# Evaluating and modeling of an event diagnosis failure in PSA

Wondea Jung, Jinkyun Park and Jae W. Kim
*Korea Atomic Energy Research Institute*
*wdjung@kaeri.re.kr*

## 1. Introduction

Event diagnosis after a reactor trip is very important for plant safety in a nuclear power plant. However, the current human reliability analysis (HRA) does not appropriately evaluate the effect of such a diagnosis failure to the plant safety. This paper shows, based on a simulation study, the potential for a diagnosis failure is much higher than what we expect. This paper summarizes the analysis results of the study, the performance time of an event diagnosis and the potential of a diagnosis failure.

## 2. Diagnosis failure and PSA/HRA

The analysis results of the accidents, such as TMI, Davis Besse, and Fort Calhoun, shows that the failure of a state identification or event diagnosis is a dominant contributor which aggravates the plant situation [1]. On the other hand, the HRA of a probabilistic safety assessment (PSA) does not deal with such a diagnosis failure appropriately, so far. However, the performance of an event diagnosis should be assessed as exactly as possible to appropriately evaluate the human contribution to the plant safety.

Table 1. Summaries of simulator experiments

| Scenarios | Scenario description | # of data |
|---|---|---|
| LOCA | Stuck open of a pressurizer safety valve | 25 |
| SGTR | A tube rupture in the steam generator #2 | 19 |
| ESDE | A rupture (30%) of a main steam line located inside of containment | 16 |
| LOAF | Loss of all feedwater including auxiliary feedwater | 19 |
| LOOP | Loss of offsite power event | 11 |
| SBO | Loss of all AC power (emergency DGs fail under loss of offsite power condition) | 11 |
| Total | 101 | 101 |

## 3. Data collection and performance analysis

To clarify the necessity of modeling of the diagnosis failure, simulator experiments have been conducted using a full-scope simulator of YGN plants. The data collection method we used is the video recording at a remote room in which the recording facilities are equipped, while at the same time two investigators observe the operators' behavior and keep a record of noteworthy events. In addition, information on the trend of the major parameters and the operators' manipulation of the components could be automatically obtained from the simulator.

Data collection has been carried out for six accident scenarios and twelve MCR operating shifts have participated in the experiment. More than 100 simulation records have been collected for six different scenarios. Table 1 shows the summaries of the data collection.

In this study, time and accuracy are used to represent the diagnosis performance. To collect the diagnosis time as well as the diagnosis accuracy, both a protocol and a timeline analysis are conducted based on the videotapes on which all kinds of operators' behaviors and communications are recorded [2]. Figure 1 shows the average time taken for the event diagnosis for the six different scenarios.

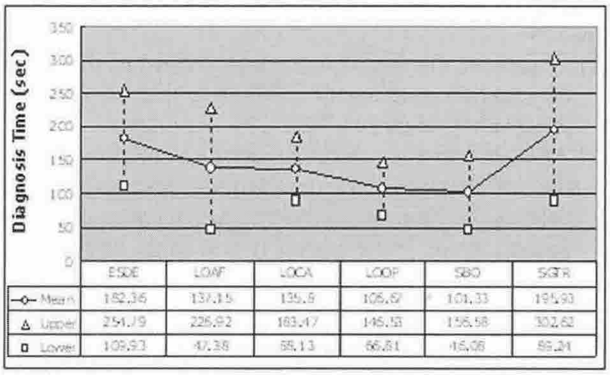

Figure 1. Diagnosis time of each scenario

Another important analysis result is the diagnosis accuracy, i.e., diagnosis error probability. Diagnosis error means all kinds of deviations in the diagnosis stage, which includes a misdiagnosis, delayed diagnosis and no response. As shown in Table 2, a total of 4 diagnosis errors were counted for 101 experimental trials. So the numerical mean of the diagnosis error probability is 0.0396, which is much higher than that of the expected one.

