

Study of A Computer-based Emergency Operating Procedure with Desirable Features for Human Operators of Nuclear Power Plants

2018, September

Tulis Jojok Suryono

Graduate School of Natural Science and Technology
(Doctor's Course)

OKAYAMA UNIVERSITY

Abstract

Operating procedures are guidance for operators to monitor, make decision and take related counter actions in normal, abnormal and emergency conditions of nuclear power plants. The initial form of operating procedures, paper-based procedures (PBPs), have some drawbacks such as high operators' workload and necessity of much time to find and execute procedures related to the events. Therefore, because of the development of computer and information technology, computer-based procedures (CBPs) were developed to overcome the problems. CBPs provide more benefits, such as dynamic information representation, providing navigational links to other necessary procedures, providing path tracking in the procedure and providing supplementary information related to the procedure.

In emergency condition, after identifying the accident based on the symptoms and anomalies in the plant, operators should take appropriate actions following the instructions in the emergency operating procedures (CBPs). Such counteractions, indicated by the change of states of components, consequently affect other plant components and also the plant behavior. The information (components influenced and future plant behavior) is important and useful for operators to help them to predict and anticipate the future condition of the plant. However, most of CBPs do not provide this additional information. The lack of this information will decrease the situation awareness of operators. In addition, in the era of resilience, operators are expected to have the ability to anticipate the future condition of the plant. Therefore, the thesis discusses the additional information as the desirable features for CBPs to increase the situation awareness of operators and to achieve resilience system.

MFM as a functional modeling is used to investigate how to derive the additional information. The counter actions are modeled by the control function of MFM, which is used to change the state of a function primitive of MFM model of PWR plant based on an operation knowledge described in the EOP of SGTR accident. The thesis also discusses the technique to derive the additional information using algorithm based on causal effect relation and influence propagation. The information is presented in the form of explanation sentences which is understandable by human operators. The information is displayed on the CBP user interface each time an operator selects a specified procedure step.

Acknowledgments

Firstly, I would like to express my sincere gratitude to my advisor Prof. Akio Gofuku for the continuous support of my PhD study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my PhD study.

I would like to convey my gratitude to Ministry of Research, Technology and Higher Education for granting scholarship Program for Research and Innovation in Science and Technologies (RISET-Pro) grant number 8245-ID for the completion of my doctoral studies. I would also like to acknowledge JSPS KAKENHI Grant Number 16H03136 which was partially supported my research activities.

I would like to thank Dr. Tetsushi Kamegawa and Dr. Taro Sugihara for the constructive comments in the interim presentation in our laboratory and also lab members for supporting my research activities in the laboratory. I would like also to thank my friends who always support during my life in Okayama in the past years.

Finally, most importantly, I would like to thank my parents, my lovely wife and my two daughters for the moral support and the prayer.

Contents

Abstract.....	i
Acknowledgments	ii
Contents	iii
List of Figures.....	v
List of Tables	vii
1. Introduction	1
1.1. Background.....	1
1.2. Research theme	2
1.3. Thesis structures	4
2. Literature Review	5
2.1. Computer-based Procedures	5
2.1.1. Overview of Operating Procedures	5
2.1.2. Computer-based Emergency Operating Procedures.....	7
2.2. Operator Support Systems	11
2.3. Situation Awareness	15
2.4. Resilience Engineering	20
2.5. Functional Information	24
3. Techniques to Derive the Additional Information Based on MFM Models	27
3.1. Overview of MFM	27
3.2. MFM Symbols	28
3.3. MFM Reasoning	29
3.4. Influence Propagation	32
3.5. Modeling of a Counteraction by MFM Control Function	34
3.6. Algorithms to Derive the Additional Information	36
3.6.1. Components influenced	36
3.6.2. Future plant behavior.....	38
3.7. Explanation Sentences	39

3.7.1.	Components influenced	39
3.7.2.	Future plant behavior	40
4.	Modeling of PWR Plant and Emergency Operating Procedure	42
4.1.	Outline of PWR Plant	42
4.2.	MFM Model of PWR Plant	43
4.3.	Modeling of EOP of SGTR	44
4.3.1.	STEP 1: Occurrence of SGTR thereafter reactor trip and safety injection	46
4.3.2.	STEP 2: Check RCP restart criteria, if not meet, trip all RCPs, otherwise go to STEP 3	48
4.3.3.	Identification and isolation of faulted steam generator	50
4.3.4.	RCS cooldown using steam dump through SG PORV or steam dump valve	51
5.	Application Results and Discussions of Deriving Additional Information.....	54
5.1.	Reactor trip and safety injection	54
5.2.	Check RCP restart criteria	59
5.3.	Identification and isolation of faulted steam generator.....	60
5.4.	RCS cooldown using steam dump through SG PORV or steam dump valve .	62
5.5.	Applicability Evaluations	63
5.5.1.	Contribution to Situation Awareness.....	64
5.5.2.	Contribution to Reduce Human Errors	65
6.	Preliminary Design of CBP User Interface with the Desirable Feature.....	67
6.1.	Process of Displaying the Additional Information	67
6.2.	Design of the CBP User Interface.....	69
6.3.	Evaluation of the Design of the CBP User Interface	71
7.	Conclusions and Future Works	74
	References	76

List of Figures

Figure 1.2-1. Outline of the research.....	3
Figure 1.2-2. Relationship among functional information, situation awareness and resilience engineering	4
Figure 2.1.1-1. Procedure hierarchy for various operation condition [7]	5
Figure 2.1.2-1. An example of CBP user interface (ImPRO) [15].....	8
Figure 2.1.2-2. Hierarchical structure of procedure, step and action [15]	9
Figure 2.1.2-3. Comparison between PBP and CBP operation [10]	9
Figure 2.2-1. Classification of operator support systems and HMI [22].....	12
Figure 2.2-2. Information flow of direct and indirect supports.....	14
Figure 2.3-1. Situation awareness and decision making [26]	16
Figure 2.4-1. Different views of work and activities in safety-I [34]	21
Figure 2.4-2. Four cornerstone of resilience engineering [31].....	22
Figure 2.4-3. Step to resilience (adopted from [38]).....	22
Figure 2.5-1 Structure models of a gasoline and an electric car [6].....	25
Figure 2.5-2. Functional model of a car [6]	25
Figure 3.2-1. MFM symbol.....	29
Figure 3.4-1 Influence propagation	33
Figure 3.5-1. MFM control function	35
Figure 3.6-1. Algorithm to derive components influenced information	37
Figure 3.6-2. Algorithm to derive future plant behavior information.....	39
Figure 4.1-1. Simplified diagram of PWR plant	42
Figure 4.2-1. MFM model of simplified of PWR plant	43
Figure 4.3-1. MFM model of counter actions of reactor trip and safety injection..	47
Figure 4.3-2. MFM model of RCP restart criteria operation	49
Figure 4.3-3. MFM model isolation of ruptured SG operation.....	51
Figure 4.3-4. MFM model of RCS cooldown using steam dump valve operation .	52
Figure 5.1-1. Part of MFM model related with reactor trip	55

Figure 5.1-2. Part of MFM model related with safety injection and stopping RCS operation	57
Figure 5.2-1. Part of MFM model related with RCP restart criteria operation	59
Figure 5.3-1. Part of MFM model isolation related with ruptured SG operation ...	61
Figure 5.4-1. Part of MFM model related with RCS cooldown using steam dump valve operation.....	62
Figure 6.1-1. Process of displaying additional information to the CBP user interface	68
Figure 6.2-1. Draft of layout of the CBP user interface	70
Figure 6.2-2. The initial display of the CBP user interface.....	70
Figure 6.2-3 Displaying the additional information on the CBP user interface.....	71
Figure 6-3-1 Method to evaluate the proposed CBP user interface.....	72

List of Tables

Table 2.4-1. Safety-I and Safety-II [35]	21
Table 3.3-1. Definition of state of MFM.....	30
Table 3.3-2 Direct influence for upstream and downstream connections [56]	31
Table 3.3-3 Indirect influence with influencer relations [56]	31
Table 3.3-4 Indirect influence with participant relations [56]	31
Table 3.3-5 Rules of means-end relations	32
Table 3.5-1 MFM control functions	35
Table 4.2-1. Description of main functions and objectives.....	44
Table 4.3-1. Simplified of EOP of SGTR [5]	45
Table 4.3-2. Parameters of modeling of counter actions for reactor trip	47
Table 4.3-3. Parameters of modeling of safety injection and stopping RCP operation	48
Table 4.3-4. Parameters of modeling of check RCP restart criteria operation.....	50
Table 4.3-5. Parameters of modeling of isolation of ruptured SG operation	51
Table 4.3-6. Parameters of modeling the RCS cooldown operation	52
Table 5.1-1. States of function primitives before and after the reactor trip operation	55
Table 5.1-2. Explanation sentences for the influences of reactor trip operation.....	55
Table 5.1-3. Future plant behavior after reactor trip operation	56
Table 5.1-4. State of function primitives before and after safety injection and stopping RCS	58
Table 5.1-5. Explanation sentences of plant behavior after safety injection and stopping RCP operation	58
Table 5.2-1. State of function primitives before and after check RCP restart criteria operation	59
Table 5.2-2. Explanation sentences of plant behavior after check RCP criteria operation	60
Table 5.3-1. States of function primitives after isolating of ruptured SG	61
Table 5.3-2. Explanation sentences of the influence of isolation of ruptured SG...	61
Table 5.4-1. States of functions before and after RCS cooldown operation	63

Table 5.4-2. Explanation sentences of influence of RCS cooldown operation.....	63
Table 5.5-1 Contribution of additional information derived to situation awareness for SGTR accident case	64
Table 6.1-1. Group of explanation sentences for isolate ruptured SG	68

Chapter 1

1. Introduction

1.1. Background

In case of an emergency situation of nuclear power plants, a lot of information, warning and alarm messages about anomaly of the plant indicated by the deviations of some components parameter (temperature, volume or pressure) from normal value will be delivered to the operators through display panels and annunciators. Operators should recognize the type of the information and alarm messages and then try to interpret, diagnose and decide what kind of event/accident happened in the plant and select some appropriate emergency operating procedures (EOP) to mitigate the accident. The counter actions should be conducted step by step following the instructions in the EOP to bring the plant back to safe operation condition and to prevent the release of radioactive material to the environment.

Nowadays, most of modern nuclear power plant main control rooms are assembled with computer-based procedures (CBPs) to increase the usability and functionalities of EOP by providing dynamic representation of procedure and display only relevant steps based on operating mode and plant status [1]. In addition, the performance of operators can be increased by using CBPs in terms of reducing workload, completion task time and operators' errors in transition between procedures [2]. Therefore, CBPs are developed and intended to make it easier for operators to monitor and control the reactor during mitigation the accident and to prevent the potential of human error caused by the misconduct of operators.

Despite the benefits offered by the CBPs, most of them do not provide functional information which provide additional information related with the purpose of procedure step and the impact of their counter actions to other components and the plant behavior. This additional information is useful for operators to understand the purpose of the instructions in the procedure. In addition, it is also important to predict and prepare the next counter actions related with the future event of the plant caused by their counter actions. This thesis studies a propose CBP with the additional information feature. The feature is one of the desirable features of the CBP as proposed in [3]: functional information display, time remaining display, and dynamic

operation permission system. The additional information (components influenced and future plant behavior) is displayed on the CBP user interface when operators select a specific procedure step on the CBP user interface. By providing this additional information, operators will have some views of the impact of their actions before taking the counter actions. It will increase the situation awareness of operators during emergency condition.

The operator actions following the instruction in the procedure can be classified as cause-effect relations because changing the level or state of a component will impact the state of other components in the system. It is relevant with the concept of cause-effect relation through control function in multilevel flow modeling (MFM)[4, 5]. Therefore, the counter actions are modeled by the control function in MFM. In addition, the control function is applied to the MFM model of PWR plant. Then by implementing cause-effect relation and influence propagation, the additional information of the impact of their actions following the simplified EOP of SGTR accident of a PWR plant of Mihama Unit 2 NPP in Japan in 1991 [6] is investigated.

1.2. Research theme

This thesis proposes the functional information as the desirable features for a computer-based emergency operating procedure to increase the situation awareness of operators in order to reduce the potential of human error and to achieve resilience. The functional information is information related with the effects of their counteractions to mitigate the accidents to the other system components and future plant behavior. The functional information, which is displayed on the CBP user interface, is useful for operators to help them to understand the purpose of the procedure steps, to make decision and to take the counter actions. In addition, it is also important for predicting and preparing the next counteractions related with the future plant behavior. Figure 1.2-1 summarizes the outline of the research.

The functional information is useful for improving the situation awareness of operators during mitigation the accident. The increasing of situation awareness will reduce the potential to human error and make it easier to achieve the resilience

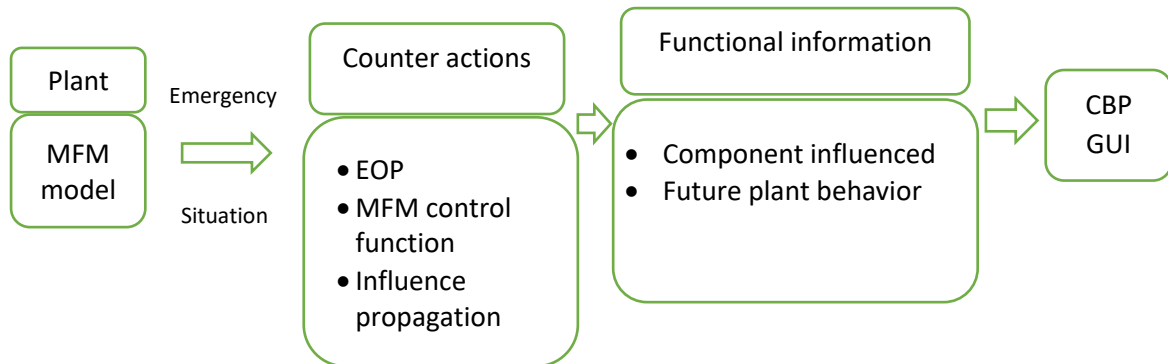


Figure 1.2-1. Outline of the research

Figure 1.2-2 shows the relationship among functional information, situation awareness and resilience engineering. Functional information, as mentioned in [7] has some features such as:

- It provides information about the role and purpose of each component which can be correlated with the system behavior
- It contains causal relation information which is useful for estimating the effect and influence of a counter actions qualitatively
- It has hierarchical modeling ability which is useful to understand system behavior in various level of aggregation.
- It contains linguistic representation which is important to present the result of causal inference to operators in understandable way.

The above features of functional information will support gathering information, interpreting the gathered information and anticipating future events in situation awareness. The achievement of capabilities in situation awareness then encourage the capabilities of monitoring and anticipating to achieve the resilience system.

