A framework to estimate the coverage of AOPs in nuclear power plants[1]

Jinkyun Park and Wondea Jung
Korea Atomic Energy Research Institute 150, Dukjin, Yuseong, Daejeon, Korea
Corresponding author: kshpjk@kaeri.re.kr

1. Introduction

The safe operation of large process control systems, such as NPPs (Nuclear Power Plants) is the most critical factor determining their sustainability. In this regard, various kinds of procedures (e.g., abnormal operating procedures; AOPs) have been used because they are helpful to specify what should be done to cope with off-normal events jeopardizing the safety of NPPs. Unfortunately, since most AOPs were developed based on operational experience, it is not easy to investigate their coverage in a systematic manner. For this reason, in this paper, a framework to estimate the coverage of AOPs in NPPs is proposed based on a SPV (Single Point Vulnerability) model.

2. Traditional way to develop AOPs

As already mentioned in Section 1, one of the straightforward ways to develop AOPs is to review historical data (i.e., OE; Operation Experience). In order to clarify this aspect, let us consider Fig. 1, which shows a simplified process of the CAP (Corrective Action Program), as suggested by the IAEA (International Atomic Energy Agency).

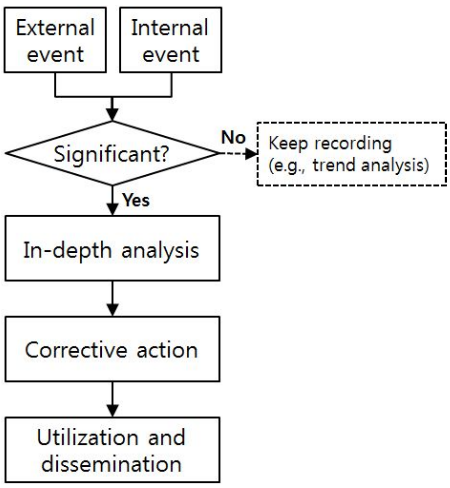

Fig. 1. Simplified process of CAP [1]

As depicted in Fig. 1, the first step is to gather remarkable events that have occurred in either a home plant (i.e., internal event) or other NPPs (i.e., external event). After that, the significance of these events should be rated with respect to their effect on the safety as well as economy of NPPs. For example, EPRI (Electric Power Research Institute) proposed three levels of event significance, such as *Critical*, *Important*, and *Minor* [2]. Here, the *Critical* event denote an event that can result in safety incidents including fatality, reportable environmental damage or major loss of electricity, while the *Minor* event represents near misses or troubles that are trivial from the point of view of the safety or productivity of NPPs.

With these classifications, when an event of which the significance belongs to the *Critical* level and *Important* level has occurred, it is necessary to identify its cause by conducting a detailed analysis. In contrast, an event corresponding to the *Minor* level is usually stored in a database that will be used as a source for further investigations, such as a trend analysis. If reasonable causes are distinguished from the in-depth analysis, proper corrective actions can be selected with respect to the nature of the event at hand. One of the typical corrective actions is the improvement of relevant procedures, such as modifying the contents of an existing AOP or writing a novel one. The last step of the CAP process is to disseminate the detailed contents of the event with the associated countermeasures to other NPPs so that they can start their own CAP process (i.e., the external event).

If we follow this CAP process, it is highly expected that the coverage of AOPs in a certain NPP will increase. However, it is still uncertain whether or not the AOPs are able to sufficiently cover all kinds of off-normal events to be occurred because the improvement of AOPs (modifying their contents or writing a novel one) is followed only after the appearance of a significant event.

3. Single point vulnerability (SPV) model

As explained in Section 2, it seems that the large volume of AOPs does not represent a sufficient coverage because there could be many significant events that we did not yet experience. One promising solution to resolve this limitation is to use a SPV (Single Point Vulnerability) model, which is one of the well-known approaches to distinguish critical components affecting the vulnerability of complex infrastructures including NPPs [3-5].

---

[1] This paper is the summary of a journal paper recently published. More detailed information on the idea of this paper can be found in Ref. [11].

The key feature of the SPV assessment is to identify the catalog of components (i.e., SPV components), which have a possibility to cause either the loss of productivity or an impairment of the operational safety of a given system. In this regard, the SPV components of NPPs commercially operating in the Rep. of Korea were recently distinguished by combining an FMEA (Failure Modes and Effects Analysis) and FTA (Fault Tree Analysis) method [3, 6]. For example, Fig. 2 shows a part of FTs (Fault Trees) representing the SPV model of the OPR1000 (Optimized Power Reactor 1000MWe) [3].