Table 2. Diagnosis accuracy of each scenario

| Scenario | # of data | # of diagnosis failure | Error probability |
|---|---|---|---|
| LOCA | 25 | 1 | 0.0400 |
| SGTR | 19 | 2 | 0.1053 |
| ESDE | 16 | 0 | 0.0000 |
| LOAF | 19 | 1 | 0.0526 |
| LOOP | 11 | 0 | 0.0000 |
| SBO | 11 | 0 | 0.0000 |
| Total | 101 | 4 | 0.0396 |

Undoubtedly a diagnosis failure does not directly cause an accident of core damage. But the diagnosis failure definitely increases the possibility of inappropriate human responses that might aggravate the plant situation, which consequently raises the potential of core damage. Supposing just 1% of the diagnosis failure induces the core damage accident, the frequency of the scenario could increase to $10^{-6}$ or $10^{-7}$, which could not be disregarded as an effect to the plant safety.

## 4. An approach to model the diagnosis failure

We suggest an approach to analyse the misdiagnosis event, namely MisDiagnosis Tree Analysis (MDTA) technique [3]. Using the MDTA technique, all the possible diagnosis paths including misdiagnosis paths and their causes could be identified. MDTA is constructed on the basis of the diagnostic rules of the emergency operating procedure (EOP). As misdiagnosis causes, three groups of causes are used: plant dynamics (PD), operator error (OE) and instrumentation failure (IF).

A brief guidance on the construction of MDTA is as follows:

(1) Represent the decision rules for an event diagnosis or situation assessment in a chronological order in the heading of an MDTA.

(2) At each decision rule, draw up the upper branch and the lower branch as representing respectively the correct decision and the wrong decision, and again for the lower branch, split it into three branches to represent the corresponding causes contributing to choosing the wrong path or decision.

(3) For each decision rule, check the possible causes that are applicable to the current decision rule, i.e. the causes that may contribute to the operators' wrong situation assessment or choosing the wrong decision path, and represent the identified causes on the corresponding branches.

(4) Continue steps (2) and (3) for all the decision rules until the final diagnosis is made. Finally, the analyst can obtain the final diagnosis results with the possible misdiagnosis paths and their causes.

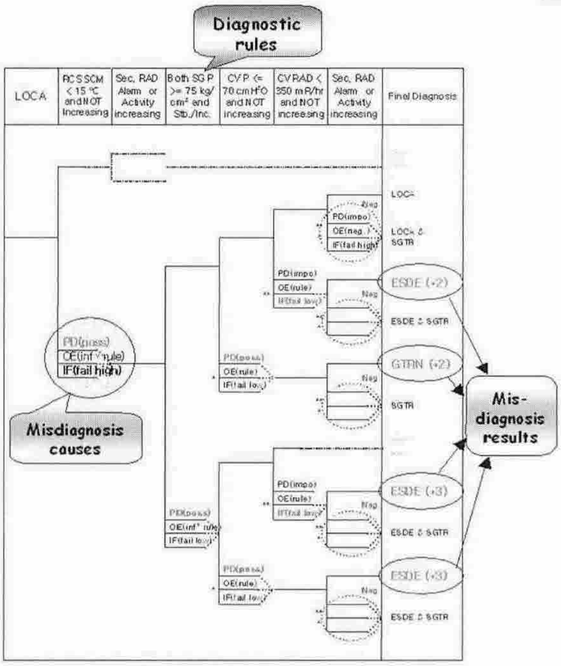

Figure 2. An example of misdiagnosis tree analysis

## 5. Conclusion

This paper showed that the potential for a diagnosis failure can be higher than what we expect based on the analysis results of a simulation study. Even though the estimation might have some restrictions in the representative simulated scenarios and population size, the results show clearly that the effect of a diagnosis failure to the plant safety could not be disregarded.

For a more realistic analysis on plant safety, a diagnosis failure should be treated in a systematic and proper way. The MDTA technique was suggested in this study to systematically analyse the potential for a diagnosis failure.

## REFERENCES

[1] Bongarra JrJp, Persensky J.J., Implementing requirements for upgrading emergency operating procedures: a regulatory perspective. Proceedings of IEEE Fourth Conference on Human Factors and Power Plants, pp208-213, 1988.

[2] J. Park, W. Jung, The requisite characteristics for diagnosis procedures based on the empirical findings of the operators' behavior under emergency situations, Journal of Reliability Engineering and System Safety, Vol. 81, pp197-213. 2003.

[3] J. Kim, W. Jung, A Systematic Approach to Analysing Errors of Commission from Diagnosis Failure in Accident Progression, *Accepted for Publication*, RESS, 2004.