Modeling Human Error Mechanism for Soft Control in Advanced Control Rooms (ACRs)

Hanan Salah Ali Aljneibi [a], Jun Su Ha [b*], Seongkeun Kang [b] and Poong Hyun Seong [b]
[a]*Khalifa Univ. of Science, Technology and Research, PO Box 127788, Abu Dhabi, UAE*
[b]*KAIST, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Republic of Korea*

[*]*Corresponding author: junsu.ha@kustar.ac.ae*

1. Introduction

In the main control rooms (MCRs) of nuclear power plants (NPPs), the plant operators interact with instrumentation and control (I&C) systems via the human-machine interface (HMI). Advanced Control Rooms (ACR) such as APR-1400 (Advanced Power Reactor-1400) ACR is designed to meet all regulatory requirements which include separation, independence, defense-in-depth and diverse requirements for the control and monitoring system. To achieve the switch from conventional analog-based design to digital design in ACRs, a large number of manual operating controls and switches have to be replaced by a few common multi-function devices which is called soft control system [1]. The soft controls in APR-1400 ACRs are classified into safety-grade and non-safety-grade soft controls; each was designed using different and independent input devices in ACRs. The operations using soft controls require operators to perform new tasks which were not necessary in conventional controls such as navigating computerized displays to monitor plant information and control devices [2]. These kinds of computerized displays and soft controls may make operations more convenient but they might cause new types of human error.

In this study the human error mechanism during the soft controls is studied and modeled to be used for analysis and enhancement of human performance (or human errors) during NPP operation. The developed model would contribute to a lot of applications to improve human performance (or reduce human errors), HMI designs, and operators' training program in ACRs. The developed model of human error mechanism for the soft control is based on assumptions that a human operator has certain amount of capacity in cognitive resources and if resources required by operating tasks are greater than resources invested by the operator, human error (or poor human performance) is likely to occur (especially in "slip"); good HMI (Human-machine Interface) design decreases the required resources; operator's skillfulness decreases the required resources; and high vigilance increases the invested resources.

2. Soft Controls and Human Errors

2.1 Soft Control in ACRs

Operator's actions in main control room follow sequence of activities or procedure functions that can be organized into four cognitive categories: monitoring and detection, situation assessment, response planning, and response implementation [3]. The soft controls are related to the response implementation since it becomes a tool to apply operators' control tasks. The main elements of a soft control are [4]: selecting display, handling display, configuring target devices, and controlling devices. Tasks in ACR are mainly categorized into two types: primary tasks and secondary tasks. The primary tasks refer to controls which are responsible for control inputs to plant systems (e.g., opening or closing valves and starting or stopping pumps) [5]. The secondary tasks which are required before performing primary tasks are related to the interface management.

2.2 Human Errors during Soft Control

A famous scheme divides human errors into two major categories such as mistakes and slips. This distinction is based on consideration of operator's intention [6]. The mistake is defined as an error due to the intention formation and are related to incorrectly assessing a situation or ineffectively planning a response. The slip is defined as an error in implementing the intention. Slips results from a failure in the execution of an action. Studies on both the mistake and the slip during the hard-wired control have been performed a lot. Existing studies on the mistake can be applied to soft controls in the same way applied to the hard-wired control but it is not for the slip. Hence only the slip is considered for the soft control modeling in this study. Another classification of errors considers operators' actions that may contribute to accidents with inappropriate actions. Human errors are classified into error of omission (EOO) and error of commission (EOC). The EOO refers to a failure to perform a task or action, whereas the EOC represents incorrect performance of a task or action [7]. The EOO and EOC categorization has been widely used in nuclear industries because they can be effectively used for safety analyses during abnormal and/or accidental situations in NPPs.

There is a study analyzed human errors that could occur during the soft controls in NPPs and classified the human error modes into six types such as operation omission, wrong object, wrong operation, mode

confusion, inadequate operation, and delayed operation [8], which is adopted with some modifications in this study for the modeling of human error mechanism of the soft control.

2.3 Workload, Resource Theory, and Vigilance

Workload is defined as the portion of the operator's limited capacity essentially required to perform a specific task [9]. More mental resources are required as the cognitive workload is increased. As the cognitive workload go above the limit of operator capacity, more human errors may occur and then human performance would be declined [10]. Cognitive workload theory is based on the availability of internal cognitive resources or efforts needed for cognitive activities. Resource theory is one type of cognitive model that has been used to account for task performance failures. The model suggested the existence of pools of mental resource and it is consumed by human information processing system on task performance. If demanded (or required) resources for a task is greater than supplied (or invested) resources by operator, higher workload and then human error are likely. To expand the supply of resources to a limited range, operator's vigilance should be increased. Vigilance is known as the person's ability to continue focus of attention and remain alert to target changes over periods of time. The loss of vigilance over time was reported to decrease task performance [10].