The applicability of providing the additional information to the CBP user interface can be confirmed from some studies results which mention that CBPs should provide high level information related to the procedure goals which help operators to understand the system as an object of action and recognize the intention of counter actions. In addition, some studies also give results that providing the functional information will increase the situation awareness of operators, especially the information of future plant behavior

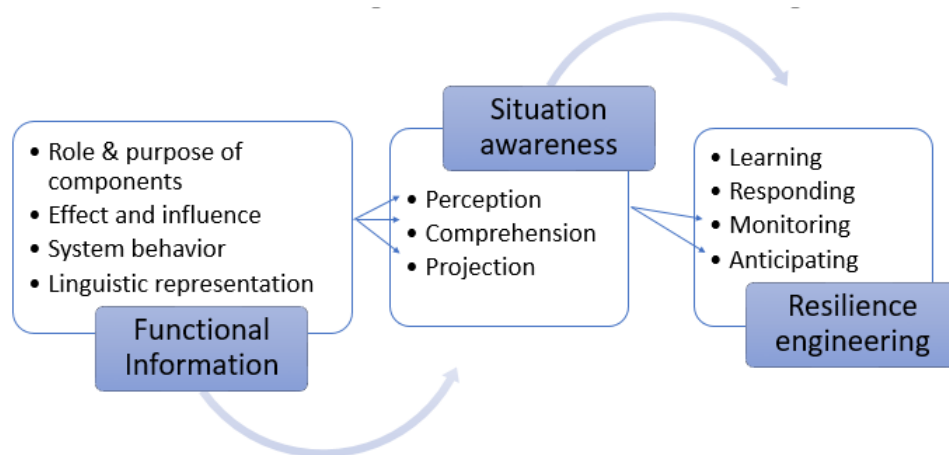


Figure 1.2-2. Relationship among functional information, situation awareness and resilience engineering

1.3. Thesis structures

The thesis consists of seven chapters. Chapter 1 introduces the background and methodology of the research. Chapter 2 provides the review of some literatures about the operator support system and computer-based procedure, the situation awareness of operators in the plant, and overview of functional modeling and its implementations. Chapter 3 introduces the techniques to derive the additional information. Chapter 4 presents the modeling the simplified PWR plant and the emergency operating procedure which is used to mitigate the accident applied to the PWR plant. Chapter 5 describes the application results and discussions of deriving the additional information and the applicability evaluations related with contributions to increasing the situation awareness and to reduce human errors. Chapter 6 introduces the preliminary design of the CBP user interface with the desirable feature. Finally, Chapter 7 concludes the thesis and some future works.

Chapter 2

2. Literature Review

2.1. Computer-based Procedures

This section discusses the overview of operating procedures which describes the hierarchy of operating procedures based on the level of anomalies happened in a plant from normal condition to severe accident conditions. Then, the discussion is only focused on emergency operating procedures (EOPs) and the development of computer-based emergency operating procedures.

2.1.1. Overview of Operating Procedures

Operation procedures provide information and guidance for operators to operate and monitor the plant during normal operation; and help them to make decision and taking counter actions during an emergency condition to mitigate the accident and to bring the plant into safe operation condition. The information and guidance are combined to minimize human error. Figure 2.1-1 shows the hierarchy of procedures for various operation conditions [8]. According to Figure 2.1-1, system operating procedures are used for normal plant operation, such as how to start up and to shut down the plant and operating the plant in normal power operation. Operators have to make sure that the plant is operated within specified limits and conditions.

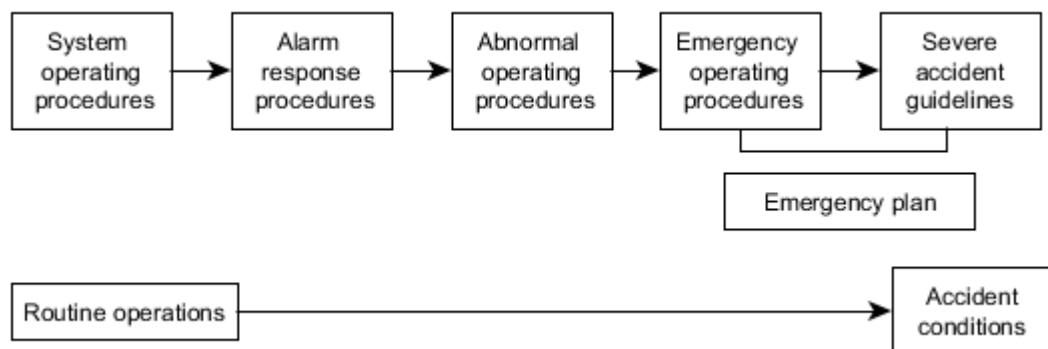


Figure 2.1-1. Procedure hierarchy for various operation condition[8]

During the life time of the plant, some anomalies may happen in the plant. Based on the anomalies, the plant conditions can be divided into three conditions: abnormal conditions, accident/emergency conditions, and severe accident conditions depending on the severity of the anomaly. In abnormal conditions, the anomalies do not cause any significant damages to safety related components and can be handled by normal control systems. The anomalies are indicated by the alarm messages and changing the parameter level of components from the normal setpoints. In this case, operators should implement an appropriate alarm response procedure to identify the anomalies. In some cases, the abnormal operation may change to a more complex operation condition if the malfunctions happened in core cooling system or in a support system. Operators should do the counter actions to compensate the malfunctions or faults following the abnormal operating procedures (AOPs). Examples of abnormal conditions are malfunction of a component of normal running plant and a fault in the function of a component of control system [8].

Moreover, accident or emergency condition, as defined by the IAEA is “deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents, beyond design basis accidents and severe accidents” [8]. Examples of accident conditions are steam generator tube rupture (SGTR), loss of coolant accident (LOCA) and loss of offsite power (LOOP). In case of emergency, the procedure used is emergency operating procedure (EOP). Operators should follow the EOP to control the plant and cannot only rely on their knowledge and experiences.

Finally, the last procedure or guidance is severe accident guidelines (SAGs), which is used to mitigate severe accident conditions. Severe accident conditions are accidents which include significant core degradation. SAGs are used when the EOPs cannot effectively preventing the core damage. Compared with EOPs which focus on preventing core damage, SAGs concentrate on maintaining other barriers for protecting the release of radioactive materials to public.

Another important thing derived from Figure 2.1-1, is the transition between individual groups of procedures (AOPs, EOPs and SAGs). It is owing to

the fact that in emergency condition, operators will work with unusual situation and unexpected plant behaviour in stressful situation. Therefore, they need reliable guidelines to properly make decision and take the actions to mitigate the abnormal or accident condition in the limited time available. An example is the transition between AOPs and EOPs which defines the entry condition into EOPs, reactor trip or emergency core cooling system actuation [8].

2.1.2. Computer-based Emergency Operating Procedures

Operators as humans have important roles in monitoring and controlling the plant. As the nature of humans, they have some limitations. They cannot only rely on their knowledge acquired from education and training and their working memory during conducting their works. Some factors, such as panic, confusing and stressful situation may affect and degrade their performance and capabilities, especially in an emergency condition. Therefore, some guidance or operating procedures are needed to help them to overcome the problems. Literature [9] mentioned that good procedures will help operators to reduce physical/mental workload, to reduce the potential of human errors, and to maintain their performance. In case of accident conditions, good emergency operating procedures (EOPs) will aid operators to mitigate the accidents.

Initially, in traditional main control rooms of nuclear power plants, EOPs are available in the form of printed documents as paper-based procedures (PBPs). However, PBPs have some drawbacks in terms of how to obtain information and their interactive abilities [10]. Other disadvantages are it is hard for operators to arrange, scan and read the PBP while conducting monitoring and controlling tasks; and it will take a long time in the diagnosis process of the plant status [11]. Moreover, there are some cognitive workload related to the working with the PBPs, such as managing multiple procedures at one time, keeping track the currently used procedures, going through some loops before obtaining the correct information to diagnose the plant status [12]. Furthermore, the static information presented in the PBPs which does not express the actual plant condition [12] also make it difficult for operators to manage the PBPs.

Due to some disadvantages of PBP mentioned above and because of the development of computer and information technology, computer-based procedures (CBPs) were developed. CBPs are designed to help operators and reduce workload related to the usage of PBPs in monitoring and controlling nuclear power plants. CBPs have been introduced in modern and advanced main control rooms of nuclear power plants, such as COMPRO [13] , COPMA-II [14], N4 Procedure [15], IMPRO [16, 17] and CPS [11]. Figure 2.1-2 shows an example of CBP user interface (ImPRO) [16].

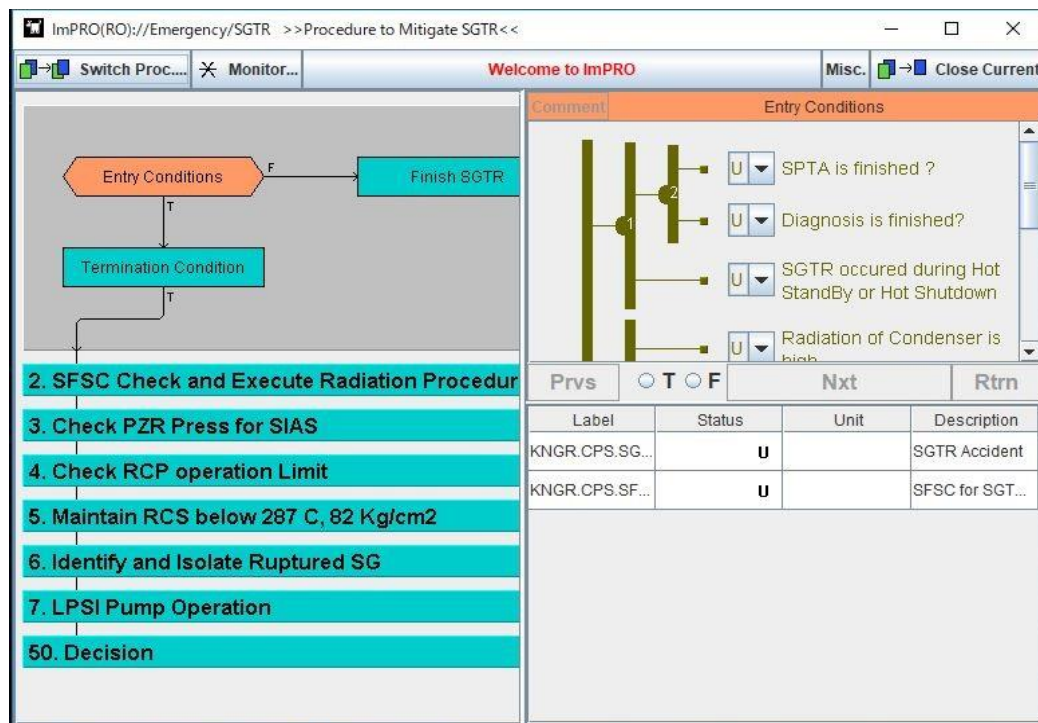


Figure 2.1-2. An example of CBP user interface (ImPRO) [16]

The CBP shown in Figure 2.1-2 uses a flowchart and logic tree diagram format. The flowchart represents the procedure and steps in a hierarchical structure owing to the fact that the objective of a procedure is achieved by completing the objectives of successive steps. In addition, some appropriate actions should be conducted to achieve the objective of each step. The hierarchical structure of procedure, step and action is provided in Figure 2.1-3 [16].

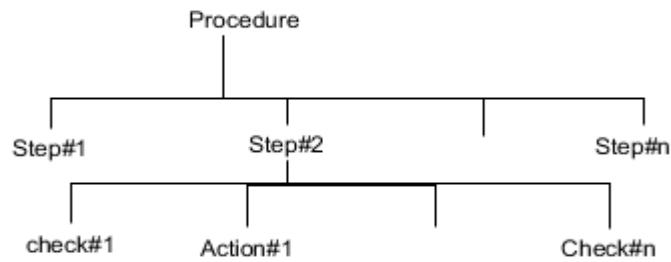


Figure 2.1-3. Hierarchical structure of procedure, step and action [16]

CBPs are integrated with visual display units (VDUs) and computer input devices (keyboard, mouse and/or touchscreen) and are located on the operators' workstation desks. In addition, in case of the malfunction of CBP, a backup should be provided, usually paper-based procedure. In this case, the seamless transition from CBP to PBP should be considered.

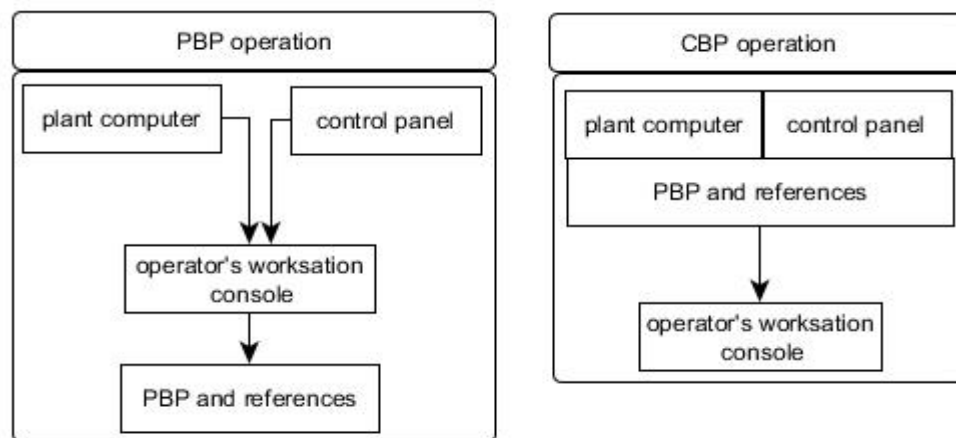


Figure 2.1-4. Comparison between PBP and CBP operation [11]

Figure 2.1-4, adopted from [11], summaries the difference between PBP and CBP comparison. In traditional main control rooms with PBP operations, operators should conduct monitoring and controlling the plant while finding the necessary information and guidelines by scanning and reading the PBPs. These conditions will increase the operators' cognitive workload and reducing operators' situation awareness. The impacts are, it will take long time to collect

and diagnose the plant status that may endanger the plant behaviour and increase the potential of human errors. On the other hand, in CBP operations, all the necessary data can be provided at the operator consoles. It will make it easier for operators to collect the information, judge the exact plant status and then make correct decision and take the appropriate actions. Therefore, CBPs have positive impacts on the performance of operators by reducing time for completion the task, reducing workload and reducing errors in transition between procedures [18] .

CBPs can be divided regarding the functionality provided by the CBPs: Type 1 CBP, Type 2 CBP and Type 3 CBP [18]. The type 1 CBPs (electronic procedure) is an electronic version of the PBP with little additional functionality. The procedures are presented in text or graphical format. The type 2 CBPs (Computer-based procedures) provide more functionalities such as automatic information retrieval and display, automatic step logic processing and display of results to support operators' decision making. The Type 3 CBPs (CBPs with procedure-based automation) incorporates all the functionalities of the Type 3 CBPs including the ability to send control commands. This type of CBPs enables to deal with multiple procedure steps.

In general, as described by [19], CBPs contain identity (title, procedure number, revision number, and date), steps of action in the form of verb and a direct object, warning, cautions, notes and supplementary information. The information is presented on the CBPs in the form of texts, graphics or combination of texts and graphs. Furthermore, some major issues related with the implementation of CBP in nuclear power plants are also considered [17]:

- Writing the procedure correctly and kind of information should be presented in the procedure.
- Format of the correct procedure and presentation of information in the procedure for easy comprehension
- Execution of correct procedure without any mistakes.
- Marking the procedure that has been conducted by one operator so that other operators in a team can know the current steps of the procedures.

