Nuclear Engineering and Technology 54 (2022) 2453–2466

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Concept of an intelligent operator support system for initial emergency responses in nuclear power plants

Jung Sung Kang, Seung Jun Lee*

Department of Nuclear Engineering, Ulsan National Institute of Science and Technology, 50, UNIST-gil, Ulsan, 44919, Republic of Korea

ARTICLE INFO

Article history:
Received 15 October 2021
Received in revised form
30 January 2022
Accepted 9 February 2022
Available online 10 February 2022

Keywords:
Operator support system
Computerized procedure system
Emergency operation
Multilevel flow modeling
Nuclear power plant

ABSTRACT

Nuclear power plant operators in the main control room are exposed to stressful conditions in emergency situations as immediate and appropriate mitigations are required. While emergency operating procedures (EOPs) provide operators with the appropriate tasks and diagnostic guidelines, EOPs have static properties that make it difficult to reflect the dynamic changes of the plant. Due to this static nature, operator workloads increase because unrelated information must be screened out and numerous displays must be checked to obtain the plant status. Generally, excessive workloads should be reduced because they can lead to human errors that may adversely affect nuclear power plant safety. This paper presents a framework for an operator support system that can substitute the initial responses of the EOPs, or in other words the immediate actions and diagnostic procedures, in the early stages of an emergency. The system assists operators in emergency operations as follows: performing the monitoring tasks in parallel, identifying current risk and latent risk causality, diagnosing the accident, and displaying all information intuitively with a master logic diagram. The risk causalities are analyzed with a functional modeling methodology called multilevel flow modeling. This system is expected to reduce workloads and the time for performing initial emergency response procedures.

1. Introduction

1.1. Background

Nuclear power plant (NPP) operators manage the plant from the main control room (MCR), where they gather information through human–machine interfaces (HMIs) in order to follow the operating procedures. To cope with design basis accidents, NPPs have many mitigation systems consisting of myriad sensors and devices. In an emergency, operators must figure out the correlation between a large number of devices and sensors and mitigate the accident simultaneously, creating highly stressful conditions for operators in emergency situations. In such cases, operators follow emergency operating procedures (EOPs) based on information gathered from the HMI systems to appropriately mitigate the accident. Human errors in emergency situations with such stressful conditions can lead to a severe accident. According to one probabilistic safety assessment (PSA) of the Korean reference plant, human error events are a major factor in core damage frequency, accounting for 44% [1]. The 1979 Three Mile Island Unit 2 (TMI-2) accident provides an example of human error leading to a severe accident due to inadequate procedures and HMI layout [2]. After the TMI-2 incident, many HMI designs and operator support systems to reduce human errors have been developed. These facts demonstrate how important a factor human error is in NPP safety, and that HMIs and procedures with appropriate designs are still needed to reduce human error.

Recently, MCRs have been updated from analog to digitalized types with the progression in computer technology [3,4]. In digital MCRs, large display panels (LDPs) show the overall plant status and alarms [5,6], while each operator has their own workstation and safety consoles [6]. The operators do not have to move around to view indicators or use control devices. Following the digitalization of the instrumentation and control (I&C) systems [7] and MCR, the procedures themselves have also shifted from paper-based procedures (PBPs) to computer-based procedures (CBPs). Although PBPs have demonstrated a good safety record through the safe operation of commercial reactors for decades, they have been identified as a latent cause of human error [8]. The main limitation of PBPs is their static characteristics, in contrast to the dynamic characteristics of the operation environment. In other words, PBPs

* Corresponding author.
E-mail address: sjlee420@unist.ac.kr (S.J. Lee).

https://doi.org/10.1016/j.net.2022.02.010

are necessarily designed to cover wide ranges of multiple potential scenarios, which requires operators to check a large amount of data to find the relevant information [8]. Excessive amounts of information increase the operators' workload and its complexity, which may lead to human error. The computerized procedure system (CPS) of the APR1400, an NPP with a digital MCR in the Republic of Korea, has been developed to prevent this excess of information and to assist operators in their ability to conduct their tasks [9]. However, since the CPS was also developed based on PBPs, it remains difficult for the dynamic changes of the plant environment to be fully reflected.

In the new digital MCR environment, software-based operator support systems can be easily adapted, with the application of appropriate operator support systems expected to enhance NPP safety. For this, various operator support systems are being developed. For example, based on a human cognitive model, INDESCO (integrated decision support systems to aid the cognitive activities of operators) has been proposed, consisting of display systems, fault diagnosis systems, CPSs, and operation validation systems [5]. A procedure compliance check (PCC) system that utilizes deep learning algorithms to monitor procedural mistakes has also been proposed [10]. In the case of the computerized operator support system (COSS) proposed by the Idaho National Laboratory, faults are detected and diagnosed early, and CBPs are utilized to advise the appropriate mitigation strategies. Because these systems are all built on existing conventional procedures, they still have limitations in terms of the static characteristics inherent in the procedures.

1.2. Objective

Many computerized operator support systems have been developed and applied for normal, abnormal, and emergency operation [11]. Among these operation modes, emergency operation situations create a dynamic operation environment because operators are under a heavy workload and the plant parameters change rapidly. In particular, certain initial operations in an emergency situation are performed prior to diagnosing the accident, and therefore they require fast performance times of operators.

The system presented in this paper, called the emergency guidance intelligent system (EGIS), is a new concept of an operator support system that can be used in place of the initial operations in EOPs. The purpose of the system is to identify dynamic information about the NPP and provide information to operators in an appropriate form during emergency operations. The EGIS has three major objectives. The first is *agile operation*, where the system reduces the time required for the initial responses through surveillance automation and parallel performance. The second objective is *dynamic operation*, where the system distinguishes current and latent risk in accordance with urgency and importance. Because the system checks the plant status in real time and provides operators with the necessary tasks, it is easy to reflect the dynamic environment of the plant. The last is *intuitive operation*, where EGIS collects dynamic information about the plant and selectively provides only the necessary information, excluding information unrelated to the required initial responses; in other words, it can reduce the workload of operators by preventing the over-transmission of information. In conveying this information to operators, a functional modeling master logic diagram allows operators to recognize information about the plant conditions quickly and intuitively.

To examine the applicability of this system, the early stages of an EOP, or the immediate actions and diagnostic procedures, were selected as a target scope (i.e., not the entire EOP). Section 2 provides a brief overview of the EOP process and its relation to the proposed system. Section 3 details the EGIS framework development, including its parameter inspector, procedure logic module, risk evaluator, and interface. Section 4 presents the results of a case study considering four scenarios to verify the performance of the proposed system. Section 5 discusses the results, and Section 6 concludes the work.

2. Emergency operating procedures

EOPs are designed to provide a basis for appropriate responses to emergency events, and therefore EOPs play an important role in securing the defense in depth concept in NPPs [12]. An EOP is largely divided into event-based procedures and symptom/state-based procedures. Before the TMI-2 accident, EOPs consisted of only event-based procedures. This type has an advantage in that the procedures can be used to effectively cope with predicted accidents. However, it is difficult to cope with contingencies using only event-based procedures, so they are currently being used in combination with symptom-based procedures. In this paper, the EGIS support system is developed based on the early stage of the EOPs. Although the procedure format varies slightly depending on the reactor type, the key elements of EOPs generally contain four key elements: immediate actions and diagnostic procedures, event related symptom based optimal recovery guidelines (ORGs), critical safety function (CSF) restoration guidelines, and CSF status trees [12]. The EOPs used in the APR1400 and the Westinghouse 3-loop pressurized water reactor (PWR), which are considered in this work for methodology development and test environment and test environment (see section 3.1 and 3.2), have these similar types of elements.

In the case of the APR1400, an emergency initiates the following progression. When the reactor is tripped, the standard post trip action (SPTA) procedure acts as the entry point. In this procedure, the operators respond to the accident by securing the CSFs. The goal of the SPTA is not to satisfy all CSF conditions, but to treat the most severe CSFs in the initial responses to the emergency. After the SPTA, operators diagnose the type of accident by following the diagnostic action (DA) procedure. The SPTA and DA procedure play the role of the immediate actions and diagnostic procedure aspect of all EOPs. The DA procedure has a flowchart structure to check the status of the plant. If the symptoms match a specific event, the operators move to the relevant optimized recovery procedure (ORP). The ORP is a procedure in the same position as ORG. After entering an ORP, the shift technical advisor checks the CSFs every 15 min. If the criteria of any CSF are not satisfied, the operators enter the DA procedure again and move to the relevant functional recovery procedure (FRP). In the other possible case, when the symptoms do not match a specific event, FRPs are conducted directly in order of highest priority. Here, the FRPs play a similar role as the CSF restoration guidelines. Otherwise, the EOP of a Westinghouse consists of Emergency-N procedures (E-1, E-2, E-3, …), and sub-procedure-N procedures (S-1, S-2, S-3, …). The E-1 procedure plays the role of the immediate actions and diagnostic procedures, while other E-N Procedures such as E-2 and E-3 correspond to the ORGs and the sub-procedures have the same goal as the CSF restoration guidelines. The overall process the relationships described above can be seen in Fig. 1 below.