3. Modeling Soft Control Human Error Mechanism

Existing studies on the mistake can be applied to soft controls in the same way applied to the hard-wired control, because the mistake is an error type due to misjudgments by operators. The soft controls are closely related to the response implementation (or operation execution) during which the slip is mostly likely. Also the slip is directly affected by the HMI change of the control system between the hard-wired type in conventional control rooms and the soft type in ACRs. Hence only the slip is considered for the soft control modeling in this study.

The modeling of human error mechanism for the soft control includes three levels of modeling such as overall performance (highest abstract level), response implementation (intermediate level), and soft control level (lowest level) modeling.

3.1 Assumptions Used in the Modeling

It is assumed that total available mental resources of an operator are fixed. When required resources for any task are available it is expected that cognitive workload levels would be manageable and there would be acceptable task performance. On other hand, when required resources for the same task are unavailable like a situation where task demands are too high, excessive cognitive workload and then poor task performance are anticipated [10]. Hence it is assumed that:

- If resources required by a task is greater than resources invested by an operator, poor human performance (or human error) is highly likely and
- If resources required by a task is smaller than resources invested by an operator, acceptable human performance (or no human error) is highly likely.

Task performance is generally achieved as long as sufficient resources are allocated to meet task demand. Then to improve the task performance, a strategy must be adopted such as decreasing required resource or increasing invested resource [10]. Here a revised resource required by a task is defined in terms of HMI design, operating procedure, and operator training, as:

- If the HMI of an ACR is well-designed, required resources by a task is decreased,
- If the HMI of an ACR is not well-designed, required resources by a task is increased,
- If the operating procedure is well-developed, required resources by a task is decreased,
- If the operating procedure is not well-developed, required resources by a task is increased,
- If the operator is well-skilled by a well-developed training program, required resources by a task is decreased,
- If the operator is not-well-skilled by a not-well-developed training program, required resources by a task is increased.

Therefore, the revised required resources is given by:

$$\widetilde{R^R} = w_H \times w_p \times w_S \times R^R \quad (1)$$

where
$\widetilde{R^R}$ = revised resource required by a task
w_H = weighting factor for the HMI design
(if well-designed, $w_H < 1$; if not well-designed, $w_H > 1$)
w_P = weighting factor for the operating procedure
(if well-developed, $w_p < 1$; if not well-developed, $w_p > 1$)
w_S = weighting factor for the operator skillfulness
(if well-skilled, $w_s < 1$; if not well-skilled, $w_s > 1$)
R^R = original resource required by a task

When an operator faces with demanding task, the vigilance levels can be increased to provides additional resources to meet the demand [10]. A revised resource invested by an operator is defined in terms of vigilance level of the operator, as:

- If the vigilance level on a task is decreased by the operator, invested resources by the operator is decreased and
- If the vigilance level on a task is increased by the operator, invested resources by the operator is increased.

Accordingly, the revised invested resource is given by:

$$\widetilde{R^I} = w_V \times R^I \quad (2)$$

where
$\widetilde{R^I}$ = revised resource invested by the operator
w_H = weighting factor for the vigilance level
(if increased-vigilance, $w_V > 1$; if decreased-vigilance, $w_V < 1$)
R^I = original resource invested by the operator
As a result, revised invested resource is dependent on the vigilance level of the operator.

3.2 Overall Performance Level Modeling

The overall performance of NPP operation is achieved by a series of cognitive activities such as monitoring and detection (MD), situation assessment (SA), response planning (RP), and response implementation (RI) [3]. The total resource of the overall tasks is given by:

$$R_T = R_{MD} + R_{SA} + R_{RP} + R_{RI} = \sum_{i=MD}^{RI} R_i \quad (3)$$

where
R_T = the total resource of the overall tasks
R_{MD} = resources for the monitoring & detection
R_{SA} = resources for the situation assessment
R_{RP} = resources for the response planning
R_{RI} = resources for the response implementation

As explained in the previous section, if the revised resources required by the tasks are greater than revised resources invested by the operator, a human error is likely to happen. Then the revised resources invested by the operator should be increased to some extent using resource allocation between concurrently performed tasks to achieve best performance. Among this trade-off of resource allocation between the cognitive activities, attention is paid to the response implementation (RI) during which the soft controls are made.

3.3 Response Implementation Level Modeling

The implementation sequence differs for the safety-grade and the non-safety-grade soft controls (SC) such that:

- Safety-grade SC is similar to the non-safety SC but has the following seven steps including addition control actions for the ESCM (ESF-CCS Soft Control Module):
  1. Scan the screens
  2. Screen selection
  3. Scan the components
  4. Component selection
  5. Direct attention to ESCM screen
  6. Pushing the confirm switch
  7. Control the target component
- Non-safety-grade SC has the following five steps:
  1. Scan the screens
  2. Screen selection
  3. Scan the components
  4. Component selection
  5. Control the target component

The response implementation consists of a combination of safety-grade and non-safety-grade soft controls required by steps of relevant operating procedures. The resources of response implementation is given by:

$$R_{RI} = \sum_{i=1}^{m} R_{SSC_i} + \sum_{j=1}^{n} R_{NSC_j} \quad (4)$$

where
R_{RI} = the resource of the response implementation
R_{SSC_i} = resources for the safety-grade SC of i-task
R_{NSC_i} = resources for the non-safety-grade SC of j-task
m = total number of the safety-grade SC
n = total number of the non-safety-grade SC

A human error is likely to happen, if the revised resources required by the tasks are greater than revised resources invested by the operator.