Related to these issues, IEC standard [20] recommends some detailed design requirements for designing the computer-based procedures. Some requirements discussed in the IEC standard, for examples are types of information should be displayed, how to present the information in understandable way and CBPs features. In addition, it also discusses the detailed design requirements, verification and validation of CBPs, integration with other support systems and training of operators for using the CBPs. O'Hara et.al in NUREG-6634 [21] also mentions the requirements for designing CBPs. Most of the standards require that the design of CBPs should consider the human factor engineering in order to reduce the potential of human errors.

2.2. Operator Support Systems

Human role is the most important for NPP safety because operators are human being, human operators operate NPP, humans engineers determine safety criteria and operators check up the fulfilment [22]. Operators also have the main role to monitor and control the reactor. As to control functions, some elements should be considered: information, identifying the situation, control decision making and control decision realization. In order to successfully and safely achieve their tasks, operator support systems are developed which will help operators in enhancing the operator performance by preprocessing the raw data, interpreting the plant state, prioritizing goals and providing advices [23].

There are some classifications of operator support systems. First classification is based on the above elements: informational support system, support system for situation evaluation, support system for making a control decision and support system for control decision realization. [22]. Another classification is based on the integration with the human machine interface (HMI) as can be seen in Figure 2.2-1 [23]. In traditional main control rooms (MCRs), which most of the systems are controlled by analog systems, the operator support systems are installed as independent systems to provide additional information [23]. On the other hand, in modern main control rooms, the operator support systems are integrated with HMI [23]. Comparing with the traditional MCR which operators may not use the information from the support systems because of the high cognitive workload, the additional information of support

systems provided in modern MCR is very useful and can reduce the workload. Therefore, the purposes of operator support system are to process and present information and advice to the operators [22] and to support cognitive process activities. In addition, operator support systems offer some benefits to operators in terms of increasing availability and reliability; reducing operation and maintenance cost; reducing equipment failure, faster fault detection and diagnosis; assisting in many areas which are difficult or time consuming; and assisting in planning and decision making.

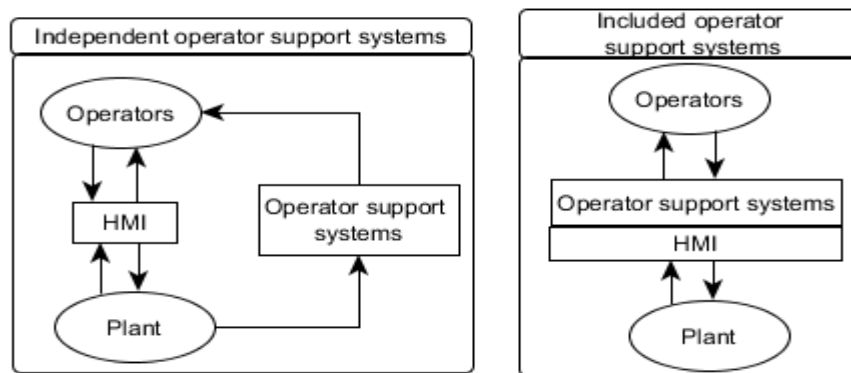


Figure 2.2-1. Classification of operator support systems and HMI [23]

Lee et al [23] mentioned some type of operator support systems which are intended to support cognitive activities:

- Support systems for the monitoring/detection activity

The purpose of monitoring and detecting activities, which are conducted by the instrumentation and alarm systems, is to detect the abnormal situation. The anomalies are indicated by the variation of instrumentation level or the changes of color or the sounding of the alarms. If there are a lot of alarms repeatedly turn on and off during the abnormal situation, it will cause operators confusion and panic. Therefore, to overcome this problem, the interface of main control room should be improved by providing fully digitalized and computer-based systems with large display panel and computer displays. In order to efficiently display the information and to make it easier for operators to find a specific control or an indicator, the features of key support should be provided in the computer displays

[23]. Another solution to overcome the problem is by providing advanced alarm system which has capabilities to categorize, filter, suppress and prioritize the alarms that let operators to focus on the most important alarms.

- Support system for situation assessment activity

Situation assessment is the activity that relates with the situation analysis, situation modeling and situation explanations. This activity is much easier to be conducted if it is supported by the fault diagnosis systems and alarm analysis systems. The fault diagnosis system is useful for operation plans based on event-based procedure because it provides expected faults for fast and easy situation assessment. However, for symptom-based procedure of operation plans, which the procedure is determined by comparing the procedure entry conditions with the current parameters, a system that suggests the appropriate procedure for a given situation will be more useful than a fault diagnosis system [23].

- Support system for the response planning activity

Response planning activity is conducted after assessing the situation following the instructions or steps of written procedures. Initially the written procedure is paper-based procedures. The information written in paper-based procedures is fixed and in natural language which in some cases difficult to understand and may cause operators to skip the procedure steps and make omission errors. Therefore, computer-based procedures (CBPs) were developed to overcome the drawbacks of paper-based procedures. CBPs provide information about procedures and steps, relation between the procedures and steps, and parameters needed to operate the plant. In order to prevent the omission errors, CBPs offer the feature of check-off plan and a brief of candidate operations.

- Support system for the response implementation activity

Although the response planning activities are based on operating procedures, operators may still make errors in executing the selected operation in response implementation activities. This type of error is a commission error and should be prevented by the response implementation support for example operation

validation system [23]. The purpose of the support system is to detect faulty operation and warn operators about them. Another example of response implementation support to prevent the commission error is the dynamic operation permission proposed by Gofuku et al [24]. The main idea of the system is to prevent only obvious commission errors and let operators do whatever they like as long as they follow the operation procedures.

Based on how operators process the information, operator support systems are divided into direct support and indirect support systems [25]. In the direct support, the gathered information can be directly used to execute the actions without any significant interpretations. Therefore, it is needed that in the direct support systems, the information should be provided in the form of everyday language which is understandable by the operators and with less interpretation efforts. CBP, if it is considered as a kind of HMI, is an example of direct support system.

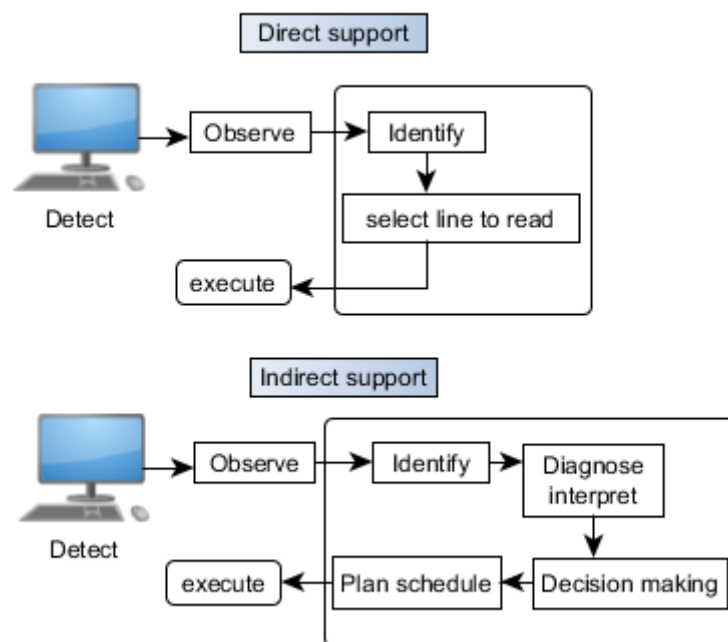


Figure 2.2-2. Information flow of direct and indirect supports

On the other hand, in the indirect support systems, operators need to interpret the perceived information before taking counter actions. Figure 2.2-2 summaries the

processing information for direct and indirect support systems [25]. It can be seen from the figure that in indirect support systems, after observing and identifying the information, operators should diagnose and interpret the information. The results can be used for decision making and plan schedule. Then, the actions can be conducted.

The direct support systems are more suitable for recovery action using the instruction and information provided in the EOP without interpreting the information. In emergency situation, operators work in stressful condition. Therefore, they need clear and understandable instructions to execute the actions without any interpretation to mitigate the accident in limited time condition. While the indirect support systems are useful for interpreting the current condition based on the anomalies in the plant in order to recognize what has occurred and what is going on in the plant. The information from alarms, indicators and monitor lights should be interpreted and the results are used to make decisions.

2.3. Situation Awareness

Situation awareness (SA), in general can be defined as the ability of operators to establish and keep the adequate understanding of “what is going on” in the system for the successful of task performance. The SA can be measured by considering characteristic of the task and the aim of analysis. The concept of situation awareness initially was used in military to make the soldiers aware of the existence of the enemy. Currently, the concept is adopted to aviation, nuclear power plant and emergency response [26]. There are several definitions about situation awareness (SA). However, mostly used definition is made by Endsley [27]: “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future”. Endsley also mentioned SA as a state of knowledge that results from a process (situation assessment).

Figure 2.3-1 summaries the definition of situation awareness. There are three levels of situation awareness: Level 1 (gathering information), Level 2 (Interpreting the gathered information) and Level 3 (anticipating future states). In case of nuclear plant, the Level 1 of SA is characterized by the needs of main control room operators to know the state of components, parameter levels such as pressure and temperature

level of a pressurizer in PWR plant, and alarm information regarding the anomaly in the plant. The ability of operators to understand, to analyze, to classify and to integrate the information perceived in Level 1 is the feature of Level 2 of SA. Finally, in Level 3 of SA, based on the achievements in Level 1 and 2 of SA, operators should be able to predict and anticipate the future events and impact of their actions. Therefore, situation awareness is how operators know the current state of the plant [28]. The situation awareness can be used to anticipate future plant behavior, to create appropriate operation plan and to prevent potential failures [29].

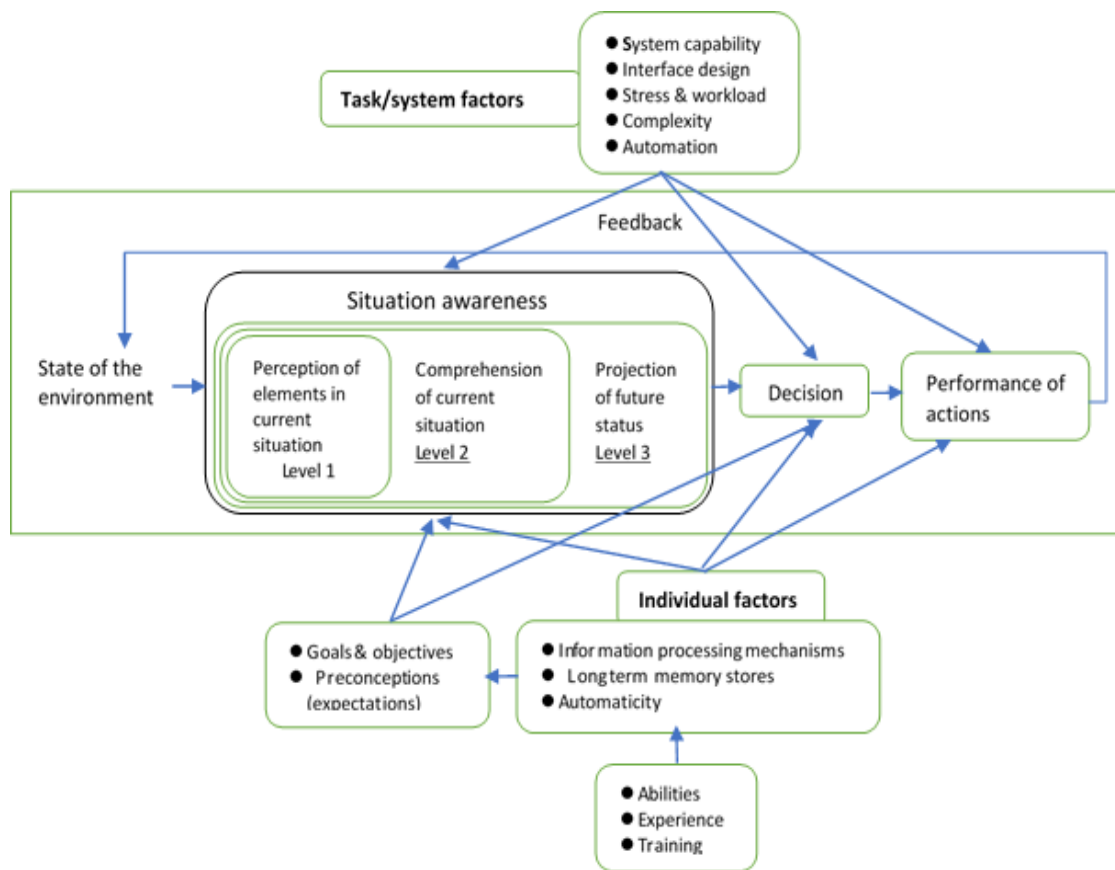


Figure 2.3-1. Situation awareness and decision making [27]

In some cases, there are some factors or reasons that cause people may fail in achieving the situation awareness. It can be happened, especially in Level 1 and Level 2 of SA as mentioned by Endsley [27] and in [26]. In Level 1 of SA it can be caused by the unavailability of the data, the difficulty to perceive the data, failure to observe

the data and misperception of data. In addition, the lack of mental model, the use of incorrect mental model and memory failure are the factors that cause the fail in achieving SA in Level 2 of SA. Furthermore, there are some indications that people losing the correct situation awareness, such as: ambiguity, confusion, lack of required information, failure to maintain critical tasks and failure to meet expected target [26]. In nuclear power plant operation, situation awareness is very important and should be improved. There are some skills that can be improved to enhance the situation awareness in the area of planning, problem solving, attention, team coordination, knowledge and communication [26].

There are some factors that affect the situation awareness: individual factors and system factors [30]. Individual factors consist of attention and working memory. Attention is related with the operator receiving information relevant with the task and whole description of the plant state. Working memory is used to store the information perceived in level 1 of SA and then to integrate with the new information for level 2 of SA and finally to determine how the future plant behavior is affected by the information in level 3 of SA. In order to manage attention and working memory, some aspects such as mental models, goal-driven processing, and automaticity should be considered [27]. Mental models are indicated by the ability of operators to achieve SA by processing and understanding a large amount of information. It can be established through training and experience. In addition, a specific goal (to develop SA) should be as a basis in the process of perceptions, interpretations and judgements to achieve the goal-driven processing. Moreover, automaticity is represented by the actions which need few attentional resources.

On the other hand, the system factors consist of interface design and system complexity. SA can be improved by providing good interface design which has information integrated from various sources or presents only information that operator must attend [31]. There are some external factors that influence the situation awareness: task, system, and individual [27]. The task environment includes task complexity, workload and pressure and stress. In an emergency condition, some tasks should be conducted to bring the plant to a safe operation state in limited time. In some cases, this condition will make them stress and then reduce the situation awareness. In addition, the necessary information provided by the system also affect

the situation awareness. Emergency operating procedures with insufficient information provided can cause operators to make a mistake in making decision and taking the actions to mitigate the accident. Finally, the individual also affects the situation awareness in terms of ability to achieve the situation awareness, ability to process the information, and objectives to interpret the environment.

