Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 100 (2015) 24 – 32

Procedia Engineering

www.elsevier.com/locate/procedia

25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014

A Soft Control Model for Human Reliability Analysis in APR-1400 Advanced Control Rooms (ACRs)

Jun Su Ha*

Khalifa Univ. of Science, Technology and Research, Abu Dhabi, UAE

Abstract

Human reliability analyses play very important roles in safety analyses for NPP operations. However, scarcity of the basic human error probability data of soft control human actions has been considered as a main bottleneck for HRAs of the soft control tasks in NPPs. In this study, the soft control tasks are analyzed and modelled to be used for development of the basic human reliability data and quantification of human error probability. Sub-tasks comprising a soft control are modelled to be observable and distinguishable as unit tasks so that the basic human error probabilities for the sub-tasks could be observed and calculated in simulator-based experimental or real field operational studies. Safety-grade and non-safety grade soft controls are modelled for controls of safety and non-safety components, respectively. Possible error modes and propagation to another unintended control action, impact on soft control operation, and final error type are analyzed to provide helpful information for applications to the final human error quantification and reduction. Considerations are provided for the soft control models developed to be used in HRAs. The results of this study would be used for development of a human reliability model and basic human reliability data and quantification and reduction of human error probability during the soft control in various large-scale process control systems such as nuclear power plant (NPPs), chemical processing plants, oil processing plant, and large military systems.

Peer-review under responsibility of DAAAM International Vienna

Keywords: soft control; human error; Advanced Control Room (ACR); APR-1400

1. Introduction

A nuclear power plant (NPP) is operated by a shift of operators whose errors might lead to a catastrophic situations and hence analyses and assessments of operators' errors have been considered very important. Especially

* Corresponding author. Tel.: +971-2-501-8335; fax: +971-2-447-2442.
E-mail address: junsu.ha@kustar.ac.ae

Peer-review under responsibility of DAAAM International Vienna
doi:10.1016/j.proeng.2015.01.338

advanced digital control systems have been introduced into advanced NPPs with lots of technical advantages as digital technologies advance rapidly. Even though advanced digital technologies applied to advanced NPPs are expected to improve operators' human performance, potential human factors issues coupled with new technologies might be troublesome. One of new technologies adopted in advanced NPPs is the soft control which is mediated by software e.g., touch screens, key board, mouse, light pens, trackballs, joysticks, and so on [1]. Operators need to navigate screens of digital computer based HMIs (Human-Machine Interfaces) to find indicators or controls and manipulate the soft controls. Due to these different interfaces, different human errors should be considered and analysed. Human errors with existing hard-wired controls had been studied a lot, however few studies have been done on the soft control in advanced control rooms (ACRs) of advanced NPPs. Especially quantification of human errors during the soft control has been considered as a challenge, because scarce human reliability data such as basic human error probabilities during soft controls have been available.

The authors had developed human error mechanism models for the soft control in ACRs for analysis and enhancement of human performance during NPP operation and in addition human factors guidelines for better HMI design, training programs, and optimal strategies for task performance had been developed based on the developed human error mechanism models [2]. In this study, the soft control tasks are analyzed and modelled to be used for development of the basic human reliability data and quantification of human error probability during the soft control based on the human error mechanism models previously developed by the authors. There are safety-grade and non-safety-grade components to be controlled in NPPs and safety-grade and non-safety grade soft controls are modelled, respectively. Primary and secondary tasks in ACRs are analyzed to be modelled as sub-tasks (steps) for a soft control task. Sub-tasks comprising a soft control are modelled to be observable and distinguishable as unit tasks so that the basic human error probabilities for the sub-tasks could be observed and calculated in simulator-based experimental or real field operational studies. Possible error modes and propagation to another unintended control action, impact on soft control operation, and final error type are analyzed to provide helpful information for further applications to the human error quantification and reduction.

