Transactions of the Korean Nuclear Society Autumn Meeting
Yeosu, Korea, October 25-26, 2018

An Unsafe Acts Autodetection Process in Nuclear Power Plant Operations

Jeeyea Ahn and Seung Jun Lee
Ulsan National Institute of Science and Technology: 50 UNIST-gil, Ulju-gun, Ulsan, 44919, Republic of Korea
jeeya@unist.ac.kr
sjlee420@unist.ac.kr

1. Introduction

It has been estimated that the human errors caused by nuclear operators are contributing greatly to the probability of the nuclear accident. Therefore, the nuclear industry has been making various attempts to reduce human error. Automating nuclear plant operation can lower the probability of causing human error. Indeed, some systems of nuclear operation (i.e. ESFAS) are automated, but in an emergency, most operations are performed manually by the operators. Although human intervention into nuclear power plants creates great uncertainty in the probability of serious accidents, it is impossible to automate all operations at once. New technologies must be secured and reliable before they can be applied. Moreover, there are concerns about automation. Endsley and Kiris (1995) suggested that these problems may be related to poor operator vigilance and complacency, leading to reductions in situation awareness (SA) and manual skills [1]. Therefore, it takes considerable time and effort to verify new technologies. Therefore, we propose a system that can slightly increase the level of automation while assisting human operators.

2. Operator assistance system - CIA

CIA is an acronym for Concealed Intelligent Agent. As the name suggests, the system hides in unneeded situations and appears when necessary to assist the operator. The kinds of help may vary, but the direction to reduce the impact of human error to the utmost is to inform the operator of the mistake in case of a mistake. In addition, the system provides a basis for judging why the operation of the operator is the wrong operation and a countermeasure for the mistake, and the operator ultimately decides what action to take with the information.

Operators may be less dependent on the system because they normally operate on their own without the help of the system. Therefore, it can be free from the problem of deterioration of the driver's ability due to automation. In addition, even if the operator makes a mistake, the final decision maker will still be a human operator, since the system does not take over, but instead warns and alert the operator. If the system gives a warning about a mistake that has been made unintentionally, the operator will be aware of his mistake and will be able to respond quickly.

3. CIA's UA auto-detection framework

A UA (unsafe act) is defined as any inappropriate commission or omission of action that may adversely affect the integrity of nuclear power plants. So how can we judge whether the operator commission or omission is UA or not? In the framework presented in this paper, UA can be detected through two stages of filtering.

1) Procedural compliance
2) Critical safety functions violation

Nuclear operators carry out operations based on procedures. The plant procedures provide instructions to guide operators in monitoring decision making and controlling the plant [2]. The operating procedures are organized in the order in which the necessary actions are taken in each situation. Therefore, if the operators do not violate the procedure or do not omit the action to be taken, it can be judged that there is no UA. However, there are cases where the operator performs other operations than the procedure. In some cases, they do not operate the device in the order given in the procedure, or they take actions that are not in the procedure. This may be due to a mistake, but it may be a violation of the operator's intended procedure. Operators operate on the basis of a lot of operating experience and know-how, so they sometimes operate in violation of the procedure according to their priorities. As a result, it may be helpful to the safety of the nuclear power plant, and if warnings are given to the operator when this intended procedure violation occurs, the reliability of the system may be degraded excessively. Therefore, through another filtering step, it is necessary to judge whether any procedural violation manipulation actually affects the safety of the nuclear power plant.