3.4 Soft Control Level Modeling

The existing human error modes of six types such as operation omission, wrong object, wrong operation, mode confusion, inadequate operation, and delayed operation are adopted with some modification in this study for the modeling of human error mechanism of the soft control level [8]. The case where an operator cannot find a relevant window or component during navigation is added. Inadequate operation is redefined as mistimed operation to include the task timing issue, as shown Table I.

Table I: Revised human error modes for the soft control [8]

Human error modes	Description	Cases
E1	Operation omission	● Omission of a step or instruction in a procedure ● Operator cannot find the relevant monitor or component.
E2	Wrong window or component	● Intended operation on wrong window or component ● Wrong operation on wrong window or component
E3	Wrong operation	● Wrong operation on right component ● Operation in wrong direction
E4	Mode confusion	● Intended operation on wrong mode ● Wrong operation on wrong mode
E5	Mistimed operation	● Errors due to task timing that within the required time for a task, the operation occur earlier or later than it supposed to be
E6	Delayed operation	● Too late operation

The revised human error modes are applied to the safety and non-safety soft control respectively. The safety-grade soft control (SSC) operates safety-related

components such as components in the Engineered Safety Feature (ESF) systems which provide various safety functions, when an abnormal situation occurs in an NPP. The non-safety-grade soft control (NSC) operates non-safety-related components in NPPs.

Modelling of safety-grade soft control (SSC): A single task of the safety-grade soft control (SSC) consists of seven steps such as scanning screens, selecting relevant screen, scanning components, selecting relevant component, directing attention to the ESCM screen, pushing the confirm switch coupled with the ESCM, and finally controlling the target component. If a slip is made by an operator during NPP operation in one of the seven steps for the SSC, it may propagate to other error. Hence the subtasks corresponding to the seven steps, task type, possible error modes, possible error propagation, impact on operation, and error type in terms of EOC and EOO taxonomy are analyzed to be modeled for the human error mechanism of the soft controls, as shown in Table II. The first subtask for a SSC is "scan for relevant window" which is an interface (I) control to find out relevant window (W) among a lot of windows for NPP operation in ACRs and it is abbreviated to I-W. Hence the task type of this subtask is the secondary (S) task. There are two possible error modes for this subtask, the window omission (E1) or the delayed operation (E6) which are defined in the Table I. The error of the window omission in this subtask refers to the situation where an operator cannot find the target window. It might propagate to another errors of the wrong window selection which may have impact on the SSC operation such that the intended SSC (ISSC) fails and an unintended SSC (USSC) might be executed if a wrong component is executed in the wrong window, which can be considered as an EOC. The delayed operation means too late operation and might propagate to the window omission which is an omission of this subtask. This leads to the ISSC failed and eventually an EOO. The second subtask is "select window" which is an interface (I) control to select (S) relevant window (W) among a lot of windows and it is abbreviated to I-SW and a secondary (S) task. Two possible error modes include the wrong window selection (E2) and the delayed operation (E6). The error of the wrong window selection might propagate to a wrong component selection and have the impact on the SSC operation such that the ISSC fails and an USSC might be executed if a wrong component is executed in the wrong window, which can be considered as an EOC.

Table II: Analysis of possible error propagation due to a slip during safety-grade soft controls (SSCs)

	[*]SSC Sub-Task		[+]Task type	Possible Error Mode	Possible Error Propagation	[**]Impact on Operation	[++]Error Type
1	Scan for relevant window	I-W	S	E1: window omission	E2: wrong window selection	ISSC fail & USSC	EOC
					E6: delayed operation	ISSC fail	EOO
				E6: delayed operation	E1: window omission	ISSC fail	EOO
2	Select window	I-SW	S	E2: wrong window selection	E2: wrong component selection	ISSC fail & USSC	EOC
				E6: delayed operation	E1: window omission	ISSC fail	EOO
3	Scan for relevant component	I-C	S	E1: component omission	E2: wrong component selection	ISSC fail & USSC	EOC
					E6: delayed operation	ISSC fail	EOO
				E6: delayed operation	E1: component omission	ISSC fail	EOO
4	Select component	I-SC	S	E2: wrong component selection	E3:wrong operation	ISSC fail & USSC	EOC
				E6: delayed operation	E1: component omission	ISSC fail	EOO
5	Direct attention to ESCM	I-O	S	E1: operation omission	E6: delayed operation	ISSC fail	EOO
				E6: delayed operation	E1: operation omission	ISSC fail	EOO
6	Approve confirm switch	I-V	S	E2: wrong switch selection	E3: wrong operation	ISSC fail & USSC	EOC
				E6: delayed operation	E1: operation omission	ISSC fail	EOO
7	Execute action	P-E	P	E1: operation omission	E6: delayed operation	ISSC fail	EOO
				E3: wrong operation	E3: wrong operation	ISSC fail & USSC	EOC
				E5: mistimed operation	E3: wrong operation	ISSC fail & USSC	EOC
				E6: delayed operation	E1: operation omission	ISSC fail	EOO

