energies

MDPI

Article

An Approach to Analyze Diagnosis Errors in Advanced Main Control Room Operations Using the Cause-Based Decision Tree Method

Awwal Mohammed Arigi, Gayoung Park and Jonghyun Kim *

Department of Nuclear Engineering, Chosun University, Gwangju 61452, Korea; awwal.arigi@chosun.ac.kr (A.M.A.); gayoungpark@chosun.kr (G.P.)
* Correspondence: jonghyun.kim@chosun.ac.kr

Abstract: Advancements in the nuclear industry have led to the development of fully digitized main control rooms (MCRs)—often termed advanced MCRs—for newly built nuclear power plants (NPPs). Diagnosis is a major part of the cognitive activity in NPP MCRs. Advanced MCRs are expected to improve the working environment and reduce human error, especially during the diagnosis of unexpected scenarios. However, with the introduction of new types of tasks and errors by digital MCRs, a new method to analyze the diagnosis errors in these new types of MCRs is required. Task analysis for operator diagnosis in an advanced MCR based on emergency operation was performed to determine the error modes. The cause-based decision tree (CBDT) method—originally developed for analog control rooms—was then revised to a modified CBDT (MCBDT) based on the error mode categorizations. This work examines the possible adoption of the MCBDT method for the evaluation of diagnosis errors in advanced MCRs. We have also provided examples of the application of the proposed method to some common human failure events in emergency operations. The results show that with some modifications of the CBDT method, the human reliability in advanced MCRs can be reasonably estimated.

Keywords: advanced MCR; human failure event; CBDT; human reliability; diagnosis; control room

Citation: Arigi, A.M.; Park, G.; Kim, J. An Approach to Analyze Diagnosis Errors in Advanced Main Control Room Operations Using the Cause-Based Decision Tree Method. *Energies* **2021**, *14*, 3832. https://doi.org/10.3390/en14133832

Academic Editor: Valerio Lo Brano

Received: 21 May 2021
Accepted: 22 June 2021
Published: 25 June 2021

1. Introduction

Digitalized control stations for critical infrastructure have been employed in numerous industries for over two decades; however, not surprisingly, the use of fully digitalized main control rooms in nuclear systems only began within the last decade. This is because the nuclear industry employs one of the highest safety standards, especially in nuclear power plant (NPP) operations, and is not readily receptive to new technologies. However, the use of digitalized main control rooms (MCRs) has become a standard in the construction of newly built NPPs. In fact, one of the main differences between the newly built NPPs and the conventional plants that have been in operation for several years is the design of the MCR [1]—newly built NPPs use fully digitalized MCRs, which is also called "advanced MCRs," while conventional plants use analog or semi-digitized MCRs. Some notable types of MCRs include the advanced power reactor-1400 (APR1400) in Korea [2], the Westinghouse AP1000 in the USA [3], and the European Pressurized water Reactor-1600 (EPR-1600) in France [4].

Recent progress in technology has led to most of the changes within advanced MCRs. Particularly, with the improvements in the capabilities of modern computers in terms of processing and presenting information, computer techniques have been introduced into the design of NPP MCRs [5]. Because these advanced MCRs often have modern human–system interfaces (HSIs), the performance of the operators would be affected. In contrast to local operators, NPP operators typically work within the confines of the MCR. Several opinions have been expressed on whether these effects of modern HSI improve or challenge operator

performance. For example, modern HSI has been suggested to improve crew performance and reduce workload [6]. In contrast, some authors [7] have assumed that modern HSIs have negative effects, such as declined primary task performance, due to attention shift to interface management and sub-optimal use of the HSI in high-workload situations due to their reduced capacity to focus on interface management tasks. An empirical study [8] suggested that problems also exist in finding the relevant information on screens, and other team members do not have adequate awareness regarding the work. Other possible effects of MCR digitalization include complexity and higher task load [9].

Human reliability analysis (HRA) is a process of assessing human performance in industrial systems through qualitative methods and predicting errors by estimating error probabilities. HRA methods are often employed to analyze operator performance in NPPs and have become a significant part of ensuring the safety of NPPs. This is because HRA has a large impact on the probabilistic safety assessments and risk-informed decisions in NPPs. The way operators carry out their functions may change because of the numerous differences between analog and digital MCRs of NPPs. Although the main performance shaping factor (PSF) categories are still relevant in advanced MCRs [10], some characteristics of these new digital MCRs may lead to new types of operator errors, which may also affect operator response during time-critical tasks [11]. Integrated human event analysis system (IDHEAS), a recently developed method (developed in 2017) [12], is not specific to digital MCRs, whereas other new methods such as human reliability evaluator for computer-based control room actions (HuRECA) [13] and empirical data-based crew reliability assessment and cognitive error analysis (EmBRACE) [14] have yet to obtain regulatory approval for implementation in NPPs. Jung et al. proposed a method of determining human error probabilities (HEP) of using soft controls (a typical feature of advanced MCRs) and their associated recovery probabilities [15]. However, integrating HEP into a holistic HRA method is challenging. The current alternative is revising the established method(s) based on the properties of advanced MCRs. The nuclear regulatory and operating organizations in Korea will consider the cause-based decision tree (CBDT) method [16] as one of the possible HRA methods in the APR1400 NPP.

HRA often involves analysis of human failure events (HFEs) from the perspective of diagnosis and execution tasks. Execution actions highly depend on diagnosis activities. If diagnosis activities are performed appropriately, the chances of proper execution increase, and most incidents can be mitigated without serious consequences. Thus, this study provides an approach to analyze diagnosis errors of HFEs in an advanced MCR by critically analyzing the CBDT method and providing modifications where necessary to suit the properties of the advanced MCR tasks.

The APR1400 is a newly built NPP with a fully digitalized advanced MCR that vastly differs from the conventional analog or semi-digitized MCRs. The characteristics of the APR1400 MCR (APRMCR) include automation, advanced alarms, computerized procedures, soft controls, large display, compact operator console, and integrated displays. Thus, this study specifically considers the APRMCR as a reference MCR. The rest of this article is organized in the following order. The unique features of the APRMCR are discussed in part two. Task analysis of the diagnosis tasks in the APRMCR is detailed in part three. The modification of the CBDT method is presented in part four. In part five, the modified CBDT method is applied to examples of human errors. Finally, the last part contains discussions of our results and conclusion.

2. Unique Features of the Advanced Main Control Room in APR1400 NPP

The major distinguishing features for the APRMCRs from analog MCRs are defined and discussed from four perspectives—alarms, displays, controls, and procedures—as depicted in Figure 1.

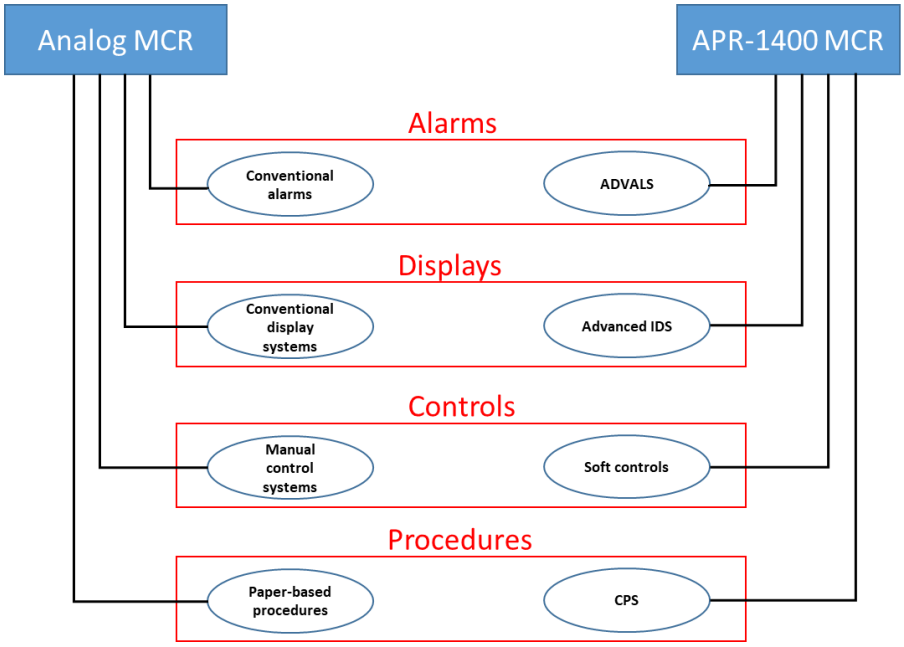

Figure 1. Distinctive features of the APRMCR versus analog MCRs.

2.1. Alarms

Conventionally, alarms are employed to continuously monitor and announce the transition of important status variables between defined conditions. They often alert operators via audio or visual signals regarding infrequent, unplanned, or undesirable changes in plant parameters or equipment status. Alarms may also indicate to the operators when the monitored status variable has returned to the normal status, and they may confirm the effect of corrective actions by audible and visible alarm coding features which unambiguously indicate when alarm conditions have cleared. As such, conventional alarm systems are employed to assist operators in determining and maintaining awareness regarding the state of the plant and its systems or functions.

The APRMCR uses an advanced alarm system (ADVALS), whose features are distinctly different from those of conventional analog MCR alarm systems. ADVALS allows the alarms to appear in a combined message and list format, and the alarms are integrated into process displays, unlike the regular tile formats used in conventional (analog) MCRs, which only display alarms in the tile format. Figure 2 shows examples of alarm presentations of both conventional MCRs and APRMCR.

The following are some other unique qualities of the ADVALS: (1) Sequencing alarms: alarms are provided in chronological order via the alarm list, unlike the analog MCR alarms system, in which the operators must remember the order of alarms. (2) Prioritizing alarms: the alarm lists are sorted automatically based on priority groupings, whereas, in analog MCR alarm systems, operators must arrange the alarms by priority. (3) Suppressing alarms: nuisance alarms (determined by processing to be less important, irrelevant, or otherwise unnecessary) are not presented to the operators, whereas in the conventional system, suppression is manually performed by the operators. (4) Spread of alarms on displays: alarms are spread into several locations on a large display panel, on several desktop displays, and in many forms, whereas alarms are statically located and displayed only as alarm tiles in analog MCRs. (5) Access to system display pages: the ADVALS message list allows direct access to system display by one or two clicks; however, in the analog MCRs, the operators physically move to access systems and system information.

