Further Considerations Proposed for Safety Design Against to Human Error including Violations in Nuclear

Yong Hee Lee
Accident Monitoring and Mitigation Dept., Korea Atomic Energy Research Institute
898-111 Daeduk-Daero., Yuseong-Gu, Daejeon,
**Corresponding author: yhlee@kaeri.re.kr*

Keywords: human error policy, violation, accident investigation, Human Error 3.0, countermeasure

1. Introduction

The possibility of human error is added to the uncertainty of cutting-edge technology, threatening social acceptance. In the design of the system, human error should be cope with in advance, but the importance of the investigation process is emerging for finding causes and selecting appropriate measures to solve pending issues derived through post-analysis. Since system change costs are inevitably incurred in experience-based feedback, human error counter-measures through hardware and functional changes are long-termed and less realistic in practice. Therefore, most countermeasures are set in a way that adds or changes control in the interface or related job to human errors experienced. This also acts as a further burden for new education and training, but the limitations of post complementation are to be clear due to rapid changes in technology as well as time delay problems.

In this study, frequent interfaces design and supplementary features in job task procedures were reviewed as countermeasures to prevent human errors with emphasis on violations. The efficiency of existing approaches to human error were reviewed according to 3E or 5C paradigm for safety, and propose additional considerations and implementation procedures necessary for setting effective countermeasures. In particular, additional considerations during the design of human interfaces and job procedures necessary to cope with new types of human error such as control priority in automation and overriding violations, were discussed.

2. Feedback of Human Error and Countermeasures in Cases including Violations

Human error was generally treated as the cause of safety accidents *(Human Error 1.0*). However, as it was found that human error itself is not the cause of the accident but caused by external factors causing human error (*Human Error 2.0*), rapid improvement and development of external factors such as interfaces were made. On the one hand, the tendency to specify the cause in human error analysis is instinctive, and removing the cause is considered the top priority. However, considering that human error is an event with a complex interaction structure between human internal factors and external system factors, the removal of simple causes is not effective as a countermeasure.

If we want to be prepared in unexpected unprepared situations such as Fukushima accident, it might be beneficial to cope with every possibility with ultimate responsibility on human errors by applying new paradigm of *Human Error 3.0* rather than safety culture. Notion of safety culture may mislead attribution error in causal investigation on events. It is trivial, artificial, and just for convenience to conclude that safety culture is a cause of event and human error

There are 5C area and 3E priority for human error response. 5C divides the areas of control measures for coping with human error into fundamental, physical, functional, administrative, and regulatory areas (INPO 2009). 3E was introduced from the basic principles of safety management that summarized the effective priorities of safety measures in the order of enforcement, education, and engineering. Engineering measures such as design are said to be the most effective countermeasures against human error, but the burden and limitations of realization are clear. Engineering countermeasures are difficult to prioritize in the case of nuclear systems due to the long-term characteristics as a large system composed of complex correlations. Therefore, there is a high tendency to result into limited engineering measures for job procedures and task interfaces that are relatively easy to change and improve.

2.1 Safety Design of Job Tasks and Procedures

Changes in job procedures consist of additional duties or changes in allocation. This is usually done in the form of a procedure manual, and is a method of adjusting or adding the details of the job. In some cases, it can be classified into the following different levels of engineering measures.

- supplementation and addition of display
- addition and modification of information
- addition and alteration of task duties

Supplementation and addition of indications is relatively simple because it changes the design of a means that provides procedures as in the procedure manual. In the case of procedural documents, the Writer's Guide may be used. In the case of computer-

based procedures, there are additional considerations considering computerization, so interface-related human factors design standards can be used. In order to add and change information, detailed analysis and verification of information requirements necessary to prevent human error is required. This will require deriving ergonomic availability requirements related to information and interfaces.