[*]I-W: Interface-Window; I-SW: Interface-Select Window; I-C: Interface-Component; I-SC: Interface-Select Component; I-O: Interface-co-Ordinate; I-V: Interface-Verification; P-E: Plant system-Execute
[+]S: Secondary; P: Primary
[**]ISSC: Intended SSC; USSC: Unintended SSC
[++]EOC: Error of Commission; EOO: Error of Omission

The other possible error mode of the delayed operation might propagate to a window omission and lead to the ISSC failed and eventually an EOO. The third subtask is "scan for relevant component", an interface (I) control to find out relevant component (C) among components on the target window. It is abbreviated to I-C and a secondary (S) task. The component omission (E1) and the delayed operation (E6) are possible error modes. The component omission refers to the situation where an operator cannot find the target component. It might propagate to a wrong component selection and have the ISSC failed and an USSC executed if the wrong component is executed, which leads to an EOC. The delayed operation might propagate to a component omission and lead to the ISSC failed and an EOO. The fourth subtask of "select component" which is an interface (I) control to select (S) relevant component (C) among components on the target window is abbreviated to I-SC and a secondary (S) task. The wrong component selection (E2) and the delayed operation (E6) are possible error modes. The error of the wrong component selection might propagate to a wrong operation and have the ISSC failed and an USSC executed if the wrong operation is executed with the wrong component selected, which is an EOC. The other possible error mode of the delayed operation might propagate to a component omission and lead to the ISSC failed and eventually an EOO. The fifth subtask is "direct attention to ESCM" which is an interface (I) control to co-Ordinate (O) the operator's attention to relevant ESCM. It is abbreviated to I-O and a secondary (S) task. The ESCM is a dedicated soft control module for the Engineered Safety Features Component Control Systems (ESF-CCSs) which provide safety functions during abnormal situation in NPPs. The ESF-CCS has multi-redundant trains such as four trains or two trains to ensure safety functions during an abnormal situations. For example the HMI of an ESCM in the ACR of APR-1400 which has four redundant trains is shown in Fig. 1.

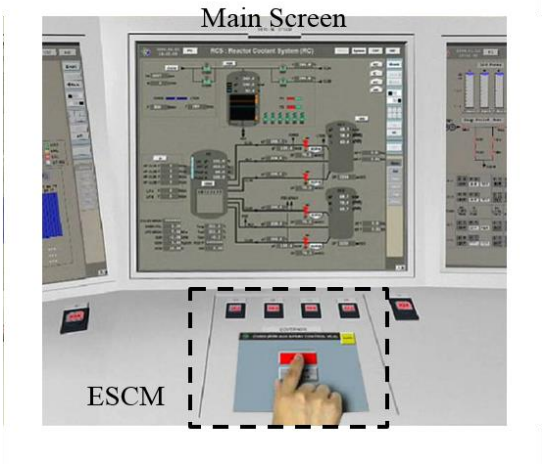

Fig. 1. The HMI design of the main screen and the ESCM in ACR of APR-1400.

It consists of one dedicated screen located below the main screen and four confirm switches corresponding to the four redundant trains as shown in Fig. 1. If an operator wants to operate a train-A ESF component out of four (A, B, C, and D) trains, the operator must select the train-A component on the main screen, shift his or her attention to the confirm switch corresponding to the train-A component out of the four confirm switches, and push (confirm) the train-A confirm switch to finally operate the train-A component on the dedicated screen. Possible error modes include the operation omission (E1) and the delayed operation (E6). The operation omission might propagate to a delayed operation and have the ISSC failed which is an EOO. The other delayed operation might propagate to an operation omission and lead to the ISSC failed and an EOO as well. The sixth subtask of "approve confirm switch" which is an interface (I) control to verify (V) the relevant train on the ESCM. It is abbreviated to I-V and a secondary (S) task. There are two possible error modes of the wrong switch selection (E2) and the delayed operation (E6). The wrong switch selection might propagate to a wrong operation and have the ISSC failed and an USSC executed if a wrong switch is pushed, which is an EOC. The other delayed operation might propagate to an operation omission and lead to the ISSC failed and an EOO as well.