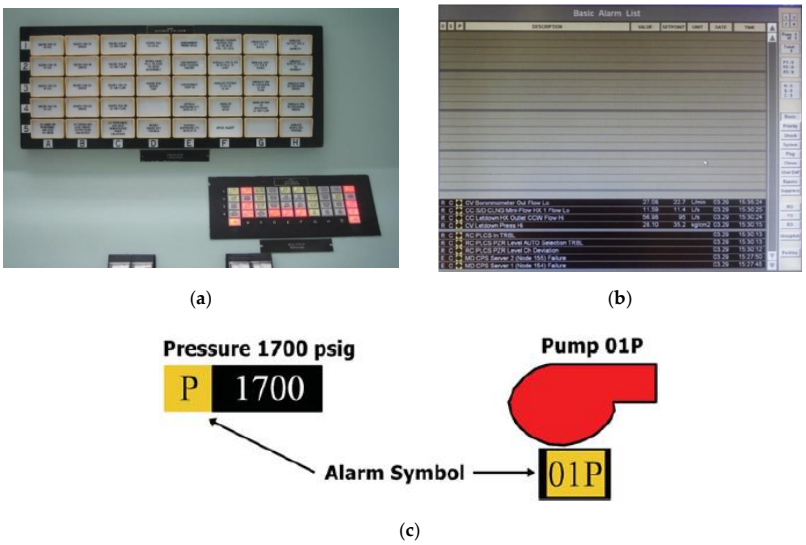

Figure 2. Examples of alarm presentations: (**a**) a tile presentation of alarms in the conventional MCR; (**b**) a list presentation of alarms in the APRMCR; (**c**) a process mimicking alarms in the APRMCR [17].

2.2. Displays

Operators typically derive the system status information of major plant components and important process parameters from MCR displays. The APRMCR has an advanced information display system (IDS), including a large display panel that is designed to allow group view, especially in situations requiring frequent communication between operators. The large display panels offer the benefits of conventional panels to avoid the notorious keyhole effect of desktop displays. The large display panel is also designed to minimize the need for the operator to navigate from one screen to the other. The advanced IDS also provides displays for both monitoring and control tasks. This includes a set of desktop screens that can be used for different purposes depending on the current need of the operator, unlike the statically laid out panels for specific purposes in conventional MCRs. This means that the panels in the conventional MCRs only show specific parameters or systems, but the panels in the APRMCR can be manipulated to display different systems and parameters depending on the operators' needs.

The advanced IDS comprise mimic presentations of the basic plant fluid systems, presentations of important subsystems (e.g., safety system trains), status information for major plant components, and important plant process parameters. This advanced IDS provides a variety of information such as technical datasheets, control logic diagrams, control and instrument diagram, and system alarm list, which are only available in paper form in conventional control rooms. This advanced IDS also provides trend graphs of important parameters, which are unavailable for conventional MCRs. The graphic information displays in this MCR have other unique characteristics such as integrated displays, information support systems such as "Aids", and procedure-based displays, most of which are not provided in conventional MCRs.

2.3. Controls

Most control devices in the APRMCR are often called soft controls. Soft controls are devices that are facilitated by software rather than hard-wired physical connections and include features such as mouse control and touch screens. Soft controls allow control room operators to control continuous processes, discrete components, and other special controllers such as control rods and turbine generators. Thus, the operators in the APRMCR use soft control systems for the operation and manipulation of equipment, which is done by manual push, pull, turn, or press actions in conventional MCRs. Thus, using soft controls, operators can select (by clicking or touching) a specific screen, choose the controller, and finally, manipulate the devices. To avoid inadvertent control of safety

systems, the safety controller in the APRMCR is isolated from the non-safety controller, unlike the conventional MCR, in which safety controllers have protection covers to prevent inadvertent manipulations.

To control safety systems in conventional MCRs, operators must remove a protective device before pressing a button, a switch, or turning a knob. However, an entirely separate soft control device is used for manipulating safety systems in the APRMCR. Operators also need to move physically to the controllers in conventional MCRs, whereas they only navigate virtually on the display systems to get to the system controls.

2.4. Procedures

NPP procedures involve instructions to guide operators in monitoring, decision-making, and controlling the NPP. Conventional MCRs have paper-based NPP procedures, whereas the APRMCR uses a computerized procedure system (CPS). The CPS supports operators in controlling the plant and reduces the demands and workload associated with paper-based procedures. The CPS provides an integrated presentation of procedural instructions and related process information required for the proper execution of the applicable procedures. The CPS has a range of capabilities, including an ability to select and display procedure on a computer screen, providing navigation links to aid in moving within or between procedures, display of process information relevant to a procedure step within the body of procedures, processing of procedure step logic and display results, and allowing access to related displays through links to a separate HSI system. Thus, unlike conventional MCRs, in which operators must search on shelves for the appropriate procedures, APRMCR operators can use a search feature that helps the operator search for the relevant feature using only keyword(s). In addition, placekeeping is mostly automated while operators use the CPS, unlike manual placekeeping performed with conventional paper-based procedures. Figure 3 shows the main display of procedure flow [18], which includes the (1) search button, (2) procedure flow pane, (3) detailed step pane, (4) pane for management of multiple procedures, (5) monitoring pane, (6) buttons for completion, suspension, and re-execution of steps, and (7) button for closing the procedures.

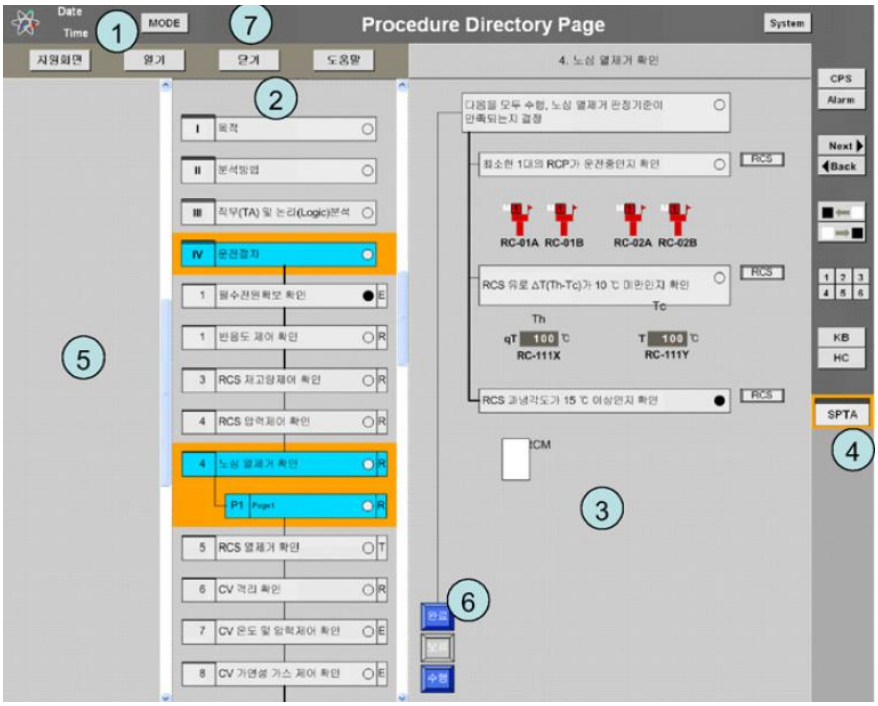

Figure 3. The main display of CPS. Reprinted from *Nuclear Engineering and Design*, Vol. 239, Jin-Hyuk Hong, Myeong-Soo lee, Do-Hyun Hwang, "Computerized procedure system for the APR1400 simulator," 3092–3104, 2009, with permission from Elsevier.

3. Task Analysis of Diagnosis in the Advanced MCR

According to Stanton et al. [19], the approach of deriving errors from task analysis is appropriate and can be validated. Therefore, we performed task analysis for operators in their use of emergency procedures during diagnosis.

3.1. Cognitive Task Model in Emergency Operations

HRA methods typically explain diagnosis based on information processing models. The information processing model adopted in this study is the one provided by A Technique for Human Event Analysis (ATHEANA) method [20]. It includes monitoring and detection, situation assessment, response planning, and response implementation. Monitoring and detection is the process of extracting information from the environment, and situation assessment involves constructing coherent, logical explanations to account for observations. Response planning involves deciding what action to take, and response implementation is the specific control action required to perform a task [21]. Only monitoring and detection, situation assessment, and response planning can be considered as part of diagnosis. To address the cognitive tasks of NPP operators in an emergency, the diagnosis steps are organized as follows: procedure selection, situation assessment, and response planning (Figure 4).

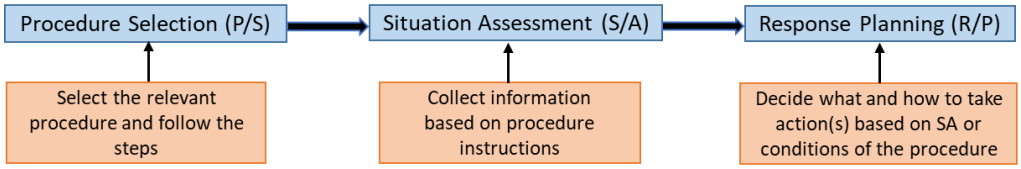

Figure 4. The sequence of diagnosis tasks in emergency operations.

In procedure selection, the operator enters the relevant emergency operating procedure and follows the necessary step(s). Situation assessment includes extraction of information from the environment based on the procedure guidelines and constructing coherent, logical explanations to account for observations. Response planning is the process of deciding what action to take, including the specific control systems to use based on situation awareness or conditions given in the procedure.

