Journal of the Korean Nuclear Society
Volume 33, Number 6, pp.596~604, December, 2001

A Quantitative Study on Important Factors of the PSA of Safety-Critical Digital Systems

Hyun Gook Kang and Taeyong Sung
Korea Atomic Energy Research Institute
150 Dukjin-dong, Yusong-gu, Taejon 305-353, Korea
hgkang@kaeri.re.kr

(Received May 24, 2001)

Abstract

This paper quantitatively presents the effects of important factors of the probabilistic safety assessment (PSA) of safety-critical digital systems. The result which is quantified using fault tree analysis methodology shows that these factors remarkably affect the system safety. In this paper we list the factors which should be represented by the model for PSA. Based on the PSA experience, we select three important factors which are expected to dominate the system unavailability. They are the avoidance of common cause failure, the coverage of fault tolerant mechanisms and software failure probability. We quantitatively demonstrate the effect of these three factors. The broader usage of digital equipment in nuclear power plants gives rise to the safety problems. Even though conventional PSA methods are immature for applying to microprocessor-based digital systems, practical needs force us to apply it because the result of PSA plays an important role in proving the safety of a designed system. We expect the analysis result to provide valuable feedback to the designers of digital safety-critical systems.

Key Words : probabilistic safety assessment, sensitivity study, digital systems, fault coverage, software failure, common cause failure

1. Introduction

The development of a methodology for the probabilistic safety assessment (PSA) of a safety-critical digital I&C system is one of the most important issues for proving the safety of a system. The PSA has been widely used in the 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. 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].

Currently, the nuclear power industry employs

the event tree/fault tree methodology for plant-wide PSA. Therefore, the model of a digital I&C system should be compatible with the current static logic-based model structure. Even though the system 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 logical structure of the fault tree makes it easy for system design engineers to understand and it is the most familiar tool for safety analysts.

Digital technology was introduced relatively recently in the nuclear power industry and some utilities adopted modern digital technologies for their I&C systems. 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 [2]. Digital technologies are adopted in the late advanced gas cooled reactors (AGRs) in the UK for safety features actuation [3]. Especially, in Korea, UCN 5&6 units are being constructed and the Korean Next Generation Reactor (KNGR) is being designed using the digital I&C equipment for the safety functions such as a plant protection system (PPS) and an engineered safety feature actuation system (ESFAS). 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. The PSA is now an accepted aspect of the demonstration of safety.

Microprocessors and software technologies make the digital system very complex to analyze. The quantitative safety assessment of these digital technologies has many difficulties. They could be programmed to check their own integrity and to monitor the integrity of each other. That is, digital systems have various fault-tolerant mechanisms. Furthermore, there are some unresolved issues on the quantification of ultra-high reliability of software.

Nowadays, the usefulness of PSA for digital applications as a demonstration of safety is generally known. Unlike conventional standards, new international standards require quantitative analysis [4]. However, many assumptions are used for quantitative analysis because of the prematureness of methodologies. Unreasonable assumptions cause biased results and insights of the analysis. Fault-free software and 100% coverage of a fault tolerance mechanism are the typical ones. In order to obtain more reasonable results, these critical assumptions should be removed.

In this paper we list the factors which should be represented by the model for PSA. In the context of PSA, we select three important factors which are expected to dominate the system unavailability. They are the avoidance of common cause failure (CCF), the coverage of fault tolerant mechanisms and software failure probability. Then, using the fault tree models, we quantitatively demonstrate the effect of these three factors on the system safety.

2. Issues in the Quantitative Safety Assessment of Digital Systems

From the viewpoint of practical PSA, we can summarize the factors which should be considered in modeling digital systems for PSA as follows:

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

and software,
- Failure mode of digital system,
- Environmental effects, and
- Digital system induced initiating events including human errors.

Among these issues, some factors should be more carefully considered in the safety assessment of digital equipment. They are expected to play a more important role in quantitative analysis. Proper treatment for the system design of 'avoidance of CCF' plays a important role. And accepting the concepts of 'imperfectness of fault-tolerant mechanism' and 'possibility of software error' might be inevitable for realistic reliability evaluation. The safety and reliability of a fault-tolerant digital system is quite sensitive to the CCF treatment, the fault coverage, and the software failure probability.

2.1. The CCF Probability of Digital Systems

CCF is the one of the main contributors of system 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 [5]. The importance of precise CCF modeling of digital equipment should be especially emphasized. The designers of safety-critical systems such as nuclear power plants have adopted a conservative design strategy and redundancy is one of the most important design strategies. They have given various functional redundancies through separated systems.