The system developed in this paper considers the early emergency responses, or in other words, it targets the immediate actions and diagnostic procedures embedded in the system. As mentioned above, as most of the tasks involved in the immediate actions are deeply related with the CSFs, the proposed system was also developed based on CSFs. The early emergency operations were selected as a first step in confirming the overall applicability of automated emergency operations; moreover, in contrast to the more complex ORPs or FRPs, the tasks required in the early stages

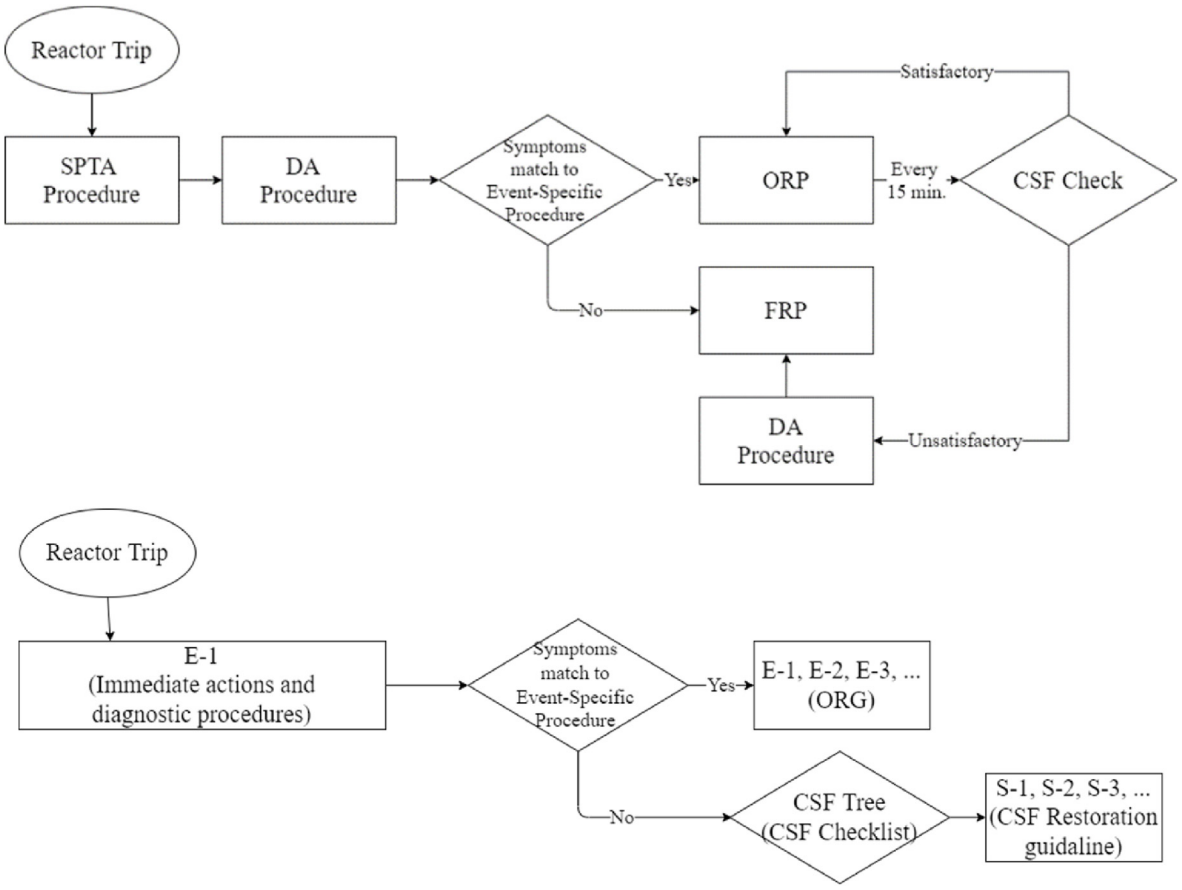

Fig. 1. General structure of the EOP system in the APR1400 (upper) and Westinghouse (Lower) reactors.

are performed relatively simply and quickly, which facilitates an easier initial review of the system's applicability.

It should be noted here that EGIS was developed in consideration of the general emergency initial operation procedure environment. It is a system aimed at replacing the immediate actions and diagnostic procedures among the EOPs and providing additional causality information not previously provided in the procedures. To validate the system, the real-time plant simulator environment is required. The development environment of EGIS is a compact nuclear simulator (CNS) developed by the Korean Atomic Energy Research Institute (KAERI) [13–15]. The CNS modeled the Westinghouse 3-loop PWR, which is a commercial reactor used in the Republic of Korea, with 993MWe output power [14]. As mentioned in above, the Westinghouse PWR EOPs consist of emergency procedures such as E-1, E-2, and E-3, as well as subprocedures such as S-1, S-2, and S-3. EGIS targeted E-1, which is the immediate actions and diagnostic process.

3. Development of EGIS

3.1. Framework

The EGIS was developed to achieve agile, dynamic, and intuitive operation; Fig. 2 illustrates its architecture. As previously mentioned, the system covers the immediate actions and diagnostics procedures. For the immediate actions procedure, the key parameters are first identified by analyzing the procedure and associated auxiliary systems. The related system information and the limits of these parameters are stored in the plant parameter database. Based on this information, the parameter inspector function, which provides parallel surveillance to reduce operation time, determines whether operator action is necessary or not. If action is deemed necessary, a list of the abnormal parameters is forwarded to the risk evaluator and the procedure logic modules. With this list, the procedure logic module provides the appropriate tasks from the procedural tasks contained in the procedure database, and the risk evaluators analyze the cause and effect of the failures. The procedure logic module, implementing the if-then-else logic of the immediate actions procedures, identifies the parameters passed through the parameter inspector and the entry conditions of the immediate actions procedures. It then provides the necessary tasks from the information to the operators. The risk evaluators are categorized by the different CSFs of the plant because each CSF has a different structure and failure propagation. The six considered CSFs in this development are as follows: subcriticality, core cooling, heat sink, reactor coolant system (RCS) integrity, containment integrity, and RCS inventory. These CSFs are the CSFs corresponding to CNS. Each CSF risk evaluator is composed of current and latent risk evaluators; the former analyzes the causality of the safety-critical parameters specified in the immediate action procedure, while the latter analyzes the causality of the parameters related to the auxiliary systems that the operator needs to be aware of but that do not require immediate action. The risk evaluators set failure as the trigger, perform fault prognosis by using multilevel flow modeling (MFM), and extract the causality sequence. The detailed process is addressed in Section 3.3. In summary, the procedure logic module provides only the tasks in the procedure that the operator is required to conduct, and the risk

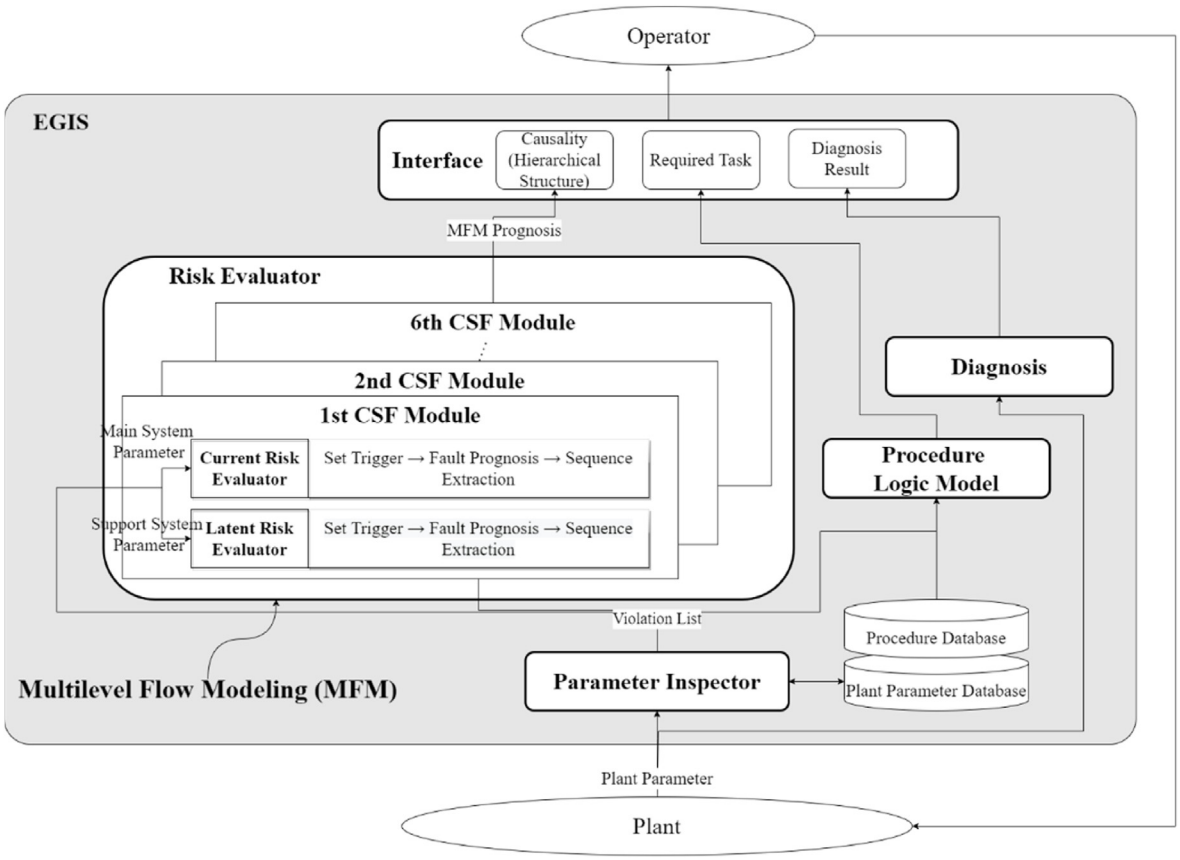

Fig. 2. The architecture of EGIS.

evaluators provide causal information about the failures that have been identified.