Situation awareness can be simplified as the ability of operators to know what is going on around them. It is relevant with the concept of four cornerstone in resilience: learning, monitoring, anticipating and responding [32]. The features provided in the functional information will increase the ability of operators in perceiving and comprehending the information and also predicting the future event in situation awareness, which in turn will support the ability of monitoring and anticipating in resilience engineering. Monitoring or “knowing what to look for” expresses that operators of a main control room should monitor the plant status and be able to find the initiating event related with the anomaly indicated by alarm and changes of parameter levels of components in the plant. In addition, the ability of operators to direct the potential changes and their impacts due to the counteractions (automatic or human actions) is a part of anticipating or “knowing what to expect”. It is also related to the ability to identify the possible future behavior, conditions or state changes that affect the functionality of the system. The next section will discuss the resilience engineering.

In an emergency situation, operators may feel confuse, nervous, panic and stress during their activities to identify, control and mitigate the accidents. In some cases, it will reduce the situation awareness of the operators, which in turn it will increase the potential to human error and will endanger the plant. Therefore, in order to keep and increase the situation awareness, the situation awareness of operators should be regularly assessed or measured. There are some methods to measure the situation awareness, as mentioned in [33]:

- Freeze probe techniques

As the name, this technique freezes a random task and blanks all displays and screens and applies a set of SA queries regarding the current situation. The queries are developed by the Subject Matter Experts (SME). Then,

participant should response the queries based on their knowledge and understanding, and the results are compared to the state of the system at the freeze point and the SA scores are calculated. Despite the benefit, which is the “direct” SA assessment, this technique has some drawbacks in terms of the level of intrusion during the task and the validity because it more relies on the memories of the participants. An example of this technique is Situation Awareness Global Assessment Technique (SAGAT) which is described in [27]

- Real time probe techniques

This technique is the development of freeze technique in which the task proceeds in real time and is not frozen. Although, this technique still has problems as in the freeze probe technique, the advantage is, the level of intrusion can be reduced. Literature [34] mentions Situation Present Assessment Method (SPAM) as an example of real time probe technique.

- Self-rating techniques

These techniques are conducted as post trial and intended to derive the subjective rating of participants’ perceived SA through a rating scale. The techniques are easy, quick and low cost to implement and do not have intrusion. However, the drawbacks of the techniques are related with the collection of SA data post-trial and their sensitivity. The Situation Awareness Rating Technique (SART) is an example of self-rating techniques [33].

- Observer techniques

The SA is measured by SME and based on predefined observable SA related behaviors expressed by participants during task performance. These techniques can be used in the real worlds because they have no impact on the task being performed although they have some questions related to the validity. An example of the technique is the Situation Awareness Behavioral Rating Scale (SABARS) which is used to assess infantry SA in field training exercises [33].

- Performance measures

The SA is assessed based on the performance of the participants during the task and recorded to determine the indirect measure of SA. In military fields, the performance is indicated for example by the “kills”, “hits” or mission success or failure [33].

- Process indices

In these techniques, the way of operators maintains the SA during task performance is recorded. For example, using eye tracker to measure participant eye movements during task performance, which is used to gather information about which parts that got more attention by the participants [33].

Furthermore, in the field of nuclear power plants, as mentioned in [26], some skills of operators should be improved to enhance the situation awareness: planning, problem-solving, attention, team coordination, knowledge and communication.

2.4. Resilience Engineering

Safety, in general can be defined as a condition in which there are no undesired issues such as incidents or accidents. It also can be defined as the ability of system to ensure that the disturbances to workers, the public and the environment are acceptably low [35]. Regarding the concept of safety, Hollnagel [35] defined the safety into Safety-I and Safety-II.

Safety-I focuses on what goes wrong in the system and assumes different views of work and activities. “Things go right” if the system is functioned and people work as expected. On the other hand, if there are malfunctions or failures it is said that “things go wrong”. Figure 2.4-1 summarizes the different views. The level of safety in safety-I is determined by how many things go wrong in the system.

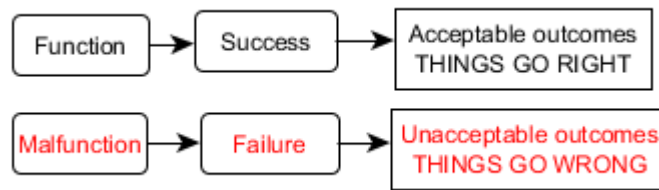


Figure 2.4-1. Different views of work and activities in safety-I [35]

Moreover, safety-I concerns about finding the cause of the events, developing an appropriate response and action to mitigate and eliminate the events that harm the system. Another concern is the prevention of transition from normal to abnormal state by increasing compliance and eliminating variability [35].

Unlike Safety-I, the concern of Safety-II is “what goes right” which means that systems should be functioned under varying conditions and more focus on the understanding of why things go right. If the system goes wrong, the first thing to do is to understand how it always goes right and do not have to find the causes which only describe the failure [35]. Literature [36] summarizes the difference between the concept of safety-I and safety-II as can be seen in Table 2.4-1.

Table 2.4-1. Safety-I and Safety-II [36]

	Safety-I	Safety-II
Definition	Determined by the number of things go wrong	Determined by the number of things go right
Management of safety	Reactive, respond when something happens	Proactive, try to anticipate developments and events
Accidents explanations	Caused by failures and malfunctions	Things basically happen in same way, regardless of the outcome
Human factor view	Liability	resource

The concept of Safety-II is relevant with the resilience engineering. After the Fukushima nuclear power plant accident in 2011, the concern of safety concept change from safety-I to safety-II. The purpose of resilience engineering is to prevent things from going wrong and to assure that things go right. A system is said to be resilience if it can adjust its functioning before, during, or following changes and disturbances [37].

Moreover, resilient engineering is not about reaching a level of safety but how well the organization performs and also does not characterize a state or condition but focuses on how process or performance are carried out [26]. Therefore, becoming resilience is different from becoming safe.

Figure 2.4-2 shows the principles of resilience engineering or the four cornerstones of resilience engineering [32]. “Knowing what to do” is related with the ability to focus on the actual which is how to respond to regular and irregular disturbances by applying a set of responses. “Knowing what to look for” is the ability to monitor a risk or a potential risk in the near future. It is related with the ability to address the critical. In addition, “knowing what to expect” is the ability to address the potential, which is how to anticipate potential changes, deviations, pressure and their consequences. Finally, the ability to address the factual is important in “knowing what has happened”, which is how to learn from experience both successes and failures.



Figure 2.4-2. Four cornerstone of resilience engineering [32]

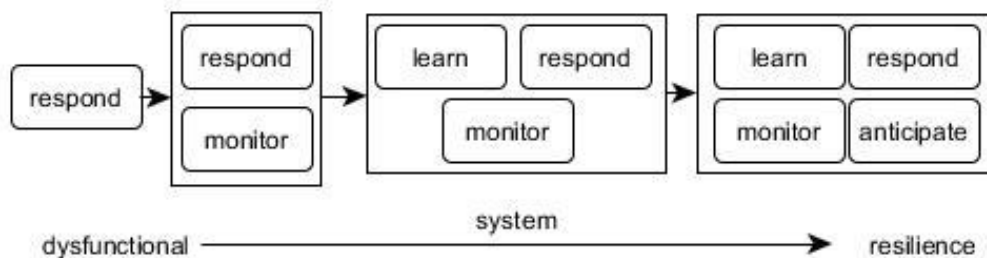


Figure 2.4-3. Step to resilience (adopted from [38])

There are some steps for people or systems to achieve resilience [38], as can be seen in Figure 2.4-3. These steps related with the improving the four abilities differently but not independently. First, for the dysfunctional system, the system only has ability to respond the regular and irregular condition in effective and flexible manner. Then the abilities are improved to respond and to monitor. The ability to monitor related with the monitor short term developments and threats and revise the risk models. In this level, a system is in the reactive safety management system. If the system can improve its abilities with the ability to learn from the past events and understand what happened and why, it becomes in the level of proactive safety management system. Finally, the system is resilience if it develops all the abilities including to learn, to respond, to monitor and to anticipate (related with the long-term threats and potential).

This thesis focuses on the ability to monitor and to anticipate. As mentioned before that monitoring is the ability to monitor a possible threat in the near term which happens in the environment and the system itself that need a response. In order to properly monitor the system and the environment, a set of valid and reliable indicators is needed [39]. Moreover, the time and resources are required to be available and need to have a monitor strategy which involve skills and knowledge [40]. In case of nuclear power plant, it includes looking at the right instruments and indicators (alarm and trends) in the control room, looking through the procedure and monitor the procedure progress to ensure that it is properly completed. If the indicators are absent, operators should rely on their plant knowledge, situation awareness and problem solving skills [39].

On the other hand, anticipating is the ability to anticipate the potential changes, disturbances, changing operating conditions in the near future and their consequences. It is related to the ability to address the potential and knowing what to expect and more influenced by learning from the past. It also includes the capability to see things from different views. Anticipating, compare with monitoring, it is not data-driven and rarely a time-critical function. Factors affecting the ability to anticipate are, for examples, knowledge and experience, quality of information and the operating procedures [41]

The operating procedures have correlation with the ability to anticipate provided that they have an explicit purpose of each procedure and notes and warning to indicate

that something happened in the system due to the deviation of parameter level of components. Monitoring and anticipating require operators to look forward in the procedures and in the operations as a whole as a means to get ready for the future events [39].

2.5. Functional Information

Nuclear power plants are equipped with automatic systems which will be actuated when an anomaly happened in the plant in order to trip the reactor to stop the fission reaction, and so on. However, the role of humans as nuclear operators is very important to maintain the safe operation and to mitigate the accident and also bring back plant to a safe condition. As mentioned in the previous section, the roles of operators include monitoring and controlling tasks. In order to complete the task properly, necessary information is needed for the operators. Such information are, for examples, the status of components or equipment, operating state of equipment, values of process parameters and condition of equipment and structures [42]. Presentation of information should simple and support the operators to perceive information easily, and also avoid misunderstanding and cognitive complexity.

The common information display systems provide the behavioral and structural information which is useful to understand the plant situation. However, because of the absence of information from the intentional aspect of plants, it is difficult to understand the goal and purpose of counter actions mentioned in operating procedures or suggested by an operator support system [43]. Therefore, the concept of functional information [43] was introduced which express the system in a high level of abstraction and why a component exist in the system [7]. As mentioned by Gofuku in [7] that “functional information can be a language to bridge a human and a machine as it corresponds with the goal-oriented thinking and the understanding process of a human”. In addition, functional information should be displayed together with behavioral, structural and operational information. Functional information describes the reason and background of components that are important for operators to understand the plant situation and the suggested actions by the operating procedure. The functional information is also useful for understanding the anomalous situation

in a system, and finding the plausible counter actions beyond that has been prepared in the operating procedures [7].

In order to get the functional information, systems are represented in functions and objectives that are interconnected using inference relations (functional modeling). The inference relations indicate the cause and effect relations among function and between functions and objectives. The functional modeling can be explained by giving an example of car as discussed in [7] and shown in Figure 2.5-1 and Figure 2.5-2. There are two types of car based on the generating the driving force, by gasoline (Figure 2.5-1. a) and by electric power (Figure 2.5.1.b). The structure, components and principle to generate the driving force between the two types of cars are different. However, the two types of the cars have the same purpose or function as means to travel or to carry baggage. Therefore, in terms of function or purpose, the two cars can be redrawn in the same hierarchical model as can be seen in Figure 2.5-2.

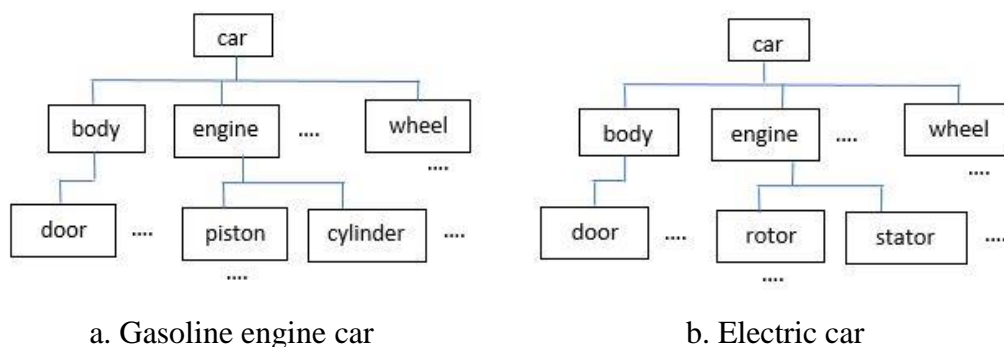


Figure 2.5-1 Structure models of a gasoline and an electric car [7]

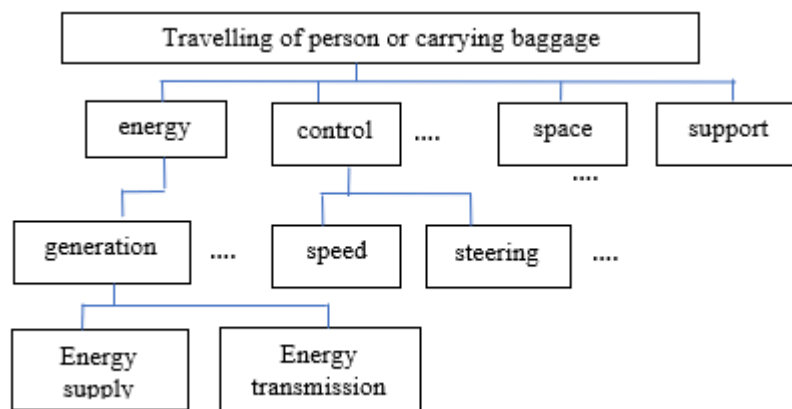


Figure 2.5-2. Functional model of a car [7]

Literature [7] mentioned that functional information has some benefits such as:

- System's behavior can be associated with the role and purpose of each component. It is useful for displaying information how to overcome an anomaly situation.
- The influence and cause-effect relation, in the functional modeling can be used to predict the qualitative effect and influence of an operation or a system failure.
- The system's behavior can be understood by the hierarchical structure in the functional modeling.
- The semantic gap in communication between operators and computer is reduced because of the capability of linguistic representation in functional modeling.

Chapter 3

3. Techniques to Derive the Additional Information Based on MFM Models

3.1. Overview of MFM

Multilevel flow modeling [4, 45, 46] was developed to model a complex plant system in terms of goals, functions, multiple levels of means-end and part-whole abstraction [46]. The means-end concept is used to model the system functions (means) to achieve goal/subgoals (end). In addition, in the part-whole concept, systems can be represented as a whole or subsystems in a hierarchical way [47]. MFM has three basic concepts: goals (objectives or purposes of the systems); functions (means to obtain the goals); and physical components (equipment to build the system) [48].

Gofuku [49] mentioned that by changing the abstraction level, it will make it easier to deal with a complicated system such as nuclear power plants for designing and managing the abnormal situation of the system. MFM has been implemented, for example, for operator support system in supervisory control [50, 51] and dynamic operation permission system [24, 52]. In addition, MFM can be used to express the information related to the plant condition in linguistic form. This functional information is very important for supporting the operators conducting their tasks to monitor and control the plant.