The digital I&C system of nuclear power plants adopt the redundant processors or input/output modules for higher safety. In the case of digital systems, the risk concentration on processor units and input/output modules of digital equipment is generally higher than that of conventional analog equipment [6]. If the same microprocessor unit is adopted as the redundancy, the risk concentration on 'one kind of equipment' will be more critical. This kind of risk concentration problem is observed not only in the processor unit but also in the input/output module. Even the products from different vendors do not guarantee the independence of faults. Global standardization and the large manufacturer in the electric parts market have led to the production of similar digital hardware products by different vendors.

For example, in the plant protection system of the Korean Standard Nuclear Plant (KSNP), there are 16 processors and 16 digital output modules which do the identical function of local coincidence logic. However, if the CCF probability of processors or digital output modules is high, these huge redundant systems might simultaneously fail to perform their function. The designer of a digital system should carefully consider the avoidance of CCF.

2.2. The Coverage of Fault-tolerant Mechanism

In the nuclear industry, watchdog timers and duplication techniques are widely used for the fault tolerance of system. They are the simplest techniques which can be used to establish a fault-tolerant system and are already applied to some nuclear applications. We can model the duplication explicitly using the fault tree method. However, the watchdog timer applications should be treated differently from the duplication.

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 faults but the coverage of the fault-tolerant mechanism is limited. We expect that this aspect can be expressed using the concept of the coverage factor, which is the ratio of successful fault detections to occurred faults. Because the

safety systems in nuclear power plants adopt 'fail-safe' concept, the successful recovery probability depends on this coverage factor and the failure probability of the recovery mechanism. When the failure probability of the recovery mechanism is negligible, the coverage factor plays a very critical role in assessing the safety. A sophisticated monitoring system is expected to show good fault-detection coverage, but a simple watchdog timer cannot be expected to show such good coverage.

The watchdog devices are widely adopted for the fault-tolerance feature of safety systems in nuclear power plants to generate a trip signal at the failure of microprocessor-based devices. Because of its simplicity, the reliability of a watchdog device is much higher than that of a microprocessor-based device. If we assume that the coverage of a watchdog mechanism is perfect, the effect of the failure of devices monitored by the watchdog timer will be negligible and the system unavailability will totally depend on the failure rate of the watchdog device and non-monitored devices. However, it is well known that the coverage of the watchdog timer is not so high because it is the simplest method among the various fault-tolerant mechanisms. That is, the assumption of 100% fault coverage of the watchdog timer will severely distort the analysis result.

2.3. The Probability of Software Failure

In order to get a reasonable result of safety assessment, the software failure probability should not be ignored. Software failure in a safety-critical digital system induces very severe problems on assessing the system safety. We cannot detect the failure of software by a hardware-based monitoring mechanism. Worst of all, it might remove the redundancy effect if the same software is installed in redundant systems.

There are ongoing debates among the researchers of software engineering about whether software failure can be treated in a probabilistic manner [1]. Generally, we recognize that software faults are design faults by definition. That is, 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. 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. Since the input signal is random, the concept of error crystal implies the random failure of software.

Unlike the reliability of hardware components, it has been proved that it is much harder to predict software reliability using a conventional model. Software reliability growth model is regarded as the most mature technique for software dependability assessment in the software engineering field. 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 [7]. 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

