Transactions of the Korean Nuclear Society Autumn Meeting
Busan, Korea, October 27-28, 2005

The MDTA-based Method for Assessing Diagnosis Failures and Their Risk Impacts: A Case Study for the SLOCA Event

Jae Whan Kim, Wondea Jung
Korea Atomic Energy Research Institute
jhkim4@kaeri.re.kr

Young Seok Son
Dong-Eui University
ysson@deu.ac.kr

1. Introduction

In the emergency situations of nuclear power plants (NPPs), diagnosis of the occurring events is crucial for managing or controlling the plant to a safe and stable state. If the operators fail to diagnose (or misdiagnose) the event(s), their responses can eventually be inappropriate or inadequate. This paper presents a method for assessing the potential for diagnosis failures of the occurring events and their risk impacts which have normally not been addressed in the conventional probabilistic safety assessment (PSA).

2. Method

The approach to the assessment of the impact of diagnosis failure on PSA is composed of three parts: 1) the assessment of the potential for diagnosis failures, 2) the identification of the probable human failure events (HFEs) that could be induced from the diagnosis failures, and 3) the quantification of the probabilities of the identified HFEs and the incorporation of them into PSA.

2.1. Assessment of the potential for diagnosis failures

The analysis of the potential for diagnosis failures (or misdiagnosis) is performed using the misdiagnosis tree analysis (MDTA) technique [1]. The guidelines for the incorporation of three misdiagnosis causes, i.e. plant dynamics (PD), operator errors (OE), and instrumentation failures (IF), into the MDTA are summarised as follows.

- Plant dynamics (PD)

The contribution of the PD factor for an event at a decision rule is evaluated by estimating the fraction of an event spectrum where the behaviour of the decision parameter does not match the established criteria of the decision rule at the operators' diagnosis time. In order to estimate that fraction in a reasonably acceptable level of detail, an event under analysis should be classified into sub-groups, each of which becomes a set of the thermal-hydraulic code analysis, by considering plant dynamic behaviours from the viewpoint of the operators' event diagnosis. For an event group that shows the potential for a mismatch, a further T/H analysis is performed to decide on the range of the mismatch. After finding out the ranges of the mismatches for all the potential event groups, one can obtain the fraction for an event spectrum to be in a mismatched condition at each decision rule.

- Operator errors (OE)

The contribution of operator errors for taking a wrong path at a decision point is assessed by assigning an appropriate probability to the selected items according to a cognitive function. The selected items are provided in Ref. [2].

- Instrumentation failures (IF)

As for an instrumentation failure, one considers the availability and reliability of the instrumentation system. Most of the instruments in NPPs have multiple channels (2 or 4 channels) of an instrumentation, hence it is assumed that the operators can identify the failed state of an instrumentation when a single channel fails during a normal operation and that the likelihood of the functional failure during an accident progression is negligible. Thus in this study the failure of multiple channels in a common mode during a normal operation is considered.

2.2. Identification of human failure events (HFEs)

The HFEs can result from the unsafe actions related to both the required functions and the unrequired or unnecessary functions. The unsafe actions in view of both functions can be defined as follows:

- Unsafe actions related to the required functions
  - Failure to initiate the required functions
  - Failure to maintain the required functions
- Unsafe actions related to the unrequired functions
  - Manual operation of unrequired or unnecessary functions

The HFEs that might be induced from the diagnosis failures are identified through the construction of the required functions for both the actual event and the misdiagnosed event.

2.3. Quantification and modeling into PSA

This section provides a rough quantification scheme for the identified HFEs for inclusion into a PSA model. The quantification of HFEs is comprised of 'Probability of a diagnosis failure', 'Probability of performing an unsafe

action under the diagnosis failure', and 'Probability of non-recovery', as seen in equation (1).

- Probability of an HFE = (Probability of a diagnosis failure) * (Probability of an unsafe action under the diagnosis failure) * (Probability of non-recovery) (1)

The key influencing factors and their contributions to performing unsafe actions and their recovery potential are provided. The selection of the influencing factors and assigning the appropriate values are based on an expert judgement or by referring to existing HRA methods such as the CBDTM [3].