3.2. Micro-Task Analysis of Diagnosis Tasks

After a reactor trip, NPP operators will typically respond using emergency operation procedures (EOPs). Thus, operators typically begin with standard post-trip actions (SPTA) and thereafter move into diagnostic action procedures, based on which operators respond with the functional recovery procedures or optimal recovery procedures. The optimal recovery procedure selected depends on the type of accident. For a case in which feed and bleed is required after a loss of all feedwater, the optimal recovery procedures may re-direct operators to the functional recovery procedures. After diagnostic action, the shift technical adviser (STA) performs the safety function status check at 15 min intervals [22].

There are two types of tasks in EOP when soft control is used: control of non-safety-related functions and control of safety-related functions. To facilitate the identification of the potential sources of error, the major diagnosis tasks (procedure selection, situation assessment, and response planning) are further broken down into micro-tasks. This decomposition to micro-tasks is guided by observations of errors in simulator experiments involving the APRMCR operators. The micro-tasks are compared between Analog MCR and the APRMCR. Figures 5 and 6 show the diagnosis paths with micro-tasks in conventional MCRs and APRMCR, respectively.

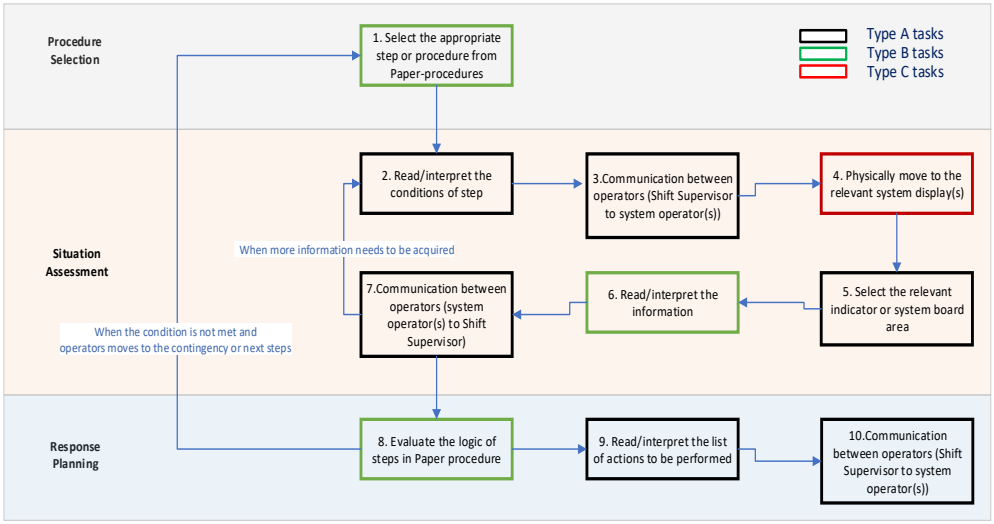

Figure 5. Diagnosis micro-tasks in the conventional MCR.

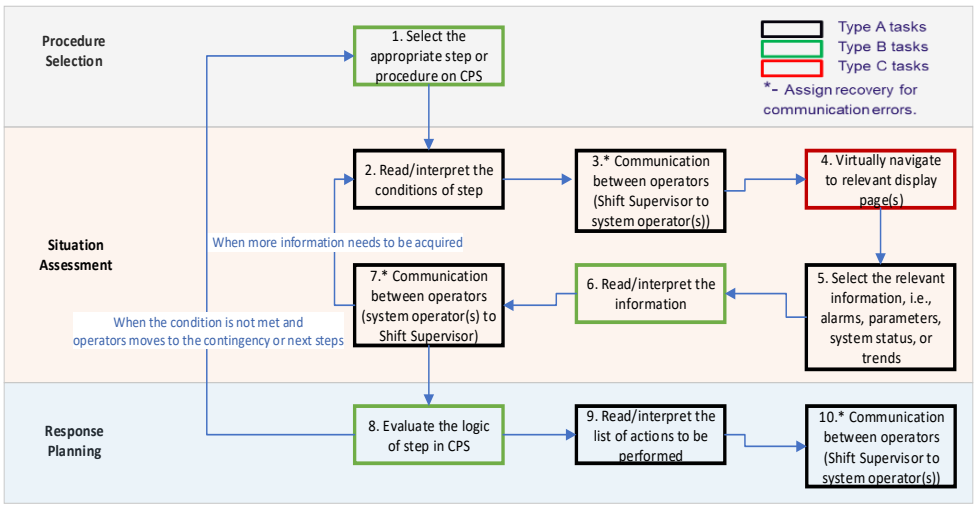

Figure 6. Diagnosis micro-tasks in the APRMCR.

3.3. Error Modes Based on APRMCR Tasks

Fundamentally, the tasks are common between conventional MCRs and the APRMCR. However, as depicted in Figures 5 and 6, the micro-tasks can be classified into three types: Type A tasks are those that are completely similar between conventional MCR and the APRMCR. Type B tasks are those that have some differences between the conventional MCR and APRMCR. Type C tasks are those that are completely different between the conventional MCR and APRMCR. The communication tasks are similar between the conventional MCR and APRMCR because the operators maintain formal three-way communication. However, in the case of APRMCR, operators can directly access each other's systems. Hence, recovery should be assigned for any communication error. Table 1 shows a comparison of the details of the micro-tasks in the conventional versus APRMCRs, along with their associated error modes. The error modes in Table 1 mostly correspond to the micro-tasks. It can also be observed that the same error codes are assigned to the correlated error modes. Hence, E2 includes "Error in reading/interpreting the procedure guides" and "Error in reading/interpreting the list of the target device(s) from procedures" as both involve reading of procedures. Communication errors from shift supervisor to the system operators and vice versa are grouped as E3, whereas errors in the reading of system parameters from displays are grouped as E6.

Table 1. Comparison of micro-tasks of conventional MCRs versus APRMCRs.

	Micro-Task in Analog MCR	Error Modes	Corresponding Error Mechanisms as Used in CBDTs	Micro-Tasks in APRMCR	Codes	Error Modes
P/S	Select the appropriate step or procedure from paper procedures	Error in selecting the appropriate paper-based procedure or step	Pce—skip a relevant step in the procedure	Select the appropriate step or procedure on CPS	E1	Error in selecting the appropriate procedure or step from CPS
S/A	Read/interpret procedure conditions of steps	Error in reading/interpreting the procedure guides	Pcf—error in interpreting instructions	Read/interpret procedure conditions of steps	E2	Error in reading/interpreting the procedure guides
S/A	Communicate between operators (shift supervisor to board operator(s))	Error in communicating the appropriate action	"Formal communication" is a PSF in the Pcc—misread or miscommunicate data error mechanism. The General HEP of 0.003 with E.F of 3 was recommended for the failure of formal communication.	Communicate between operators (shift supervisor to system operators)	E3	Error in communicating the appropriate action
S/A	Physically move to the relevant system displays	Failure to move to the systems displays	N/A	Virtually navigate the interfaces to the relevant system display pages	E4	Error in navigating the interfaces to the relevant system display
S/A	Select the relevant indicator or system board area	Failure to select the correct indicator	"Indicator easy to locate" is a PSF in the Pcc—misread or miscommunicate data error mode. A HEP of 0.003 with an EF of 3 was recommended.	Select the relevant information (i.e., alarms, parameters, system status, or trends)	E5	Failure to select the correct indicator on the monitor
S/A	Read/interpret alarm information via color combinations on alarm tiles and sounds	Error in reading/interpreting details of the alarm information from alarm tiles display	Pcc—misread or miscommunicate data. The main PSF is a "good/bad indicator" with a HEP of 0.001 and Pcb—data unattended to (inattention).	Read/interpret details of the alarm information from ADVALS (via mimics, message lists, and tiles)	E6	Error in reading/interpreting details of the alarm information from ADVALS
S/A	Read/interpret system status	Error in reading/interpreting system status	Pcd—misleading information	Read/interpret system status	E6	Error in reading/interpreting system status on advanced IDS
S/A	Read/interpret parameter value	Misreading or misinterpreting parameter value	Pcc—misread or miscommunicate data	Read/interpret parameter value	E6	Misreading or misinterpreting parameter value
S/A	Read/interpret the parameter trends based on current and previous values on the indicators	Failure to read or interpret parameter trends	Pca—unavailability of the required data to MCR operators Pcb—data unattended to (inattention)	Read/interpret the parameter trends (displays show historical trends)	E7	Failure to read or interpret parameter trends
S/A	Communicate between operators (board operator(s) to shift supervisor)	Error in communicating the appropriate information	"Formal communication" is a PSF in the Pcc—misread or miscommunicate data error mechanism. The General HEP of 0.003 with E.F of 3 is recommended for the failure of formal communication.	Communicate between operators (system operator(s) to shift supervisor)	E3	Error in communicating the appropriate information
R/P	Evaluate the logic of procedure steps	Failure to follow the diagnostic logic from procedures	Pcg—error in interpreting diagnostic logic Pch—deliberate violation of procedure	Evaluate the logic of procedure steps in CPS	E8	Failure to follow the diagnostic logic from the CPS
R/P	Read/interpret action list to decide the target device(s)	Error in reading/interpreting list of target device(s) from procedures	Pcc—misread or miscommunicate data	Read/interpret action list to decide the target device(s)	E2	Error in reading/interpreting the list of target device(s) from procedures to decide target device(s) for manipulation

4. Modification of the CBDT Method

4.1. The CBDT Method

The CBDT method for human error analysis was developed at the Electric Power Research Institute to quantify post-initiators. This is an analytical method that considers specific causes of human cognitive error and evaluates the impact of PSFs (tree branching criteria for each CBDT tree) on an HFE-specific basis, e.g., whether the operator has a high or low workload to check or monitor, should he use the front or back panel, and whether the indicator sounds an alarm or not. The CBDT method provides a systematic framework for analyzing decision or diagnosis errors.