The final seventh subtask of "execute action" which is a plant (P) system control to execute (E) the relevant component is abbreviated to P-E and hence it is a primary (P) task. There are four possible error modes of the operation omission (E1), the wrong operation (E3), the mistimed operation (E5), and the delayed operation (E6). The operation omission might propagate to a delayed operation and have the ISSC failed and eventually an EOO. The wrong operation and the mistimed operation might propagate to an wrong operations and have the ISSC failed and an USSC executed, if an wrong action or an ill-timed action is made, which is an EOC. The other delayed operation might propagate to an operation omission and lead to the ISSC failed and an EOO. All these analyses of the possible error propagations due to a slip during an SSC are incorporated in the success-fail tree of an SSC, as shown in Fig. 2. Each subtask has two states of success or fail in the success-fail tree. A recovery process will be held until a success trail is accomplished in each fail case. However if a recovery fails during one of the subtasks, an EOC or an EOO might be made through the error propagation analyzed in Table II. The best scenario for the success of an SSC is made given that all the subtasks are successful, whereas the worst scenario for the success of an SSC is made when all the subtasks are failed and recovered sequentially. All the success cases are modeled in terms of the resources required for tasks, as follows:

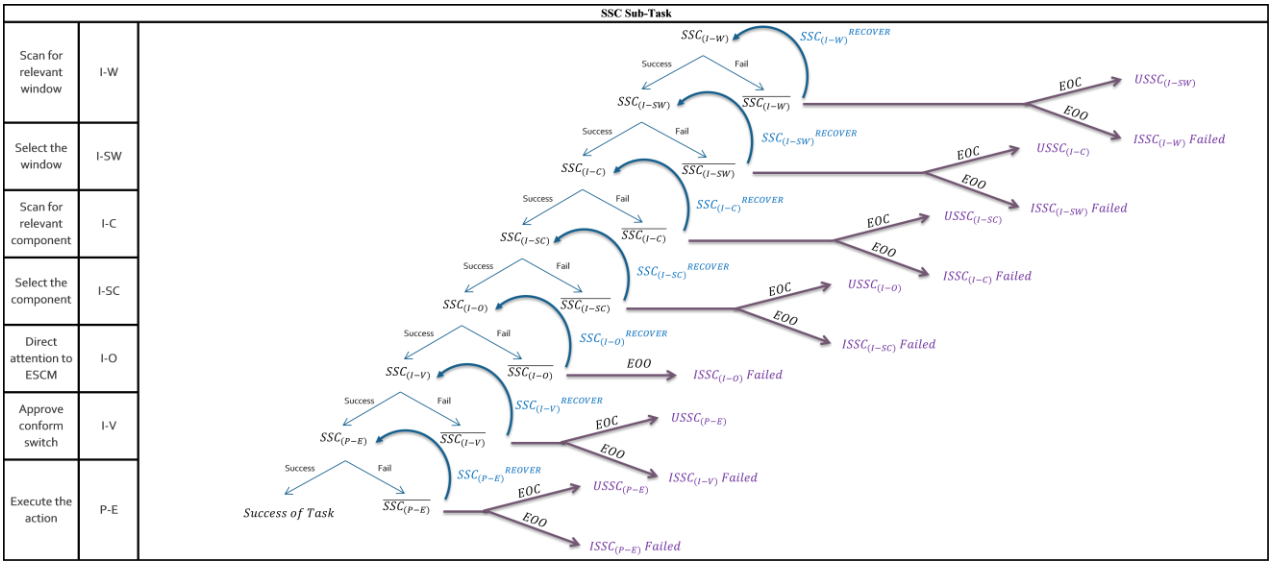

Fig. 2. Success-fail tree for safety-grade soft controls (SSCs).

Case 1: Success in seven subtasks (the best case):

$$R^R_{SSC} = R^R_{SSC_{(I-W)}} + R^R_{SSC_{(I-SW)}} + R^R_{SSC_{(I-C)}} + R^R_{SSC_{(I-SC)}} + R^R_{SSC_{(I-O)}} + R^R_{SSC_{(I-V)}} + R^R_{SSC_{(P-E)}} \quad (5)$$

where
R^R_{SSC}= required resource for an SSC,
$R^R_{SSC_{(I-W)}}$= required resource for I-W of an SSC,
$R^R_{SSC_{(I-SW)}}$= required resource for I-SW of an SSC,
$R^R_{SSC_{(I-C)}}$= required resource for I-C of an SSC,
$R^R_{SSC_{(I-SC)}}$= required resource for I-SC of an SSC,
$R^R_{SSC_{(I-O)}}$= required resource for I-O of an SSC,
$R^R_{SSC_{(I-V)}}$= required resource for I-V of an SSC,
$R^R_{SSC_{(P-E)}}$= required resource for P-E of an SSC.

Case 2: Success in six subtasks and fail and recovery in one subtask:

$$R^R_{SSC} = \sum_i R^R_{SSC_i} + R^R_{\overline{SSC_i}} + R^R_{SSC_i^{RECOVER}} \quad (6)$$

where *i = (I-W), (I-SW), (I-C), (I-SC), (I-O), (I-V), or (P-E),*
$R^R_{\overline{SSC_i}}$= required resource for the fail of *SSCi*,
$R^R_{SSC_i^{RECOVER}}$= required resource for the recovery of *SSCi*.