Nomenclature

ACR	Advanced Control Room
APR-1400	Advanced Power Reactor-1400
CVCS	Chemical Volume Control System
EOC	Error Of Commission
EOO	Error Of Omission
ESCM	ESF-CCS Soft Control Module
ESF	Engineered Safety Feature
ESF-CCS	ESF Component Control System
HMI	Human Machine Interface
INSC	Intended NSC
ISSC	Intended SSC
KINS	Korea Institute of Nuclear Safety
NPP	Nuclear Power Plant
NSC	Non-safety-grade Soft Control
RCS	Rod Control System
SIS	Safety Injection System
SSC	Safety-grade Soft Control
UNSC	Unintended NSC
USSC	Unintended SSC

2. Human error during soft control

2.1. Soft control in APR-1400 NPPs

Operators' tasks in NPPs are performed through cognitive activities such as monitoring and detection, situation assessment, response planning, and response implementation [3]. In ACRs, the response implementation is related to soft control. There are two types of operators' tasks in ACRs such as primary tasks and secondary tasks [1]. The primary tasks refer to control tasks to plant systems (e.g., opening/closing valves and starting/stopping pumps). The secondary tasks which are required to perform primary tasks; are related to the interface management (e.g., navigating screens and handling different types of input devices).

The ACR in APR-1400 has been designed with digital and computer technologies. The original standard design of APR-1400 ACR adopted the non-safety-grade universal soft controller for safety-grade and non-safety-grade system controls which had been adopted in the ACR designs of N4 reactor (France) and AP 600 (the USA). However, the safety standard of IEEE 603 [4] requires the separation of displays required for safety system control from those for non-safety system control and independence among diverse channels. Hence the KINS (Korean regulatory body) requested the designer (or developer) to change the design of soft controller according to the requirements in IEEE 603. The designer (or developer) changed the design accordingly and conducted a human factors experimental study to verify the suitability of the revised design with various performance measures. They concluded that the separation design (safety-grade vs. non-safety-grade) with confirm switches (only for safety-grade) would be most beneficial in terms of human factors [5].

Safety-grade soft controls are designed separately and independently of non-safety-grade soft controls in APR-1400 ACRs. The non-safety-grade soft controls are performed by selecting and clicking target components (non-safety-grade) on the monitoring screens using a mouse, whereas the safety-grade soft control require selecting and clicking target components (safety-grade) on the monitoring screens using a mouse and additional operations of touch screen devices on independent control panels called ESF-CCS Soft Control Module (ESCM), as shown in Fig. 1.

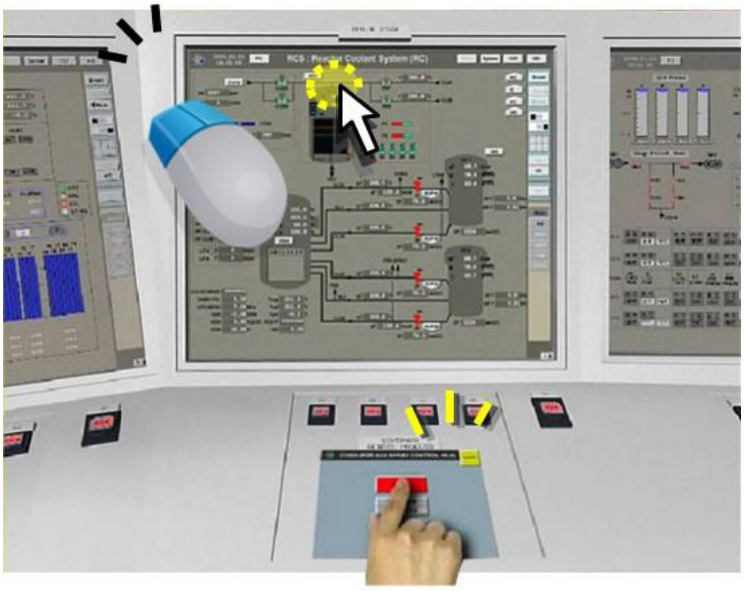

Fig. 1. Safety-grade vs. Non-safety-grade soft control.

2.2. Human error during soft control

There have been lots of human error taxonomies in literatures. One of them is the slip and mistake taxonomy which is based on consideration of intention [1]. The slip is defined as an error in implementing the intention. Thus, while one action is intended, another is accomplished. The mistake is defined as an error in intention formation and related to incorrectly assessing the situation or ineffectively planning a response.

A lot of studies have been performed on the mistake and the slip with the hard-wired control. Existing studies on the mistake can be applied to the soft control in the same way applied to the hard-wired control because intention formation has no difference between hard-wired and soft controls. However the slip error during soft controls is totally different from that during hard-wired controls. In this study, only the slip error is considered for the soft control modelling. Another widely used taxonomy of errors in NPPs considers the operator's actions that may contribute to accidents with inappropriate actions. Errors are classified into error of omission (EOO) and error of commission (EOC) [1]. The EOO refers to forgetting a task or sub-task, whereas the EOC represents doing the task incorrectly. This taxonomy is used in this study to figure out the soft control error propagation. Lee et al. (2011) analyzed the human errors modes during soft controls and classified the human errors modes into six types: operation omission (E1), wrong object (E2), wrong operation (E3), mode confusion (E4), inadequate operation (E5), and delayed operation (E6) [6].

