Evaluation method for common cause failure hazards on non-safety related system

Yun Goo Kim[*], Jong Beom Lee

Korea Hydro and Nuclear Power Co., ltd, Central Research Institute, Daejeon, Korea
[*]*Corresponding author: ygkim.stpn@khnp.co.kr*

1. Introduction

Hazard of Common-cause failures (CCFs) have been identified and needed to be evaluate for digital I&C (DI&C) systems. Recently, US NRC published draft version of BTP 7-19 Revision 8, which provide guidance for evaluation of CCFs on DI&C systems [1]. Specially, revised BTP 7-19 addresses the graded approach for the evaluation based on the safety significance of the DI&C systems. This paper review the graded approach for non-safety related system and provide qualitative assessment approach based on quantitative CCF analysis.

2. Graded approach addressed on BTP 7-19

The proposed graded approach is based on the safety significant and safety grade of system. Table 1 shows the summary of the graded approach

Table 1 Graded approach of the CCF evaluation

	Safety-Related	Not Safety-Related
Safety Significant	A1 Diversity and defense in depth assessment	B1 Qualitative assessment
Not Safety Significant	A2 Qualitative assessment	B2 Qualitative assessment

For the safety significant safety-related system, diversity and defense in depth assessment is required and for other cases, qualitative assessment is required. The qualitative assessment considers three factors that a) design attributes and features of the DI&C system or component; b) quality of the design process of the DI&C system or component; and c) applicable operating experience regarding the DI&C system or component. It also requests that the qualitative assessment demonstrating the likelihood of the CCF hazard is sufficiently low based on any of the following criteria; a) design attributes and features of the proposed system that reduce the likelihood of CCF hazards; b) quality of the design process of the DI&C system that reduces the likelihood for CCF hazards due to latent defects in the software or software-based logic in the DI&C system or component; c) The applicable operating experience regarding the DI&C system or component collectively supports a conclusion that the DI&C system or component will operate with high reliability for the intended application. Operating experience in most cases can serve to compensate for weakness in addressing the other two criteria. d) The proposed system will not result in a failure that could invalidate the plant licensing basis.

Also, BTP 7-19 address spurious operation (spurious actuation) assessment. For the safety significant safety related system, it requires any of the combination of a) means to eliminate CCF b) use of diverse means, c) consequences of CCF evaluation. For others cases, it requires any of the combination a) qualitative assessment, b) use of diverse means, c) consequences of CCF evaluation. In other word, BTP 7-19 allows to select methods for the CCF evaluation but still requires evaluation of consequences of CCF as one of proper evaluation method. In this paper, the detail consideration of evaluation method for CCF hazard on non-safety related system is proposed.

3. Failure effect evaluation method.

For the CCF evaluation of non-safety related control system, the CCF hazard to safety goal should be analyzed. There are various functions on non-safety related control system. The failure sets of control system function that threat the safety goal should be decided. Fig.1 show the evaluation process of CCF hazard on non-safety related control system

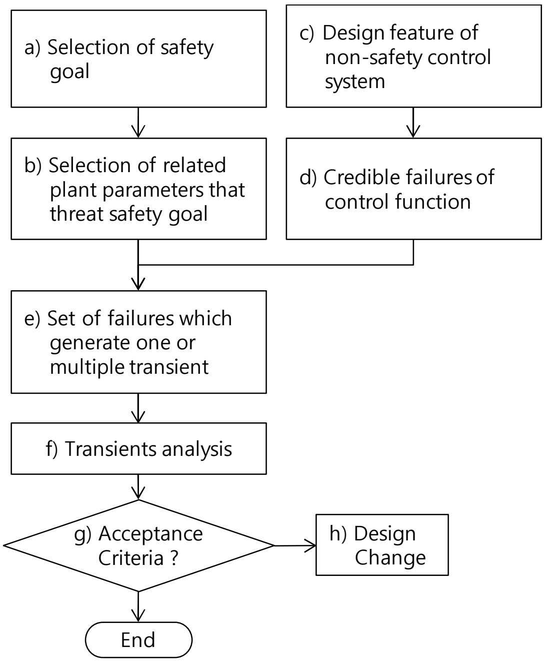
a) Selection of safety goal
c) Design feature of non-safety control system
b) Selection of related plant parameters that threat safety goal
d) Credible failures of control function
e) Set of failures which generate one or multiple transient
f) Transients analysis
g) Acceptance Criteria ?
h) Design Change
End

Figure 1 CCF hazard evaluation for non-safety related control system

First of all, the safety goal needs to be defined. The plant safety can be demonstrated through reviewing the plant safety goals. The plant safety goals are summarized as follows; fuel cladding integrity, primary system integrity, and offsite radiation release. Each safety goal can be affected by various plant conditions. In the APR1400 I&C system, the same distributed control system (DCS) controller is used in most non-safety related control systems, such as the feed water control system (FWCS), the steam bypass and control system (SBCS), the pressurizer level control system (PLCS), the pressurizer pressure control system (PPCS), and the reactor power cutback system (RPCS) [2]. CCF on non-safety related control system may have spurious operation and the combination of spurious operation may have same negative effects to the safety goal of the plant. For the CCF evaluation, the worst case of combination of failure should be considered.