In Fig. 3, the roles of each module are compared to existing procedures. For the risk evaluator module, the corresponding SPTA+DA and E-1 item is dashed because it does not provide auxiliary information (cause-related, auxiliary system information). In the case of the Westinghouse reactor, since it does not provide a detailed diagnostic flowchart like APR1400, the knowledge of the operator is required. In addition to replacing existing procedures, EGIS also serves to assist the cognitive processes in which operators perform their duties. Table 1 provides a comparison between the immediate actions procedure and EGIS in terms of human cognitive processes.

Concurrently with the performance of the immediate actions procedure, the diagnosis module in EGIS performs the diagnostic procedure by utilizing an artificial intelligence model and provides

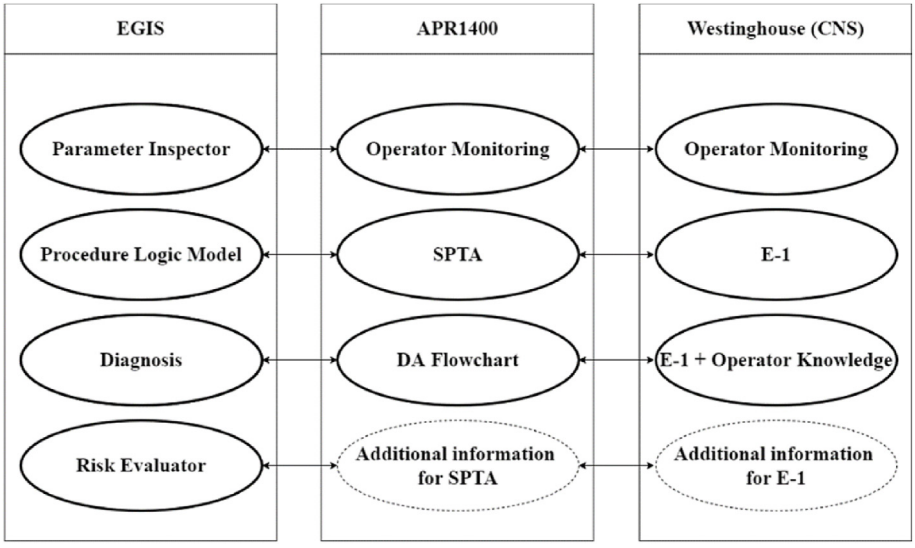

Fig. 3. Role comparison between EGIS and the EOPs of the two reactor types.

Table 1
Comparison of the immediate actions procedure and EGIS in terms of cognitive processes.

	Cognitive Process	the immediate actions procedure	EGIS
1	Monitoring/ Detection	Operators sequentially conduct all monitoring tasks.	The parameter inspector module monitors the plant status in parallel and provides only the parameters requiring a response to the operators.
2	Situation Assessment	Operators diagnose faults using procedural information and operator knowledge.	Operators diagnose faults using procedural information and operator knowledge. Fault causality from the risk evaluator modules is additionally provided.
3	Response Planning	Operators check the logic of the procedural steps and select the necessary tasks.	The procedure logic module identifies the required tasks with if-then-else logic and provides them to the operators.
4	Response Implementation	Operators perform the necessary tasks via HMIs.	Operators perform the necessary tasks via HMIs.

operators with the appropriate procedure that matches the diagnostic results. Choi and Lee developed such a model that performs diagnosis using a gated recurrent unit (GRU), a type of artificial intelligence model structured into the developed recurrent neural network model to learn the serial context, and demonstrated a high level of diagnostic accuracy [16]. Because NPP data is serial, GRUs have been employed for fault diagnosis and abnormal diagnosis in addition to accident diagnosis [17,18]. The previously developed autonomous diagnostic model based on GRU is inserted into the diagnostic module of EGIS; more details about the function of the employed model can be found in Ref. [16].

Finally, the interface receives the required tasks, causality, and diagnosis result from the three modules of EGIS (procedure logic module, risk evaluators, and diagnosis module, respectively) and provides this information to the operator in the appropriate form. Further details about the key elements of EGIS are given in the following sections.

3.2. Parameter inspector and procedure logic modules

The immediate actions procedure consists of if-then-else syntaxes, so it can be easily modeled with rule-based logic. In particular, in the early stages of emergency situations, the characteristics of the initial responses are relatively simple compared to those of the more complex responses of later stages, making a rule-based model easier to apply to this limited condition. The E-1 procedure was first analyzed to figure out which components and instruments are required to be included in the parameter database and covered by the parameter inspector. Table 2 lists the analyzed parameters corresponding to CSF6, which is RCS Inventory, as an example. For all CSFs, the parameter inspector compares the parameter information with the real state of the plant. Parameters that exceed their set points are passed to the procedure logic module and relevant risk evaluator, with information about which particular component, system, and CSF they belong to.

The purpose of the procedure logic module is to check the procedure tasks based on the abnormal parameters and provide only the necessary tasks to the operator. As an example of this operation, Fig. 4 shows a comparison between the original form of the procedure for a key E-1 procedure task, the reactor coolant pump stop task, and the procedure logic module for the same task. The reactor coolant pump shutdown task requires two conditions: at least one of the safety injection pumps is still operating, and the pressurizer pressure is lower than 97 kg/cm^2. The parameters KCHGP1,2,3 refer to the statuses of the safety injection pumps (open/close), and ZINST65 refers to the pressurizer pressure in the CNS. Like this, the procedure logic module provides the operator with the necessary tasks of the E-1 procedure in a rule-based manner.

3.3. Risk evaluator

As described above, the risk evaluators aim to conduct causal analyses of the anomalies that are identified by the parameter inspector in real time. Based on the E-1 procedure, the parameter inspector monitors the components and provides a list of abnormal parameters. From this list, each risk evaluator sets the anomalies as a trigger and performs a prognosis using MFM. One of the functional modeling techniques, MFM is a methodology for qualitative reasoning, in which the concepts of means-end and whole-part decomposition and aggregation are important aspects [19]. This methodology represents a component as a function and mimics the correlations among components and systems, where each function and correlation is linked to a goal. MFM is usually represented by a flow system with mass and energy flow; its typical symbols are shown in Fig. 5.

The purpose of MFM is not to model simple systems but rather to optimize methodologies for grouping complex systems and functions. Included in IAEA's classification of modeling technology (2008) as one of the nuclear power plant modeling techniques [20]. MFM has been used in various studies including nuclear power plant diagnosis and risk analysis, with examples as follows. Lind and Zhang presented an application for diagnosis in nuclear power plants with large-scale systems (PWR, fast breeder reactor) [21]. While another study proposed a method of planning alternative countermeasures in a severe accident situation using MFM [22], namely several alternative plans for a boiling water reactor in a station blackout situation. Research has also been conducted in which MFM was applied to the APR+, similar to the APR1400; in the study, the MFM model was used to systematically filter thousands of scenarios that cause core damage in NPPs and identify any potential mitigation options [23].

As such, various studies have used MFM to model nuclear power plants for application in causal and consequence analysis. As described above, MFM is also used in EGIS as the risk evaluator. By implementing MFM, the systems and components are grouped according to the CSFs with the objectives connected, and similar to other MFM applications, consequence analyses are performed on failures. But unlike previous studies, in this case the consequence tree derived through the consequence analysis is utilized. The consequence tree allows one to track how a failure influenced an objective through what path. If the consequence tree can be processed to contain an appropriate level of information and be provided to the operator, it will help the operator identify the causality of the power plant problems.

An example MFM is given in Fig. 6 for the RCS inventory (CFS6). The bottom flow structure is simply modeled with the safety injection coolant mass flow structure (bottom left) and the electric energy flow structure (bottom right). The middle flow structure is modeled with the RCS mass flow structure, and the top is modeled

Table 2
CSF6 (RCS inventory) parameters in the parameter database.