The CBDT approach assumes situation-specific error conducive factors; i.e., it assumed two situation-specific failure modes, and each one includes four error mechanisms. Failure mode 1 is the failure of the system information–operator interface. This mode has four error mechanisms—availability of information (Pca), failure of attention (Pcb), misread/miscommunicate data (Pcc), and misleading information (Pcd). Failure mode 2 is the failure of the operator-procedure guideline interface. It has four mechanisms: skip a step in the procedure (Pce), misinterpret instructions (Pcf), misinterpret the decision logic (Pcg), and deliberate violation (Pch).

Meanwhile, the CBDT method is primarily concerned with the quantification of HEPs rather than the identification of human errors. The HEPs for each error mechanism—"a" through "h"—must be estimated by using separate decision trees for each error mechanism. The relevant branch points on the trees are selected based on the scenario conditions to arrive at the error mechanism HEP. Most values given in the end branch of the decision trees are based on the values presented in the regulatory guide, NUREG/CR-1278 [23]. The final HEP for each HFE is calculated using the sum of all HEPs from each of the error mechanisms while considering the recovery actions given by Equation (1) [24].

$$\text{HEP} = \sum (\text{Error probability of each error mechanism} \times \text{recovery failure probability}) \quad (1)$$

4.2. Task Categories and Applicability of the CBDT Method

Based on the task analysis depicted in Figures 5 and 6 and a review of the CBDTs and their applied PSFs, the APRMCR tasks can be categorized into three types: Type A: operators in the conventional MCRs and the APRMCR have the same task/error modes, and their nature of application or PSFs are the same. For such tasks, the current CBDT requires no modifications. Type B: operators in the conventional MCRs and the APRMCR experience some differences in task/error modes; thus, the nature of application or PSF can differ. For such tasks, modifications are required. Type C: operators in the APRMCR experience entirely new tasks/error modes compared to the operators in the conventional MCRs. For this case, a new approach is necessary.

Table 2 shows the error modes (based on analysis in Table 1) for each task type and the corresponding CBDT error mechanisms for the analysis of the error mode.

Table 2. Task types with applicable CBDTs.

Type A Tasks (No Modifications to CBDTs Are Required)	Type B Tasks (Modifications to CBDTs Are Required)	Type C Tasks (A New Approach in the CBDT Is Necessary)
E2—Error in reading/interpreting the procedure guides —Error in reading/interpreting list of actions/device(s) from procedures to decide target device(s) for manipulation. Pcf—error in interpreting instructions	E1—Error in selecting the appropriate procedure or step from CPS. Pce—skip a step in the procedure	
E3—Error in communicating the appropriate action —Error in communicating the appropriate information Pcc—misread or miscommunicate data	E7—Failure to read or interpret parameter trends. Pca—unavailability of the required data to MCR operators Pcb—data unattended to (inattention)	E4—Error in navigating the interfaces to the relevant system display. The PSF of "indicator easy to locate" in Pcc would directly influence navigation error. Pcc—misread or miscommunicate data
E5—Failure to select the correct indicator on the screen. Pcc—misread or miscommunicate data		
E6—Error in reading/interpreting details of the alarm information from ADVALS —Error in reading/interpreting system status on the advanced IDS —Misreading or misinterpreting parameter value Pcc—misread or miscommunicate data Pcd—misleading information	E8—Failure to follow the diagnostic logic from the CPS Pcg—error in interpreting diagnostic logic Pch—deliberate violation of procedure	

4.3. Modification of the CBDT Method

Table 2 shows that there are a total of four (4) error modes in which some corresponding CBDTs need to be modified: E1 (error in selecting the appropriate procedure or step from CPS), E7 (failure to read or interpret parameter trend from the advanced IDS), E8 (failure to follow the diagnostic logic from the CPS), and E4 (error in navigating the interfaces to the relevant system display). Details of the modifications are described as follows.

4.3.1. Modification of CBDT for Treatment of E1

Pce—skip a step in the procedure—is the corresponding error mechanism for the CBDT method for treating E1 (error in selecting the appropriate procedure or step). Pce has the following PSFs: "Obvious vs. Hidden," "Single vs Multiple," "Graphically distinct," and "Placekeeping aids." However, the PSF of "Placekeeping aids" would reduce HEP because placekeeping is fully automated in the CPS of the APRMCR. Hence, the basic HEP should be revised.

The original HEP values used in the Pce CBDT are from Table 20-7, items 2 and 4, of the technique for human error rate prediction (THERP) [23], which represent omission errors when written procedures with long lists are used with placekeeping and when the procedure is not used or improperly used. We noted that THERP recommended higher HEPs for longer lists because they required more cognitive attention than shorter lists. This was adopted originally in CBDT to maintain a conservative approach. We assume that automated placekeeping in the CPS reduces the possibility of omissions per item of instruction because the operators require lower cognitive attention for placekeeping in the CPS. Thus, we recommend the use of the lower range of HEPs—i.e., HEP values from the THERP Table 20-7, items 1 and 3 [23], which originally represent omission errors when using written procedures with short lists. Thus, in the modified CBDT (MCBDT), the HEP for placekeeping is 0.001 versus 0.003, as represented in Table 3. "F" indicates failure nodes and "R" indicates recovery nodes. The sources of the HEP values are also indicated in Table 3.

Table 3. Pce evaluation HEPs in MCBDT and their sources.

Factor	Current CBDT	Source	MCBDT	Source
F1—Obvious vs. Hidden instructions	0 vs. 0.1	Estimated from simulator exercises by THERP	0 vs. 0.1	Estimated from simulator exercises by THERP
F2—Single vs Multiple procedure/column flowchart	0 vs. 0.003	General HEP in THERP	0 vs. 0.003	General HEP in THERP
R3—Graphically distinct step	0.333 vs. 1	Estimate from THERP	0.333 vs. 1	Estimated from THERP
F4—Placekeeping aids	0.003 vs. 0.01	Table 20-7, items 2 and 4, in THERP	0.001 vs. 0.003	Table 20-7, items 1 and 3, in THERP

The question by the HRA analyst for analyzing the "Placekeeping aids" branch of the Pce CBDT should now be (modified) as follows: "Do all crew members use the automated placekeeping aids for checking off, marking through completed steps, and marking pending steps?" This is based on the premise that even when only some of the crews use or rely on the automated placekeeping function of the CPS, the presence of such automation will always serve as good support for the operator, either in the form of recovery or by simply lowering the cognitive task. If it is evaluated that all the operators use the placekeeping aids, the upper branch (HEP = 0.001) should be selected; otherwise, the lower branch (HEP = 0.003) should be selected. The final branch HEPs for the Pce are derived using Equation (2). Figure 7 shows the final Pce in the MCBDT.

$$\text{Pce} = (\text{F1} + \text{F2} + \text{F4})\ (\text{R3}) \quad (2)$$

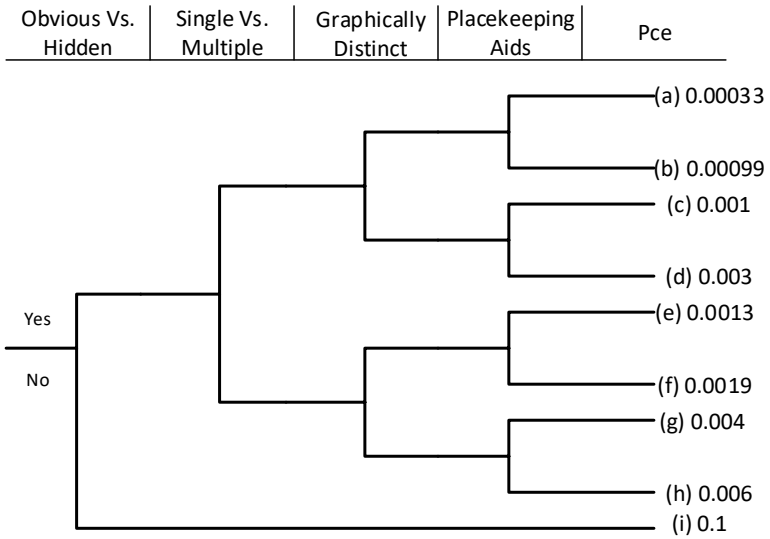

Figure 7. Pce in the MCBDT.

4.3.2. Modification of CBDT for Treatment of E7

E7 (failure to read or interpret parameter trend) can be treated with the Pcb decision tree. According to the current Pcb CBDT, the question to be asked to evaluate the PSF "Check vs. Monitor" in the Pcb tree is whether "the operators need to check or monitor a value?" Monitoring is required to interpret parameter trends. APRMCR supports monitoring in various ways, including trends of parameters. The APRMCR has analog-type trend-charts (with limit marks) along with digital indicators of parameters. Thus, the PSF "Check vs. Monitor" in the Pcb tree may be modified by revising the HEP for "monitoring" because monitoring is supported in the APRMCR. The HEP value recommended for the "Check" branch is zero; i.e., it is negligible (according to the current CBDT) because operators are required to perform only a one-time check of a parameter. The HEP for the "monitor" branch is the general HEP of 0.003. Therefore, we adopt a HEP of 0.00189 (approximately 0.002) based on experimental data for errors in "trend" monitoring in the human reliability data extraction (HuREX) database [25]. The factors for Pcb, their HEPs, and the sources of the HEP values are indicated in Table 4. "F" indicates failure nodes, while "R" indicates recovery nodes. The final branch HEPs for the Pcb error mechanism are derived using Equation (3), and Figure 8 shows the final Pcb in the MCBDT.

$$\text{Pcb} = \text{R1} \times (\text{F2} + \text{F3}) \times \text{R4} \quad (3)$$

Table 4. Pcb evaluation HEPs in MCBDT and their sources.

