*Transactions of the Korean Nuclear Society Autumn Meeting*
*PyeongChang, Korea, October 30-31, 2008*

# Framework for Quantification of Human Errors in Testing and Maintenance

Gyunyoung Heo[1*], Jin Kyun Park[2]
[1] *Kyung Hee University, Yongin-si, Gyeonggi-do, 446-701, Korea*
[2] *Korea Atomic Energy Research Institute, Daeduckdaero, Yusong-Gu, Daejeon, 305-353, Korea*
[*] *Corresponding author: gheo@khu.ac.kr*

## 1. Introduction

Once some people believed both performance and safety could not be achieved at the same time, which means they are contradictory each other. However, it is no more surprising fact that performance and safety in Nuclear Power Plants (NPPs) forms a strongly positive correlation, which means they are complementary. Safety researches must be, therefore, effective in enhancing not only safety but also performance. Traditionally the concern of nuclear safety researches has been focused on accident scenarios or reactor conditions after an unexpected shutdown. While these focuses are effective to prevent core damage and to ultimately increase a safety margin, it does not analyze the initiating scenarios causing such an unexpected shutdown and does not deal with electric loss resulting from slight problems, which is much more common in operating power plants than the occurrence of the unexpected shutdown. It should be noted that even a slight problem can result in a serious consequence if it gets accumulated.

In 1931, H.W. Heinrich noticed that statistical evidence indicated that for every industrial accident of major proportion there were 30 accidents, and some 300 potential incidents, which is referred to as "Heinrich's Law." A more important insight of Heinrich's Law than the statistical observation is that we should investigate the seed of accidents which are very likely to overlook. This study shares the same motivation as that of Heinrich's Law. The paper proposes a framework for quantifying the human errors and estimating their consequence in testing and maintenance tasks. While the human errors in testing or maintenance can always take place, their consequence is sometimes quite allowable, but sometimes very significant. First, authors investigated the major source of human errors resulting in downtimes. Second, it will be proposed how to convert the human errors into the model quantifying their results. It is referred to as an 'interpreter.' Finally it will be delineated how to estimate the frequency of such human errors, the rate of shutdowns, or the electric loss.

## 2. Methods and Results

### *2.1 Source of Human Errors*

It is reported that a quarter of unexpected shutdowns in Korean NPPs is caused by human errors. Moreover, more than 80% of human errors are being originated from the ordinary Testing and/or Maintenance (T&M) tasks. [1] Those tasks are classified into 1) a periodic T&M which is based on a preventive approach and 2) a non-periodic T&M which is based on corrective approach. While the periodic T&Ms normally follow the regular procedures, the non-periodic T&Ms for an unforeseen failure are difficult to prepare appropriate procedures in a timely and precise manner. Both periodic and non-periodic T&M can result in electric loss, transient, or even reactor shutdown. However, it is known from field experiences that the procedures for non-periodic T&M are more vulnerable in preventing those malfunctions because of the lack of the integrity or completeness of the procedures.

Since the malfunction of a primary system is generally more sensitive to reactor shutdown than that of a secondary system, the procedures for the periodic T&M are better equipped. This means the T&M procedures belonging to a secondary system are relatively lacking while the number of non-periodic T&M in a secondary system is more frequent. It is, therefore, expected that the T&M in a secondary system is more likely to cause the malfunctions, which is the same as the fact given by statistics.

Unfortunately there have not been many concerns in investigating human errors in the T&M of, particularly, a secondary system. Even if Generation Risk Assessment (GRA) deals with productivity and profitability of NPPs on the basis of Probabilistic Safety Assessment (PSA), [2] its coverage does not reach the study's goal. In order to achieve the objective described in the introductory part, we attempted to establish the framework and the detailed methodologies effectively dealing with human errors during the T&M in a secondary system.

### *2.2 Overall Structure of Framework*

The framework for quantifying human errors taking place during the T&M in a secondary system is shown in Figure 1. The entire notion is composed of four essential components, 1) the primary human error analyzer, 2) the frequency estimator, 3) the risk estimator, and 4) the derate estimator.