COMP	TYPE	SYSTEM	HMI	FUNCTION	VALUE
PRZ PRESSURE	SIGNAL	SIAS	RCS	6	126.59
CTMT PRESSURE	SIGNAL	SIAS	RHR	6	0.3515
SG#1 PRESSURE	SIGNAL	SIAS	RCS	6	41.1
SG#2 PRESSURE	SIGNAL	SIAS	RCS	6	41.1
SG#3 PRESSURE	SIGNAL	SIAS	RCS	6	41.1
SI SIGNAL	SIGNAL	SIAS	REACT CONT	6	1
CHRGP1	PUMP	HPSI	RHR	6	1
CHRGP2	PUMP	HPSI	RHR	6	1
CHRGP3	PUMP	HPSI	RHR	6	1
RHRP	VALVE	LPSI	RHR	6	1
ACCUM VALVE (HV39)	VALVE	ACCUM	RHR	6	1
RWST ISO VALVE (LV615)	VALVE	HPSI	RHR	6	1
SI ISO VALVE (HV22)	VALVE	HPSI	RHR	6	1
VCT ISO VALVE (LV616)	SIGNAL	SI	RHR	6	0
RHR HX TO RCS ISO VALVE (LV603)	VALVE	LPSI	RHR	6	1
RWST TO RHRP ISO VALVE (HV8)	VALVE	LPSI	RHR	6	1
HV22 FLOW	FLOW RATE	HPSI	RHR	6	
CL#1 SI FLOW	FLOW RATE	SI	N/A	6	
CL#2 SI FLOW	FLOW RATE	SI	N/A	6	
CL#3 SI FLOW	FLOW RATE	SI	N/A	6	
HL#1 SI FLOW	FLOW RATE	RAS	N/A	6	
HL#2 SI FLOW	FLOW RATE	RAS	N/A	6	
RWST TO CHP FLOW	FLOW RATE	HPSI	N/A	6	
RHR TO CL1 FLOW	FLOW RATE	LPSI	N/A	6	
RHR TO CL2 FLOW	FLOW RATE	LPSI	N/A	6	
RHR TO CL3 FLOW	FLOW RATE	LPSI	N/A	6	
RHR FLOW FROM RWST	FLOW RATE	LPSI	N/A	6	
RHR FLOW FROM SUMP	FLOW RATE	RAS	N/A	6	
RHR FLOW AT ECCS MODE	FLOW RATE	SI	N/A	6	150

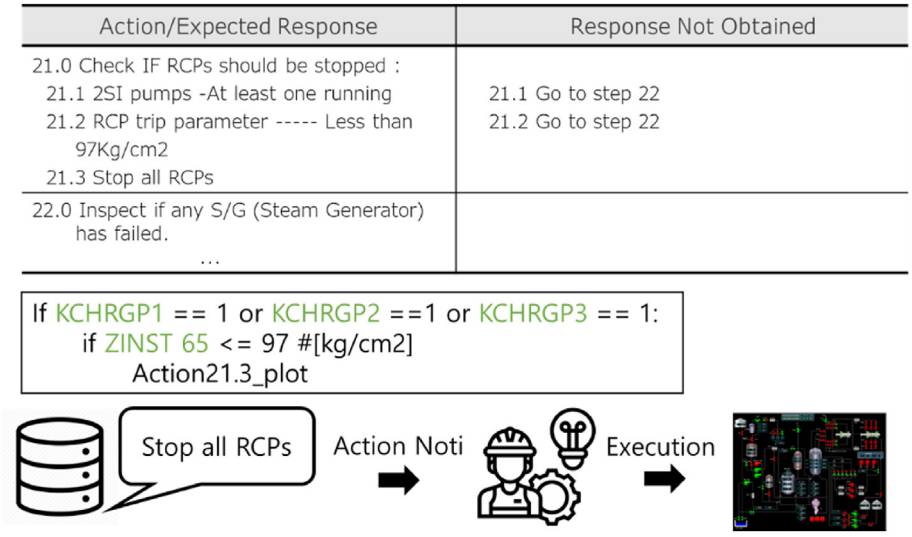

Fig. 4. Comparison of the E-1 procedure (upper) and procedure logic module (lower) for the RCP stop task.

with the heat energy flow structure that represents the heat exchange between the primary and secondary systems. A list of the abbreviations in Fig. 6 is given in Table 3.

Prognosis works in the following way. If the charging pump (CHP), which acts as a high-pressure safety injection (HPSI) pump, fails as shown in Fig. 7, the CHP state is set up as low (i.e., set the trigger). This trigger then propagates to the goal along with the flow structure. In Fig. 7, failure of the CHP (tra19, bottom) leads to a failure of the HPSI mass flow structure, which in turn affects the inventory of the reactor pressure vessel (sto8, RPV). This leads to the failure of the primary RCS mass flow structure, which affects the heat exchange (tra3) between the RPV and the steam generator, and ultimately leads to core cooling (obj1). Like this, MFM performs a prognosis of which system and which functionality is finally affected by the component failures identified in the risk evaluator.

The risk evaluator modules are classified into current risk and latent risk evaluators. The current risk evaluators, which derive from the E-1 procedure, require an immediate response from the operator. On the other hand, the latent risk evaluators target the support systems that help the frontline systems. The support system components that affect the safety systems but have a large available time are specifically targeted; for example, the component cooling water system (CCWS), backup electrical system (ES), and refueling water storage tank (RWST) only have an effect after a

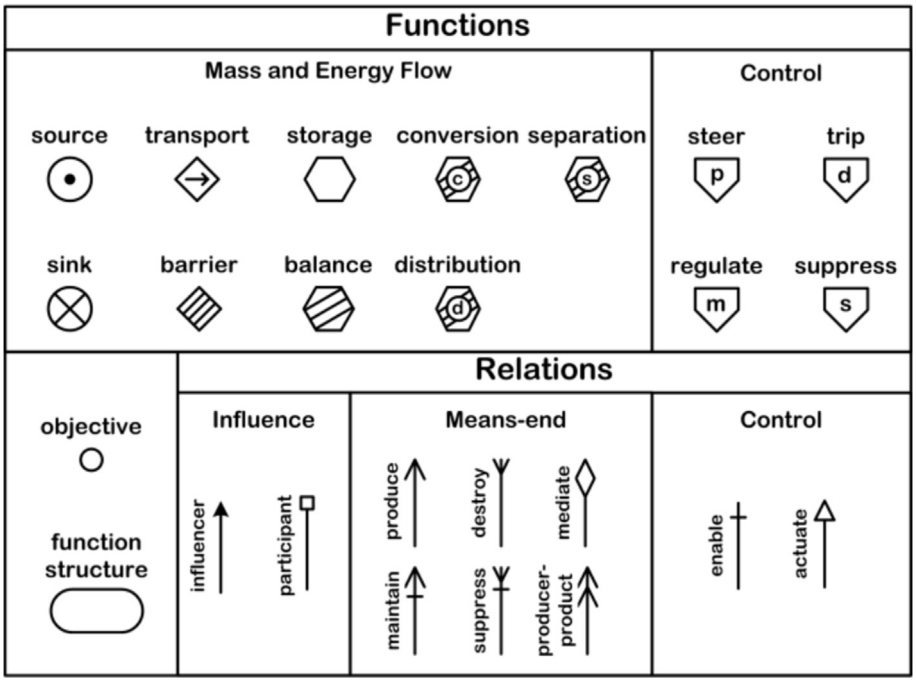

Fig. 5. Basic symbols used in MFM [19].

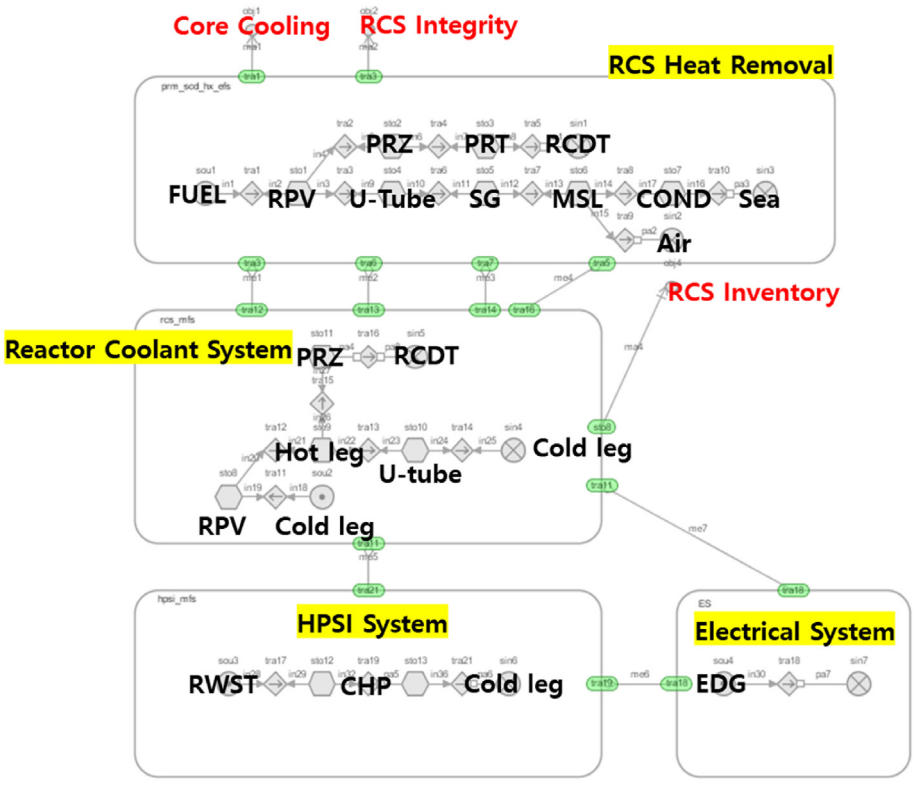

Fig. 6. MFM for RCS inventory (CSF6).

considerable amount of time. Since MFM is a flow logic with no concept of time, additional models are needed for latent risk. These models have the same structure as the current risk evaluators, but with different targets.

Notably, the current and latent risk evaluators are modeled based on the CSFs and work in parallel, in contrast to the existing E-1 procedure, in which CSF tasks are performed sequentially. As the EGIS performs the CSF-related surveillance tasks in parallel and provides operators with only the relevant information, the system can reduce the time spent performing the E-1 while also

Table 3
Abbreviations in the RCS inventory MFM model.