Factor	Current CBDT	Source	MCBDT	Source
R1- Low vs. High Workload	1 vs. 5	THERP Table 20-16a, Item 4	1 vs. 5	THERP Table20-16a, Item 4
F2- Check vs. Monitor	0 vs. 0.003	General HEP in THERP (as an estimate to monitor with sufficient frequency)	0 vs. 0.00189	HuREX [25]
F3- Front vs. Back panel	0 vs. 0.003	General HEP in THERP	0 vs. 0.003	General HEP in THERP
R4- Alarmed vs. Not Alarmed	0.05 vs. 1	Table 20-23 (reciprocal of Item 10) in THERP	0.05 vs. 1	Table 20-23 (reciprocal of Item 10) in THERP

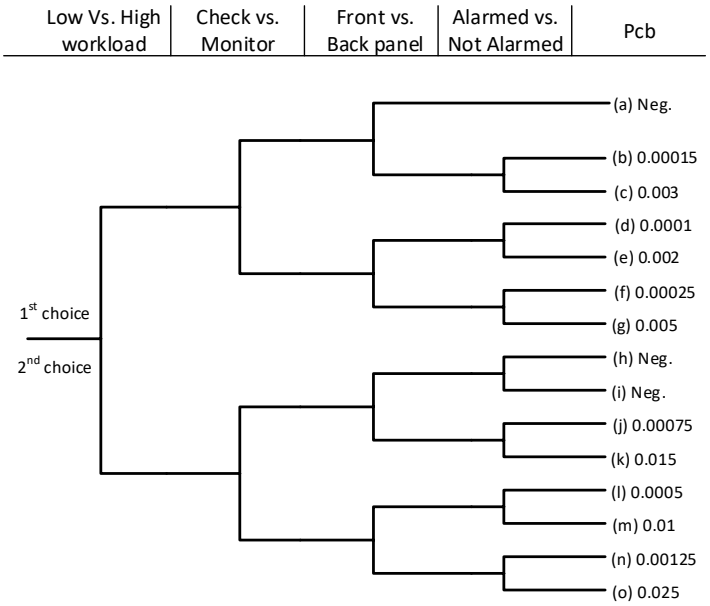

Figure 8. Pcb in the MCBDT.

4.3.3. Modification of CBDT for Treatment of E8

E8 (failure to follow the diagnostic logic from the CPS) can be treated with the Pcg decision tree. The CPS in the APRMCR automatically evaluates the procedure logic in some situations. In other situations, the operator can override the automated logic evaluation. Thus, HEPs would be reduced with less cognitive effort by the operator performing procedure logic evaluation. This must be noted in the evaluation of the Pcg decision tree. To reflect the reduced HEPs, the Pcg tree should be modified by revising the questions for evaluation by a human reliability analyst. Thus, at each branch of the Pcg tree, the use of automatic logic should be checked. Table 5 shows the modified version of the analysis questions for each branch of the Pcg tree.

Table 5. Modified guide for Pcg decision tree analysis.

Branches in the Pcg Tree	Questions in the Current CBDT	Questions in MCBDT	Possible Answers and Branch HEPs on the Pcg Tree of MCBDT
"NOT" statement	Does the step contain the word "not"?	Assign Option 2 when the procedure logic is automated. Assign Option 1 when the "not" statement is present. Otherwise, assign Option 2.	Option 1, HEP = 0.018 Option 2, HEP = 0
AND or OR statement	Does the procedure step present diagnostic logic in which more than one condition is combined to determine the outcome?	Assign Option 2 when the procedure logic is automated. Assign Option 1 when the procedure steps present diagnostic logic in which more than one condition is combined to determine the outcome. Otherwise, assign Option 2.	Option 1, HEP = 0.001 Option 2, HEP = 0
Both AND and OR	Does the step contain a complex logic involving a combination of of ANDed and ORed terms?	Assign Option 2 when logic is automated. Assign Option 1 when the procedure step contains a complex logic involving a combination of ANDed and ORed terms. Otherwise, assign Option 2.	Option 1, HEP = 0.03 Option 2, HEP = 0
Practiced scenario	Has the crew practiced executing this step in a scenario similar to this one in a simulator?	Has the crew practiced executing this step in a scenario similar to this one in a simulator? If yes, assign Option 1. If no, assign Option 2.	Option 1, HEP = 0.333 Option 2, HEP = 1.0

The final branch HEPs in Pcg remain the same and have not been modified (see modified Pcg tree in Figure 9). If the logic is always automated, the final HEP will be negligible. If not, the remaining branches can be followed as is on the current CBDT Pcg tree. With this approach, the automated logic would be catered for.

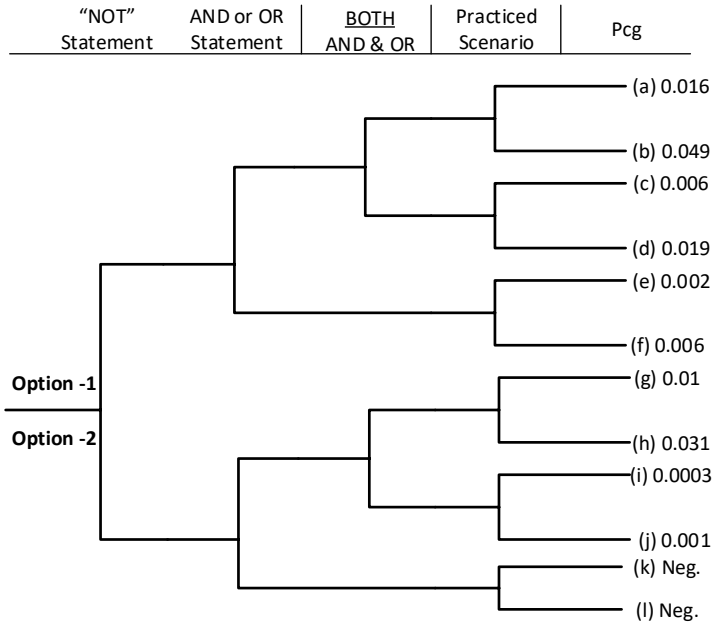

Figure 9. Pcg in the MCBDT.

4.3.4. Modification of CBDT for Treatment of E4

E4 (error in navigating the interfaces to the relevant system display) is a unique error mode that requires a novel approach. However, the navigation errors are mostly affected by the operators' ability to easily find the indicators on the screen. Therefore, in terms of analysis and quantification, the failure of operators to find the indicators and the navigation errors should be tightly coupled. We attempted this by modifying the Pcc branch: "Ind. Easy to Locate." This is done by considering the possibility of an increase or decrease in navigation error due to the hardship or ease, respectively, of locating indicators in the APRMCR. Table 6 depicts an analysis of the HEPs derivable from the analysis of both display quality and navigation errors.

Table 6. Evaluating "indicator easy to locate" on the Pcc tree.

	HEPs in the Current CBDT			HEPs in the MCBDT		
Options	**Physical Navigation**	**Control Board Quality**	**Total HEP**	**Virtual Navigation**	**Control Display Quality**	**Total HEP**
Yes (good case)	Not applied	0	0 (Used for upper branch)	0 (good)	0 (good)	0 (Used for upper branch)
				0 (good)	0.003 (bad)	0.003
				0.00596 (bad)	0 (good)	0.00596
No (bad case)	Not applied	0.003 Source: Table 20-9, Item 4 in THERP	0.003 (Used for lower branch)	0.00596 (bad) Source: HuREX data [26]	0.003 (bad) Source: Table 20-9, Item 4 in THERP	0.00896 (Used for the lower branch)

The operators in the conventional MCR typically must physically move to the control board to perform an action; however, the current CBDT does not consider the physical navigation errors (i.e., not applied). However, operators in the APRMCR must virtually navigate to the relevant displays. In this study, a navigation task is defined as the action of operators to switch from one screen to another to find the relevant screen/displays. Hence, we can adopt the basic HEP for "wrong screen switching/selection" in a digitized control room, as estimated in Kim et al. [26]. The value of basic HEP for a virtual navigation error is 0.00596.

The APRMCR interfaces have a basic design principle: the operator should need no more than 2 (two) clicks to reach any desired page or screen. Virtual navigation should be evaluated by the HRA analyst as bad when significant interface management (a couple of clicks) is required for an operator to view the indicator necessary to perform a task. Otherwise, virtual navigation HEP is negligible. Table 6 shows that when considering both display quality and virtual navigation errors, there are four possible HEP outcomes: (1) Zero (0) when both display and virtual navigation are evaluated as good; (2) 0.003 when only virtual navigation is evaluated as good; (3) 0.00596 when only the display is evaluated as good; and (4) 0.00896 when both display quality and navigation are evaluated as bad. In keeping with the tradition of the CBDT method of taking the conservative option, only the two extreme cases of HEP being zero (i.e., negligible) and 0.00896 are adopted in the MCBDT method. Therefore, whether the display only, the navigation only, or both navigation and displays are evaluated as bad, the lower branch (with HEP = 0.00896) is selected.

As both navigation errors and display quality must be assessed to evaluate "Ind. Easy to locate," the question for the HRA analyst should also be modified as follows: Is the layout, demarcation, labeling, and necessary navigation such that it is easy to locate the required indicator? The answer is no if there are obvious human factor deficiencies in these areas, which are plausible candidates for confusion (the correct indicators are sufficiently similar so that the values displayed would not cause the operator to recheck the identity of the indicator after reading it) or a couple of clicks is necessary for an operator to see the indicator. Table 7 shows the factors for Pcc, their HEPs, and the sources of the HEP values. "F" indicates failure nodes. The final branch HEPs for the Pcc are derived using Equation (4). Figure 10 shows the final Pcc in the MCBDT.

$$\text{Pcc} = \text{F1} + \text{F2} + \text{F3} \quad (4)$$

Table 7. Branch HEPs for Pcc used in the MCBDT method.