3. Soft control modeling for human reliability analysis

3.1. Considerations for the soft control modeling

Conventionally the human error quantification are made by multiplying or integrating the basic human error probability of a target human action and evaluated weights of relevant performance shaping factors in human reliability analyses (HRAs) for hard-wired controls. Data for the basic human error probability for the hard-wired controls in NPPs have been provided in lots of the literature such as the HRA handbook in NPPs [7]. However, scarcity of the basic human error probability data of soft control human actions has been considered as a main bottleneck for HRAs of the soft control tasks in NPPs. The soft control tasks should be analyzed and modeled in a consistent and systematic manner in order to develop the basic human error probability data of soft control human actions. Data of sub-tasks of a soft control task could be observed, collected and evaluated with simulator-based experimental or real field operational studies to develop the basic human error probability data. Hence sub-tasks comprising a soft control should be modelled to be observable and distinguishable as unit tasks so that the basic human error probabilities for the sub-tasks could be observed and calculated. Another important aim of HRAs is to identify the impact of human errors and provide countermeasures for human error reduction. In order to facilitate these, possible error modes and propagation to another unintended control action, impact on soft control operation, and final error type should be included in the modeling.

3.2. Soft control task analysis and modeling

The soft control tasks in APR-1400 ACRs consist of several secondary tasks (interface control tasks) such as scanning and selecting relevant window containing a target control devise and scanning and selecting the target control device within the selected window and primary tasks (plant system control tasks) such as controlling the target control device. Especially for safety-grade soft controls primary tasks are performed on a separate and independent ESCM with additional secondary task such as pushing the confirm switch located immediately above the ESCM as shown in Fig. 1. Human errors of soft controls are basically associated with the failure of a primary task. Even though one or more of the secondary tasks failed in a soft control task, if they are recovered in a timely manner, the final primary task can be successful. A failure or failures of relevant secondary tasks lead to the failure of a primary task if recovery action (s) to the failure (s) of the secondary tasks is (are) not successful. In order to

develop the soft control model for HRAs, primary and secondary tasks in ACRs are analyzed to be categorized into observable sub-tasks for a soft control task.

3.3. Safety-grade soft control modeling

The Safety-grade Soft Controls (SSCs) are generally required during an abnormal or emergency situation in NPPs for which engineered safety feature (ESF) systems are designed to provide safety functions. ESF systems consist of various ESF components such as pumps, valves, and so on which are controlled by relevant SSCs. As modeled in Fig. 2, the SSCs are performed through a series of combination of secondary and primary tasks. Firstly the window which has the target control component which controls relevant ESF component must be scanned and selected (which are secondary tasks). A lot of sub-systems are designed in a NPP such as RCS (Rod Control System), CVCS (Chemical Volume Control System), SIS (Safety Injection System), and so on. A lot of windows for each or some of components of the sub-systems are designed on HMIs in ACRs. Operators have to select relevant windows to do required tasks. Secondly the target control component on the window must be scanned and selected for controlling the target ESF component (secondary tasks). After selecting the relevant window, the relevant control component to the ESF component to be controlled have to be found out and selected among lots of control components within the window. If the target control device is selected (clicked), attention should be paid to the ESCM located below the screen which has the control window (secondary tasks) as shown in Fig. 1. Thirdly the confirm switch should be pushed to confirm the relevant control device is selected correctly (secondary tasks). ESF systems generally have redundant trains which have the same function to increase the reliability of ESF systems. In APR-1400 they have four redundant trains for ESF systems and hence operators have to push the relevant confirm switch of train to the ESF component to be controlled. Finally the ESF component is controlled by controlling the target control component on the ESCM (primary task).