One of the crucial benefits using FTs is that the catalog of SPV components can be easily identified by analyzing the list of MCSs (Minimal Cut Sets) composed by one or more BEs (Basic Events), which denote plausible causes resulting in significant losses in terms of the productivity and safety of NPPs. If we are able to soundly identify the catalog of SPV components, then it is expected that this catalog is very important for preventing the occurrence of off-normal conditions. This strongly implies that the contents of AOPs, which are essential for coping with various kinds of off-normal conditions, can be determined by comparing the catalog of SPV components. In other words, it is possible to assume that the contents of AOPs should be able to cover anticipated conditions to be caused by the failure of the SPV components. Conversely, it is possible to estimate the coverage of AOPs if their contents are compared with the anticipated conditions resulted from the SPV components.

However, there is a critical problem in implementing this idea. The first one is the number of MCSs to be generated from a given FT. For example, in the case of FTs representing the SPV model of the OPR1000, the number of MCSs being obtained from the calculation of the AIMS-PSA (Advanced Information Management System for Probabilistic Safety Assessment) and FTREX (Fault Tree Reliability Evaluation expert) software [7, 8] with the truncation limit of 1.00E-11 is about 138,000. However, it is impractical to compare all the SPV components that are identified from these MCSs with the contents of the associated AOPs. Accordingly, it is inevitable to establish an index that is helpful for distinguishing the relative significance of MCSs in a systematic way. For this reason, the concept of a DIF (Difficulty, Importance and Frequency) is applied to develop an MCSC (MCS Criticality) index.

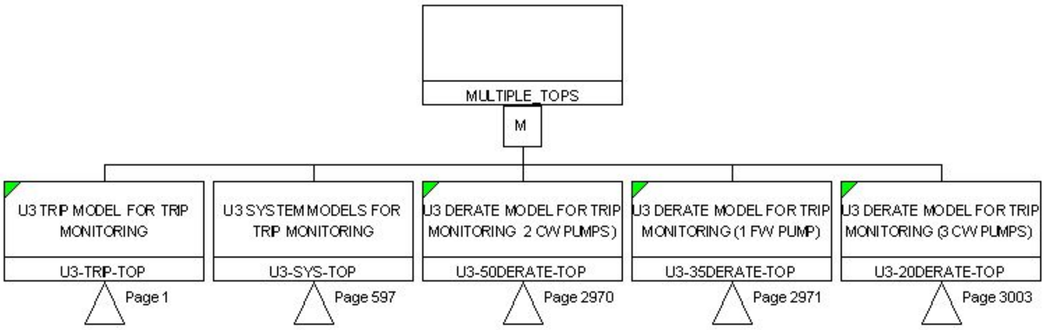

Figure 2. A part of FTs representing the SPV model of the OPR1000 (adopted from Ref. [3])

4. MCS criticality

One of the traditional issues in training and/or education is to decide a task inventory to be drilled, which is able to enhance the effectiveness of the training (or education). In this regard, the DIF concept is one of the promising solutions because it is possible to distinguish the criticality of a task based on the multiplication of three kinds of intuitive dimensions: (1) how hard to perform a task properly (*Difficulty*), (2) how serious consequences are expected if the performance of the task is done improperly (*Importance*), and (3) how often the task should be performed (*Frequency*) [DOE, 1994; DOD, 2001]. The more interesting point is that this concept can be easily applied to the evaluation of MCS criticality.

First, it is expected that the sum of the probabilities of BEs included in a given MCS directly represents the *Frequency* dimension. Second, the *Difficulty* dimension can be rated by considering the meaning of a system propagation. For example, the system propagation of a certain component is one if its failure only affects one component (i.e., one-to-one relation). In contrast, if the failure of a certain component generates four different components, its system propagation becomes four. In this case, since the configuration of the latter should be more complicated than the former, it is reasonable to say that a task related to the latter is more difficult than that of the former. Third, two kinds of risk importance measures are meaningful for reflecting the *Importance* dimension.

From the point of view of an FT analysis, there are several measures used to quantify the impact of each BE on the risk of a given system [9]. Of them, the most popular measures are the FV (Fussel-Vesely) and RAW (Risk Achievement Worth) [10]. In brief, the FV denotes the fractional contribution of a certain component failure to the total risk of the system while the RAW denotes the amount of the fractional increase in the risk if the component failure has occurred. In other words, the FV is effective for listing a safety-critical component of which the failure occupies a large portion of the total risk, while the RAW is convenient for clarifying a component, of which the failure results in a large amount of risk. Subsequently, US NRC proposed criteria to determine the risk significance score of a given BE as depicted in Fig. 3.