Factor	Value	Source
F1—Indicator easy to locate	0 vs. 0.00896	Table 20-9, item 4, in THERP HuREX data [26]
F2—Good/bad Indicator	0 vs. 0.001	Table 20-10, item 1, LBa in THERP
F3—Formal communications	0 vs. 0.003	General HEP in THERP

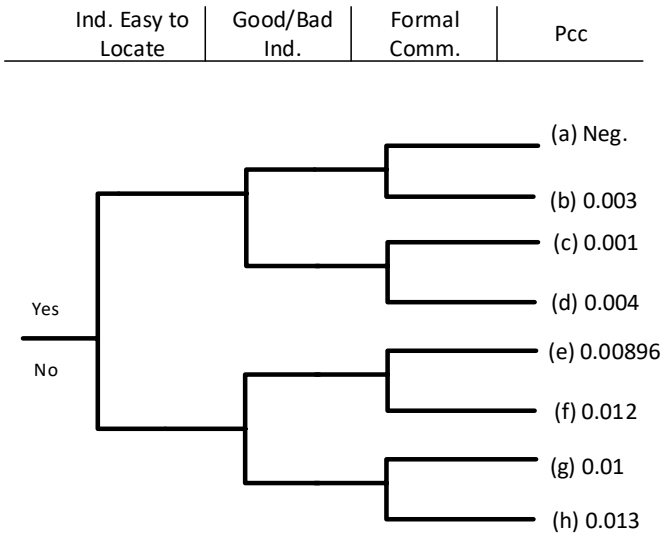

Figure 10. Pcc tree in MCBDT.

5. Application of the Modified CBDT Method for Advanced MCRs

HRA often proceeds with the selection of important human actions for a specified scenario. Examples of the application of the proposed method are presented in this section based on some selected scenarios. The HEPs of critical operator actions modeled in a probabilistic safety assessment of an APRMCR were evaluated using the MCBDT method. The characteristics of each of the HFEs are defined. The success criteria and primary cues of the HFEs were also identified in the analysis before determining the HEPs.

5.1. The Event of Initiating Emergency Boration to the Reactor Coolant System

The initial condition for this scenario is that the NPP is in full power and steady-state operation. The initiating event is an anticipated transient without scram event. A negative reactivity is induced by injecting boric acid water to maintain a long-term shutdown margin and prevent re-continuation after the transient event. Even if the plant is stabilized after the initial pressure transient, the pressure of the reactor coolant system (RCS) may be too high to inject borated water into the RCS to control the level of reactor coolant and reactivity. The success criterion is that the operator should inject borated water into the RCS using the chemical and volume control system. The HFE, in this case, is the "operator fails to initiate emergency boration to the RCS." A preceding system failure to this HFE is the failure of an automatic reactor trip.

The relevant procedure is the SPTA procedure. The instruction for diagnosis is "inject borated water into the RCS so that the shutdown margin is 6.5%Δk/k" and is described in step 1.C2 of the SPTA procedure. The initial cue is the number of non-inserted full-strength control element assemblies, whereas the recovery cue is the charging flow or shutdown margin. The diagnosis HEP evaluation for this HFE using the MCBDT is summarized in Table 8, and Figure 11 depicts the branching paths in the modified trees; i.e., Pcb, Pcc, Pce, and Pcg. Thus, the final diagnosis HEP for this HFE is 2.0×10^{-3} (i.e., $1.5 \times 10^{-3} + 5.0 \times 10^{-4}$).

Table 8. Evaluating the diagnosis error for operator failure to initiate emergency boration.

Error Mechanism	Evaluation	Branch	Initial Branch HEP	Recovery Factor (s)	Final Branch HEP
Pca	All the required information is displayed, information is correct, and training for this event is adequate.	a	Neg.	-	-
Pcb	High workload is due to time constraints, action is "check," cues are indicated on the displays, and it is assumed that there is no alarm.	i	Neg.	-	-
Pcc	Relevant ergonomic design is well done, navigation is good, and formal communication is used.	a	Neg.	-	-
Pcd	"All cues are as stated" is rated "No," while warning of differences is rated as "Yes."	b	3.0×10^{-3}	5.0×10^{-1} *	1.5×10^{-3}
Pce	Relevant instructions are clearly marked as steps, a single procedure is used, instructions are graphically non-distinct, and placekeeping is automated.	a	1.0×10^{-3}	5.0×10^{-1} *	5.0×10^{-4}
Pcf	Instructions have standard and unambiguous wordings.	a	Neg.	-	-
Pcg	No decision logics and operator practiced this scenario.	k	Neg.	-	-
Pch	It is assumed that operators trust the procedures.	a	Neg.		

* As this HFE affects the state of safety function, it is assumed that evaluation by other operators such as STA is possible. Neg. denotes that the HEP is negligible.

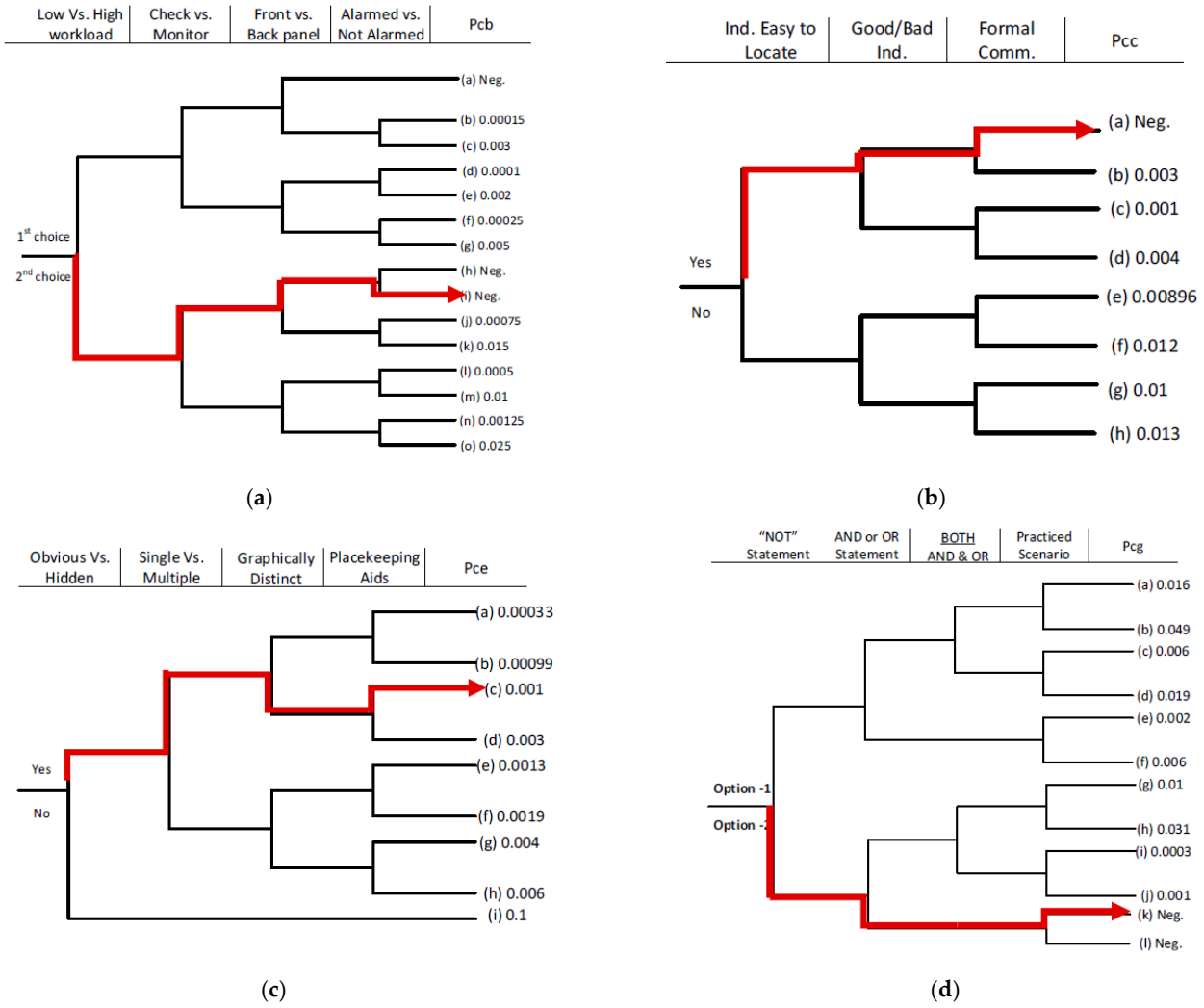

Figure 11. Branching paths in the modified trees. (**a**) Pcb; (**b**) Pcc; (**c**) Pce; and (**d**) Pcg for the evaluation in Table 7.

5.2. The Event of Starting Auxiliary Feedwater Charging Pump for the Reactor Coolant Pump Seal

The initial condition for this scenario is that the NPP is in full power and steady-state operation. Several initiating events can lead to this HFE, including a total loss of component cooling water and a loss of offsite power. In case the sealing injection water and component cooling water are simultaneously lost, either of the two must be recovered within 3 min. Otherwise, the reactor coolant pump (RCP) should be manually stopped. In this case, the operator will start the auxiliary charging pump for RCP seal recovery. Similarly, in the event of a loss of offsite power accident, the operator first attempts to restore the sealing water, as instructed in step 6 of EOP-06. The operator must activate the auxiliary charging pump to recover sealed water. The success criterion is that the operator should align valves and start auxiliary charging pumps for RCP seal injection. The HFE, in this case, is the "operator fails to start the auxiliary charging pump for RCP seal." A preceding system failure to this HFE is the failure of an automatic reactor trip.

The instruction for diagnosis is as follows: "Is the component cooling water or sealing injection water supplied to the RCP lost?". It is described in step 1.C2 of the SPTA procedure. The initial cue is the RCP 1A seal leakage, while the recovery cue is the recovery of the RCP seal. The diagnosis HEP evaluation for this HFE using the MCBDT is summarized in Table 9. Thus, the final diagnosis HEP for this HFE is 2.0×10^{-3}.

Table 9. Evaluating the diagnosis error for operator failure to start the charging pump for RCP sealing.

