Procedures and Techniques for the PSA of Digital I&C System

Hyun Gook Kang • Heung Sup Eom • Seung-Cheol Jang
Integrated Safety Assessment Team, Korea Atomic Energy Research Institute
P.O. Box 105, Yuseong, Daejeon, 305-600, Korea
hgkang@kaeri.re.kr

1. Introduction

UCN 5&6 nuclear units (OPR-1000) are being constructed and the Korean Next Generation Reactor (APR-1400) is being designed by using digital I&C equipment for the safety functions such as a reactor protection system, an engineered safety feature actuation system, and a safety equipment control system. Even though the use of digital equipment for safety-related functions provides many advantageous features, there are still many arguable safety issues remaining.

Design, configuration management and maintenance are important application areas for the probabilistic safety assessment (PSA). Digital I&C systems are natural candidates for PSA applications. From the viewpoint of the PSA, the digital techniques are very different from the conventional techniques of analog I&C systems because of some unique features.

This article aims at giving an overview for the important issues of digital system PSA and at presenting the current status of technology development for each issue. Korea Atomic Energy Research Institute (KAERI) has performed an initiative research in order to meet risk information needs for digitalized safety-critical systems in Korea. The technologies presented in this article especially focusing on those developed in the KAERI.

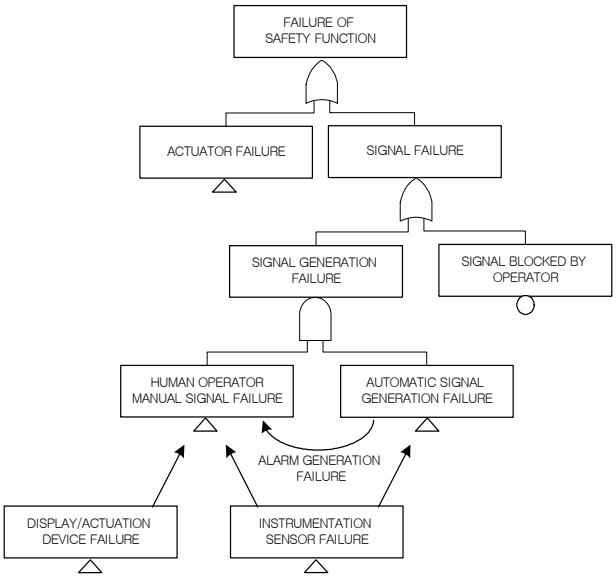

Figure 1. The schematic of the concept of the safety function failure mechanism in a digital I&C system

2. Procedures for the PSA of Digital I&C System

In order to develop the model for the PSA, the system configuration and operating environment should be investigated. The PSA model aims at quantifying the risk from the failure of a safety function. The first step is identifying hazard of the system failure. That is, we consider the fail-to-hazard failure modes only. It is notable that many of I&C systems are designed under the fail-to-safe philosophy. In some cases such as a safety-critical network failure, additional investigation is required to clearly identify the hazard status from the safe status. And the understanding on the failure mechanism of a safety function is important as shown in Figure 1.

The function of I&C system is usually initiated by the input signals. Thus, the availability and the validity of input signal are very important. In some cases, there could be redundant input signals or an operator's manual input. As shown in reference [1], the development of a PSA model requires in-depth analysis for input availability including a document survey, a simulation and expert judgment.

We should investigate the processing mechanism of the digital system which usually consists of many redundant components and utilizes the network communication and self-monitoring algorithms. Experience shows that the self-monitoring or fault-tolerant mechanisms effectively enhance a system's availability. Quantification of the coverage of these advanced algorithms is very important. The treatment of a possible software failure is also a very important topic. The common-cause failure group should be carefully identified with consideration of the development/operation environment.

A human operator could play as a backup of an automated digital I&C system. For the quantification of the failure probability of such a manual action, we must consider the dependency between an automated system and an operator. For example, if an instrumentation sensor failure occurs, it will cause the concurrent failure of both signal generation mechanisms. The malfunction of automated system could also be an error-forcing context for the human operator.

3. Procedures for the PSA of Digital I&C System

3.1 Software Failure Probability

Generally, we recognize that software faults are design faults by definition. That is, software is deterministic and its failure cannot be represented by 'failure probability'. When we focus on the software of a specific application, however, the software could be treated based on a probabilistic method because of the randomness of the input sequences (concept of 'error crystals in software').

