Effect of *k*-out-of-*n* Redundancy in Reactor Protection System in Consideration of Common Cause Failure

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

A reactor protection system (RPS) in a nuclear power plant includes multiple processing channels for ensuring both safety and economy. Lu and Lewis [1] suggested a method of unavailability and spurious operation probability (SOP) estimation for this kind of multiple redundant safety system. They insisted that independent failures are the main focus of the study since sufficient diversities including physical and technical separation among channels are effective in circumventing common cause failures (CCFs).

There are two shutdown systems in a CANDU nuclear plant and these two systems use two different equipments to avoid CCF. However, pressurized water reactors in Korea, including OPR1000, do not equipped with completely different safety systems for reactor protection. The redundancy is the major echelon for reducing the risk from CCFs. In this circumstance, CCFs should be considered carefully in calculating the unavailability and the SOP.

2. Unavailability

The unavailability is defined as the probability that a system will fail when a demand arrives. The unavailability of a RPS is the failure probability of trip signal generation when a plant is in abnormal status. Suppose that the *n* channels are identical and concurrent operation of *k* channels will initiate the reactor trip. When there are greater than or equal to $n-k+1$ channels that fail during an emergency, this *k*-out-of-*n* system is unavailable. Independent failures and CCFs in these channels are assumed to be symmetric.

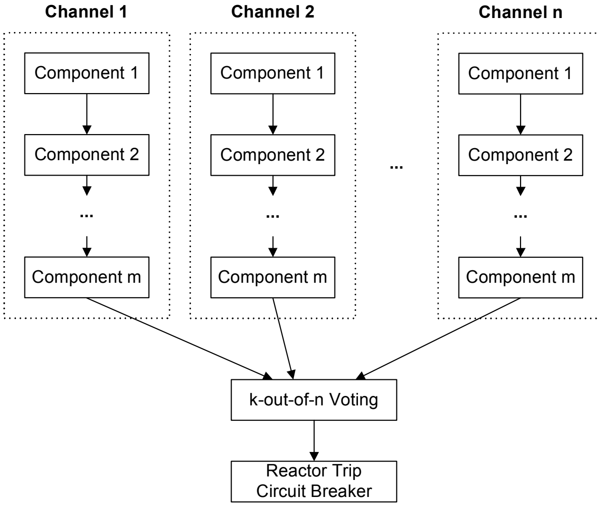

Figure 1. Typical layout of RPS
(*k*-out-of-*n* redundant processing channels)

The unavailability (U) of signal generation consists of two factors: automated system failure and human operator failure (q_{OP}). For the system illustrated in Figure 1, Q_i denotes the probability that exactly i channels fail. When $i \geq n-k+1$, Q_i implies the failure of automated signal generation system such as RPS. If we assume the serial structure of components in a channel i, Q_i is sum of components' unavailability ($q_{i,j}$). $q_{i,j}$ can be divided into independent failure ($q_{i,j(Ind)}$) and CCF ($q_{i,j(CCF)}$).

$$\begin{aligned} U &= q_{OP} \sum_{i=n-k+1}^{n} Q_i \\ &= q_{OP} \sum_{i=n-k+1}^{n} \sum_{j=1}^{m} q_{i,j} \\ &= q_{OP} \sum_{i=n-k+1}^{n} \sum_{j=1}^{m} (q_{i,j(Ind)} + q_{i,j(CCF)}) \end{aligned}$$

q_j denotes the failure probability of component j. If q_j is small enough, $q_{i,j(Ind)}$ can be simplified since $(1- q_j)^{n-i} \approx 1$. Alpha factor method is applied to calculate the CCF probability. The method for calculating alpha factors ($\alpha_i^{(n)}$) and α_t is explained in reference [2].

$$q_{i,j(Ind)} = \binom{n}{i} q_j^{\,i} (1-q_j)^{n-i} \approx \binom{n}{i} q_j^{\,i}$$

$$q_{i,j(CCF)} = \binom{n}{i} \frac{i}{\binom{n-1}{i-1}} \frac{\alpha_i^{(n)}}{\alpha_t} q_j = n \frac{\alpha_i^{(n)}}{\alpha_t} q_j$$

Then unavailability, U, can be simply rewritten as

$$U \approx q_{OP} \sum_{i=n-k+1}^{n} \sum_{j=1}^{m} \{ \binom{n}{i} q_j^{\,i} + n \frac{\alpha_i^{(n)}}{\alpha_t} q_j \} .$$

3. Spurious Operation Probability

In the case of RPS spurious operation, we ignore the human operator's recovery probability, since the reactor shutdown rods inserted immediately by gravity when the automated signal generated by RPS and a human operator has no chance to recover the spurious reactor trip signal.