Abbreviation	Full name	Abbreviation	Full name
RCS	Reactor coolant system	MSL	Main steam line
PRZ	Pressurizer	COND	Condenser
PRT	Pressurizer relief tank	RWST	Refueling water storage tank
RCDT	Reactor coolant drain tank	CHP	Charging pump
RPV	Reactor pressure vessel	EDG	Emergency diesel generator
SG	Steam generator		

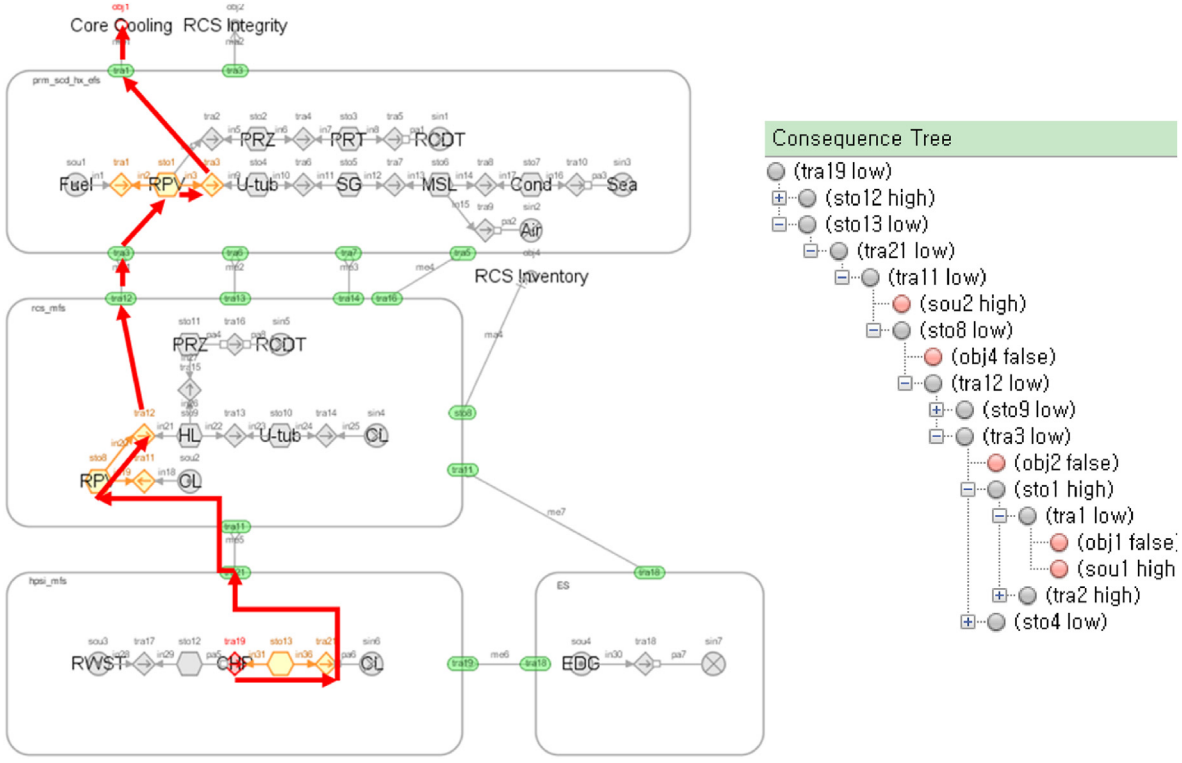

Fig. 7. CHP failure prognosis in MFM.

prioritizing the risk related to the abnormalities.

3.4. Interface

All the information provided by the procedure logic module, risk evaluators, and diagnosis module should ultimately be provided in a properly processed form to the operator. It should be noted that conventional LDPs are utilized in all operation modes and are therefore not optimized for emergency operation. In addition, only component and instrumentation information are provided, with the correlations between the components and instrumentation not identified. Such correlation information is indirectly verified using EOPs and operator knowledge. To address this, EGIS collects the dynamic plant state information and provides operators with the plant states through a hierarchical structure. This provides a more intuitive understanding than conventional procedures and helps to reduce operator workloads. Hierarchical structures can be easily constructed due to the characteristic features of MFM: means-end and whole-part. Plant correlations are modeled in MFM, consisting of the components and systems, which connect to sub-goals and main goals. These MFM models are then processed into master logic diagrams (MLDs), as shown in Fig. 8, allowing operators to see the overall status of the plant at a single glance. As the CSFs are a top priority, equating to safe NPP operation, the CSFs are placed at the top of the list, the sub-goals to maintain the CSFs are placed directly underneath it, and the related systems are placed at the bottom. The interface thus provides functional-oriented information to the operator rather than device-oriented information. The advantages of providing functional-driven information are to quickly identify the situation and prevent excessive information provision to the operator. In the case operators want more detailed information, they may simply click the system button, which shows information about the devices and auxiliary systems that belong to the lower part of the system and provides the tasks needed in the system.

As can be seen in Fig. 9, there are five main blocks in the EGIS interface. The upper left corner is the plant function-system overview, a hierarchical MLD that provides a quick view of the state of the plant. It consists of the major systems with main goals and sub-goals while omitting the detailed components. Systems appear in rectangles while the goals appear in circles. If a failure occurs in a system and action is required, the color of the system button will change and the border will flash red. At this point, when the operator clicks the button, a detailed window of the system pops up and displays the necessary actions. The bottom left is an overall task panel that allows operators to identify the required tasks. The

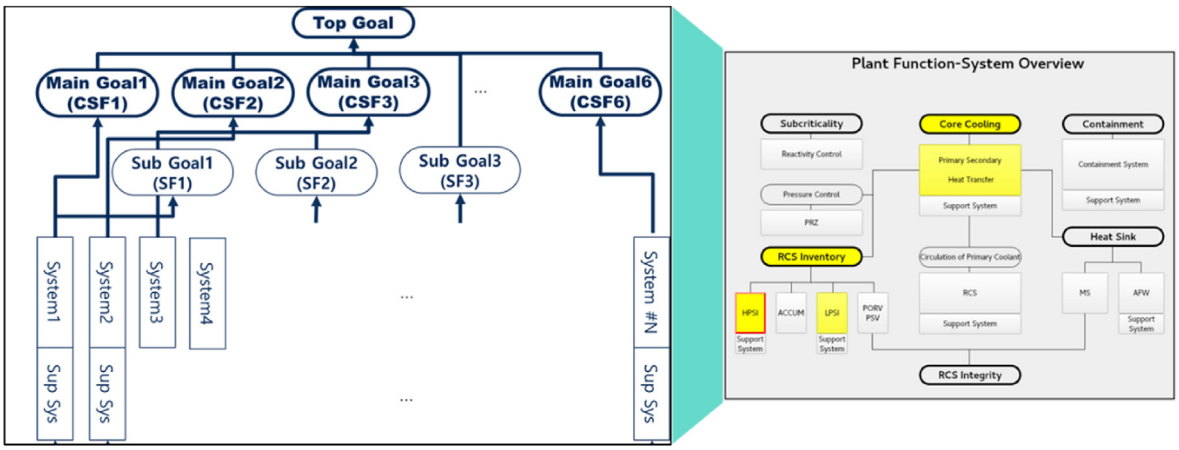

Fig. 8. MLD development process.

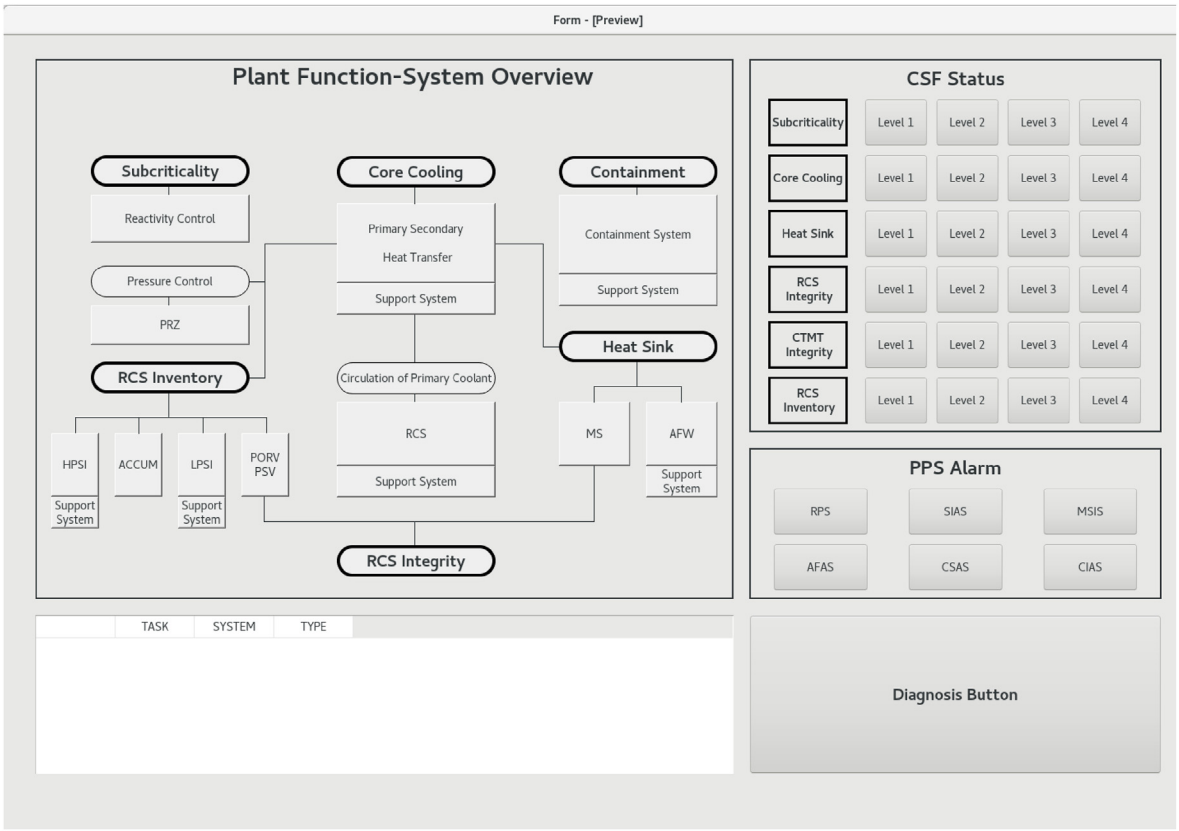

Fig. 9. EGIS interface.