MFM is a method to represent complex industrial system in term of functions and objectives and the interconnection among them in high level of abstraction. Unlike other object-oriented modeling, MFM offers some benefits. In other object-oriented modeling (such as UML or hierarchical colored Petri-net), as mentioned in [53], the validity of diagnosis result is the main focus and do not reveal the diagnosis process to the operators. It means that operators do not understand what happened in a diagnostic system based on other-oriented modeling techniques. On the other hand, MFM provides comprehensive diagnosis based on perspective of human on the objective of the system. MFM breaks down the system into means-ends and whole-part dimension. In the means-ends dimension, MFM depicts the relationships among functions to achieve the system objective. On the other hand, the system is described

in different levels of aggregation in whole-part dimension. In addition, MFM provide realization relation which corresponds physical components with their functions, for example, function of transporting water can be realized by a pump. Furthermore, another important aspect of MFM is its ability to conduct consequence reasoning which is very useful for assessing the plant situation and system performance. The consequence reasoning is based on influence propagation, which indicates that the change of state of a function or objective will change the state of other neighboring functions or objectives (downstream connections). Regarding this study, the consequence reasoning and influence propagation are very useful to comprehensively gather the proposed additional information (components influenced and future plant behavior).

3.2. MFM Symbols

Figure 3.2-1 shows the MFM symbols used for constructing an MFM model. The symbols consist of functions primitives (such as source, transport and storage) and relations (influence, means-end and control). The function primitives correlate with the plant components. For example, a transport function is correlated with a pipe and a tank is represented by a storage function. An MFM model generally consists of mass flow structures, energy flow structures, control structures and objectives.

Each function primitive is connected by influence relations (influencers or participants). The influencer means that the relation influence the amount of material delivered by a transport function connected to a flow function (source, sink, storage or balance). If the transport function is passively provided or received material from the flow function, it is said that the relation is participant. Moreover, other relations are means-end relations which connect flow structures with objectives (produce, maintain, destroy and suppress) or connect function primitives with flow structures (produce-product and mediate). The flow structures or functions represent means to achieve objectives (end).




























Function (mass-energy flow)			Function (control)			
source 	transport 	storage 	steer 	trip 	regulate 	suppress 
sink 	barrier 	balance 	Other			
conversion 	distribution 	separation 	objective 	threat 	function structure 	
Relations						
Influence		Means-end			Control	
influencer 		produce 	maintain 	destroy 	enable 	disable 
participant 		suppress 	mediate 	produce-product 	actuate 	

Figure 3.2-1. MFM symbols

3.3. MFM Reasoning

As mentioned in previous section that MFM is a tool to represent the complex industrial plants in block of symbols that correlated with functions and goals. In addition, it is also a tool to analyze and reason about the system performance based on relations between states of functions and objectives. Cause-effect relations are used to conduct reasoning in MFM. Owing to the fact that MFM decomposes a complex system in means-ends and whole part dimensions, the cause-effect in both dimensions has to be considered [54]. Therefore, there are two patterns related with the cause-effect relations involving “goal to function” and “function to function” in MFM models: influence relation and means-end relations [45].

Influence relations

The flow structures are constructed by the interconnected function primitives. The interconnections also created the cause-effect relations between states of function primitives. The relations are called influence relations. There are two types of influence relations: direct influences and indirect influences. As mentioned before that the cause-effect relations are based on the states of the function primitives, the state of the function primitives in the MFM model should be defined as provided in Table 3.3-1.

The definition of the states of MFM is based on [55]. However, in this thesis, some modifications have been proposed in order to cover some conditions in real plants. Such modification, for example, is to treat “no flow” in “transport” function primitive, which indicates that there is no mass/energy transferred from one component to another component. The underlined states indicate the modified parts of the definition. The “no volume” state is additionally defined to treat no liquid mass condition of a tank-type component.

Table 3.3-1. Definition of state of MFM

Symbols	States
source	normal, high output flow potential, low output flow potential, <u>no output flow potential</u>
sink	normal, high input flow, low input flow, <u>no input flow</u>
transport	normal, high flow, low flow, <u>no flow</u>
storage	normal, high volume, low volume, <u>no volume</u>
barrier	normal, leak
balance	Normal (balance), unbalance (fill or leak)
threat	exist (high), exist (low), non-exist
objective	true (high), true (low), false

In direct influences, the influence is indicated by how transport functions influence other function primitives. The function primitives connected to a transport function in the mass or energy flow will be influenced by the state of the transport function in both its upstream and downstream directions [54]. On the other hand, if the transport function is influenced by other function primitives, it is called indirect influences [54]. The influencer and participants connections impact the influence in the indirect influence but not in the direct influence. Literature [55, 57, 46] describe the detail about the formulas for direct influence and indirect influence and some examples are provided in this thesis. The examples of rule for direct influence for both upstream and downstream connections, adopted from [56] are provided in Table 3.3-2. On the other hand, the rule for indirect influence is different between with influencer relations and participant relations, as can be seen in Table 3.3-3 and Table 3.3-4, respectively.

Table 3.3-2 Direct influence for upstream and downstream connections [56]



Inference upstream		
Cause	Consequence	
tra2-4: high flow	sou1-2: low output flow potential sto2-3: low volume	
tra2-4: low flow	sou1-2: high output flow potential sto2-3: high volume	
Inference downstream		
Cause	Consequence	
tra6-9: high flow	sto4-5: high volume sin1-2: high input flow	
tra6-9: low flow	sto4-5: low volume sin1-2: low input flow	

Table 3.3-3 Indirect influence with influencer relations [56]



Inference upstream		
Cause	Consequence	
sto6: high volume sin3: high input flow	tra10, tra11: low flow	
sto6: low volume sin3: low input flow	tra10, tra11: high flow	
Inference downstream		
Cause	Consequence	
sou3: high output flow potential sto7: high volume	tra12, tra13: high flow	
sou3: low output flow potential sto7: low volume	tra12, tra13: low flow	

Table 3.3-4 Indirect influence with participant relations [56]

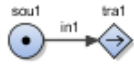
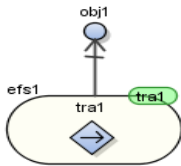
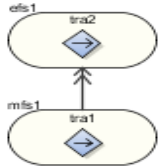
Inference upstream		
Cause	Consequence	
sto8: high volume sin4: high input flow	tra14, tra15: low flow	<pre>graph LR; tra14 -- pa6 --> sto8; sto8 --> tra15; tra15 -- pa7 --> sin4</pre>
sto8: low volume sin4: low input flow	N/A	
Inference downstream		
Cause	Consequence	
sou4: high output flow potential sto9: high volume	N/A	<pre>graph LR; sou4 -- pa8 --> tra16; tra16 --> sto9; sto9 -- pa9 --> tra17</pre>
sou4: high output flow potential sto9: high volume	tra16, tra17: low flow	

Means-end relations

There are two types of means-end relations. First is the connection between flow structures and objectives. It is connected with the produce, maintain, destroy or suppress relations. Second is the connection between function primitives and flow

structures using producer-product and mediate relations. The means-end relations also contribute to the cause-effect relations between states of function primitives and objectives. The examples of rules of means-end relations is given in Table 3.3-5. It can be seen that, for example, if the objective obj1 is true (high state) then the transport function tra1 will in high flow condition.

Table 3.3-5 Rules of means-end relations

Patterns	Cause	Consequence
	sou1	tra1
	High output flow potential	High Flow
	Low output flow potential	Low Flow
	obj1	tra1
	True (high)	High Flow
	True (low)	Low Flow
	tra1	tra2
	High Flow	High Flow
	Low Flow	Low Flow

3.4. Influence Propagation

The concept of cause-effect relation is implemented in MFM. The usage of cause-effect concept was proposed by the study to generate plausible counter operations based on MFM models created by the past symbol set [12]. Because this study uses current symbol set of MFM, the rules of influence propagation proposed in the literature [56] are used, there are two types of cause-effect relations: direct and indirect influence. In a direct influence, the state change of a function primitive, for example, transport function will cause state changes of neighboring functions connected to the transport function. On the other hand, in an indirect influence, the state change of a function primitive is caused by other functions. The concept is the

basis for influence propagation rules. Figure 3.4-1 depicts the influence propagation in an MFM model.

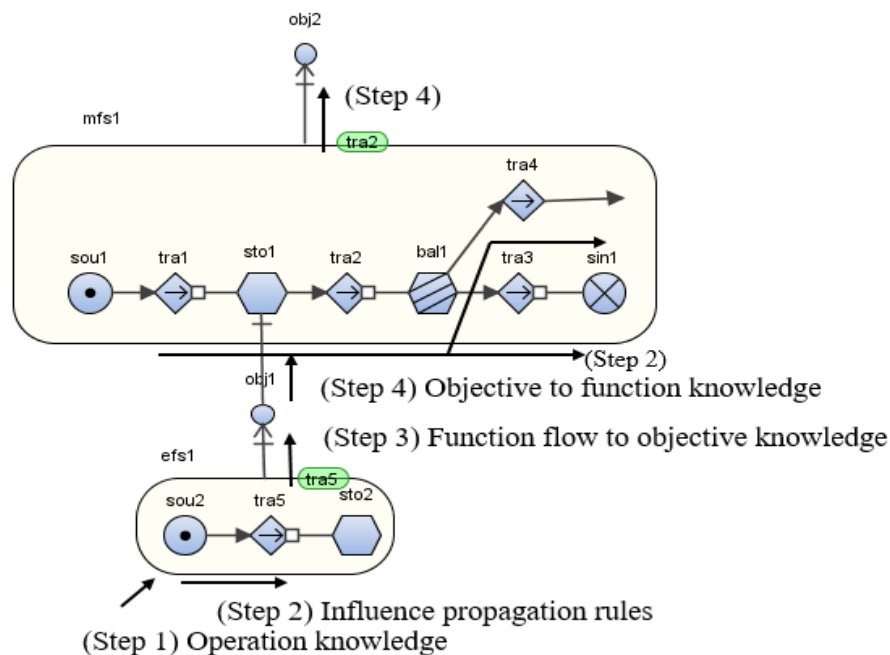


Figure 3.4-1 Influence propagation

First of all, in step 1, an operational action on a component will change the state of the function primitives that is realized by the component. The state change in qualitative level is given by an operation knowledge that correlates an action of a component with a state change of the function realized by the component. An example of the operation knowledge is that closing a valve changes the state of correlated transport function from “normal” to “no flow.” The state change then influences the downward function primitives in the function structure that the function primitives belong to (step 2). Moreover, by using the knowledge that correlates a function flow with an objective (step 3), the change of function state will influence the objective connected to the function by a means-end relation in Figure 3.4-1. On the other hand, the objective is also connected to a function by a control relation. The state change of the objective will influence the state of the function. Then, the state change influences the states of all related function primitives (step 4). Therefore, it can be concluded that the change of the state of the function primitive correlated with the component that a counter action (by automatic system or human operators) is made will influence

the states of function primitives, objectives and then propagates the influence in some parts of system.

As an example of the influence propagation rules, an MFM model of tank process is used, in which the model is similar to the MFM model in Figure 3.4-1. In this case, efs1 represents the energy flow in the pump and obj1 is the objective to keep the pump running. The water flow in the tank is represented by mfs1, while the main objective to maintain the correct water level in the tank is represented by obj2. Initially, all of states of function primitives is in a normal condition and the objectives are enabled. In order to describe the influence propagation rules, let no electrical energy supplied to the pump. It is indicated by no output flow potential in sou1 (operation knowledge). The state change of sou1 will influence the downstream connections, tra5 to change from normal flow to no flow. Because there is no energy flow in the pump, the objective obj1 “to keep the pump running” cannot be achieved. The failure of achievement of obj1 will disable the tra1 (pump) and change the state from normal flow to no flow. It means that there is no water flow from the pump. This condition then change the state of all downstream connections from normal to no flow. The state change finally influences the input flow of sto2 to no input flow. It indicates that the tank is not filled with the water which cause the objective obj2 “to keep the level in the tank” is not achieved

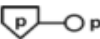
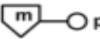
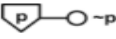
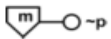
3.5. Modeling of a Counteraction by MFM Control Function

Operator’s action or a counteraction conducted by human is a manual intervention to the system based on the knowledge, conditions or predefined values to change the state of a component in order to achieve an objective of changing the plant state in a safer one and/or of mitigating influence of an anomaly. The effort of operators to mitigate the accident by executing the instruction in the EOP, for example, operating the auxiliary feedwater system to regulate the level of faulted and intact SG after determining and isolating the ruptured SG can be categorized as a counteraction. The concept of counter action is relevant with the concept of control function in the MFM. Therefore, the control function in MFM is used to model the operator’s actions.

The control functions of MFM are applied in this study to model the counter actions on an EOP. Control function is proposed by Lind [44, 57] and has been

implemented in some studies [46, 58]. There are several types of control functions [44] in MFM as can be seen in Table 3.5-1.

Table 3.5-1 MFM control functions

Task	Symbol	Purpose
Steering		Ensure that p is produced
Regulation		Ensure that p is maintained
Tripping		Ensure that ~p is produced
Interlock		Ensure that ~p is maintained

Counter actions represent the actions which change something from one plant condition to another condition. Because a counter action will change state or create a new state of a function primitive, the basic control function for modeling the counter actions is the steering (producing) control function.

Following the idea proposed in [44], the model of operator's action is represented in Figure 3.5-1. In the figure, only the relevant function primitives in mass flow structure mfs1 are shown. The explanations of the control function are as follows. The conditional operation of the control function is to change the state of the storage function sto1, for example from low volume to high volume. The conditional operation is connected to the objective function obj1 using produce relation (pr1).

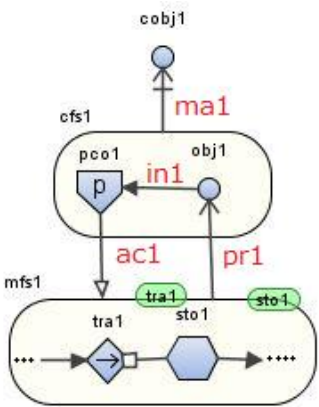


Figure 3.5-1. MFM control function

Therefore, the objective of the system is to change the state of the sto1. If the sto1 represents the tank, then the objective is to change the volume of the tank. Based on the conditional operation and the objective, the control function pco1 is activated (in1) and then change the state of transport function tra1 in mfs1 indicated by the actuation relation (ac1). If the all the conditions are satisfied, the control objective (cobj1) which is connected to mfs1 using maintain relation (ma1) is achieved.

In case of modeling the counter actions of EOP, the objective and the conditional operation is represented by the purpose of the procedure step. In Figure 3.5-1 it is represented by the intended state of sto1. The counter action or the human action is represented by the control function pco1 and the component or function to be controlled is the transport function tra1. If it is intended that the volume of the sto1 is high, then the transport function tra1 should be controlled or the state should be changed from low flow to high flow.

3.6. Algorithms to Derive the Additional Information

Additional information is information related with the impact of an automatic system operation and human action is very important and the information can help operators to understand and follow the procedure steps. This section proposes the algorithms to generate the additional information: component influenced and future plant behavior. The algorithms apply the influence propagation described in the previous section based on an MFM model.