The SSC is modeled as a four-step process (see Fig. 2) in this study each step of which is modeled to be observable and distinguishable as follows:

- SSC_{I-W} : SSC sub-task of Interface control of relevant Window selection
- $\overline{SSC_{I-W}}$: Failure of SSC_{I-W}
- SSC_{I-W}^{R} : Recovery from $\overline{SSC_{I-W}}$
- SSC_{I-C} : SSC sub-task of Interface control of relevant Component selection
- $\overline{SSC_{I-C}}$: Failure of SSC_{I-C}
- SSC_{I-C}^{R} : Recovery from $\overline{SSC_{I-C}}$
- SSC_{I-S} : SSC sub-task of Interface control of pushing relevant confirm Switch
- $\overline{SSC_{I-S}}$: Failure of SSC_{I-S}
- SSC_{I-S}^{R} : Recovery from $\overline{SSC_{I-S}}$
- SSC_{P-C} : SSC sub-task of Plant system control of relevant Component on ESCM
- $\overline{SSC_{P-C}}$: Failure of SSC_{P-C}
- SSC_{P-C}^{R} : Recovery from $\overline{SSC_{P-C}}$
- ISSC : Intended SSC
- $\overline{\text{ISSC}}$: Failure of ISSC
- USSC : Unintended SSC
- UNSC : Unintended NSC
- EOC : Error of Commission
- EOO : Error of Omission

The best sequence for the success of a SSC task would be definitely the case where all the sub-tasks have been performed successfully without any failure and recovery. Even though any one or more of SSC sub-tasks fail(s), the SSC task can be successful if it is (or they are) recovered in a timely manner. The worst sequence for the success of a SSC task would be the case where all the sub-tasks have failed and recovered in an appropriate time interval. The possible error modes and propagation to another unintended control action, impact on the SSC operation, and final

error type in terms of EOO and EOC are analyzed in Table 1, which is expected to be effectively used for the human error quantification and reduction.

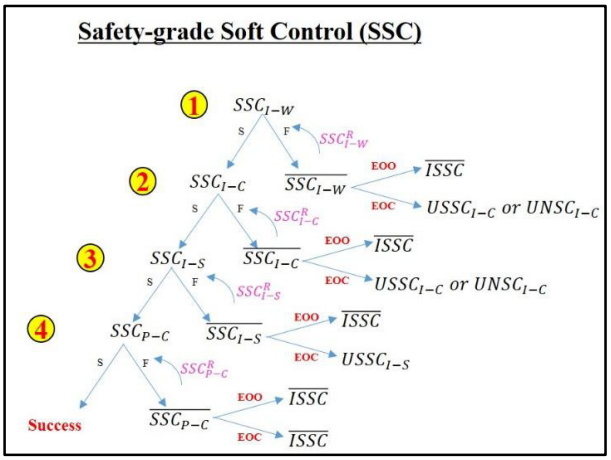

Fig. 2. Modeling of Safety-grade Soft Control (SSC).

3.4. Non-safety-grade soft control modeling

The Non-safety-grade Soft Control (NSC) is modeled in the similar way to the SSC except for the separate and independent control with the ESCM. The NSC is required in all the NPP operating modes for which operating systems but safety-related systems are designed to provide general functions for the NPP operation. As modeled in Fig. 3, the NSCs are performed through a series of combination of secondary and primary tasks. Firstly the window which has the target control component which controls a general plant component must be scanned and selected (secondary tasks). A lot of windows for each or some of components of general sub-systems are designed on HMIs in ACRs. Operators have to select relevant windows to do required tasks. Secondly the target control component on the target window must be scanned and selected for controlling the general plant component (secondary tasks). A pop-up control window is generated on the target window. Finally the general plant component is controlled by controlling the target control component on a pop-up window (primary task).

The NSC is modelled as a three-step process (see Fig. 3) each step of which is modeled to be observable and distinguishable as follows:

- NSC_{I-W} : NSC sub-task of Interface control of relevant Window selection
- $\overline{NSC_{I-W}}$: Failure of NSC_{I-W}
- NSC^{R}_{I-W} : Recovery from $\overline{NSC_{I-W}}$
- NSC_{I-C} : NSC sub-task of Interface control of relevant Component selection
- $\overline{NSC_{I-C}}$: Failure of NSC_{I-C}
- NSC^{R}_{I-C} : Recovery from $\overline{NSC_{I-C}}$
- NSC_{P-C} : NSC sub-task of Plant system control of relevant Component on pop-up window
- $\overline{NSC_{P-C}}$: Failure of NSC_{P-C}
- NSC^{R}_{P-C} : Recovery from $\overline{NSC_{P-C}}$
- INSC : Intended NSC
- $\overline{INSC}$: Failure of INSC
- USSC : Unintended SSC
- UNSC : Unintended NSC

The best sequence for the success of a NSC task would be the case where all the sub-tasks have been performed successfully without any failure and recovery. Similar to the SSC task, even though a failure happens (or some failures happen) during NSC sub-tasks, the NSC task might be successful if it is (or they are) recovered in an appropriate time interval. The worst sequence for the success of a NSC task would be the case where all the sub-tasks have been failed and recovered in an appropriate time interval. The possible error modes and propagation to another unintended control action, impact on the NSC operation, and final error type in terms of EOO and EOC are analyzed in Table 2.