Error Mechanism	Evaluation	Branch	Initial Branch HEP	Recovery Factor (s)	Final Branch HEP
Pca	All the required information is displayed, information is correct, and training for this event is adequate.	a	Neg.	-	-
Pcb	High workload is due to time constraints, action is "check," cues are indicated on the displays, and it is assumed that there is no alarm.	i	Neg.	-	-
Pcc	Relevant ergonomic design is well done, navigation is good, and formal communication is used.	a	Neg.	-	-
Pcd	All cues are as stated in the procedures.	a	Neg.	-	-
Pce	Relevant instructions are clearly marked as steps and multiple procedures (procedures related to RCP seal cooling recovery and EOP) are used, instructions are graphically non-distinct, and placekeeping is automated.	g	4.0×10^{-3}	5.0×10^{-1} *	2.0×10^{-3}
Pcf	Instructions have standard and unambiguous wordings.	a	Neg.	-	-
Pcg	No decision logics and operators have practiced this scenario.	k	Neg.	-	-
Pch	It is assumed that operators trust the procedures.	a	Neg.		

* As RCP sealing water affects major safety variables; it can be monitored by other operators. Neg. means that the HEP is negligible.

5.3. The Event of Recovery of an Auxiliary Feedwater Actuation Signal

The initial condition for this scenario is that the NPP is in full power and in steady-state operation. Several initiating events can lead to this HFE, excluding large or medium break loss of coolant accidents (LLOCA and MLOCA). After the initiating event, the auxiliary feedwater actuation signal (AFAS) is automatically generated as the level of the steam generator water decreases. However, if no signal is generated, the operator must manually generate AFAS. The success criterion is that operator should initiate the auxiliary feedwater system to control the steam generator level. The HFE, in this case, is the "operator fails to recover AFAS 1."

The instruction for diagnosis is "a. Verify that the steam generator satisfies at least one of the following: • The level of at least one steam generator is between 25% and 90% • Total water supply to all steam generators exceeds 41 L/s (147.6 ton/h) and steam generator water level recovers to between 25% and 90%" and is described in step 6.a of the SPTA procedure. The initial cue is the steam generator low-level alarm (<25% WR), whereas the recovery cue is the actuation of AFAS. The diagnosis HEP evaluation for this HFE using the MCBDT is summarized in Table 10. Thus, the final diagnosis HEP for this HFE is 2.0×10^{-3} (i.e., $1.5 \times 10^{-3} + 5.0 \times 10^{-4}$).

Table 10. Evaluating the diagnosis error for recovery of an auxiliary feedwater actuation signal.

Error Mechanism	Evaluation	Branch	Initial Branch HEP	Recovery Factor (s)	Final Branch HEP
Pca	All the required information is displayed, information is correct, and training for this event is adequate.	a	Neg.	-	-
Pcb	High workload is due to time constraints, "check" action is required, cues are the same as indicated on the displays, and it is assumed that there is no alarm.	i	Neg.	-	-
Pcc	Relevant ergonomic design is appropriate, navigation is good, and formal communication is used.	a	Neg.	-	-
Pcd	Not all the cues are as stated in the procedures. Though, warnings of possible discrepancies are indicated.	b	3.0×10^{-3}	5.02×10^{-1} *	1.5×10^{-3}
Pce	Relevant instructions are clearly marked in steps, a single procedure is used, instructions are graphically non-distinct, and placekeeping is automated.	g	1.0×10^{-3}	5.0×10^{-1} **	5.0×10^{-4}
Pcf	Instructions have standard and unambiguous wordings.	a	Neg.	-	-
Pcg	Only the "or" logic is present, but it is automated. The scenario is practiced.	k	Neg.	-	-
Pch	It is assumed that operators believe in the adequacy of the procedures.	a	Neg.		

* As the STA performs the safety function status check, recovery of Pcd is credited with high dependency. ** The steam generator level affects the temperature and pressure control on the primary side, so it can be checked by other operators. Neg. means that the HEP is negligible.

5.4. The Event of Performing Aggressive Secondary Cooling for a Small Break Loss of Coolant Accident

The initial condition for this scenario is that the NPP is in full power and steady-state operation. The initiating event leading to this HFE is a small break loss of coolant accident (SLOCA). If the operation of the safety injection system (SIS) fails during a SLOCA, RCS pressure is reduced below the shutdown water level of the shutdown cooling pump. However, the shutdown cooling pump should inject coolant before the core is exposed and damaged. The operator must perform heat removal on the secondary side through the atmospheric dump valve (ADV). The success criterion is that the operator should open and control one or more main steam atmospheric dump valves (MSADVs). The HFE, in this case, is the "operator fails to perform aggressive secondary cooling for SLOCA." A preceding failure in the event sequence is the failure of automatic safety injection.

The instruction for diagnosis is, "Is the SI flow rate less than 166.6 L/min due to the high pressure of the RCS?" and is described in step 13-IC-02 of the functional recovery procedure #04 (RCS inventory control). The initial cue is the lack of safety injection (SI) flow, whereas the recovery cue is the restoration of normal RCS temperature and pressure. The diagnosis HEP evaluation for this HFE using the MCBDT is summarized in Table 11. Thus, the final diagnosis HEP for this HFE is 4.0×10^{-3} (i.e., $3.0 \times 10^{-3} + 1.0 \times 10^{-3}$).

Table 11. Evaluating the diagnosis error for performing an aggressive secondary cooling for SLOCA.

Error Mechanism	Evaluation	Branch	Initial Branch HEP	Recovery Factor (s)	Final Branch HEP
Pca	All the required information is displayed, information is correct, and training for this event is adequate.	a	Neg.	-	-
Pcb	High workload is due to SI failure, actions are checked, cues are the same as indicated on the displays, and it is assumed that there is no alarm.	i	Neg.	-	-
Pcc	Relevant ergonomic design is appropriate, navigation is good, and formal communication is used.	a	Neg.	-	-
Pcd	Not all the cues are as stated in the procedures. Though, warnings of possible discrepancies are indicated.	b	3.0×10^{-3}	-	3.0×10^{-3}
Pce	Relevant instructions are clearly marked in steps, and a single procedure is used, which is graphically non-distinct, with automated placekeeping.	g	1.0×10^{-3}	-	1.0×10^{-3}
Pcf	Instructions have standard and unambiguous wordings.	a	Neg.	-	-
Pcg	No diagnostic logic for this HFE and the scenario is practiced.	k	Neg.	-	-
Pch	It is assumed that operators believe in the adequacy of the procedures.	a	Neg.		

5.5. The Event of Performing Core Heat Removal during the Early Phase of Feed and Bleed Operation

The initial condition for this scenario is that the NPP is in full power and steady-state operation. Several initiating events can lead to this HFE, excluding large or medium break loss of coolant accidents and total loss of component cooling water. In the event of an initiating event, if secondary heat removal operation is not possible or adequate, decay heat may be removed by feed and bleed operation to prevent core damage. After the secondary side heat removal operation fails, at least two safety injection pumps should inject coolant, and the front discharge valve must be opened in the two pilot sections by the operator to release the steam. The success criterion is that the operator should open pilot-operated safety relief valves for RCS heat removal. The HFE, in this case, is the "operator fails to open pilot-operated safety relief valves in the early phase for feed and bleed operation." A preceding system failure to this HFE is the failure of the secondary heat removal system.

The instruction for diagnosis is to enter the functional recovery procedure #06 (core and RCS heat removal) step 125 for "verifying once-through cooling conditions" (HR-3) directed from the EOP-05 (verifying heat removal via steam generator) step 7.C1. The initial cue is the steam generator level (2% wide range), whereas the recovery cue is the restoration of the RCS temperature and pressure to acceptable levels. The diagnosis HEP

evaluation for this HFE using the MCBDT is summarized in Table 12. Thus, final diagnosis HEP for this HFE is 1.79×10^{-3} (i.e., $4.5 \times 10^{-4} + 1.3 \times 10^{-3} + 4.29 \times 10^{-5}$).

Table 12. Evaluating the diagnosis error for core heat removal in early feed and bleed.

Error Mechanism	Evaluation	Branch	Initial Branch HEP	Recovery Factor (s)	Final Branch HEP
Pca	All the required information is displayed, information is correct, and training for this event is adequate.	a	Neg.	-	-
Pcb	High workload is due to failure of the secondary heat removal system, action is checked, cues are indicated on the displays, and it is assumed that there is no alarm.	i	Neg.	-	-
Pcc	Relevant ergonomic design is appropriate, navigation is good, and formal communication is used.	a	Neg.	-	-
Pcd	Not all the cues are as stated in the procedures. Warnings of possible discrepancies are credited because it contains references to other documents.	b	3.0×10^{-3}	1.5×10^{-1} *	4.5×10^{-4}
Pce	Relevant instructions are clearly marked in steps, multiple procedures are used with are graphically distinct instructions, and placekeeping is automated.	e	1.3×10^{-3}	-	1.3×10^{-3}
Pcf	Instructions have standard and unambiguous wordings.	a	Neg.	-	-
Pcg	The procedure contains more than one condition which is not automated. Contains "and" and "or" logics that are automated and the scenario is practiced.	e	3.0×10^{-4}	1.43×10^{-1} **	4.29×10^{-5}
Pch	It is assumed that operators believe in the adequacy of the procedures.	a	Neg.		

* Because the STA performs the safety function status check, recovery of Pcd and Pcg is credited with moderate dependency. ** The steam generator level affects temperature and pressure control on the primary side, so it can be checked by other operators. Neg. means that the HEP is negligible.

6. Discussion and Conclusions

Although NPPs with advanced MCRs have recently begun operation, nuclear regulatory agencies are yet to approve a novel HRA method that realistically estimates HEPs based on the new and unique qualities of advanced MCRs. This proposed MCBDT serves as a bridge to resolve this issue because this approach can easily gain the confidence of regulators. The development of this MCBDT method has been extensively described in Sections 3 and 4 of this manuscript. More so, results obtained from the application examples in Section 5 show that the derived HEPs are within reasonable limits and in line with HRA good practice guides [27].