3.6.1. Components influenced

Figure 3.6-1 shows the algorithm to generate the information of components influenced n as a consequence of a counter action (automatic or human action) following the instructions of an EOP. Followings are the explanation of the algorithm. As described in section 3.5, the counter action is represented by control function in MFM model. Each operation in an EOP is in advance correlated with a control function structure. The correlation is made by “operation condition”. The operation condition is composed of the name of operation, control flow function corresponding to the operation, and state modifier to express the change of the state of the function

primitive that is controlled by the operation. As an example, consider the process of increasing the volume of water in a tank. In this case, the operation condition and system objective are to increase the level of water in the tank (“tank”, “high volume”). Based on the operation condition, the control function is actuated to start the pump and open the valve which allow water to flow and fill in the tank.

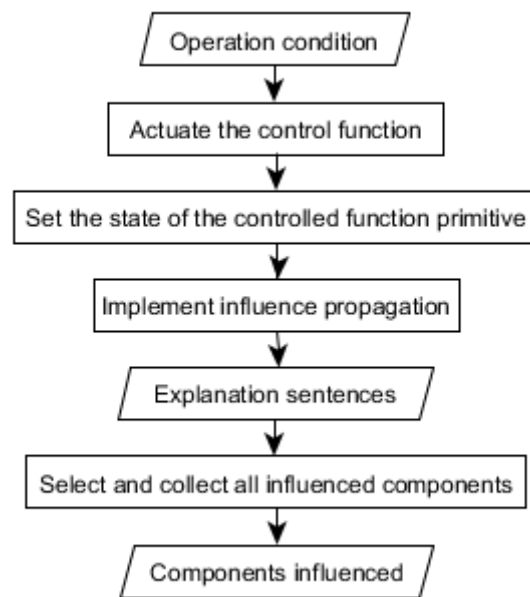


Figure 3.6-1. Algorithm to derive components influenced information

The next step is to propagate the state change of downward function primitives in the function flow structures that include the affected function primitive using influence propagation. If there is a relation with other function flow structures by “means-end relations”, the influence is propagated to the function flow structures. In addition, the influence also impacts the objective connected to the flow structure. If all the influences have been investigated, the results of the influence propagation can be expressed by using “explanation sentences” which describe the state change of function primitives (function components) and the state change of physical components (realized components). The realized components are identified using “realization relations” that correlate functions primitives with the physical components. The “realization relations”

contain a list of function primitives and their correlations with physical components and related mass or energy flow structure, using the following format:

realization relation: (“function primitive”; “physical component”; “mass/energy”;
“object name”)

For example, a storage function (sto) is correlated with a tank and water stored in the tank. In this case, the realization relation can be expressed as (“sto”; “tank”; “mass”; “water”).

3.6.2. Future plant behavior

The counter action (automatic or human action), as mentioned in the previous section, impacts the conditions of system components. Consequently, the future plant behavior is also changes because of the operation actions. By the use of an MFM model, the plant behavior can be correlated with the achievement of function objectives or the change of the states of function primitives in a system. Information about future plant behavior is also important for operators to understand the consequence of procedure steps.

The algorithm to derive the future plant behavior is provided in Figure 3.6-2. To begin with, the first five steps are similar with the algorithm for deriving the components influenced (Figure 3.6-1). Therefore, the explanation sentences made by the algorithm to derive the components influenced are partially used by this algorithm.

The next step is to select and collect one main explanation sentence for each component from the explanation sentences for the component considering the main function. Main function means a system or a component which is important for safety and should be considered by operators.

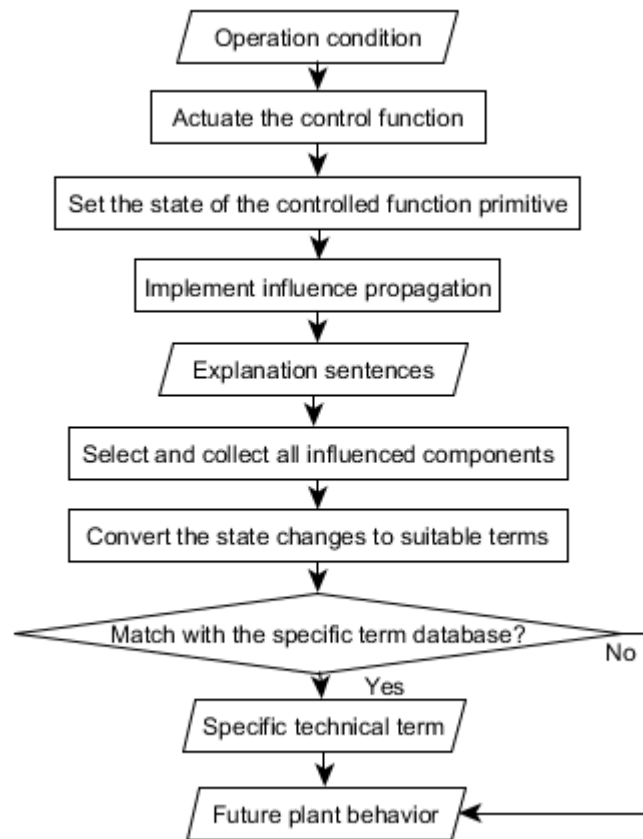


Figure 3.6-2. Algorithm to derive future plant behavior information

3.7. Explanation Sentences

MFM is useful tool for investigation of cause-effect relation of influence of counter actions to derive the functional information. The functional information should be presented to operators in understandable way. It can be expressed using explanation sentences. The explanation sentences are derived based on the algorithms proposed in the previous section. The explanation sentences are generated for component influenced and future plant behavior.

3.7.1. Components influenced

The explanation sentences can be generated using the following pattern:

(a) Function primitives

(state of function primitive) + “of” + “mass/energy” + “in” + (function primitive)

(b) Realizing components of function primitives

(state of function primitive) + “of” + (object name of mass/energy) + “in” + (physical component)

In the pattern, “mass” is used if the function primitive is included in a mass flow structure, and “energy” is used if it is included in an energy flow structure. The converted explanation sentences are sometimes not natural English expressions due to the simple conversion technique. However, an operator will understand the meaning.

Finally, from the explanation sentences of pattern (b), the influenced components are selected and collected. The “main components” database is provided for selecting and collecting the influenced components from the explanation sentences. If the influenced components are in the list of “main components” database, they are set as components influenced and written using following format:

The components influenced: (“influenced physical components”)

3.7.2. Future plant behavior

Regarding the future plant behavior, the explanation sentence is made by setting suitable terms that represent the plant behavior to the parts of the following sentence pattern:

(state of function primitive) + “of” + (object name of mass/energy) + “in” + (physical component)

Furthermore, special technical terms expressing plant behavior, which are derived from operational procedures or accident management, such as safety injection (SI), reactor trip, etc. are also stored in a database called “specific term” database that correlates a term with the state of function primitive. For example, the specific term “hot shutdown” can be given for some plant behavior such as reactor trip (no flow of heat in reactor vessel), turbine trip (no flow of

mechanical energy in turbine) and generator trip (no flow of electrical energy in generator), and so on. Finally, based on the algorithm in Figure 3.6-2., if some state changes of influenced components are matched with the “specific term” database, then the future plant behavior is expressed in specific technical term. Otherwise, if they are not matched, the future plant behavior is expressed using the selected sentences for components.

Chapter 4

4. Modeling of PWR Plant and Emergency Operating Procedure

4.1. Outline of PWR Plant

This chapter describes the overview of PWR structure diagram and the MFM model of the PWR plant. Then, the steam generator tube rupture (SGTR) accident of a PWR plant is considered as a case study in this study. Operators should mitigate the accident following the emergency operating procedure in step by step.

In this study, a simplified diagram of pressurized water reactor (PWR) plant is used, as can be seen in Figure 4.1-1 [59]. A PWR system has primary system and secondary system. Primary system transfers heat generated in the fuel and stored in reactor vessel to the steam generator. The steam generator produces steam and then the steam is introduced to turbine to rotate the electric generator. The mechanical energy to rotate is in turn converted to electricity (electrical energy). The steam that some heat energy is lost will be delivered to the condenser and condensed into water and then transferred to the steam generator.

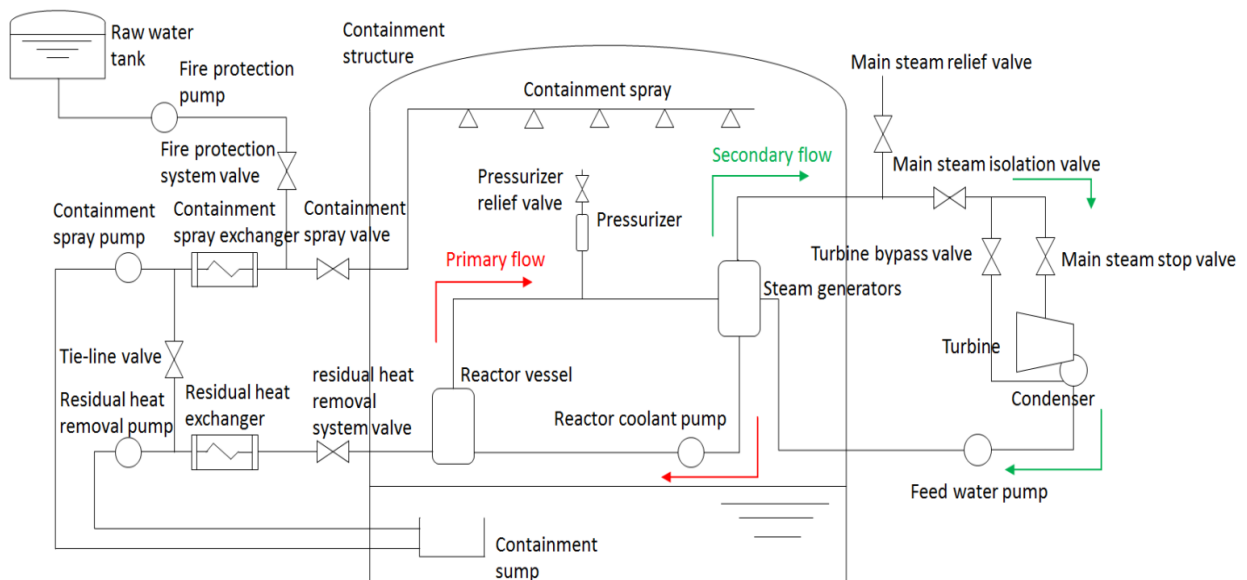


Figure 4.1-1. Simplified diagram of PWR plant

A PWR also has safety systems which will be functioned in case of emergency. When an anomaly happens in the plant, the reactor will be automatically shut down

by the reactor trip and the safety injection signal is actuated to operate the emergency core cooling system (ECCS) to provide water to the reactor coolant system (RCS). Although the reactor is shutdown, it still produces decay heat. The decay heat should be removed to cooldown the reactor by bypassing the turbine and dumping the steam to the condenser. The cooldown process then is completed by the residual heat removal system.

4.2. MFM Model of PWR Plant

In order to investigate how the MFM can model the counter actions on an EOP, a simple MFM model of a PWR plant based on the PWR diagram in Figure 4.1-1 is constructed, as provided in Figure 4.2-1.

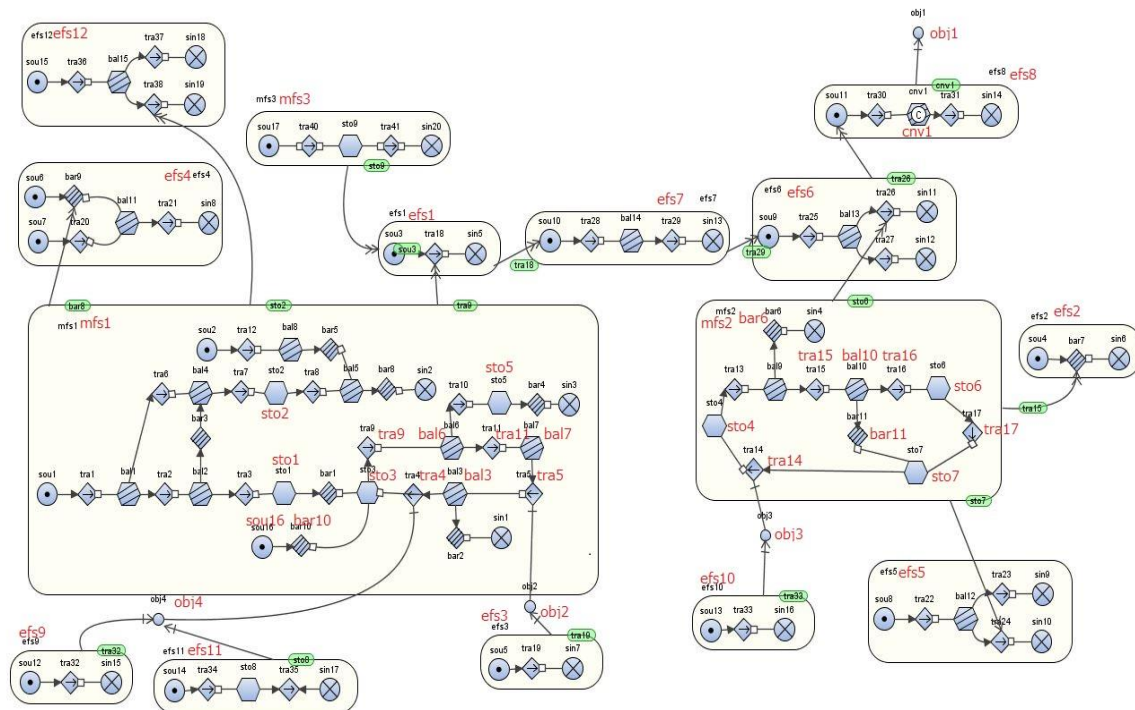


Figure 4.2-1. MFM model of simplified of PWR plant

This model is a modification of the MFM model developed by [59]. The MFM model includes major PWR systems (primary system by mass flow structure mfs1 and secondary system by mfs2) and safety systems such as emergency core cooling system (efs9), residual heat removal system (sto1) and internal spray system (sto2).

Table 4.2-1 describes some main flow structures, functions and objectives which will be discussed in this paper.

The main objective (obj1) of the MFM model of the PWR system is to generate the electricity. It can be accomplished by converting the heat energy into electrical energy. Initially the heat is generated in fuel (sou3 in efs1) installed in reactor vessel (sto3 in mfs1) and by fission reaction (represented by the energy flow structure efs1). The heat is transferred from primary system to secondary structure (efs7) through the steam generator ball4 (primary side) and sin3 (secondary side). Furthermore, the heat is converted into mechanical energy in efs6 to rotate the turbine and generator (efs8). Finally, the electrical energy is produced (obj1).

