개발팀)		
출판지	대전	발행기관	KAERI
페이지	58 p.	도표	있음(○), 없음()
발행년	2002.1.		
크기	21×29.7cm		
참고사항			
비밀여부	공개(○), 대외비(), — 급비밀	보고서종류	기술보고서
연구위탁기관		계약번호	
초록	<p>디지털 시스템의 정량적 안전성평가(PSA) 방법론은 현재 국내외에서 명확히 정립된 바가 없다. 그러나 현실적으로는 원전의 안전계통에 디지털 기기가 도입되고 있어 그 안전성의 정량평가가 중요한 현안으로 대두되고 있다. 이에 기존 PSA 방법론을 기반으로 하여 디지털 계통의 안전성을 평가하기 위한 연구를 수행하였으며, 다음의 내용을 포함하고 있다.</p> <ol style="list-style-type: none"> 1. 디지털계통의 PSA에서 모델링되어야 할 계통특성을 도출하고 설명하였다. 2. 실제 디지털계통의 분석에 있어서 주요하게 다루어져야 할 내용을 수학적 접근을 통해 도출하고 그 물리적 의미를 설명하였다. 3. 민감도 분석을 통해 도출된 특성들이 최종 PSA결과에 미치는 영향을 정량적으로 보였다. 		
주제명키워드 (10단어내외)	디지털 시스템 신뢰도, 확률론적 안전성 평가		

BIBLIOGRAPHIC INFORMATION SHEET

Performing Org. Report No.		Sponsoring Org. Report No.		Standard Report No.		INIS Subject Code	
KAERI/TR-2026/2002							
Title / Subtitle		The PSA of Safety-Critical Digital I&C System: The Determination of Important Factors and Sensitivity Analysis					
Project Manager and Department		H.G. Kang (Integrated Safety Assessment team)					
Researcher and Department		T.Y. Sung (ISA team), H.S. Eom (ISA team), H.S. Jeong (Hanaro), J.K. Park (ISA team), K.Y. Lee (ARTD team), and J.K. Park (ARTD team)					
Publication Place	Taejon	Publisher	KAERI		Publication Date	2002.1.	
Page	58 p.	Ill. & Tab.	Yes(<input type="radio"/>), No (<input type="radio"/>)		Size	21 × 29.7cm	
Note							
Classified	Open(<input type="radio"/>), Restricted(<input type="radio"/>), ___ Class Document		Report Type	Technical Report			
Sponsoring Org.				Contract No.			
Abstract (15-20 Lines):		<p>This report is prepared to suggest a practical probabilistic safety assessment (PSA) methodology of safety-critical digital instrumentation and control (I&C) systems. Even though conventional probabilistic safety assessment methods are immature for applying to microprocessor-based digital systems, practical needs force to apply it because the result of probabilistic safety assessment plays very important role in proving the safety of a designed system. Microprocessors and software technologies make the digital system very complex and hard to analyze the safety of their applications.</p> <p>The aim of this study is: (1) To summarize the factors which should be represented by the model for probabilistic safety assessment and to propose a standpoint of evaluation for digital systems. (2) To quantitatively presents the results of a mathematical case study which examines the analysis framework of the safety of digital systems in the context of the PSA. (3) To show the results of a sensitivity study for some critical factors.</p>					
Subject Keywords (About 10 words)		Digital system reliability, Probabilistic safety assessment					