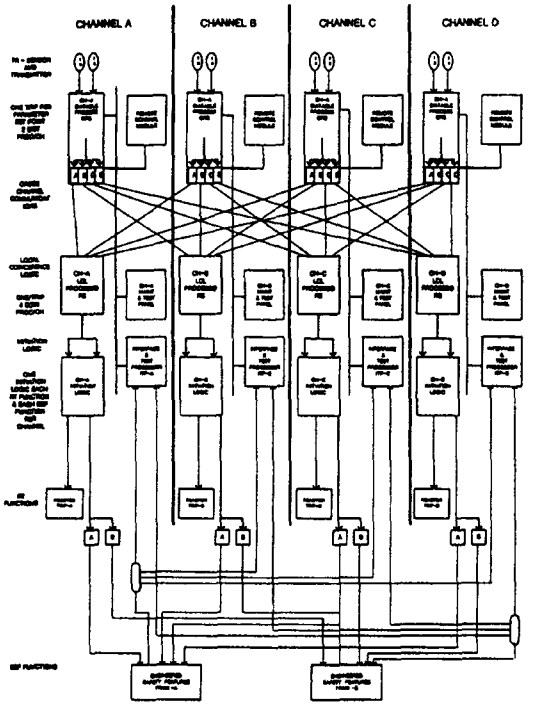

Fig. 1. The Schematic Diagram of the PPS

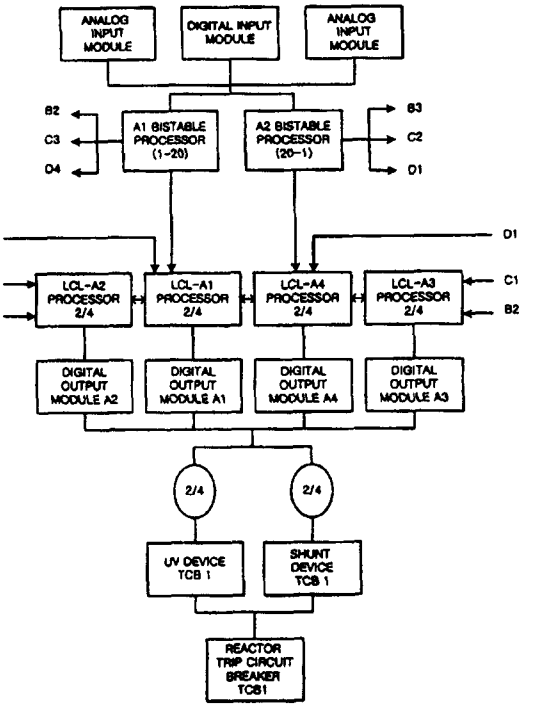

Fig. 2. The Functional Diagram of Each Channel of the PPS

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. In order to show the integrity of developed software, the software should undergo a test phase even if 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.

3. PSA Model of the Assumed PPS of KSNP

We established the PSA model of the assumed digital PPS of KSNP for the sensitivity study. The PPS is one of the most important safety-critical digital systems. The detailed system description and design concept of KSNP are not fully available because it is in the construction phase. In this paper, we assumed the layout and component of PPS of KSNP, so the results shown in this paper are based on various assumptions for unknown parts. Although the data of the assumed digital PPS is not complete, a sensitivity study in early phase can provide a quantitative comparison between the design alternatives and support decision-making for design improvement.

3.1. The System Description and Assumptions

We assumed that the PPS has four channels and each channel contains two bistable (BS) processors and four local-coincidence-logic (LCL)

processors. Each LCL processor produces the output signal using independent digital output module. We use rough assumptions for various aspects except three important factors. The adequacy of assumptions is not guaranteed and the model requires further refinement. The aim of this study is to demonstrate the effect of three important factors and to provide comparison result among design alternatives. Kim, et al. [8] reported the design concept of PPS as shown in Figure 1 and 2.

Watchdog timers monitor the status of LCL processors and LCL processors monitor BS 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. We assume that every LCL processor contains the identical software program and the software failure induces CCF. We also treat the failure probability of software as a variable.

3.2. Sensitivity Study

Using KwTree, which is the fault-tree analysis software package produced by Korea Atomic Energy Research Institute, we perform the sensitivity studies. 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 KSNP. As mentioned in the introduction, we only consider three important factors. Since this sensitivity analysis is concentrating on the digital system itself, the sensitivity on the other components such as trip circuit breakers, interposing relays, sensors and transducers is out of scope. For the simplicity of analysis, only two trip parameters are considered in this study.

The effect of the diversity of input/output modules is examined. In this study, related to the design of input/output modules, we perform the analysis on the following three design alternatives: the case in which the system uses the identical input modules and the identical output modules, the case in which the system uses two kinds of input modules, and the case in which the system uses two kinds of input modules and output modules. We ignore the CCF probability between two kinds of devices.

For each design alternative, we establish a separate fault tree model to perform sensitivity studies. Unfortunately, there is no widely accepted method except experiment for estimating the quantitative value of fault coverage factor and the software failure probability. In this sensitivity study, we use several discrete values of 0.3, 0.4, 0.6, 0.7, and 1.0 for the value of fault coverage factor. We also use 0.0, 1.0E-6, 1.0E-5, and 1.0E-4 for the value of software failure probability. That is, we performed a total of 60 ($3 \times 5 \times 4$) calculations.

3.3. The Result of PSA

The PSA results show that the system unavailability is very sensitive to the software failure probability and the coverage of watchdog timer. The differences of system unavailability among the design alternatives are also significant. Tables 1 to 3 show the results of three design alternatives. Figure 3 to 5 show the graphical illustration of the effects of three important factors on the system unavailability.

Of course, the best unavailability of 4.80E-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 1.60E-5.

Table 1. 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

Table 2. 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

Table 3. 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

4. Discussions

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.