That is $p_{OP} \approx 1$. Suppose the probability of spurious operation of a given channel (P_i) in a k-out-of-n system is the same for each channel. The failures of channels more than or equal to k will cause spurious operation. If we assume the serial structure of components in a channel i and each of component may cause spurious operation signal with probability of $p_{i,j}$, P_i is sum of $p_{i,j}$s. $p_{i,j}$ consists of two parts ($p_{i,j(Ind)}$ and $p_{i,j(CCF)}$).

$$S = p_{OP} \sum_{i=k}^{n} P_i \approx \sum_{i=k}^{n} P_i \approx \sum_{i=k}^{n} \sum_{j=1}^{m} p_{i,j}$$

$$\approx \sum_{i=k}^{n} \sum_{j=1}^{m} (p_{i,j(Ind)} + p_{i,j(CCF)})$$

If p_j is small enough, $p_{i,j(Ind)}$ and $p_{i,j(CCF)}$ can be calculated as follows:

$$p_{i,j(Ind)} = \binom{n}{i} p_j^{\,i} (1-p_j)^{n-i} \approx \binom{n}{i} p_j^{\,i}$$

$$p_{i,j(CCF)} = \binom{n}{i} \frac{i}{\binom{n-1}{i-1}} \frac{\alpha_i^{(n)}}{\alpha_t} p_j = n \frac{\alpha_i^{(n)}}{\alpha_t} p_j$$

Then SOP, S, can be simply rewritten as

$$S \approx \sum_{i=k}^{n} \sum_{j=1}^{m} \{ \binom{n}{i} p_j^{\,i} + n \frac{\alpha_i^{(n)}}{\alpha_t} p_j \}$$

4. Application to 2/3 and 2/4 System

We will illustrate an example for q_{OP}=0.001, q_j=0.001 and p_j=0.002 for the case of 2-out-of-3 system and 2-out-of-4 system. For the simplicity, m=1. The generic values are used for $\alpha_i^{(n)}$s which are shown in Table 1.

The results of calculation are shown in Table 2. The change from 2-out-of-3 system to 2-out-of-4 system will reduce the unavailability by 27% but increase the SOP by 34%.

Table 1. Generic values of alpha factors [2]

i n	3	4
1	0.9500	0.9500
2	0.0242	0.0213
3	0.0258	0.0101
4		0.0186

Table 2. Results of unavailability and SOPs for 2/3 and 2/4 systems

		2/3		2/4	
U	$\sum q_{i,j(Ind)}$	3.0E-9	1.4E-7	4.0E-12	1.0E-7
	$\sum q_{i,j(CCF)}$	1.4E-7		1.0E-7	
S	$\sum p_{i,j(Ind)}$	1.2E-5	2.9E-04	2.4E-5	3.9E-4
	$\sum p_{i,j(CCF)}$	2.8E-4		3.6E-4	

The effect of CCF is dominant contributor in any case. Especially for the unavailability, the CCF effect dominates the results and the effect of independent failure is negligible. This result clearly shows the importance of CCF in unavailability calculation.

5. Expansion to Complicated Structure

In digitalized applications, the structure of RPS is much more complicated than 2-out-of-3 or 2-out-of-4. The design of digitalized RPS may include repeated selective voting logics and selective voting logics. The signal flow in the system may not be straight forward and one processor may refer other processors' results for monitoring or for signal processing. The human error probability (q_{OP}) might be dependent on the status of the automatic signal processing system. For these complicated structures, the analytic equations derived here are hard to be applied directly.

As shown in previous studies [3,4], fault tree is useful method to model these complicated structure systems in an explicit manner. For the practical application, use of the simplified CCF modeling method [3] is recommended. The error from the simplification and the limitation of modeling should be further investigated for some very large redundancy cases (such as 8 or 16 channels).

6. Concluding Remarks

The method for calculating the unavailability and SOP of k-out-of-n system is developed. The example application shows that the CCF dominates the results especially for unavailability.

Acknowledgement

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

REFERENCES

[1] Lixuan Lu and Gregory Lewis, "Configuration determination for k-out-of-n partially redundant systems," Reliability Engineering and System Safety (2008), doi:10.1016/j.ress.2008.02.009.

[2] Mee Jeong Hwang, et al., "Guidelines for System Modeling: Common Cause Failures (rev.1)," KAERI/TR-2916/2005.

[3] Hyun Gook Kang, Seung-Cheol Jang and Jejoo Ha, "Fault Tree Modeling for Redundant Multi-Functional Digital Systems," International Journal of Performability Engineering, Vol. 3, No. 3, 2007.

[4] Hyun Gook Kang and Seung-Cheol Jang, "Application of Condition-based HRA Method for a Manual Actuation of the Safety Features in a Nuclear Power Plant," Reliability Engineering & System Safety, Volume 91, Issue 6, June 2006.