blocks on the right are composed of the CSF statuses, necessary alarms (ESFAS alarm, and diagnostic buttons. The diagnostic buttons are disabled until the diagnosis is completed, after which they are activated with the appropriate EOP.

4. Case study

The EGIS was developed using a compact simulator, CNS. To verify its performance, four main types of test scenarios were considered, as shown in Table 4. The accident scenarios are divided into a single accident and a combination of an accident and failures. For the latter, three types of faults are combined with an accident: abnormalities in the automatic operation signals of the plant protection system (PPS), system failures that require immediate action (current risk), and system failures that require operator recognition (latent risk). The acronyms used in Table 4 are listed in Table 5.

The first scenario is a simple accident that is able to be mitigated with automated systems without additional operator response. In this situation, there is no additional action to be taken in the E-1 procedure, as most of the tasks are done via PPS. This leads to a rapid transition from the E-1 procedure to immediate diagnosis. As shown in Fig. 10, in the EGIS interface, there is no alarm in the plant function-system overview window, but the RCS Inventory CSF status changes to level 2 due to the loss of coolant accident (LOCA)

Table 4
Test scenario categories.

Scenario	Description	Example
1 Accident (No action required)	Auto diagnosis is performed immediately because no additional operation is required in EGIS.	LOCA, SGTR, ESDE
2 Accident + PPS Failure	The PPS is recovered manually or the PPS operating devices are operated manually. Diagnosis is performed after the completion of all tasks.	LOCA + SIAS failure, LOCA + CIAS failure
3 Accident + System Failure (current risk)	Problematic components are checked and the alternative components are manually operated. Diagnosis is performed after completion of all tasks.	LOCA + CHP failure, SGTR
4 Accident + System Failure (latent risk)	After checking problematic components, the tasks are performed or skipped following operator discretion. Diagnosis is performed after completion of all tasks.	LOCA + RWST level low, LOCA + CCWP failure

Table 5
Acronyms in the test scenario categories.

Abbreviation	Full name	Abbreviation	Full name
LOCA	Loss of Coolant Accident	PPS	Plant Protection System
SGTR	Steam Generator Tube Rupture	CCWP	Component Cooling Water Pump
ESDE	Excess Steam Dump Event		

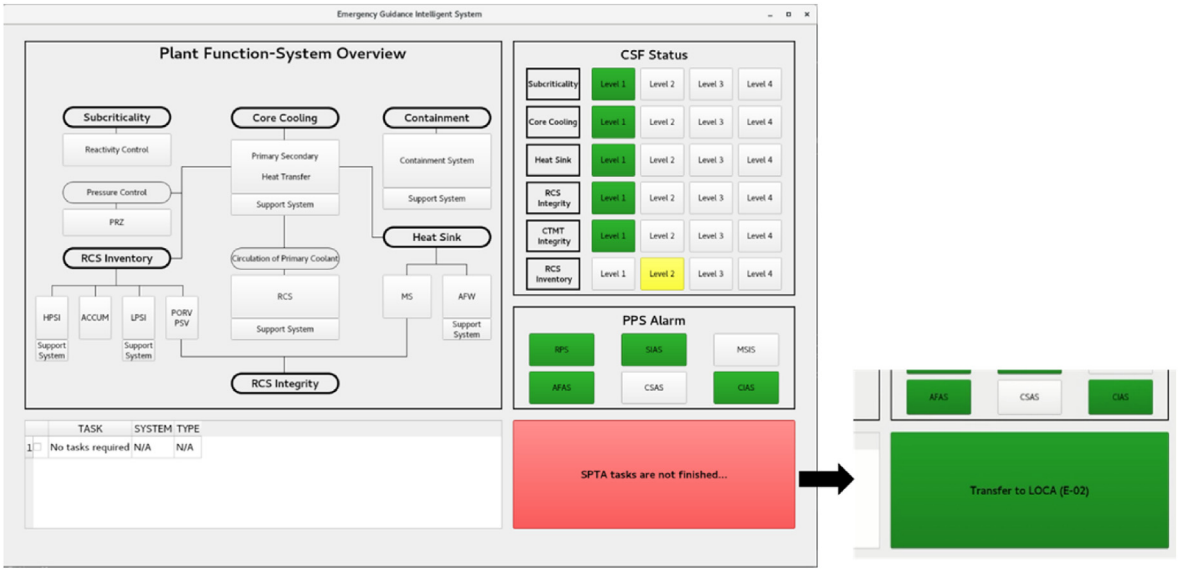

Fig. 10. EGIS test scenario 1 operation overview, 30 cm^2 LOCA.

malfunction. EGIS performs auto diagnosis because operators do not have to perform any responses. After the diagnosis is complete, the diagnosis result is displayed on the diagnostic button.

The second scenario is related with the PPS. As previously described, most of the E-1 procedure tasks are conducted through the PPS, and accordingly, monitoring the PPS is a major task in the E-1 procedure as important actions are made through automatic operation signals. Thus, in EGIS, the interface was designed to provide PPS monitoring in the ESFAS alarm window. In this scenario, a 30 cm^2 break LOCA occurs and the safety injection actuation signal (SIAS) is not automatically initiated, in which case the operator should activate the SIAS manually or operate the SIAS automatic operation devices. The failure types of SIAS can be classified into two categories, namely when a manual backup is possible and impossible through the HMI. Fig. 11 shows the case when the manual backup is possible. The HPSI and low-pressure safety injection (LPSI) system blocks turn yellow because the related systems are not appropriately aligned because of the SIAS failure. Additionally, the SIAS button flashes red in the ESFAS panel because there is a problem with the SIAS. When the operator clicks the SIAS button, the SIAS window pops up that allows the operator to check the SIAS automatic operating condition variables and manually activate the signal. When the SIAS is activated, all devices operate normally, and the plant status window alarms are disabled. Diagnosis is then performed automatically, and the diagnostic results are displayed on the diagnostic button. If the manual backup is not possible, recovery is performed using analog backup facilities in an actual power plant environment. Since there is no such facility in the experimental environment, recovery is performed by manually operating and arranging the devices that normally operate automatically for SIAS.

The third test scenario involves a LOCA with CHP failure event. The CHP is essential for safe injection as a HPSI pump. In this scenario, the standard flow rate of safety injection has failed due to the

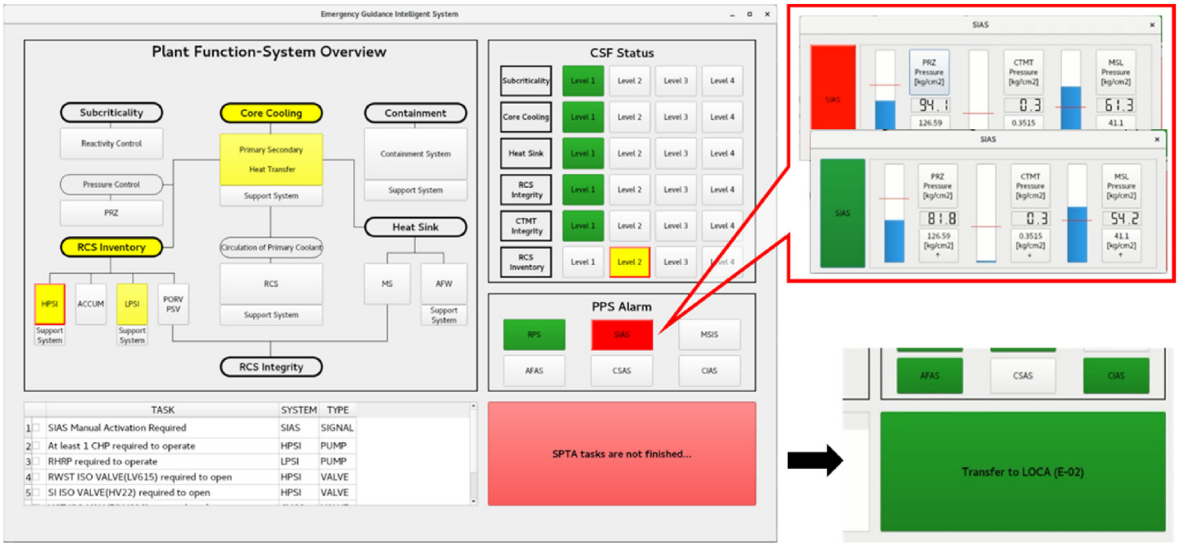

Fig. 11. EGIS test scenario 2 operation overview, 30 cm^2 LOCA + SIAS actuation failure.