#### 2.2.1 Primary Human Error Analyzer

The role of the primary human error analyzer is to connect the possible human errors in the T&M procedures with the estimators. In the human error interpreter, each line of a T&M procedure is converted into a possible error mode, for example, such as omission, wrong action, or wrong object with appropriate components in a secondary system. The

error modes are consecutively entered to each estimator so that they are able to produce relevant information such as frequency, contribution on Core Damage Frequency (CDF), or electric loss.

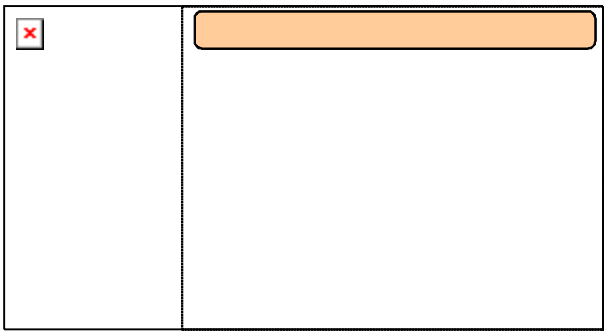

**Figure 1. Framework for quantifying human errors of T&M tasks, GRE-HRE (Generation Risk Assessment for Human Related Events)**

2.2.2 Estimators

The framework is operating three estimators. They are taking roles of quantifying human related events about primary human errors and identifying the result of a primary human error. The results of a primary human error could be a reactor/turbine trip, power cutback, or partial load derate, which is dependant on the error's nature and impact.

Frequency estimator

The major role of the frequency estimator is to quantify the possibility of a human error that has been elucidated from the primary human error analyzer. To this end, crucial sets of Performance Shaping Factors (PSFs) that can affect the occurrence of a human error are systematically considered.

Risk estimator

In case the propagation of human errors in the systems directly contributing a reactor or turbine shutdown, referred as a single point failure or vulnerability, [2] or power cutback, the risk estimator provides the changed CDF on the basis of the fault tree analysis for secondary systems and support systems. The fault tree analysis facilitates feeding the updated initiating events to a conventional PSA.

Derate estimator

The derate estimator computes the electric loss assuming the power plant is under quasi-normal operation. The estimator is developed by PEPSE [3]. This model includes all of the bare-bone systems related with electricity generation, and is connected with the support systems contributing the performance of electric generation. The support systems are shared with that of the risk estimator. The derate estimator enables to provide electric loss under a system configuration resulting from human errors.

2.2.3 Feedback

All of the results from the estimators can be characterized by the function of frequency, risk, and derate, which is ultimately related to financial measure. If there is any noticeable observation, the T&M procedure needs to be corrected or revised by remedial actions.

*2.3 Process of Developing Models*

Investigating regulatory documents and maintenance history, we are taking into account of the entire sets of secondary systems for developing the quantification models as follows:

- Main steam systems - Condenser/Condensate systems
- Circulating water - Equipment cooling water system
- Turbine support systems - Generator support systems
- Instrument air - Electric load

The fault trees in the risk estimator implement the trip logics with single point failure modes, reactor power cutback logics, and reactor or turbine trip signals. In the derate estimator, the PEPSE, commercial Rankine cycle simulation toolbox, mainly simulates thermo-hydraulic systems. The configuration of a PEPSE model can be changed by the availability of support systems, for example, such as valve arrangement or heater out-of-service. In both estimators, the availability of instrument air and electric load is given a great deal of weight.

## 3. Conclusion

This study was motivated by the need of quantifying human errors during the T&M, particularly, in a secondary system. The originality of the model can be found in 1) considering human errors in GRA, 2) developing fault trees for secondary systems, and 3) quantifying electric loss under various plant configurations. This study is still on going at Kyung Hee University and Korea Atomic Energy Research Institute, and the detailed achievements for each module in Figure 1 are going to be released.

## ACKNOWLEDGEMENT

This research was supported by "The Mid- and Long Term Nuclear R&D Program" of Ministry of Education, Science and Technology (MEST), Korea.

## REFERENCES

[1] Korea Institute of Nuclear Safety, Operational Performance Information System, http://opis.kins.re.kr
[2] Electric Power Research Institute, Inc., Generation Risk Assessment Plant Implementation Guide, TR-1008121, Palo Alto, USA, 2004.
[3] Minner G.L., et al., PEPSE and PEPSE-GT Volume 1 Manual, User Input Description, Scientech, Inc., Idaho Falls, USA, 2002.