Case 3: Success in five subtasks and fail and recovery in two subtasks:

$$R^R_{SSC} = \sum_i R^R_{SSC_i} + R^R_{\overline{SSC_i}} + R^R_{\overline{SSC_j}} + R^R_{SSC_i^{RECOVER}} + R^R_{SSC_j^{RECOVER}} \quad (7)$$

where, *i or j =(I-W), (I-SW), (I-C), (I-SC), (I-O), (I-V), or (P-E) and i≠j.*

Case 4: Success in four subtasks and fail and recovery in three subtasks:

$$R^R_{SSC} = \sum_i R^R_{SSC_i} + R^R_{\overline{SSC_i}} + R^R_{\overline{SSC_j}} + R^R_{\overline{SSC_k}} + R^R_{SSC_i^{RECOVER}} + R^R_{SSC_j^{RECOVER}} + R^R_{SSC_k^{RECOVER}} \quad (8)$$

where *i, j,* or *k* =*(I-W)*, *(I-SW)*, *(I-C)*, *(I-SC)*, *(I-O)*, *(I-V)*, or *(P-E)* and *i≠j≠k.*

Case 5: Success in three subtasks and fail and recovery in four subtasks:

$$R^R_{SSC} = \sum_i R^R_{SSC_i} + R^R_{\overline{SSC_i}} + R^R_{\overline{SSC_j}} + R^R_{\overline{SSC_k}} + R^R_{\overline{SSC_l}} + R^R_{SSC_i^{RECOVER}} + R^R_{SSC_j^{RECOVER}} + R^R_{SSC_k^{RECOVER}} + R^R_{SSC_l^{RECOVER}} \quad (9)$$

where, *i, j, k,* or *l*=*(I-W)*, *(I-SW)*, *(I-C)*, *(I-SC)*, *(I-O)*, *(I-V)*, or *(P-E)* and *i≠j≠k≠l.*

Case 6: Success in two subtasks and fail and recovery in five subtasks:

$$R^R_{SSC} = \sum_i R^R_{SSC_i} + R^R_{\overline{SSC_i}} + R^R_{\overline{SSC_j}} + R^R_{\overline{SSC_k}} + R^R_{\overline{SSC_l}} + R^R_{\overline{SSC_m}} + R^R_{SSC_i^{RECOVER}} + R^R_{SSC_j^{RECOVER}} + R^R_{SSC_k^{RECOVER}} + R^R_{SSC_l^{RECOVER}} + R^R_{SSC_m^{RECOVER}} \quad (10)$$

where, *i, j, k, l,* or *m*=*(I-W)*, *(I-SW)*, *(I-C)*, *(I-SC)*, *(I-O)*, *(I-V)*, or *(P-E)* and *i≠j≠k≠l≠m.*

Table III: Analysis of possible error propagation due to a slip during non-safety-grade soft controls (NSCs)

*NSC Sub-Task			+Task type	Possible Error Mode	Possible Error Propagation	**Impact on Operation	++Error Type
1	Scan for relevant window	I-W	S	E1: window omission	E2: wrong window selection	INSC fail & UNSC	EOC
					E6: delayed operation	INSC fail	EOO
				E6: delayed operation	E1: window omission	INSC fail	EOO
2	Select window	I-SW	S	E2: wrong window selection	E2: wrong component selection	INSC fail & UNSC	EOC
				E6: delayed operation	E1: window omission	INSC fail	EOO
3	Scan for relevant component	I-C	S	E1: component omission	E2: wrong component selection	INSC fail & UNSC	EOC
					E6: delayed operation	INSC fail	EOO
				E6: delayed operation	E1: component omission	INSC fail	EOO
4	Select component	I-SC	S	E2: wrong component selection	E3:wrong operation	INSC fail & UNSC	EOC
				E6: delayed operation	E1: component omission	INSC fail	EOO
5	Execute action	P-E	P	E1: operation omission	E6: delayed operation	INSC fail	EOO
				E3: wrong operation	E3: wrong operation	INSC fail & UNSC	EOC
				E5: mistimed operation	E3: wrong operation	INSC fail & UNSC	EOC
				E6: delayed operation	E1: operation omission	INSC fail	EOO

*I-W: Interface-Window; I-SW: Interface-Select Window; I-C: Interface-Component; I-SC: Interface-Select Component; P-E: Plant system-Execute
+S: Secondary; P: Primary
**INSC: Intended NSC; UNSC: Unintended NSC
++EOC: Error of Commission; EOO: Error of Omission

Case 7: Success in one subtasks and fail and recovery in six subtasks:

$$R_{SSC}^{R} = \sum_{i} R_{SSC_i}^{R} + R_{\overline{SSC_i}}^{R} + R_{\overline{SSC_j}}^{R} + R_{\overline{SSC_k}}^{R} + R_{\overline{SSC_l}}^{R} + R_{\overline{SSC_m}}^{R} + R_{\overline{SSC_n}}^{R} + R_{SSC_i}^{R^{RECOVER}} + R_{SSC_j}^{R^{RECOVER}} + R_{SSC_k}^{R^{RECOVER}} + R_{SSC_l}^{R^{RECOVER}} + R_{SSC_m}^{R^{RECOVER}} + R_{SSC_n}^{R^{RECOVER}} \quad (11)$$

where, *i*, *j*, *k*, *l*, *m* or *n*=(*I-W*), (*I-SW*), (*I-C*), (*I-SC*), (*I-O*), (*I-V*), or (*P-E*).

