Transactions of the Korean Nuclear Society Autumn Meeting
Busan, Korea, October 27-28, 2005

Design Information from the PSA for Digital Safety-Critical Systems

Hyun Gook Kang • 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

Many safety-critical applications such as nuclear field application usually adopt a similar design strategy for digital safety-critical systems. Their differences from the normal design for the non-safety-critical applications could be summarized as: Multiple-redundancy, highly reliable components, strengthened monitoring mechanism, verified software, and automated test procedure. These items are focusing on maintaining the capability to perform the given safety function when it is requested.

For the past several decades, probabilistic safety assessment (PSA) techniques are used in the nuclear industry to assess the relative effects of contributing events on plant risk 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. The applications of PSA provide not only the analysis results of already installed system but also the useful information for the system under design.

The information could be derived from the PSA experience of the various safety-critical systems. Thanks to the design flexibility, the digital system is one of the most suitable candidates for risk-informed design (RID).

In this article, we will describe the feedbacks for system design and try to develop a procedure for RID. Even though the procedure is not sophisticated enough now, it could be the start point of the further investigation for developing more complete and practical methodology.

2. Dominant Risk Contributors

The safety-critical functions of an I&C system could be defined as: Generating automatic actuation signal and providing information for the human operator. Then the 'risk' from this system is the failure of signal generation or information provision when a demand event occurs.

From the PSA viewpoint, the risk is defined as the system unavailability within the demand period [1].

$$SU = q_1+q_2+ \dots + q_i + \dots +q_n \quad (1)$$

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

where SU denotes the system unavailability, q_i is the probability of cutset i, and p_j is the probability of basic event j. Since $p_j < 1$, the combined cutset which consists of more basic events affects smaller on the system unavailability.

The safety-critical systems usually adopt the multiple redundancy strategy. This higher redundancy would clearly reduce the risk from the single failure of components, but raise the importance of the common cause failure (CCF) analysis. The CCF implies the concurrent failure of multiple redundancies due to the environmental shock, the common installation/ maintenance fault, or the design/manufacturing flaw.

From the experience, the dominant risk contributors related to the digital signal processing system could be identified as:

$q_1 = Pr(OP) \times Pr(IM\ CCF) \times Pr(MM\_IM)$

$q_2 = Pr(OP) \times Pr(PM\ CCF) \times Pr(MM\_PM)$

$q_3 = Pr(OP) \times Pr(OM\ CCF) \times Pr(MM\_OM)$

OP denotes the failure of a human operator to manually initiate the given safety signal. IM, OM and PM denote the failure of input module, output module, and processor modules, respectively. MM denotes the failure of monitoring mechanism. The failure of each module could be successfully recovered if it is detected by the monitoring mechanism. The software failure should be treated as a part of the CCF of the processor modules.

It is also notable that the operator plays as the backup of an automatic processing system and the operator performance largely depends on the information supplied by information processing system.

The simple equations in this section clearly present what the dominant factors are.

3. Procedure for Risk-Informed Design

The main goal of the RID for the safety-critical digital system would be the reduction of system unavailability in a balanced manner. However, the repeated PSA including a fault tree development and cutset analysis would not be practical. In this section, in order to reduce the design efforts and enhance the efficiency of design feedback, we propose a procedure with dominant risk contributors instead of full scope PSA. The RID procedure could be summarized as following steps:

1) Derive the dominant risk contributors and their correlation with system unavailability
2) Determine the design factors of which characteristics is related to the dominant contributors
3) Develop an unavailability equation of which variables are design factors

The step 1) is typically illustrated in the previous section. This step aims to find important events and derive the equation which explains the relationship between the events and system unavailability.

The step 2) depends on the design status. If the modules or components could be redesigned, the module reliability and hardware monitoring coverage could be enhanced. This flexibility should be covered by this step.

If the hardware modules are already specified and their arrangement is the only object of design, then the system configuration should be divided into several design factors such as the voting mechanism of multiple processing channels and the inspection period derived from the maintenance strategy.

The step 3) is the process which translates the PSA events into the design factors. The PSA events are hard to understand for design staffs, so these events should be interpreted to the design factors which are more familiar to designers. Some of these relationships will be linear but the other might be nonlinear.

For instance, the upgrading the electrical components in a specific module (e.g., a processing module) will reduce the probability of corresponding module (Pr(PM CCF)) in a linear manner by reducing the independent failure probability of the module since the Pr(PM CCF) is linearly proportional to the Pr(PM).

The change of voting mechanism will cause nonlinear change in system unavailability. For example, the estimates of the CCF probability for the selective two-out-of-four voting logic and pure two-out-of-four voting logic do not have linear relationship [2]. The human error probability is also an example of nonlinear relationship with the information system failure [3].

The step 3) should be highlighted in the proposed procedure. In order to perform the step 3), the careful investigation on the target system and the PSA methodologies is required.

In some cases, the availability (not unavailability) of the target system affects the initiating event frequency and causes the plant risk in different way from that described in this section. If the ways of the design changes affecting the risk are identified in several independent forms and their relationship could mathematically derived, all of them could be treated in the same manner as in equation (1). That is, above procedure is just one of the typical examples of representing a design change to the risk and its coverage could be extended.

For example, if the voting logic (VL), the watchdog timer coverage (WC), and the reliability of an A/D converter in the IM (AD) are the design factors, the relationship with the system unavailability could be expressed as:

$SU = q_1+q_2+ q_3+ \ldots$

$q_1 = \alpha_1 \times fn(VL, AD)$

$q_2 = \alpha_2 \times fn(VL, WC)$

$q_3 = \alpha_3 \times fn(VL)$

where α_i denotes the fixed constant of *i*th cutset, and $fn(X_j)$ represents the function of X_j's property. The fn(AD) and fn(WC) are linear, but fn(VL) is nonlinear.

5. Conclusion

In this paper, we propose a conceptual RID procedure for the safety-critical digital systems. This procedure could be extended for general system if further investigation is performed. The RID in early phase is expected to increase the safety of a final product and reduce the cost for modification. Some sensitive design factors such as software failure quality could be treated in the frame of this study. For example, the number of software testing can be determined in consideration with the system risk.

The development of a more sophisticated methodology which could describe the nonlinear relationship in a clear manner for various applications is recommended.

Acknowledgement

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

REFERENCES

[1] H.G. Kang and T. Sung, "An analysis of safety-critical digital systems for risk-informed design," Reliability Engineering and Systems Safety, Vol. 78, 2002.

[2] H.G. Kang, et al., "The Common Cause Failure Probability Analysis on the Hardware of the Digital Protection System in Korean Standard Nuclear Power Plant," KAERI/TR-2908/2005.

[3] H.G. Kang and S. Jang, "Application of Condition-Based HRA Method for a Manual Actuation of the Safety Features in a Nuclear Power Plant," Reliability Engineering and System Science, to be published in 2005.