The most critical factor is the diversity of components. It should be noted that even the products from different vendors do not guarantee the independence of faults as mentioned above. Furthermore, input/output modules are not the objects of monitoring in conventional system design, so their redundancy does a very important role in sustaining the system safety. For the full

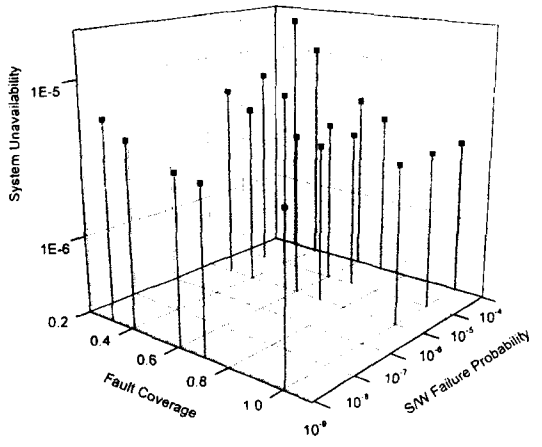

Fig. 3. The Graph of System Unavailability Along Fault Coverage and Software Failure Probability when the Identical Input Modules and the Identical Output Modules are Used

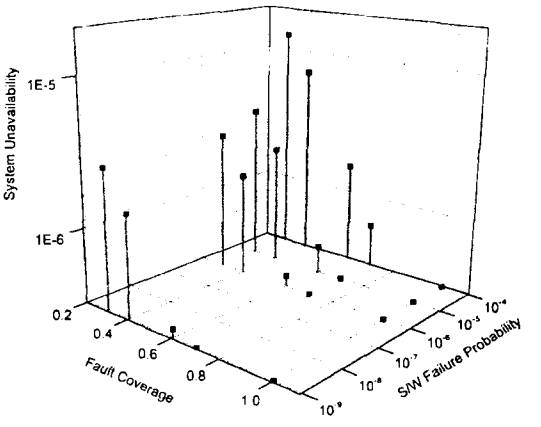

Fig. 5. The Graph of System Unavailability Along Fault Coverage and Software Failure Probability when Two Kinds of Input Modules and Two Kinds of Output Modules are Used

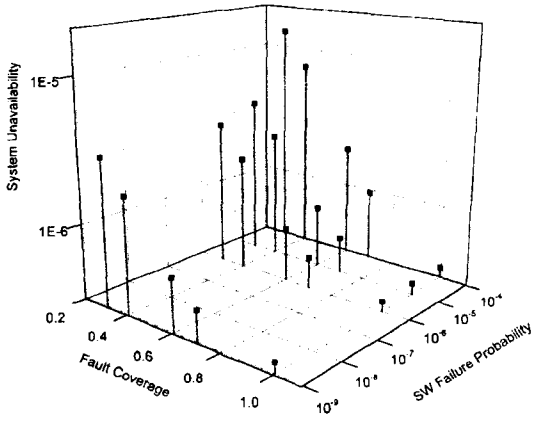

Fig. 4. The Graph of System Unavailability Along Fault Coverage and Software Failure Probability when Two Kinds of Input Modules and the Identical Output Modules are Used

diversity of digital equipment, we should be very careful to avoid CCF. The analysts also should be careful to make assumption of independence.

We are now faced with an urgent need for digital systems' safety analysis but there exist some important unresolved problems which are complex and correlated. In this paper, we select and analyze three critical factors but even among these three factors, there exist some correlations. For example, if the coverage of the fault-tolerant mechanism is unity, the effect of the software failure probability on the system safety is negligible. From the viewpoint of unavailability of total system, we can compensate for the effort on proving complete software with a large coverage of monitoring mechanism. We quantitatively show this trade off in this paper.

5. Conclusions

In this paper we list the factors which should be represented by the model for probabilistic safety assessment and select three important factors which are expected to dominate the system unavailability in the context of PSA. They are the avoidance of common cause failure, the coverage

of fault tolerant mechanisms and software failure probability. We quantitatively demonstrate the effect of these three factors. From the result of this sensitivity study, we conclude that the CCF avoidance should be the most important strategy of the PPS design.

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.

Acknowledgement

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

References

1. R. M. White and D. B. Boettcher, "Putting Sizewell B digital protection in context," Nuclear Engineering International, pp. 41-43, April (1994).
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. 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).
5. NUREG/CR-4780, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, February (1988).
6. Hyun Gook Kang & Taeyong Sung, "PSA as a Measure of Digital Systems' Safety," Proceedings of the Korean Nuclear Society Spring Meeting, Cheju, Korea, May (2001).
7. B. Littlewood and L. Strigini, "Validation of ultrahigh dependability for software based systems," Communications of ACM, Vol. 36, No. 11, (1993).
8. 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, (2000).