Table 4.2-1. Description of main functions and objectives

Main flow structures		Main functions	
Symbols	Description	Symbol	Description
mfs1	Primary system	sto3	Reactor vessel
mfs2	Secondary system	tra9	Heat transfer
efs1	Heat production	sto5	Pressurizer
efs7	Heat transfer from primary to secondary system of SG	bal7	SG primary side
efs6	Conversion from heat to mechanical energy	tra5	RCP
efs8	Conversion from mechanical to electrical energy	sto4	SG secondary side
efs9	ECCS	sou16 & bar10	Safety injection
efs11	CVCS	sto2	Containment spray exchanger
efs3	RCP	bar8	Containment spray valve
mfs4	Pressurizer heater	sto1	Residual heat exchanger
es13	PORV	sou2	Raw water tank
efs14	Pressurizer spray	tra15	MSIV
efs10	Feedwater pump	tra16	Main steam stop valve
efs5	Condenser	sto6	turbine
efs2	MSIV	sto7	condenser
efs4	Containment spray valve		
efs12	Containment spray exchanger		
mfs3	Control rods		
Objectives			
		Symbol	description
		obj1	Electricity production
		obj2	Pumping primary coolant
		obj3	Provide feedwater
		obj4	Maintain cooling the reactor
		obj10	Maintain subcooling

4.3. Modeling of EOP of SGTR

As a case study, a typical accident of PWR plant caused by a steam generator tube rupture (SGTR) is applied to the MFM model of PWR plant. Some counter actions should be conducted to mitigate the accident step by step following the instruction of

EOP of SGTR. In this case, a simplified EOP of SGTR accident of Mihama Unit 2 [6] is used. Table 4.3-1 shows the steps of the EOP. The reason for choosing the SGTR accident is because it is one of common and potential accident in PWR plants and there are some operator actions depending on the plant conditions. The common causes of the SGTR accident are the degradation and ageing process and also stress corrosion cracking [60]. The SGTR accident should be mitigated following some safety functions: reactor trip, core cooling, steam generator overfills prevention and steam generator isolation.

Table 4.3-1. Simplified of EOP of SGTR [6]

Steps	Descriptions
STEP 1	Occurrence of SGTR thereafter reactor trip and SI
STEP 2	Check RCP restart criteria, if not meet, trip all RCPs, otherwise go to STEP 3
STEP 3	Identification and isolation of faulted steam generator
STEP 4	Regulate the level of faulted steam generator (8% - 50% of narrow range)
STEP 5	Regulate the level of intact steam generator (8% - 10% of narrow range)
STEP 6	Reset SI signal
STEP 7	Recover power of all AC Power
STEP 8	RCS cooldown using steam dump through SG PORV or steam dump valve
STEP 9	Check availability of PZR normal spray Start PZR normal spray, if available. If NOT available, open PZR PORV or use PZR auxiliary spray
STEP 10	Check RCS pressure less than faulted SG pressure and PZR level more than 8%. If NOT, go to STEP 9
STEP 11	Check cease of SI
STEP 12	Regulate PZR level between 50% and 75% using charging flow
STEP 13	Make PZR water saturated by heater
STEP 14	Operate only one RCP
STEP 15	Start RCS depressurization
STEP 16	STOP

The SGTR accident is indicated by the decreasing of pressurizer level and pressure, increasing the level of steam generator, and increasing radiation in main steam line. The safety system will trip the reactor to stop the heat production and safety injection system is actuated to provide the cooling to the reactor coolant system. The next steps are the rupture SG should be identified and isolated in order to prevent the release of radioactive material to the environment through the ruptured SG and turbine. Moreover, although the reactor is shutdown, the residual heat remains in the system. Therefore, it should be removed by cooling down the reactor cooling system by steam dump through SG power operated relief valve (PORV) in case of the condenser is not available or through steam dump valve directly to the condenser. As

the RCS is cooled down and the core temperature is decreased to a certain value, the RCS should be decreased until the pressure remains stable and the safety injection can be stopped. Consequently, one reactor coolant pump can be operated to cool the core and then the RCS can be depressurized by reverse leak through break, blowdown through faulted SG or steam dump.

This section discusses the modeling of EOP by using MFM model of PWR plant including operator actions for SGTR accident. Some procedure steps of simplified of EOP of SGTR in Table 4.3-1 will be discussed. Each counter action in procedure step is represented by an MFM control structure following the idea of Figure 3.5-1 in Section 3.5.

4.3.1. STEP 1: Occurrence of SGTR thereafter reactor trip and safety injection

The reactor trip and safety injection are actuated automatically by safety system when anomalies happen in the plant which cause the decrease of the level of pressurizer. Figure 4.3-1 shows the modeling of counter actions of reactor trip and safety injection. As can be seen in the figure that there are MFM control functions which represent the counter actions (cfs1: reactor trip, cfs2: safety injection, cfs3: stopping RCP). The action of stopping RCS is caused by the safety injection. Therefore, the discussion of safety injection is together with the stopping RCS.

Reactor trip

Reactor trip occurs due to the low pressurizer pressure level and automatically trips the turbine and main feedwater system. It will decrease core power to decay heat levels, terminate the steam flowing through the turbine and actuate the steam dump (turbine bypass). During the accident, the reactor trip is automatically done by the safety system. Reactor trip is realized by the insertion of control rods to the reactor core. The control rods will absorb neutron for producing fission reaction and stop heat production in the reactor core.

In the MFM model, the reactor trip operation is represented by a control structure cfs1. The operation condition is the low level of pressurizer pressure

(low volume of sto5), which is connected to the objective of the system obj1 to shut down the reactor. Based on this condition, the control function pco1 will be actuated to change the state of tra41 in mfs3 (control rods) in high flow. Table 4.3-2 provides the parameters of modeling the counter action for the reactor trip operation.

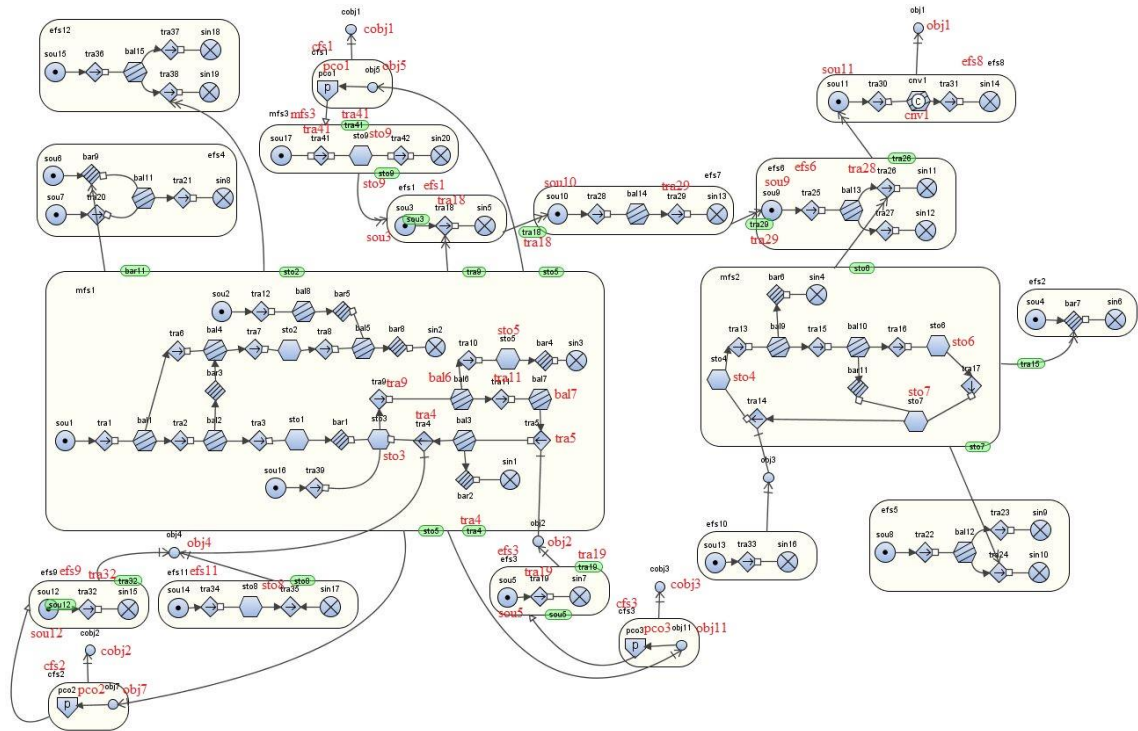


Figure 4.3-1. MFM model of counter actions of reactor trip and safety injection

Table 4.3-2. Parameters of modeling of counter actions for reactor trip

Reactor trip		
Items	Physical components	MFM model
Operation condition	Low pressurizer level	Low volume of sto5
Objective	To shut down the reactor and to stop the heat production in the reactor vessel	obj1
Control function	Insert the control rods	pco1, high flow of tra41
Controlled component	Control rods	tra41
Control objective	To insert control rods into the fuel rods	cobj1

Safety injection and stopping the RCP

In the MFM model, the safety injection is represented by control structure cfs2, as can be seen in Fig 4.3-1. The purpose of the control structure cobj2 is to

start ECCS (efs8). The control function pco2 will actuate the electric power (sou12) in the ECCS if the level of pressurizer (sto5) is low.

Furthermore, the safety injection also causes the RCP stop to operate. In the MFM model in Figure 4.3-1, a system to control the RCP is represented by the control structure cfs3. As the cause of stopping the RCP is the safety injection which is based on the pressurizer level, therefore it can be considered that the operation condition for stopping the RCS is the low volume of sto5. Consequently, the pco3 will change the state of sou5 from normal to no output flow potential. Table 4.3-3 summarizes the parameters of the modeling counter actions for safety injection and stopping RCP.

Table 4.3-3. Parameters of modeling of safety injection and stopping RCP operation

Safety injection operation		
Items	Physical components	MFM model
Operation condition	Low level of pressurizer	Low volume of sto5
Objective	To provide water to the RCS	obj7
Control function	To start the ECCS	pco2: set the state of sou12 to high output flow potential
Controlled component	ECCS pump	sou12 in efs9
Control objective	To start the ECCS	cobj2
Stopping RCP operation		
Items	Physical components	MFM model
Operation condition	Low level of pressurizer	Low volume of sto5
Objective	Stop provide cooling to the RCS	obj11
Control function	Stop the RCP operation	pco3: set the state of sou5 to no output flow potential
Controlled component	RCP	sou5
Control objective	To stop the RCP operation	cobj3

4.3.2. STEP 2: Check RCP restart criteria, if not meet, trip all RCPs, otherwise go to STEP 3

As mentioned in the previous section, after safety injection, the RCP is stopped. In order to maintain the cooling of the RCS, it is important to check whether the RCP should be restarted or not. The RCP is restarted if the pressurizer level and sub-cooling of the RCS are more than predefined value [6]. Because MFM is a tool for qualitative analysis, the criteria will be considered as high (more than a predefined value) or low (less than a predefined value). In this paper, only

Table 4.3-4. Parameters of modeling of check RCP restart criteria operation

Check RCP restart criteria		
Items	Physical components	MFM model
Operation condition	Pressurizer level	Low or high volume of mass in sto5
Objective	Provide water to the RCS from the RCP or do nothing	obj12
Control function	Start or stop the RCP	pco4: if sto5 (high), set the state of sou5 to high output flow potential pco4: if sto5 (low), do nothing
Controlled component	RCP	sou5
Control objective	To start or remain stop the RCP	cobj4

4.3.3. Identification and isolation of faulted steam generator

The next step of mitigation of the SGTR accident is identification the ruptured steam generator (SG). The ruptured SG can be identified by the level of SG, the level difference among SGs and radiation monitoring in SG blowdown line. Afterwards, the ruptured SG should be isolated. The isolation of ruptured SG operation is intended to depressurize the primary and secondary system to minimize the leakage from primary to secondary and to ensure the integrity of the core and primary system, and to prevent the release of radioactive material through the turbine. The ruptured SG is isolated by closing the main steam isolation valve (MSIV).

The MFM model related with the isolating ruptured SG operation is shown in Figure 4.3-3. The isolation of ruptured SG is represented by the control flow structure cfs5 and control function pco5. In this case, the “low volume” in sto6 is the operation condition which represents the “low” or “no” volume of steam that contains radioactive material in the turbine (objective of the system). Based on the causal reasoning of MFM, in order to make the low (no) volume in sto6, the transport function tra15 should be in low (no) flow. Therefore, the pco5 is actuated to change the state of tra16 from normal (high) flow to low (no) flow. The parameters of modeling of the isolation of ruptured SG is summarized in Table 4.3-5.

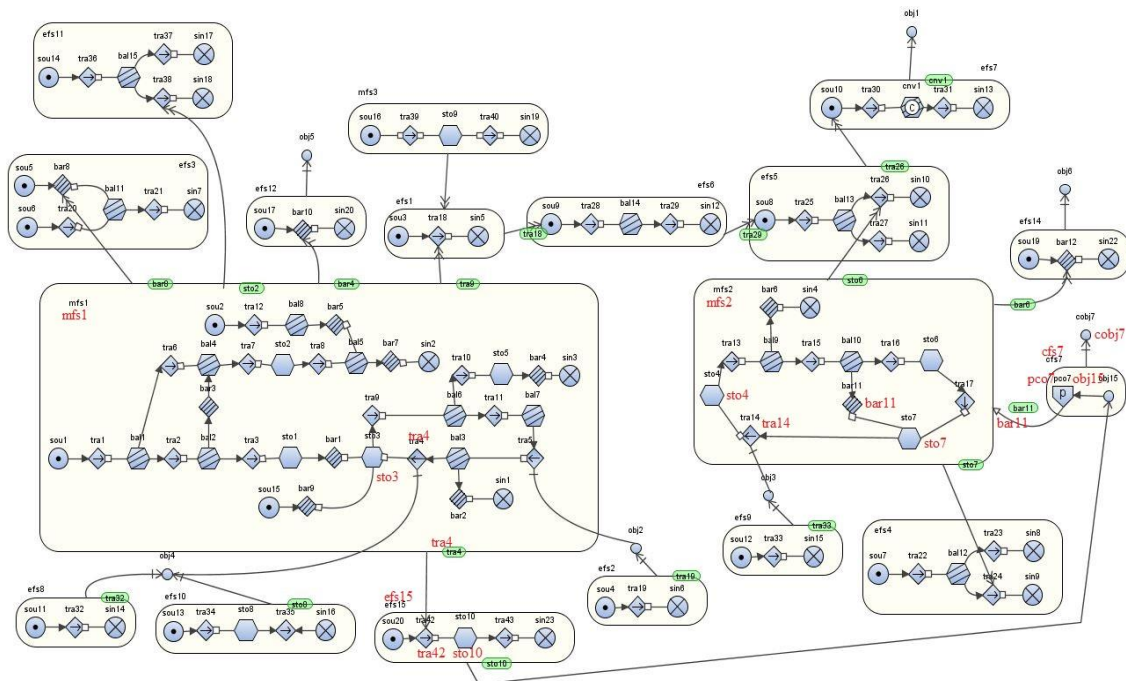


Figure 4.3-4. MFM model of RCS cooldown using steam dump valve operation

Table 4.3-6. Parameters of modeling the RCS cooldown operation

Regulate of SG level		
Items	Physical components	MFM model
Operation condition	Low temperature of RCS	Low volume of sto10 in efs15
Objective	To decrease the temperature of RCS	obj15
Control function	Open the steam dump valve	pco7: disable the bar11
Controlled component	Steam dump valve	bar11
Control objective	To open the steam dump valve	cobj7

After the reactor trip and safety injection operation, the reactor is in hot shutdown condition. It means that the residual heat remains in the system and should be removed by dumping the steam from the SG in order to cooldown the RCS. In case of the condenser is available, the steam can be dumped by bypassing the turbine and opening the steam dump valve to let the steam directly flowing to the condenser. In Figure 4.3-4, the temperature level of the RCS is represented by the state of sto10 in efs15 (energy flow of RCS). Therefore, the operation condition is the low volume of sto10 which is correlated with the obj15, which in turn actuate the control function pco7 to disable the barrier function bar11. If the

barrier function is disabled, it means that the mass or energy can be transferred through the function. Therefore, it can be considered that the barrier function acts as a transport function

Chapter 5

5. Application Results and Discussions of Deriving Additional Information

The algorithms to derive the additional information and the explanation sentences described in the Chapter 3 are applied to the counter actions of executing procedure step of EOP to mitigate the SGTR accident of the MFM model of a PWR plant. Some investigations also have been conducted by the author in [62, 63, 64]. The derivation results for some procedure steps will be discussed including automatic actions and operator actions in this chapter.