Additional information for human error response has four different levels such as *alerts, warnings, cautions, and notifications*, so separate considerations will be needed in the content and method of the information. They can be provided in procedure itself and procedural features. Adding and changing jobs means new functions or functional changes derived to prevent human error. Additional tasks to prevent human error can be various types of tasks such as inspection, confirmation, review, and approval.

2.2 Safety Design of Human Machine Interfaces

Engineering measures to respond to human errors should achieve fundamental safety through changes in process functions, but are not realistic in the nuclear field. New design of IMT (interface management task) may be required over just adding some supplementary information. In particular, it is ideal to eliminate human error opportunities by excluding human intervention through automation, but it cannot be done frequently because it requires a lot of effort and a long time.

Instead, it may be effective to block the possibility of human error on the interface, which is the window of the job where human intervention takes place. In order to completely block human error, it is not easy because absolute judgment on human error is required. In general, design changes that inform the possibility and risk of human error and provide information and opportunities for humans to withdraw and change, or correct and supplement themselves are realistic.

2.3 Design Considerations against to Violations

The design approach to violations is very poor. This is because violations have traditionally been excluded from the scope of human error in the field of ergonomics. In addition, the issue of responsibility for violations takes precedence, so it was developed as a legal discussion. However, *Human Error 3.0*, which proposes to adopt the ultimate responsibility for safety, including violations, emphasizes the need for more active engineering design for violations. Among the engineering designs to cope with violations, considerations necessary for job procedures and interfaces are as follows.

As in human error response, information and support related to violations must be provided carefully. Information for coping with violations expected generally requires the following items of information.

- Whether it is a violation: target object, related party, viewpoint of *WHY*, etc.
- Contents of violation: rules, criteria, results, etc.
- Management of violations: responsibility, punishment, supervision, status, etc.

In addition, support is needed to deal with violations. More deliberated support over simple notice or caution alert is needed for ways to recognize or confirm violations, as well as ways to avoid violations if possible.

3. Considerations for Safety Design Against to Human Errors including Violations

Countermeasures based on human error experience are realized by changing the operating nuclear system. The contents of the direct case will be clearly changed, but the following additional considerations are needed for a more effective response.

3.1 Fundamentals for Safety Design to Human Errors

As a countermeasure against human error, the basic principle of engineering design is to minimize the possibility of human error. To this end, suitability is secured to satisfy human factors guidelines that provide various criteria for human characteristics and limitations, which mean the possibility of human error.

Designs that exceed user characteristics and limitations, such as consistency and compatibility issues, should be checked prior to workload that can ensure adequate job performance. Basically, performance and safety should not be recognized as the same or continuous dimension. Ergonomic inconsistencies will have to be managed through the entire life-cycle of the system.

To this end, the nuclear field adopts a systematic approach such as HFEPRM(NUREG-0711) by USNRC. Operational experiences such as human error cases should be managed from the first functional analysis of conceptual design until sufficiently resolved by the issue tracking system during the lifetime.

3.2 Safety Verification and Validation against to Human Error Cases

Measures for probability as well as countermeasures for direct corresponding cases and the same errors and defects are needed. Even now, measures are being taken through review of similar vulnerabilities and dissemination of human error cases. However, the risks to be addressed in human error countermeasures are not human errors themselves that occurred in the past, but all types of human errors that are likely to occur. To this end, it is necessary to actively analyze the probability of the future by introducing a new paradigm such as a new paradigm of *Human Error 3.0*.

In integrated verification, procedural documents are reviewed centering on improved facilities, but integrated verification without appropriate education and training is fatal (as seen in the B-737 Max disastrous accident case).

In addition, attention should be paid to scenarios applied to verification. In well-prepared extracted conditions, the integrated performance of all available human factors is checked by operation performance, but safety verification requires simulation of human error situations and confirmation of the level at which the possibility of human error is excluded. A wider range of human errors should be considered in the design and stress testing of accident management and coping functions highlighted after the Fukushima accident.