As the automation of procedure logic highly depends on the logic designer, we assumed that only primary-level logic is implemented in the analyzed HFEs. This means that when there is a secondary-level logic (a logic within another logic), we assume that it is not automated. In the case in which both primary and secondary-level logic is automated, the proposed MCBDT method is still applicable. This allows flexibility such that multiple scenarios of logic automation can be analyzed. Although recovery and dependency have been applied in some application examples (in Section 5), we have excluded the details because the rules applied do not differ from those of the current CBDT, which may be found in the reference [16]. While we have assumed in the analysis of the HFEs (in Section 5) that the operators have adequate training in the use of CPS, maintaining operator proficiency in the use of paper-based procedures (the backup procedures) may be challenging. Therefore, in case of failure of the CPS, the HEP will be higher because of the PSF that reflects a lack of adequate training, and thus, the lower branch for "Practiced scenario" on the Pcg tree should be used. Moreover, the failure of CPS is beyond the purview of HRA and should be modeled separately in the probabilistic safety assessment model.

In this work, numerous PSFs used in the current CBDT have been assessed to be relevant in advanced MCRs. However, because the types of systems are different compared with conventional MCRs, the HEP values currently associated with such PSFs may not be sufficiently accurate and can be improved. The HuREX database also includes HEPs derivable from APRMCR and is believed to allow HEP estimation and PSF correlation

for generic task types as well as new task types. However, correlating the APRMCR task types derived in this work with the HuREX taxonomy proved to be challenging. Similar to the CBDT method, the MCBDT method is not meant to be used in isolation but will be a complement to other methods based on empirical data from full-scale advanced NPP simulators. Hence, MCBDT can be used when the relevant empirical data are deemed to be overly optimistic, limited, or unavailable.

In conclusion, we developed a systematic technique to adapt the current CBDT method for use in HFE analysis in advanced MCRs using MCBDT. The reference advanced MCR used for this analysis is the APRMCR designed in Korea. The MCBDT was derived by appropriate task analysis, modification of HEPs, and modification of analysis questions, where necessary. In future research in this area, an empirical study can be performed to derive specific HEPs for operator tasks in advanced MCRs such that they are directly applicable to all the error modes and PSFs used in the MCBDT method. The recovery potential of operators in advanced MCRs has increased in a few ways compared to conventional MCRs. Hence, details regarding how this affects HEP quantification would be treated in future studies.

Author Contributions: Conceptualization, A.M.A. and J.K.; methodology, A.M.A.; software, A.M.A.; validation, A.M.A. and G.P.; formal analysis, A.M.A.; investigation, A.M.A.; resources, J.K.; data curation, G.P.; writing—original draft preparation, A.M.A.; writing—review and editing, A.M.A.; visualization, A.M.A.; supervision, J.K.; project administration, J.K.; funding acquisition, J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Multi-Unit Risk Research Group (MURRG), Republic of Korea, grant number 1705001.

Acknowledgments: This work was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KOFONS) and granted financial resources by the Multi-Unit Risk Research Group (MURRG), Republic of Korea (No. 1705001).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

ADVALS	Advanced alarm system
APRMCR	APR1400 MCR
CBDT	Cause-based decision tree
CPS	Computerized procedure system
EF	Error factor
EOPs	Emergency operation procedure
HIS	Human–system interface
HRA	Human reliability analysis
HEP	Human error probability
HFE	Human failure event
IDS	Information display system
MCR	Main control room
MCBDT	Modified CBDT
NPP	Nuclear power plant
PSF	Performance shaping factor
RCP	Reactor coolant pump
RCS	Reactor coolant system
SPTA	Standard post-trip action
STA	Shift technical adviser
THERP	Technique for human error rate prediction

References

1. Dirksen, G.; Eisinger, A. A comparison of conventional and computerized HMI in main control rooms from a human reliability standpoint. In Proceedings of the PSAM Top Conf Hum Reliab Quant Hum Factors, Risk Manag, Munich, Germany, 7–9 June 2017; pp. 7–9.
2. Ha, J.S.; Seong, P.H.; Lee, M.S.; Hong, J.H. Development of human performance measures for human factors validation in the advanced MCR of APR-1400. *IEEE Trans. Nucl. Sci.* **2007**, *54*, 2687–2700.
3. Schulz, T.L. Westinghouse AP1000 advanced passive plant. *Nucl. Eng. Des.* **2006**, *236*, 1547–1557. [CrossRef]
4. Twilley, R.C. EPR development—An evolutionary design process. *Nucl. News* **2004**, *47*, 26–30.
5. Kim, I.S. Computerized systems for on-line management of failures: A state-of-the-art discussion of alarm systems and diagnostic systems applied in the nuclear industry. *Reliab. Eng. Syst. Saf.* **1994**, *44*, 279–295. [CrossRef]
6. Roth, E.; O'Hara, J. *Integrating Digital and Conventional Human-System Interfaces: Lessons Learned from Lessons Learned from a Control Room Modernization Program*; Division of Systems Analysis and Regulatory Effectiveness, Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission: Washington, DC, USA, 2002.
7. O'Hara, J.M.; Brown, W.S. *The Effects of Interface Management Tasks on Crew Performance and Safety in Complex, Computer-Based Systems*; Overview and Main Findings, Nureg/Cr-6690; Division of Systems Analysis and Regulatory Effectiveness, Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission: Washington, DC, USA, 2002; p. 1.
8. Kaarstadt, M.; Strand, S. *Work Practices: Field Study of Challenges and Opportunities in a Computer-Based Nuclear Power Plant Control Room. (HWR-953)*; OECD Halden Reactor Project: Halden, Norway, 2010.
9. Liu, P.; Li, Z. Comparison between conventional and digital nuclear power plant main control rooms: A task complexity perspective, part I: Overall results and analysis. *Int. J. Ind. Ergon.* **2016**, *51*, 2–9.
10. Porthin, M.; Kling, T.; Liinasuo, M. New Challenges for Performance Shaping Factors in Advanced Control Rooms. In Proceedings of the PSAM Top. Conf. Hum. Reliab. Quant. Hum. Factors, Risk Manag, Munich, Germany, 7–9 June 2017.
11. Stubler, W.F.; O'Hara, J.M.; Kramer, J. *Soft Controls: Technical Basis and Human Factors Review Guidance*; Brookhaven National Laboratory: Upton, NY, USA, 2000.
12. Xing, J.; Parry, G.W.; Presley, M.; Forester, J.A.; Hendrickson, S.; Dang, V. An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal Events At-Power Application, Nureg-2199. 2017; Volume 1. Available online: https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr2199/index.html (accessed on 2 October 2020).
13. Kim, J. *The HuRECA-Based Human Reliability Analysis Procedure for Computer-Based Control Room Actions*; Korea Atomic Energy Research Institute: Daejon, Korea, 2012.
14. Kim, Y.; Kim, J.; Park, J.; Choi, S.Y. *An HRA Method for Digital Main Control Rooms—Part I: Estimating the Failure Probability of Timely Performance*; Korea Atomic Energy Research Institute: Daejon, Korea, 2019.
15. Jang, I.; Jung, W.; Seong, P.H. Human error and the associated recovery probabilities for soft control being used in the advanced MCRs of NPPs. *Ann. Nucl. Energy* **2016**, *87*, 290–298.
16. Parry, G.W. *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment*; Electric Power Research Institute: Palo Alto, CA, USA, 1992.
17. Kim, D.Y.; Kim, J. How does a change in the control room design affect diagnostic strategies in nuclear power plants? *J. Nucl. Sci. Technol.* **2014**, *51*, 1288–1310. [CrossRef]
18. Hong, J.H.; Lee, M.S.; Hwang, D.H. Computerized procedure system for the APR1400 simulator. *Nucl. Eng. Des.* **2009**, *239*, 3092–3104. [CrossRef]
19. Stanton, N.A.; Baber, C. Validating task analysis for error identification: Reliability and validity of a human error prediction technique. *Ergonomics* **2005**, *48*, 1097–1113. [CrossRef]
20. Barnes, M.J.; Bley, D.; Cooper, S. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*; Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission: Washington, DC, USA, 2000.
21. Forester, J.; Kolaczkowski, A.; Cooper, S.; Bley, D.; Lois, E. *ATHEANA User's Guide Final Report*; Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission: Washington, DC, USA, 2007.
22. Kim, Y.; Kim, J.; Park, J.; Choi, S.; Kim, H. *An HRA Method for Digital Main Control Rooms—Part II: Estimating the Failure Probability Due to Cognitive Error*; Korea Atomic Energy Research Institute: Daejon, Korea, 2020.
23. Swain, A.D.; Guttmann, H.E. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications-Final Report*; Sandia National Labs.: Albuquerque, NM, USA, 1983.
24. Arigi, A.M.; Park, J.; Lim, H.K.; Kim, J. Analysis of human-induced initiating events in a multi-unit loss of offsite power scenario. *J. Nucl. Sci. Technol.* **2020**, *57*, 121–132. [CrossRef]
25. Kim, Y.; Park, J.; Kim, H.E.; Shin, S.K.; Presley, M. Quantifying PSF Effects on Human Reliability in Digital Control Rooms based on Simulation Records. In Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, Venice, Italy, 1–5 November 2020; Research Publishing: Singapore, 2020; p. 2547. [CrossRef]
26. Kim, Y.; Park, J.; Jung, W.; Jang, I.; Hyun Seong, P. A statistical approach to estimating effects of performance shaping factors on human error probabilities of soft controls. *Reliab. Eng. Syst. Saf.* **2015**, *142*, 378–387.
27. Kolaczkowski, A.; Forester, J.; Lois, E.; Cooper, S. *Good Practices for Implementing Human Reliability Analysis (HRA)*; Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission: Washington, DC, USA, 2005.