Software reliability growth model is the most mature technique for software dependability assessment, which estimates the increment of reliability as a result of a fault removal. In safety-critical systems, however, this approach is known to be inappropriate [2].

In highly reliable software, the number of observed failures during a test is expected to be zero. 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. 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:

$$C = prob(T \le U) = \sum_{t=1}^{U} p(1-p)^{t-1} = p[\frac{1-(1-p)^{U}}{1-(1-p)}]$$

The failure probability is denoted p.

In order to assess the expected failure rate of software, we should also consider the lifecycle of software. As we anticipate that the application of software verification and validation methodologies could reduce the number of potential faults, this effect should be reflected in the probability estimation of the basic events. Applying the Bayesian belief network [3], [4] methodology to the PSA of digital equipment will make it possible to integrate the many aspects of the software engineering and the quality assurance. However, it should be noted that there are also some difficulties on establishing the BBN including topology obtaining and data gathering.

3.2 Automatic Testing/Checking

Experience shows that these fault-tolerant mechanisms effectively enhance a system's availability but that they are not perfect. Digital systems have various kinds of faults and the coverage of a fault-tolerant mechanism is limited. When the safety-critical systems in nuclear plants adopt 'fail-to-safe' concept, the coverage factor plays a critical role on assessing the safety of digital systems.

Among various self-testing mechanisms, the simplest way to establish a fault-tolerant system is the application of watchdog timer. Unfortunately, the results of a fault injection simulation show just around 50% for fault coverage [5], [6].

Automatic self testing could be applied to the digitalized safety-critical systems. In comparison with the conventional manual test interval such as 30 days, this automatic testing will be performed very frequently such as once per 8 hours. If we could give the credibility of this testing, the system unavailability will be much improved.

3.3 Assessment of human failure probability

The PSA provides a unifying mean of assessing a system's safety including the activities of human operators. For a human failure, we have to consider two different aspects. One is a human operator as a generator of manual signals for mitigation when an accident happens. The other is a human operator as an initiator of spurious plant transients.

The failure of a human operator to generate the mitigation signal could be treated as an error of omission (EOO) which is followed by the failure of the automatic signal generation. Therefore, the probability of an EOO should be evaluated based on the assumptions regarding the reasons of an automatic generation failure. This complicate situation can be modeled by using condition-based human reliability assessment [7].

The initiation of spurious transient by a human operator could be treated as an error of commission (EOC) which has the potential for being significant contributors to plant risk.

Acknowledgement

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

REFERENCES

[1] Kang, H.G. and Jang, S.C. and Lim, H.G.., ATWS Frequency Quantification Focusing on Digital I&C Failures, Journal of Korea Nuclear Society, Vol. 36, 2004.

[2] Parnas, D.L., Asmis, G.J.K., Madey, J., Assessment of Safety-critical Software in Nuclear Power Plants, Nuclear Safety, Vol. 32, No. 2., 1991.

[3] Dahll, G., The use of Bayesian Belief Nets in Safety Assessment of Software based System, HWP-527, Halden Project, 1998.

[4] Eom, H.S., et al., Survey of Bayesian Belief Nets for Quantitative Reliability Assessment of Safety Critical Software Used in Nuclear Power Plants, Korea Atomic Energy Research Institute, KAERI/AR-594-2001, 2001.

[5] Kim, S.J., Seong, P.H., Lee, J.S., Kim, M.C., Kang, H.G., Jang, S.C., A method for evaluating fault coverage using simulated fault injection for digitalized systems in nuclear power plants, Reliability Engineering & System Safety, Volume 91, Issue 5, 2006.

[6] Lee, J.S., Kim, M.C., Seong, P.H., Kang, H.G., Jang, S.C, Evaluation of error detection coverage and fault-tolerance of digital plant protection system in nuclear power plants, Annals of Nuclear Energy, Volume 33, 2006.

[7] Kang, H.G. and Jang, S.C., Application of Condition-Based HRA Method for a Manual Actuation of the Safety Features in a Nuclear Power Plant, Reliability Engineering and System Science, Volume 91, Issue 6, 2006.