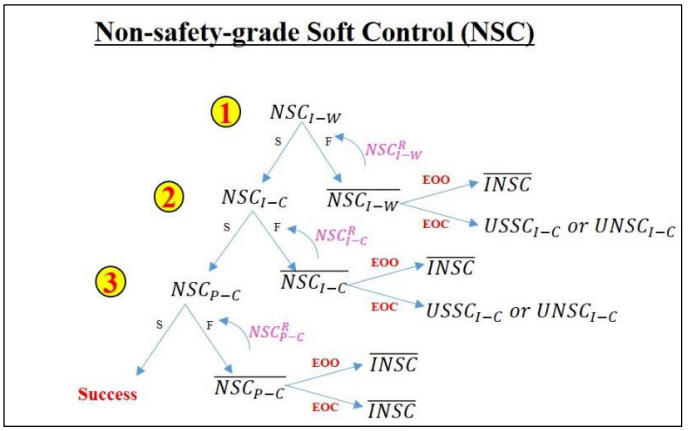

Fig. 3. Modeling of Non-safety-grade Soft Control (NSC).

Table 1. Analyses of possible error mode, propagation, impact, and type of safety-grade soft control (SSC) sub-tasks.

SSC Sub-task	Possible Error Mode	Possible Error Propagation to Another Control Action	Impact on Operation	Error Type
I-W	E1 : operation omission	No propagation	ISSC failed	EOO
	E2 : wrong window selection	E2 : wrong component operation	USSC or UNSC done	EOC
	E6 : too late operation	No propagation	ISSC delayed if recovered	EOC
I-C	E1 : operation omission	No propagation	ISSC failed	EOO
	E2 : wrong component selection	E2 : wrong component operation	USSC or UNSC done	EOC
	E6 : too late operation	No propagation	ISSC delayed if recovered	EOC
I-S	E1 : operation omission	No propagation	ISSC failed	EOO
	E2 : wrong switch selection	E2 : wrong component operation	USSC done	EOC
	E6 : too late operation	No propagation	ISSC delayed if recovered	EOC
P-C	E1 : operation omission	No propagation	ISSC failed	EOO
	E3 : wrong operation	No propagation	ISSC failed	EOC
	E5 : inadequate operation (1) too long/short (2) too much/little (3) Mistimed (4) incomplete	No propagation	ISSC failed	EOC
	E6 : too late operation	No propagation	ISSC delayed if recovered	EOC

Table 2. Analyses of possible error mode, propagation, impact, and type of non-safety-grade soft control (NSC) sub-tasks.

NSC Sub-task	Possible Error Mode	Possible Error Propagation to Another Control Action	Impact on Operation	Error Type
I-W	E1 : operation omission	No propagation	INSC failed	EOO
	E2 : wrong window selection	E2 : wrong component operation	USSC or UNSC done	EOC
	E6 : too late operation	No propagation	INSC delayed if recovered	EOC
I-C	E1 : operation omission	No propagation	INSC failed	EOO
	E2 : wrong component selection	E2 : wrong component operation	USSC or UNSC done	EOC
	E6 : too late operation	No propagation	INSC delayed if recovered	EOC
P-C	E1 : operation omission	No propagation	INSC failed	EOO
	E3 : wrong operation	No propagation	INSC failed	EOC
	E5 : inadequate operation (1) too long/short (2) too much/little (3) Mistimed (4) incomplete	No propagation	INSC failed	EOC
	E6 : too late operation	No propagation	INSC delayed if recovered	EOC

