Common Cause Failure Analysis for the Digital Plant Protection System

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

1. Introduction

Safety-critical systems such as nuclear power plants adopt the multiple-redundancy design in order to reduce the risk from the single component failure. The digitalized safety-signal generation system is also designed based on the multiple-redundancy strategy which consists of more redundant components. The level of the redundant design of digital systems is usually higher than those of conventional mechanical systems. 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.

This research aims to develop the practical and realistic method for modeling the CCF in digital safety-critical systems. We propose a simple and practical framework for assessing the CCF probability of digital equipment.

Higher level of redundancy causes the difficulty of CCF analysis because it results in impractically large number of CCF events in the fault tree model when we use conventional CCF modeling methods. We apply the simplified alpha-factor (SAF) method to the digital system CCF analysis. The precedent study [1] has shown that SAF method is quite realistic but simple when we consider carefully system success criteria. The first step for using the SAF method is the analysis of target system for determining the function failure cases. That is, the success criteria of the system could be derived from the target system's function and configuration. Based on this analysis, we can calculate the probability of single CCF event which represents the CCF events resulting in the system failure [2].

In addition to the application of SAF method, in order to accommodate the other characteristics of digital technology, we develop a simple concept and several equations for practical use.

2. Target System Analysis

The digital system is usually operated based on more complex logics when we compare it with the analog system because multiple functions could be performed in single processor. Therefore the CCF probability calculation of the digital system should be carefully treated. This study presents the case study of the application of simplified alpha-factor method to the digital plant protection system (DPPS) of the Korean Standard Nuclear Power Plant (KSNPP).

The target system, DPPS, consists of five kinds of component: Digital output (DO) module, local coincidence logic (LCL) processor module, Bistable processor (BS) module, analog input (AI) module, and digital input (DI) module.

The DO and LCL modules have the same success criteria which could be conceptually illustrated as in Figure 1. The failure of interrupting the electricity from the top to the bottom implies the failure of system. The BS, AI and DI modules also have their own success criteria. Because of page limitation, the criteria of each module cannot be described in a detailed manner in this paper.

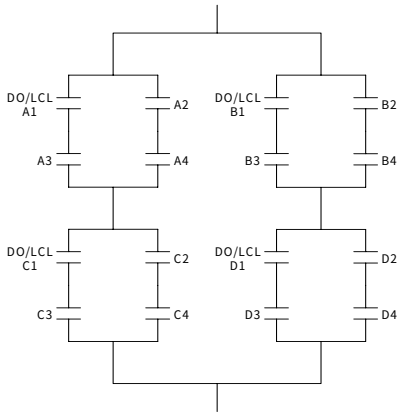

Figure 1. The conceptual illustration of the success criteria of the DO and LCL modules in KSNPP

3. Application of the SAF Method to the DPPS

For the convenience of explanation, we present one example case of the LCL processor module here. In order to apply the SAF method, we must determine whether each case of the CCF causes the system function failure or not based on the logic in Figure 1. The result could be tabulated as in Table 1.

From the basic parameter [2], the probability of single CCF event can be defined as:

$$Q_{CCF} = \sum_{k=2}^{m} ({}_{m}C_{k} \times p_{k} Q_{k}^{m}) = \sum_{k=2}^{16} ({}_{16}C_{k} \times p_{k} Q_{k}^{16}) \qquad (1)$$

From the reference [3], the probability of the CCF of k out of 16 components, Q_k^{16}, under the non-staggered test condition is defined as:

$$Q_k^{16} = \frac{k}{{}_{15}C_{k-1}} \cdot \frac{\alpha_k^{16}}{\alpha_t} \cdot Q_t \qquad (2)$$

where, the α_k^{16} denotes the portion of k components' CCF over 16-component CCF group and $\alpha_t = \sum_{i=1}^{16} i \cdot \alpha_i^{16}$.

Table 1. The ratio of the number of system failure CCFs to that of possible CCFs for the LCL processor modules

No. of CCF components (k)	${}_{16}C_k$	No. of system failure CCF (F_k)	p_k ($=F_k/{}_{16}C_k$)
1	16	0	0.000
2	120	0	0.000
3	560	0	0.000
4	1820	8	0.004
5	4368	96	0.022
6	8008	520	0.065
7	11440	1680	0.147
8	12870	3584	0.278
9	11440	5264	0.460
10	8008	5352	0.668
11	4368	3728	0.853
12	1820	1756	0.965
13	560	560	1.000
14	120	120	1.000
15	16	16	1.000
16	1	1	1.000

Table 2. The ratio of the number of system failure CCFs to that of possible CCFs for the LCL processor modules

k	α_k	Q_k / Q_t
2	0.010950	0.0012640
3	0.007795	0.0001928
4	0.006158	0.0000469
5	0.004350	0.0000138
6	0.002542	0.0000044
7	0.001939	0.0000023
8	0	0.0000000
9	0	0.0000000
10	0	0.0000000
11	0	0.0000000
12	0	0.0000000
13	0	0.0000000
14	0	0.0000000
15	0	0.0000000
16	0.004551	0.0630381
CCF coefficient (Q_{CCF} / Q_t)		0.07097

Note that the database for determining the α_k^{16} for digital components is not available and even generic alpha factors for 16-component CCF group are not available now. Therefore we use the extended generic alpha factors which are modified based on those for 8-component group with the assumption that the CCFs of more than 8 components are due to a lethal shock. Table 2 shows the result from this calculation. It should be noted that the results in Table 2 must be refined based on the further study on the 16-component group alpha factor.

4. CCF in the Same Functioning Modules from Different Vendors

The different modules from different vendors could be used to perform the same safety function in order to reduce the CCF probability. The parts such as memory chips or capacitors, however, could be produced by the same vendor or the same process.

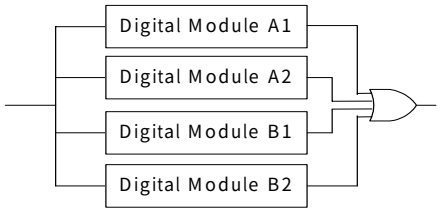

Figure 2. An example of the different modules for the same function

Figure 2 shows an example. Let's assume that module A consists of two kinds of parts: The same parts as in module B (*m*), and the other parts (*n*-*m*). Total number of parts which directly perform the safety function in the module A1 equals to *n*. In order to accommodate this situation in the fault tree CCF modeling, we must consider three basic events for the module A1: Independent failure of A1, CCF in module A group, and CCF in module A/B group.

$$p^{CCF(all)} = \frac{T}{2}\sum_{i=1}^{m}\rho_{4(i)}\lambda_i\,,\ p^{CCF(A)} = \frac{T}{2}\sum_{j=m+1}^{n}\rho_{2(j)}\lambda_j \qquad (3)$$

$$p^{A1} = \frac{T}{2}\sum_{i=1}^{n}\lambda_i - P^{CCF(A)} - P^{CCF(all)} \qquad (4)$$

5. Conclusion

In this paper, we propose a simple and practical framework for assessing the CCF probability of digital equipment. The proposed method is expected to accommodate several characteristics of digital technology in a more effective manner.

Acknowledgement

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

REFERENCES

[1] S.H. Han, "PSA of the PRHRS design of SMART-P," Technical note, ISA team, KAERI, 2004.

[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] M.J. Hwang, et al., "Guidance for Common Cause Failure Analysis," KAERI/TR-2444/2003.