3. Application & Results

The method has been applied to the small loss of coolant accident (SLOCA) event. The analysis of diagnosis failures and their probability are provided in Figure 1. As shown in Figure 1, the paths and causes leading to final misdiagnoses are represented with their estimated probabilities. According to the MDTA results, the SLOCA event has the potential for misdiagnosing as the excess steam demand event (ESDE) with a probability of 6.44E-03 and as the general transient event (GTRN) with a probability of 3.0E-05. In total, the diagnosis failure probability for the SLOCA event is estimated to be about 6.47E-03.

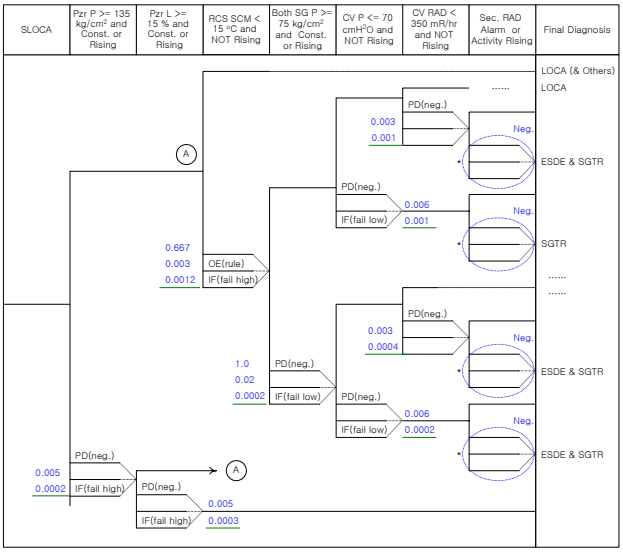

Figure 1. The MDTA result on the SLOCA event

As the probable HFEs that could be induced by the misdiagnosis of SLOCA as ESDE or GTRN, the following two HFEs are considered representatively.

- Premature termination of HPSI
- Failure to generate SIAS manually
- Failure to initiate an aggressive cooldown

The identified HFEs are quantified and modeled into a PSA event tree as seen in Figure 2. The conditional probability that the operators perform such unsafe actions under the diagnosis failure is estimated to be 2.0E-2, 2.0E-3, and 1.0, respectively. As seen in Figure 2, the total contribution of the diagnosis failures to the plant risk, i.e. core damage frequency (CDF), is calculated to be a value of '4.0E-7'. This value corresponds to a 26.5 % increase in the CDF of the SLOCA event and a 5.4 % increase in the total CDF.

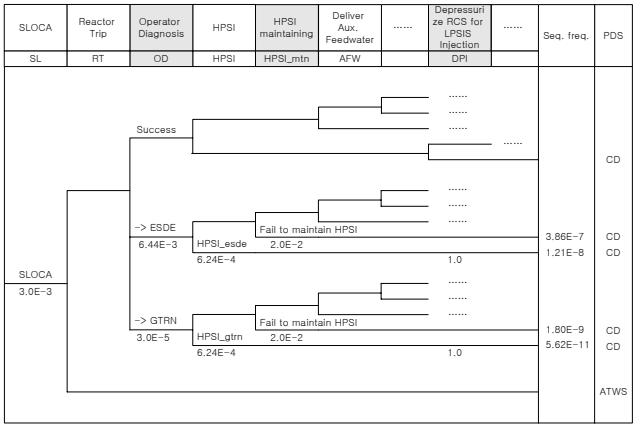

Figure 2. Incorporation of the identified HFEs into a PSA ET

4. Conclusion

This paper introduced a method for assessing the potential for diagnosis failures and their impacts on human behaviours and a plant safety. The potential for diagnosis failures is analysed by conducting the misdiagnosis tree analysis (MDTA). The MDTA framework provides an appropriate taxonomy of misdiagnosis causes and their quantification schemes. The method also provides some guidance on the identification of the unsafe actions that might occur from the misdiagnoses, and on a rough quantification scheme for their assessment and modeling into a PSA framework. According to the quantification result for a risk impact of the diagnosis failure of the SLOCA event, it seems not to be negligible.

REFERENCES

[1] J.W. Kim, W. Jung, J. Park, A Systematic Approach to Analysing Errors of Commission from Diagnosis Failure in Accident Progression, RESS, Vol. 89, pp. 137-150, 2004.
[2] J.W. Kim, W. Jung, J. Park, D. Kang, A Human Reliability Analysis Method for identifying and Assessing the Errors of Commission from a Diagnosis Failure, KAERI/TR-2901/2005.
[3] J. Grobbelaar, J. Julius, Guidelines for Performing Human Reliability Analyses, Draft Report, June 2003.