4. Considerations for use of Soft Control Models in HRAs

The soft control models are developed in this study so that they can be used for HRAs. Firstly, the models can be used to develop a human reliability model. A single soft control action can be performed successfully in a variety of ways, as can be seen in Fig.3 and 4. The success paths include the best case without any failure and recovery in the sub-tasks, the cases having several failures and recoveries in some of the sub-tasks, and the worst case with every sub-task failed and recovered. The failure paths are also included in the soft control models. Hence they can be used for the development of a reliability model of a single soft control action. Secondly, if a reliability model for a soft control action has been developed, the basic human error probability data modeled in the reliability model should be observed and evaluated in simulator-based experimental or real field operational studies. Failure data during sub-tasks of soft control tasks should be observed and recorded in a very-well controlled experimental environment and an appropriate probability distribution model for the evaluation of the basic human error probability should be selected considering assumptions that must be satisfied for the probability model to hold. During the experimental studies the assumptions coupled with the probability model should be tested and verified. Finally, the models should be used for PSFs (Performance Shaping Factors) evaluation for the final human error quantification [8]. The sub-tasks identified, possible error modes, error propagation to another control action, and impact on operation should be analyzed in a comprehensive way to evaluate weights of PSFs for the human error quantification. Operators' behavior observation and analysis techniques including eye tracking systems might be a great option for the development of basic human error probabilities [9].

5. Conclusions and further study

Scarcity of basic human error probability data of soft control human actions has been considered as a main bottleneck for HRAs of the soft control tasks in NPPs. In this study, soft control tasks in NPPs have been modeled for the HRAs considering primary and secondary tasks in ACRs. The models include the safety-grade soft control (SSC) model with a four-step process and the Non-safety-grade soft control (NSC) model with a three-step process. These steps (sub-tasks) were modeled to be observable and distinguishable so that basic human error probability

data could be observed and calculated in simulator-based experimental or real field operational studies. Possible error modes and propagation to another unintended control action, impact on soft control operation, and final error type have been analyzed to provide helpful information for further applications to the human error quantification and reduction. The results of this study are expected to be used for development of a human reliability model for a soft control task and relevant basic human error probability data and quantification of final human error probabilities with evaluation of PSFs in various large-scale process control systems such as nuclear power plant (NPPs), chemical processing plants, oil processing plant, and large military systems. As further studies a mathematical reliability model for the soft control will be studied, which will be followed by a simulator-based experimental study for collecting and evaluating basic human error probabilities of sub-tasks of the soft controls in ACRs.

Acknowledgements

This work was supported by the project of "Suitability Evaluation of Main Control Room in APR-1400 Nuclear Power Plant" under a grant from the Khalifa University Internal Research Fund (KUIRF; Fund # 210021, Program # B4011).

References

[1] W.F. Stubler, J.M. O'Hara, Soft Control: Technical Basis and Human Factors Review Guidance, NUREG/CR-6635, US Nuclear Regulatory Commission, 2000.
[2] H.S.A Aljneibi, J.S. Ha, A Study on Human Error Mechanism of Soft Control in APR-1400 Advanced Control Rooms (ACRs), 28th Enlarged Halden Project Meeting, Roros, Norway, 2014.
[3] M. Barriere, D. Bley, S. Cooper, J. Forester, A. Kolaczkowski, W. Luckas, G. Parry, A. Ramey-smith, C. Thompson, D. Whitehead, and J. Wreathall, Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), NUREG-1624, US Nuclear Regulatory Commission, 2000.
[4] IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, USA: The Institute of Electrical and Electronics Engineers, Inc.
[5] S.G. Kang, Y.G. Kim, Y.C.Shin, S.J. Jo, "Human Factors Engineering Suitability Verification of APR 1400 Soft Control and Safety Console, Proceedings of Korean Nuclear Society, Vol. 2, 2003.
[6] S.J. Lee, J.H. Kim, S.C. Jang, Human Error Mode Identification for NPP Main Control Room Operations using Soft Controls. Journal of Nuclear Science and Technology, Vol. 48, No. 6, pp. 902–910, 2011.
[7] A.D Swain, H.E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, US Nuclear Regulatory Commission, 1983.
[8] S.J. Lee, J.H. Kim, W.D. Jung, Quantitative Estimation of the Human Error Probability during Soft Control Operations. Annals of Nuclear Energy, Vol. 57, pp. 318–326, 2013.
[9] J.S.Ha, P.H. Seong, Experimental Investigation between Attentional-resource Effectiveness and Perception and Diagnosis in Nuclear Power Plants. Nuclear Engineering and Design (NED), Vol. 278, pp. 758-772, 2014.