failure of CHP #1. At least two CHPs must be operated to meet the safety injection flow rate, but in this case only one automatically operates due to the failure. In the existing E-1 procedure, numerous tasks appearing in the procedure must be sequentially checked before CHP operation. The EGIS, on the other hand, does not need to follow the same sequential progression because all surveillance tasks are performed simultaneously. EGIS starts when the reactor is tripped or meets the trip condition. All CSF surveillance tasks are performed simultaneously, and in this scenario, only the task related to CHP operation is alerted. The failure is passed to the MFM model, which performs prognosis. The prognosis results are displayed in the plant function-system overview panel, as shown in Fig. 12. Because of the CHP problem, the HPSI system block to which the CHP belongs changes color to yellow. This color change propagates the associated RCS Inventory, Primary Secondary Heat Transfer, and Core Cooling blocks. The operator then clicks on the flashing HPSI block at the bottom for a pop-up detailed status display for the HPSI. Through the HPSI status window, the operator confirms the failure of CHP #1 and starts CHP #3 manually. After the plant condition normalizes, the diagnosis module completes the diagnosis. The diagnostic results are displayed on the diagnostic button. When the operator clicks the button, EGIS opens the appropriate EOP and is terminated.

A fault with CHP #1 corresponds to an immediate hazard that must be identified with action taken in the existing E-1 procedure. Unlike the 3rd scenario considering such current risk, the 4th scenario is selected for latent risk. Latent risk refers to a situation in which the effects of a failure appear after some substantial amount of time. Hence, while immediate action by the operator is not necessary, required actions should be recognized in advance in the case of latent risk. In EGIS, the latent risk factors can also be identified in the MFM model. The 4th test scenario considers a situation with a low level of the refueling water storage tank (RWST). This tank is a coolant source for HPSI and LPSI. When the level of the RWST is less than 37.5%, the CNS automatically closes the RWST isolation valves (LV615, HV9) and the flow formation of the HPSI and LPSI stops. Since additional tasks should be done to reopen the isolated valves, being aware of this situation in advance can help

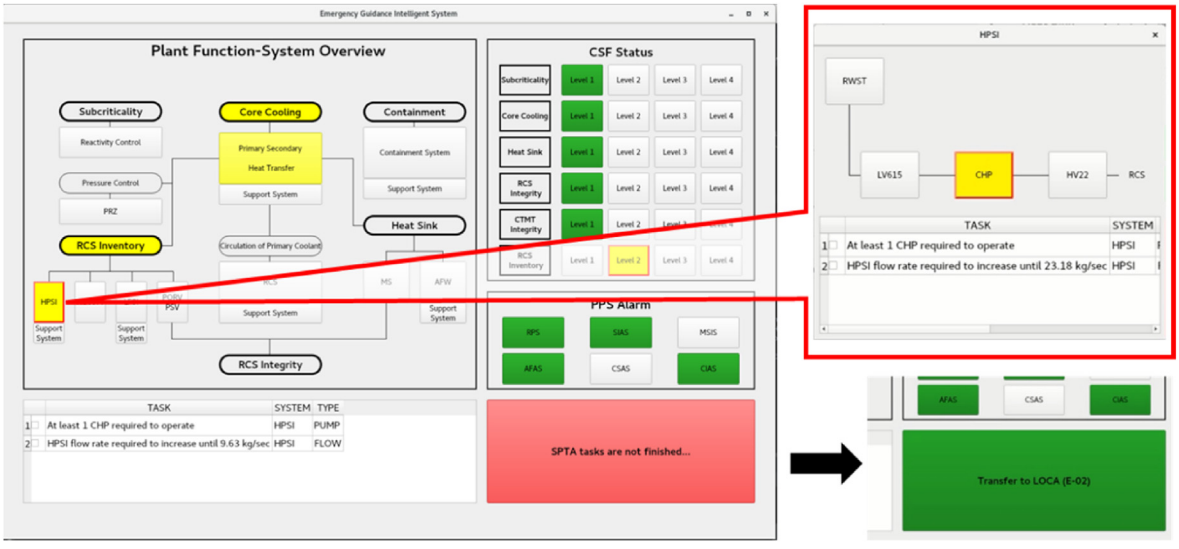

Fig. 12. EGIS test scenario 3 operation overview, 30 cm^2 LOCA + CHP #1 failure, highlighting the HPSI window display.

facilitate emergency operations. As a result of setting the RWST level to 38% via error injection in this scenario, EGIS shows in the MLD that the Core Cooling function will fail because of the HPSI and LPSI systems. By clicking the HPSI or LPSI button, the operator can identify that the function is unsatisfactory due to the RWST malfunction. The MLD and HPSI states in this scenario are shown in Fig. 13. If the operator judges that the risk requires immediate mitigation, the operation can be performed, but if it is not immediately necessary, the relevant alarm can be skipped by clicking the check box.

In the four scenario tests conducted to verify that the EGIS can replace the E-1 procedure, the EGIS appropriately processed the information provided by the E-1 procedure for the assumed scenario and provided it to the operator. The system can also identify potential risks that cannot be identified in E-1 procedure. One of the great advantages of EGIS is the rapidity of response through the parallel performance of surveillance tasks. To verify its agility, a comparison analysis was conducted between the number of tasks that must be performed in the existing procedural method and the number of tasks that must be performed with EGIS. The number of tasks was determined by the number of devices or instruments that the operator should check on the CNS HMI. A total of 71 tasks were identified in the E-1 procedure in these case studies. The diagnostic procedure tasks in E-1 are not considered. As can be seen in Table 6, the total reduction in the number of tasks applying EGIS was over 95% in all four scenarios. The tasks in E-1 procedure not only help perform the necessary operations, but also help identify the overall situation of the plant. Therefore, it is difficult to compare E-1 and EGIS simply with the number of tasks. However, EGIS provides important information through a hierarchical interface to understand the plant situation, and enables efficient operation because it provides only the necessary tasks to the operator.

5. Discussion

The emergency guidance intelligent system or EGIS aims to replace the immediate actions and diagnostic procedures, which are the initial operation procedure in an emergency. And to verify this, the demo system is developed in the CNS simulator environment and case studies are performed. EGIS performs the initial procedure in the form of a combination of a rule-based model and MFM, since the initial response requires relatively simple and quick action. The disadvantage of rule-based logic is that its performance can decrease as the number of rules increases, and therefore it is impossible to cope with all situations. However, applying rule-based models to the emergency initial response is relatively easy as it represents one portion of the tasks in the entire emergency operation. In addition, even in the case that the rule-based models fail to respond, there will be no significant problem in coping since redundant emergency mitigation tasks are performed in the subsequent ORGs and CSF restoration guidelines. In other words, even if omission occurs due to situations outside the rules, safety-critical tasks can still be performed because they are covered in duplicate in the subsequent ORGs and CSF restoration guidelines.

The EGIS greatly reduces the number of tasks performed and helps operators to respond quickly by providing only the necessary actions to the operator from the particular tasks that must be performed in the existing E-1 procedure. This is expected to reduce the time to conduct the initial response in an emergency. Further research is necessary to quantify how quickly the EGIS can perform E-1. Also, to verify E-1 agility, ergonomic experiments will be conducted by comparing the operation times in EGIS and the CPS for E-1.

The most problematic issue with EGIS is that operator support systems can potentially degrade the quality of operation due to possible misinformation or unnecessary, overloaded information. Therefore, strict verification of the effectiveness of these operator support systems is essential. To this end, an appropriate evaluation is planned as a future study by applying a validation methodology for the operator support system. Such evaluation methods include the operator support system effectiveness measurement methodology using a Bayesian belief network (BBN) proposed by Lee, Kim, and Seong [24], or the HMI evaluation methodology using information theory proposed by Kang and Seong [25]. These various evaluation methodologies will be applied to quantitatively evaluate the extent of the performance improvement that EGIS provides compared to current CPSs.