Case 8: Success in one subtasks and fail and recovery in six subtasks:

$$R_{SSC}^{R} = \sum_{i} R_{\overline{SSC_i}}^{R} + \sum_{i} R_{SSC_i}^{R^{RECOVER}} + \sum_{i} R_{SSC_i}^{R} \quad (12)$$

where, *i* = (*I-W*), (*I-SW*), (*I-C*), (*I-SC*), (*I-O*), (*I-V*), or (*P-E*).

<u>Modelling of non-safety-grade soft control (NSC)</u>: The non-safety-grade soft control (NSC) consists of five steps such as scanning screens, selecting relevant screen, scanning components, selecting relevant component, and controlling the target component. However directing attention to the ESCM screen and pushing the confirm switch coupled with the ESCM which are included in an SSC are not parts of an NSC. Similar to the SSC analysis, the subtasks corresponding to the five steps, task type, possible error modes, possible error propagation, impact on operation, and error type in terms of EOC and EOO taxonomy are analyzed and modeled in Table III and Fig. 3. Similar to the SSC modeling, all the success cases are modeled in terms of the resources required for tasks, as follows:

Case 1: Success in five subtasks (the best case):

$$R_{NSC}^{R} = R_{NSC_{(I-W)}}^{R} + R_{NSC_{(I-SW)}}^{R} + R_{NSC_{(I-C)}}^{R} + R_{NSC_{(I-SC)}}^{R} + R_{SSC_{(P-E)}}^{R} \quad (13)$$

where
R_{NSC}^{R} = required resource for an NSC,
$R_{NSC_{(I-W)}}^{R}$ = required resource for *I-W* of an NSC,
$R_{NSC_{(I-SW)}}^{R}$ = required resource for *I-SW* of an NSC,
$R_{NSC_{(I-C)}}^{R}$ = required resource for *I-C* of an NSC,
$R_{NSC_{(I-SC)}}^{R}$ = required resource for *I-SC* of an NSC,
$R_{NSC_{(P-E)}}^{R}$ = required resource for *P-E* of an NSC.

Case 2: Success in four subtasks and fail and recovery in one subtask:

$$R_{NSC}^{R} = \sum_{i} R_{NSC_i}^{R} + R_{\overline{NSC_i}}^{R} + R_{NSC_i}^{R^{RECOVER}} \quad (14)$$

where *i* = (*I-W*), (*I-SW*), (*I-C*), (*I-SC*), or (*P-E*)
$R_{\overline{NSC_i}}^{R}$ = required resource for the fail of NSC_i
$R_{NSC_i}^{R^{RECOVER}}$ = required resource for the recovery of NSC_i.

Case 3: Success in three subtasks and fail and recovery in two subtasks:

$$R_{NSC}^{R} = \sum_{i} R_{NSC_i}^{R} + R_{\overline{NSC_i}}^{R} + R_{\overline{NSC_j}}^{R} + R_{NSC_i}^{R^{RECOVER}} + R_{NSC_j}^{R^{RECOVER}} \quad (15)$$

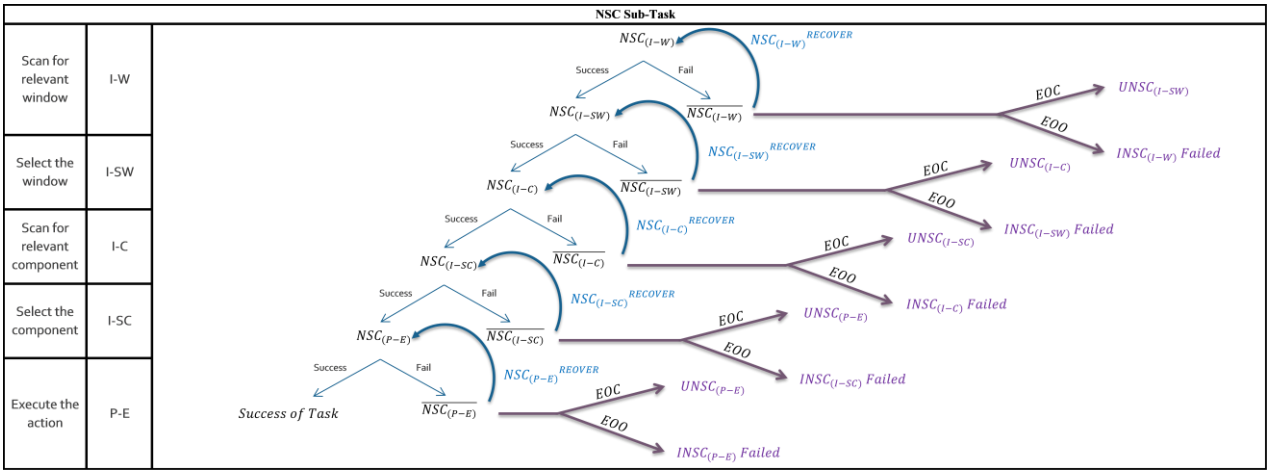

Fig. 3. Success-fail tree for non-safety-grade soft controls (NSCs).