The progress of automation and autonomy through the introduction of AI are emerging, but verification centered on errors is needed. This is because the fundamental exclusion of the possibility of human error is not achieved, and it may result in the possibility of new errors as well as deformation and transfer of risks.

3.3 Proactive Inclusion of Violations for Safety

Design Explicit consideration of new types of human error, such as violations, is needed especially for security. Engineering measures against violations have been regarded as relatively inadequate and ineffective until now. However, engineering countermeasures against permitted violations and possible malicious violations detected through driving experiences become crucial nowadays, and human error cases should be derived and verified more actively in safety designs. Recently, discussions have been made to include insider threats, etc. from a security perspective beyond traditional safety as part of integrated safety verification.

Additionally, proactive design to vulnerability of plausible human errors including violations is demanding in automatic and autonomous features such as SMR as similar as autonomous electric cars during turn-over and overriding automations.

4. Conclusions and Discussions

It is not easy to derive effective countermeasures from human error analysis due to rapid changes in technology and the resulting uncertainties as well as sensitivity to human error. In this paper, additional considerations were presented by discussing frequent job procedures and design supplementation measures for interfaces as engineering countermeasures against human error. This will be beneficial in overcoming the limitations that simple cause identification and direct elimination are not realistic. In particular, in the case of violation-type errors, it has an important meaning in enabling human error response through engineering design in order not to put direct control such as punishment as a countermeasure. In addition, it has an important meaning in achieving the design introduction and ultimate autonomy of AI and automation, which require prior consideration of the possibility of human error. The results of this study can be considered as part of the basic policy on human error due to the introduction of new technologies and strengthening safety requirements in the field of high reliability safety such as nuclear power.

ACKNOWLEDGMENT

This paper is supported by the Nuclear Safety Research Program grant funded by Nuclear Security and Safety Commission (NSSC) and KOFONS (No. 2003010).

REFERENCES

[1] Lee, Y.H., Human Error 3.0 Concept for High Reliability Era, Proc. ESK-2015-Fall, 2015
[2] Lee, Y.H., Human Factors Engineering Approach to Safety Culture, Proc. ESK-2016 Fall, 2016
[3] Lee, Y.H., Human Error 3.0 Concept to Cope with the Organized Irresponsibility, ESK-2019 Spring, 2019
[4] Lee, Y.H., A Preliminary Review on a More-Effective and Practical Approach to Violations, ESK-2019-Fall, 2019
[5] Lee, Y.H., A Revisit to Technical Issues & Approaches for Human Error Event Investigations, ESK-2019-Fall, 2019
[6] Lee, Y.H., A Preliminary Study on the Culpability of Violation Errors in Nuclear Events and their Investigations, KNS 2020-Autumn, 2020
[7] Lee, Y.H., Discussions on the Post Human Error Activities for 21-st Century - Focused to Effective Coping with Violations, ESK-2021 Spring, 2021
[8] Lee, Y.H., A Scrutinized Step Proposed to More Effective Human Error Investigations for including Violations and their Countermeasures, KNS-2021 Spring, 2021
[9] Lee, Y. H., A Preliminary Survey on the Counter-measures to Violation Errors for the Establishment of Human Error Policy in Nuclear, ESK-2021 Fall, 2021
[10] Lee, Y.H., An Educational Approach proposed for Effectively Coping with Violation-Type Human Errors, ESK 2022 Spring, 2022 (to be presented)
[11] Lim, H. K. et al., Reanalysis of Fatal Industrial Accident Cases from the Viewpoint of Violation Type Human Errors, Korea Atomic Energy Research Institute (NSTAR-20NS41-135), 2020.
[12] Lim, H.K., et al., Development of An Objective Judgement Procedure for Determining Involvement of Violation-Type Unsafe Acts Causing Industrial Accidents, J. Korean Society of Safety vol. 39, 2021
[13] Rasmussen, J., Concept of Human Error: Is it Useful for the Design of Safety Systems? Safety Science Monitor, 3(1), 1999