In general, the tasks involved in the immediate actions and diagnostic procedures are relatively simple. And in an environment with validated integrated systems, operators can perform the tasks in the immediate actions and diagnostic procedures faster and easier than those in the ORGs or CSF restoration guidelines. From

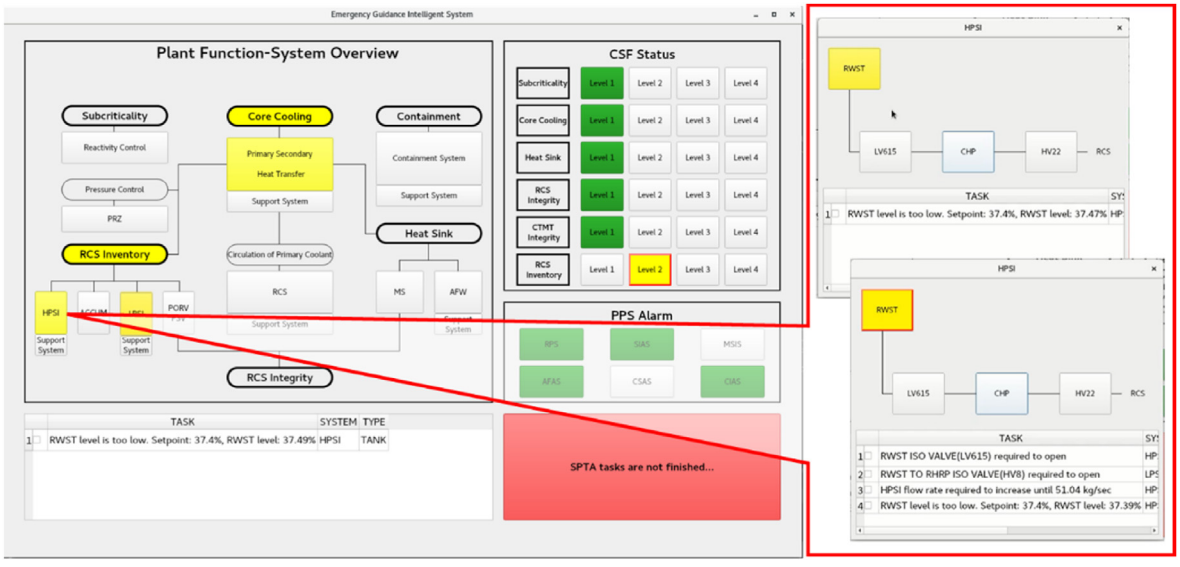

Fig. 13. EGIS test scenario 4 operation overview, 30 cm^2 LOCA + RWST low level, highlighting HPSI window displays.

Table 6
CNS task number reduction between E-1 procedure and EGIS.

Scenario	E-1 Task Number	EGIS Task Number	Reduction Rate
Accident (30 cm^2 LOCA)	71	0	100%
Accident + PPS Failure (30 cm^2 LOCA + SIAS actuation failure)	71	3	95.77%
Accident + System Failure (30 cm^2 LOCA + CHP #1 failure)	71	1	98.59%
Accident + System Failure (30 cm^2 LOCA + RWST low level)	71	0	100.00%

this perspective, the current impact of EGIS may seem low. However, EGIS has a strength in its ability to analyze the effect of failures and provide causality to operators visually, factors that are difficult to check in existing procedures. In addition, factors that can have a serious impact on safety functions can also be identified in advance with EGIS. As described in Section 4, in the RWST low level scenario, the supply of water to both HPSI and LPSI may be restricted due to the RWST low-level alarm. Of course, the frequency of this case is very low, but the current procedure does not check this component. In contrast, since EGIS models the flow system using MFM, such kind of anomaly can be readily identified because MFM modeled the RWST as the source of the SI mass flow system. In this way, events with high consequence and low frequency can also be considered via EGIS, even those omitted in existing procedures due to low frequency. In addition, beyond the scope of this initial study, future research will be conducted to develop an operator support system targeting a comprehensive EOP system that encompasses the ORGs and CSF restoration guidelines, for which the EGIS framework will provide the basis.

6. Summary and conclusion

Human error has a profound effect on the safety of nuclear power plants. Properly designed HMIs and procedures are needed to ensure the continued safety of NPPs. While a number of operator support systems, such as the CPS, have been developed to prevent human error, since the procedures were developed based on conventional PBPs, there is a limit to reflecting the dynamic nature of plant situations. The CPS currently applied to the APR1400 also has this static structure. To reflect dynamic characteristics, prevent possible overloading of information, and provide only the appropriate information, this paper proposed an operation support system, EGIS. The objective of this system is to replace the immediate actions and diagnostic procedures in responding to the early stages of an emergency. The system was designed in consideration of agility, dynamics, and intuitiveness, with dedicated modules as follows. The system checks the plant status through the parameter inspector model. From the monitoring information, the procedure logic module decides which tasks are required, and the risk evaluators analyze the causality of the fault. The risk evaluators combine a rule-based model with MFM to analyze the causality of how a component failure affects particular systems and goals. The diagnosis module diagnoses accidents through a GRU model. The information is intuitively provided to the operator through a hierarchical structure and color-coded information on the EGIS interface screen. Verification of the system was performed in this work with four emergency accident scenario tests. Results showed that the proposed EGIS performed more quickly than the existing operation method and also reduced the workload of the operator.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work was supported by a National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No.NRF-2018M2B2B1065653).

This work was also supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KoFONS) using a financial resource granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea (No. 2106007).

References

[1] W. Jung, J. Park, J. Kim, J. Ha, Analysis of an operators' performance time and its application to a human reliability analysis in nuclear power plants, IEEE Trans. Nucl. Sci. 54 (5) (2007) 1801–1811.
[2] J. Ahn, C. Carson, M. Jensen, K. Juraku, S. Nagasaki, S. Tanaka, Reflections on the Fukushima Daiichi Nuclear Accident: toward Social-Scientific Literacy and Engineering Resilience, Springer Nature, 2015.
[3] J. Park, D. Lee, W. Jung, J. Kim, An experimental investigation on relationship between PSFs and operator performances in the digital main control room, Ann. Nucl. Energy 101 (2017) 58–68.
[4] J.M. O'Hara, R.E. Hall, Advanced control rooms and crew performance issues: implications for human reliability, IEEE Trans. Nucl. Sci. 39 (4) (1992) 919–923.
[5] S.J. Lee, P.H. Seong, Development of an integrated decision support system to aid cognitive activities of operators, Nucl. Eng. Technol. 39 (6) (2007) 703.
[6] Y.C. Shin, H.Y. Chung, T.Y. Song, Advanced MMIS Design Characteristics of APR1400, 2003.
[7] H. Yoshikawa, T. Nakagawa, Y. Nakatani, T. Furuta, A. Hasegawa, Development of an analysis support system for man-machine system design information, Control Eng. Pract. 5 (3) (1997) 417–425.
[8] J. Oxstrand, K. Le Blanc, Computer-Based Procedures for Field Workers in Nuclear Power Plants: Development of a Model of Procedure Usage and Identification of Requirements, Idaho National Laboratory External Report, 2012.
[9] J.-H. Hong, M.-S. Lee, D.-H. Hwang, Computerized procedure system for the APR1400 simulator, Nucl. Eng. Des. 239 (12) (2009) 3092–3104, https://doi.org/10.1016/j.nucengdes.2009.09.024.
[10] J. Ahn, S.J. Lee, Deep learning-based procedure compliance check system for nuclear power plant emergency operation, Nucl. Eng. Des. 370 (2020) 110868.
[11] Operator Support Systems in Nuclear Power Plants, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 1992.
[12] I.A.E. Agency, Development and Review of Plant Specific Emergency Operating Procedures, Internat. Atomic Energy Agency, 2006.
[13] C.S. Ham, et al., Development of Compact Nuclear Simulator, Korea Advanced Energy Research Inst., 1988.
[14] K.-C. Kwon, J.-C. Park, C.-H. Jung, J.-S. Lee, J.-Y. Kim, Compact Nuclear Simulator and its Upgrade Plan, 1997.
[15] J.C. Park, et al., Equipment and Performance Upgrade of Compact Nuclear Simulator, 1998.
[16] J. Choi, S.J. Lee, A sensor fault-tolerant accident diagnosis system, Sensors 20 (20) (2020) 5839.
[17] H. Wang, M.-j. Peng, A. Ayodeji, H. Xia, X.-k. Wang, Z.-k. Li, Advanced fault diagnosis method for nuclear power plant based on convolutional gated recurrent network and enhanced particle swarm optimization, Ann. Nucl. Energy 151 (2021) 107934.
[18] J.M. Kim, G. Lee, C. Lee, S.J. Lee, Abnormality diagnosis model for nuclear power plants using two-stage gated recurrent units, Nucl. Eng. Technol. 52 (9) (2020) 2009–2016.
[19] M. Lind, An introduction to multilevel flow modeling, Int. Electron. J. Nucl. Saf. Simulat. 2 (1) (2011) 22–32.
[20] On-line Monitoring for Improving Performance of Nuclear Power Plants Part

2: Process and Component Condition Monitoring and Diagnostics, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 2008.
[21] M. Lind, X. Zhang, Functional modelling for fault diagnosis and its application for NPP, Nucl. Eng. Technol. 46 (6) (2014) 753–772.
[22] M. Song, A. Gofuku, Planning of alternative countermeasures for a station blackout at a boiling water reactor using multilevel flow modeling, Nucl. Eng. Technol. 50 (4) (2018) 542–552.
[23] I.S. Jeon, H.G. Kang, Development of an optimal mitigation strategy by estimating the conditional core damage probability with time-dependent recovery actions, Ann. Nucl. Energy 142 (2020) 107381.
[24] S.J. Lee, M.C. Kim, P.H. Seong, An analytical approach to quantitative effect estimation of operation advisory system based on human cognitive process using the Bayesian belief network, Reliab. Eng. Syst. Saf. 93 (4) (2008) 567–577.
[25] H.G. Kang, P.H. Seong, Information theoretic approach to man-machine interface complexity evaluation, IEEE Trans. Syst. Man Cybern. Syst. Hum. 31 (3) (2001) 163–171.