Fig. 2 depicts the minimum DNBR related failure effect relations. It can be used to evaluate the failure effects on plant safety goal. For example, the DNBR decreases when the heat flux of the fuel rod increases or a critical heat flux in the reactor coolant decreases. The heat flux of the fuel rod increases when the reactivity increases. The reactivity increases when the reactor coolant system (RCS) temperature decreases due to the negative moderator to the temperature coefficient in the NPP. The RCS temperature decreases when the heat transfer to the secondary system increases. The heat transfer will increase when the secondary system temperature decreases or the secondary system flow rate increases. The reactivity also increases when the neutron flux increases. Meanwhile, the critical heat flux decreases when the RCS temperature increases

Therefore, when 2nd system temperature is decreasing (F in Fig.2), the heat flux from fuel (B in Fig.2) is increasing, but when 2nd system temperature is increasing, the critical heat flux on fuel (I in Fig.2) is decreasing. In other word, 2nd system temperature has two opposite effects to the DNBR. For each cases, the amount of DNBR changes should be analyzed to decide worst spurious operation of 2nd system temperature related system. For the analysis, every expected spurious operation of non-safety control system should be evaluated together. After that the worst case of failure combination can be selected with the suggested failure effect evaluation model. In this case, heat flux increase (B in Fig.2) has more negative effects.

4. Discussion

The failure effect analysis method for the CCF on non-safety related control systems has been proposed. Because there are numerous possible failure cases, the effect based assessment method was used. The analysis results of the worst-case failure scenario satisfy the acceptance criteria of the safety analysis in the transient and accident analyses. This results shows that the appropriate actuation of the safety systems, and the inherent sufficient safety margin, keep the plant in acceptance criteria of safety goal. The proposed analysis method also can be used to evaluate multiple failures in complex systems.

REFERENCES

[1] U.S. NRC, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, NUREG-0800, Standard Review Plan, BTP 7-19, Rev 7, July 2016.

[2] Korea Hydro & Nuclear Power Co., Ltd., APR1400 Design Control Document Tier 2, Chapter 7 Instrumentation and Controls, APR1400-K-FS-14002-NP, 2014

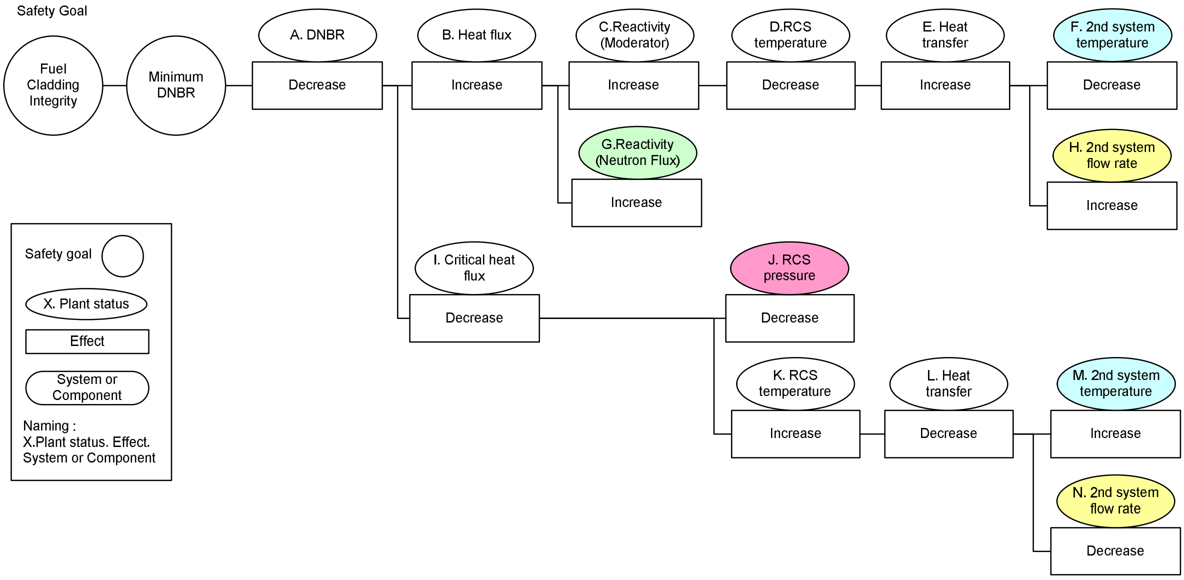

Figure 2. Failure effect analysis modeling of the fuel cladding integrity and control system failure.