3.1 Procedural Compliance

The first filtering step, which is a violation of the procedure, can be implemented as a CPN model to determine whether the actual order matches the performance of the operator. The CPN is a suitable way to implement complex processes such as the continuation of the nuclear power plant operating procedure [3]. Analyze the procedures and systemize the entry conditions and the tasks to be performed for each step. In order to implement the procedure as a CPN model, the steps must be configured based on the

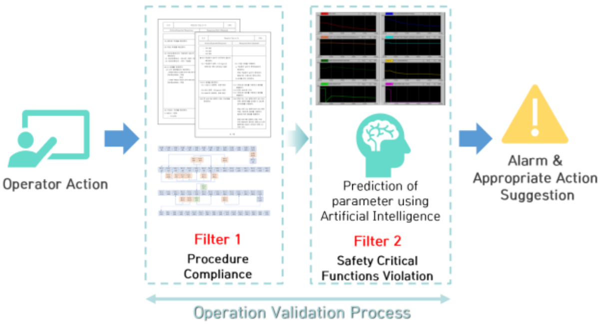

Fig. 1. The Framework of the UA auto-detection process

job to be performed. Each job is represented by a transition, and the conditions under which the job is to be performed (i.e., the procedural step and the current plant state) are represented by Place. In order for a transition to occur, several conditions of the system must be satisfied. The condition information can be denoted by Token. Each Place is classified into 4 types.

Types of place - definition

- Type A - Jump; jump to another step
  ex) Transfer to step 17
- Type B - Simple Execution; operating without condition judgment
  ex) Start the air compressor and supply I/A to the containment vessel.
- Type C - Simple Decision; Operating by simple judgment
  ex) Is the S/G level at least 6%?
- Type D - Complex Decision; Operating by complex and dynamic judgment
  ex) Determine if SI flow should be reduced.
  - Is the RCS pressure stable or increasing?

Based on the procedure, the CPN model obtains information on the variables of the plant and the operation of the operator in real time and judges whether the operator is operating according to the procedure. If a procedural violation occurs, it is filtered to determine if it is intended or a mistake.

In the case of Type A, it is a type of place that goes to another stage without any judgment or manipulation. When you reach this place, the token moves to the next place. In the case of Type B, it is a place to perform the operation without any condition. If the operator fails to perform the prescribed operation or if he/she has performed erroneously, it is determined that the procedure is in violation. In the case of Type C, it is a place to perform the operation with simple judgment. The parameters of the plant should be compared with the values given in the procedure and operation should be carried out if necessary. If a wrong action is taken or missed, it is judged to be a violation of the procedure. A simple comparison of plant variables can be implemented through simple rules. Type D is the place of performing the job by variable weight or comprehensive judgment, not simply comparing the variable values. This can be done through time series data analysis or artificial intelligence learning.

3.2 Critical Safety Functions Violations

As a second filter, the parameters related to the critical safety functions of the nuclear power plant could be the indicators. If you predict how the relevant variables will change due to any manipulation or omission of the operator and present the results, you will be able to determine if this is a real mistake when procedural violations occur. These two stages of filtering can prevent excessive degradation of the system. Predicting safety-related function-related variables can be implemented using artificial intelligence learning. If the predicted result shows a violation of the essential safety function, it can be judged that the procedural violation of the operator means UA. By presenting the judged UA to the operator together with the judge's reason, the operator can carry out the recovery measure against the UA by the final judgment. It is expected that the probability of nuclear accidents due to human errors will be reduced.

4. Conclusions

Operator supporting methods are being developed to reduce the effects of operator mistakes in nuclear plant operation. Nuclear power plant automation systems are also evaluated as contributing to lower the number of human errors. However, due to a number of issues surrounding the automation (reliability and dependability of automation), it is not possible to automate nuclear plant operations at once. In this paper, we propose a solution that is somewhat free from those automation issues. If the performance of nuclear operators is improved by utilizing the CIA system, it will be a first step to solve some of the anxiety caused by nuclear power plant automation problems. But before this system can be trusted by its operators, the CIA system's warnings and grounds for its reliance should be clear and reliable.

REFERENCES

[1] Endsley, M.R., Kiris, E.O., 1995. The out-of-the-loop performance problem and level of control in automation. Human Factors 37 (2), 381–394.

[2] *Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance*, U.S.NRC, NUREG/CR-6634

[3] S.J. Lee, P.H. Seong, Development of automated operating procedure system using fuzzy colored petri nets for nuclear power plants, Annals of Nuclear Energy 31 (2004) 849–869