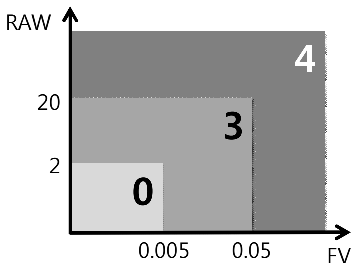

Figure 3. Risk significance socre with respect to the FV and RAW

As can be seen from Fig. 3, a component failure of which the FV value is greater than 0.05 or the RAW value is greater than 20 will have the highest level of the risk significance (i.e., 4). In contrast, the failure of a component will have the lowest level of the risk significance (i.e., 0), if its FV and RAW value are less than 0.005 and 2, respectively. Accordingly, the *Importance* dimension can be determined as the sum of risk significance scores that are calculated for all BEs included in a given MCS.

5. General conclusion

It is apparent that the sufficient coverage of AOPs is one of the prerequisites for improving the operational safety of NPPs because they provide a series of proper actions to be conducted by human operators, which are crucial for coping with off-normal conditions caused by the failure of critical components. In this light, the catalog of BEs (i.e., SPV components) identified from an SPV model could be a good source of information to enhance the coverage of AOPs. Unfortunately, because of the avalanche of the number of corresponding MCSs, it is inevitable to develop a screening process that allows us to select critical MCSs. For this reason, the MCSC score is defined along with the DIF concept. Based on the MCSC score, a framework that allows us to systematically investigate the coverage of AOPs is proposed in Ref. [11]. In addition, in order to validate the appropriateness of the proposed framework, the root causes of unexpected reactor trip events that have occurred in the Rep. of Korea over the last three years are compared with BEs identified from the analysis of the SPV model of OPR1000 units. As a result, it is estimated that the coverage of AOPs being used in OPR1000 is about 63%.

It should be noted that there are a couple of limitations in this study. For example, the precision of the abovementioned coverage entirely depends on that of the SPV model being scrutinized by the proposed framework. This implies that independent reviews of SMEs (Subject Matter Experts) who have sufficient knowledge on both the configuration and operation of NPPs are unavoidable to confirm the appropriateness of the suggested framework. Nevertheless, if we recognize a lack of a systematic approach to determine the coverage of AOPs, it is strongly expected that the suggested framework is meaningful for improving the operational safety of NPPs.

Acknowledgment

This work was supported by Nuclear Research & Development Program of the National Research Foundation of Korea grant, funded by the Korean government, Ministry of Science, ICT & Future Planning (Grant Code: 2012M2A8A4025991).

REFERENCES

[1] IAEA, Effective corrective actions to enhance operational safety of nuclear installations, IAEA-TECDOC-1458, International Atomic Energy Agency, 2005

[2] EPRI, Corrective Action Program Guideline, 1015838, Palo Alto, CA, 2008

[3] Bae, Y., Lee, E., Chi, M., Development and application of plant trip risk evaluation model. In: Proceedings of ICAPP2013, April 14-18, Jeju Island, Rep. of Korea, 2013

[4] Baker, G. H., A vulnerability assessment methodology for critical infrastructure facilities. Available at: http://works.bepress.com/george_h_baker/2, 2005

[5] NEI, Industry guideline for monitoring the effectiveness of maintenance at nuclear power plants, NUMARC 93-01, Revision 4A, 2011

[6] Hyun, J. W., Yeom, D. U., and Song, T. Y., Selection of single point vulnerability through the failure mode effect analysis of equipment in newly built nuclear power plant, The Transactions of the Korean Institute of Electrical Engineers Vol. 61, No. 4, p. 509-512, 2012

[7] Jung, W. S., Yang, J., and Ha, J., Development of measures to estimate truncation error in fault tree analysis, Reliability Engineering and System Safety, vol. 90, iss. 1, p. 30-36, 2005

[8] Yang, J., Development of an integrated risk assessment framework for internal/external events and all power modes, Nuclear Engineering and Technology, vol. 44, no. 5, p. 459-470, 2012

[9] Vaurio, J. K., 2011. Importance measures in risk-informed decision making: ranking, optimization and configuration control, Reliability Engineering and System Safety, vol. 96, p. 1426-1436

[10] Van der Borst, M., and Schoonakker, H., 2001. An overview of PSA importance measures, Reliability Engineering and System Safety, vol. 72, p. 241-245

[11] J. Park and W. Jung, "A systematic framework to investigate the coverage of abnormal operating procedures in nuclear power plants,' Reliability Engineering and System Safety, Vol. 138, p. 21-30, 2015.