where, *i* or *j* =(*I-W*), (*I-SW*), (*I-C*), (*I-SC*), or (*P-E*) and $i \neq j$

Case 4: Success in two subtasks and fail and recovery in three subtasks:

$$R_{NSC}^{R} = \sum_{i} R_{NSC_i}^{R} + R_{\overline{NSC_i}}^{R} + R_{\overline{NSC_j}}^{R} + R_{\overline{NSC_k}}^{R} + R_{NSC_i}^{R^{RECOVER}} + R_{NSC_j}^{R^{RECOVER}} + R_{NSC_k}^{R^{RECOVER}} \quad (16)$$

where *i*, *j*, or *k* =(*I-W*), (*I-SW*), (*I-C*), (*I-SC*), or (*P-E*) and $i \neq j \neq k$

Case 5: Success in one subtasks and fail and recovery in four subtasks:

$$R_{NSC}^{R} = \sum_{i} R_{NSC_i}^{R} + R_{\overline{NSC_i}}^{R} + R_{\overline{NSC_j}}^{R} + R_{\overline{NSC_k}}^{R} + R_{\overline{NSC_l}}^{R} + R_{NSC_i}^{R^{RECOVER}} + R_{NSC_j}^{R^{RECOVER}} + R_{NSC_k}^{R^{RECOVER}} + R_{NSC_l}^{R^{RECOVER}} \quad (17)$$

where, *i*, *j*, *k*, or *l*=(*I-W*), (*I-SW*), (*I-C*), (*I-SC*), or (*P-E*) and $i \neq j \neq k \neq l$

Case 6: Fail and recovery in all the five subtasks (the worst case):

$$R_{NSC}^{R} = \sum_{i} R_{\overline{NSC_i}}^{R} + \sum_{i} R_{NSC_i}^{R^{RECOVER}} + \sum_{i} R_{NSC_i}^{R} \quad (18)$$

where, *i* = (*I-W*), (*I-SW*), (*I-C*), (*I-SC*), or (*P-E*)

4. Conclusions and Further Study

In this study the human error mechanism during the soft controls is studied and modeled to be used for analysis and enhancement of human performance (or reduction of human errors) during NPP operation. The models for the soft controls are developed based on a human performance model in NPPs, human error studies, and cognitive workload, resource, and vigilance theories which are well supported by existing human factors studies. The developed model for the soft controls are expected to be effectively used for analyses of human error (or human performance) during the soft controls and improvement of human performance (or reduction of human error) in terms of HMI design, procedure development, and operator training program. However experimental studies should be conducted to conclude the validity of every details modeled in this study, which is left as a further study.

REFERENCES

[1] Kim WW, Lee JW, Park KS. APR1400 Soft Control System Design and Implementation. KEPCO E&C. 2013.
[2] Lee SJ and Jung W. Issues in Soft Control Operations in Advanced Main Control Rooms. Korea Atomic Energy Research Institute, Paper No. KA094. 2013.
[3] Barriere M, Bley D, Cooper S, Forester J, Kolaczkowski A, Luckas W, Parry G, Ramey-smith A, Thompson C, Whitehead D, Wreathall J. Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA). Rev.01, NUREG-1624, US NRC. 2000.
[4] International Atomic Energy Agency. Integration of Analog and Digital Instrumentation and Control Systems in Hybrid Control Rooms, IAEA NUCLEAR ENERGY SERIES No. NP-T-3.10. Vienna: IAEA Library Cataloguing in Publication Data. 2010.
[5] Lee SJ and Jung W. Task Analysis of Soft Control Operations Using Simulation Data in Nuclear Power Plants. In Lee SJ and Jung W. Human Interface and the Management of Information. Information and Interaction for Health, Safety, Mobility and Complex Environments. Las Vegas, NV, USA: Springer Berlin Heidelberg. 2013.
[6] Stubler WF, O'Hara JM, Kramer J, Higgins JC. Soft Controls: Technical Basis and Human Factors Review Guidance. NUREG/CR-6635. U.S.A.: Brookhaven National Laboratory. 2000.
[7] Swain AD and Guttmann HE, Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Application. NUREG/CR-1278, US N.R.C. (2-16, J-11). 1983.
[8] Lee SJ, Kim J, JANG SC. Human Error Mode Identification for NPP Main Control Room Operations using

Soft Controls. Journal of Nuclear Science and Technology. 2011: 48(6): 902–910.
[9] O'Donnell RD and Eggemeier FT. Workload assessment methodology. In Boff KR, Kaufman L, and Thomas J. (Eds.). Handbook of Perception and Human Performance: Vol. II. Cognitive Processes and Performance, John Wiley & Sons. 1986.
[10] Embrey D, Blackett C, Marsden P, Peachey J. Development of a Human Cognitive Workload Assessment Tool. Crown. 2006.