5.1. Reactor trip and safety injection

Figure 5.1-1 shows the related part of MFM model with reactor trip operation. The counter action is modeled by the control structure cfs1 with the operation condition is the low volume of mass in sto5. Then, the reactor trip controller (pco1) changes the state of tra41 in mfs3 from no flow to high flow, which in turn, following the cause-effect relation and influence propagation, the high flow of tra41 causes “no output flow potential” in sou3 in efs1 that corresponds to no heat generation in reactor core region. Then, based on the influence propagation, there is no energy flow through tra18 to sin5 in efs1. Moreover, the influence propagated to efs7 changes the state of sou10 to “low/no output flow potential” and to “low/no flow” in tra29. Consequently, the efs6 has no energy flow because of “no output flow potential” in sou9 and “no flow” in tra28. The final influence is, because there are “no flow” in tra28 and “no output flow potential” in sou11, the conversion function cnv1 will not be enabled. Therefore, the objective obj1 to produce electricity to the grid will not be achieved.

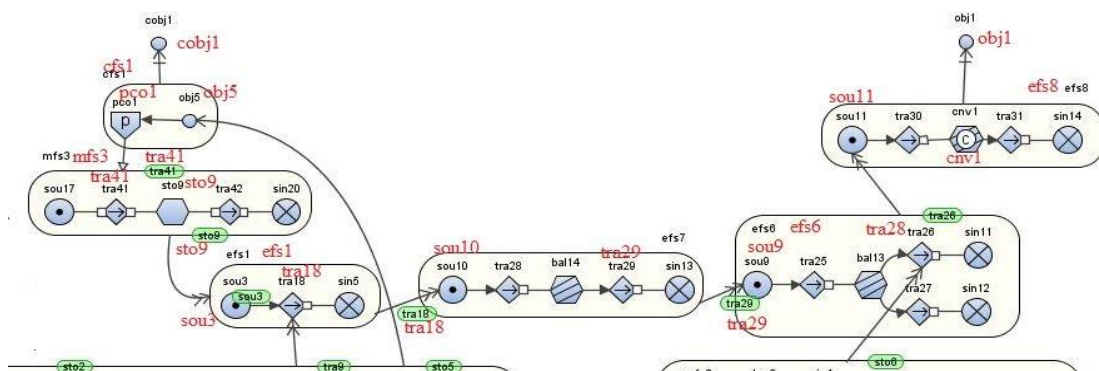


Figure 5.1-1. Part of MFM model related with reactor trip

Table 5.1-1. States of function primitives before and after the reactor trip operation

Counter action	Initial state	After counter action
Reactor trip	Tra41 (no flow), sou3 (normal), tra18 (normal), sou10 (normal), tra29 (normal), sou9 (normal), tra28 (normal), sou11 (normal), cnv1 (enable), obj1 (true)	tra41 (high flow), sou3 (no output flow potential), tra18 (no flow), sou10 (no output flow potential), tra29 (no output flow potential), sou9 (no output flow potential), tra28 (no flow), sou11 (no output flow potential), cnv1 (disable), obj1 (false)

Table 5.1-2. Explanation sentences for the influences of reactor trip operation

Functions	Functional components	Realizing components
tra41 in mfs3	High flow of mass in tra41	High flow of control rods in Reactivity control system
sou3 in efs1	Low (No) flow output potential of energy in efs1	Low (No) flow output potential of heat in Fuel rods
tra18 in efs1	Low (no) flow of energy in tra18	Low (no) flow of heat in Reactor vessel
sin5 in efs1	Low (No) flow input of energy in sin5	Low (No) flow of heat in Reactor vessel
sou10 in efs7	Low (No) flow output potential of energy in sou10	Low (No) flow output potential of steam in SG
tra28 in efs7	Low (No) flow of energy in tra28	Low (No) flow of heat of water in primary side of SG
bal14 in efs7	Balance of energy in bal14	Balance of heat in SG tube
tra29 in efs7	Low (No) flow of energy in tra29	Low (No) flow of heat of steam in secondary side of SG
sin13 in efs7	Low (No) flow input of energy in sin13	Low (No) flow input of heat of steam in secondary side of SG
sou9 in efs6	Low (No) flow output potential of energy in sou9	Low (No) flow output potential of heat of steam in Turbine
tra25 in efs6	Low (No) flow of energy in tra25	Low (No) flow of heat of steam in Turbine
bal13 in efs6	Balance of energy in bal13	Balance of heat in Turbine
tra26 in efs6	Low (No) flow of energy in tra26	Low (No) flow of mechanical energy in Turbine
sin11 in efs6	Low (No) flow input of energy in efs6	Low (No) flow input of mechanical energy in Turbine
sou11 in efs8	Low (No) flow output potential of energy in efs8	Low (No) flow output potential of mechanical energy in Generator
tra30 in efs8	Low (No) flow of energy in tra30	Low (No) flow of mechanical energy in Generator
cnv1 in efs8	Low (No) energy conversion of energy in cnv1	Low (No) flow of energy in Generator
tra31 in efs8	Low (No) flow of energy in tra31	Low (No) flow of electrical energy in Generator
sin14 in efs8	Low (No) flow input of energy in sin14	Low (No) flow of electrical energy in Electric grid

The change of states of function primitives caused by the reactor trip operation and the influence propagation is given in Table 5.1-1. The influence propagation due to the reactor trip operation can be expressed using explanation sentences as shown in Table 5.1-2. The explanation sentences are derived based on the “realization relation” database and the pattern described in Subsection 3.7.1. The “realization relation” contains data of function primitives and the correlated components as mentioned in Table 4.2-1, such as mfs3 represents the control rods; and the heat transfer from primary to secondary system of steam generator is represented by efs7. Therefore, from Table 5.1-2, it can be concluded that the components influenced by the reactor trip operation are control rods, reactor vessel, steam generator, turbine, generator and electric grid. If it is expressed in components influenced sentence, it becomes:

The components influenced: “Control rods, Reactor vessel, Steam generator, Turbine, Generator, Electric grid”.

Moreover, the future plant behavior after the reactor trip operation can be determined using the algorithm described in Subsection 3.7.2 and from the explanation sentences in Table 5.1-2. In this case, the information is selected and collected from one main explanation sentence for each component from the explanation sentences of “realizing components” field in Table 5.1-2 for the component considering the main function.

Table 5.1-3. Future plant behavior after reactor trip operation

Action/operation	Future plant behavior	Specific technical term
Reactor trip operation	Low (no) flow of heat in Reactor vessel	Hot shutdown
	Low (No) flow of heat of water in primary side of SG	
	Low (No) flow of heat of steam in secondary side of SG	
	Low (no) flow of mechanical energy in Turbine	
	Low (no) flow of electrical energy in Generator	
	Low (no) flow of electrical energy in Electric grid	

The future plant behavior information is provided in Table 5.1-3. Then, the set of state changes (plant behaviors) are matched with the “specific term”

described in Subsection 3.7.2. From the table, it is found that in case of reactor trip operation, the state changes of influenced components are matched with the “specific term” and correlated with a technical term “hot shutdown”. Therefore, it can be concluded that the future plant behavior after reactor trip operation is such that the plant is in hot shutdown condition.

Safety injection and stopping RCP operation

The counter actions of safety injection and stopping RCP operations are represented by the control structure cfs2 and cfs3, respectively, as can be seen in Figure 5.1-2. The safety injection controller (cfs2) changes the state sou12 in efs9 (representing the energy flow of ECCS) from no output flow potential to high output flow potential, which indicates that there is enough electric power to be transferred through tra32 (high flow) to start the ECCS to provide cooling to the RCS. In this case, the objective obj4 to provide cooling the RCS through the ECCS is achieved (true).

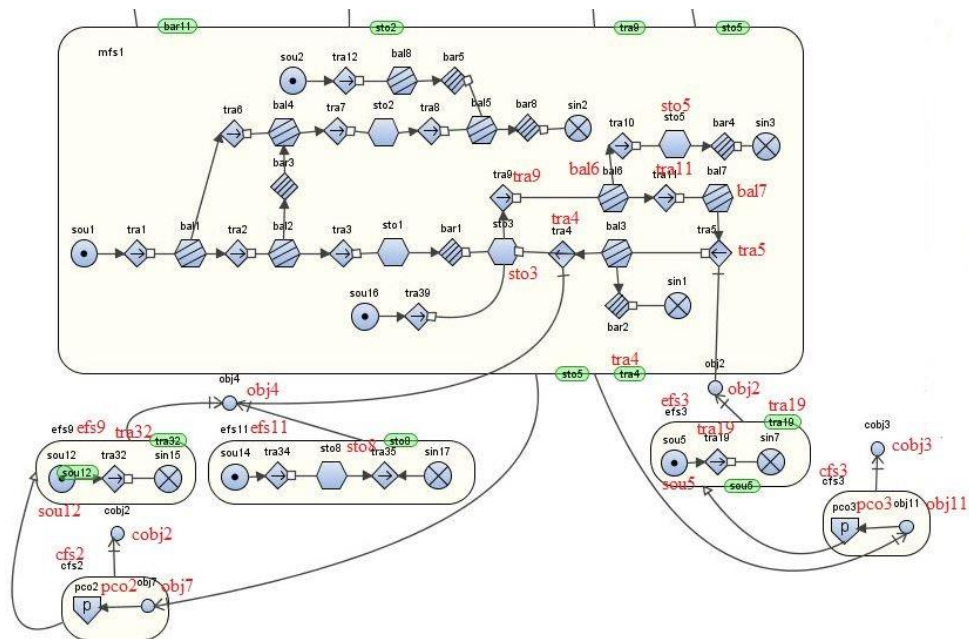


Figure 5.1-2. Part of MFM model related with safety injection and stopping RCS operation

On the other hand, the stopping RCP controller (cfs3) will stop the electric power flowing to the RCP (efs3), indicated by the no output flow potential in sou5. This condition impacts the state of tra19 to change from normal to no flow and then disables the objective obj2 to provide water to the RCS. Table 5.1-4 provides the state of function primitives before and after safety injection and stopping RCP operation. In addition, the explanation sentences of the plant behavior caused by safety injection and stopping RCP operation are provided in Table 5.1-5.

Table 5.1-4. State of function primitives before and after safety injection and stopping RCS

Counter action	Initial state	After counter action
Safety injection	sou12: no output flow potential tra32: no flow obj4: false tra4: low flow	sou12: no output flow potential tra32: high flow obj4: true tra4: high flow
Stopping RCP	sou5: normal tra19: normal obj2: true tra5: normal	sou5: no output flow potential tra19: no flow obj2: false tra5: no flow

Table 5.1-5. Explanation sentences of plant behavior after safety injection and stopping RCP operation

Functions	MFM Model	Realized components
sou12 in efs9	High flow output potential of energy in sou12	High output flow potential of electricity in ECCS
tra32 in efs9	No flow of energy in tra12	No flow of electricity in ECCS
tra4 in mfs1	High flow of mass in tra4	High flow of water in RCS
sou5 in efs3	no flow output potential of energy in sou5	no flow output flow potential of electricity in RCP
tra19 in efs3	No flow of energy in tra19	No flow of electricity in RCP
tra5 in mfs2	No flow of mass in tra5	No flow of water in RCP

From Table 5.1-5, it can be seen that the main components influenced by the safety injection and stopping the RCP are emergency core cooling system (ECCS), reactor coolant system (RCS) and reactor coolant pump (RCP). In addition, the future plant behavior after the counter actions can be derived from the realized components field in Table 5.1-5. There is no special term of the future plant behavior.

5.2. Check RCP restart criteria

The related part of the MFM model of checking RCP restart criteria operation is provided in Figure 5.2-1. The counter action is modeled by the control function cfs4. The operation condition is the state of sto5 (pressurizer) and is correlated with the obj12 to actuate control function pco4 in cfs4 to change the state of sou5 in efs3 (RCP). Then, the impacts of the two possible counter actions to the other components and plant behavior can be investigated using cause-effect relation and influence propagation as can be seen in Table 5.2-1.

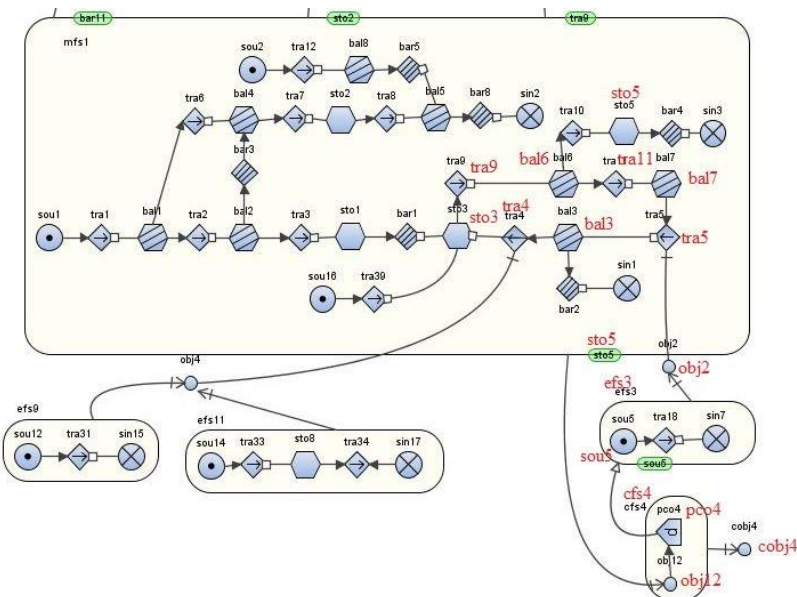


Figure 5.2-1. Part of MFM model related with RCP restart criteria operation

Table 5.2-1. State of function primitives before and after check RCP restart criteria operation

Action	Pressurizer (sto5) level	Initial state	After counter action
Check RCP restart criteria	high	sou5 (no output flow potential), efs3 (no flow), obj2 (false), tra5 (no flow)	sou5 (high flow output potential), efs3 (high flow), obj2 (true), tra5 (high flow)
	low	sou5 (no output flow potential), efs3 (no flow), obj2 (false), tra5 (no flow)	sou5 (no output flow potential), efs3 (no flow), obj2 (false), tra5 (no flow)

Table 5.2-2. Explanation sentences of plant behavior after check RCP criteria operation

Functions	MFM Model	Realized components
sou5 in efs3	High flow output potential of energy in sou5	High flow output potential of electricity in RCP
tra18 in efs3	High flow of energy in tra18	High flow of electricity in RCP
tra5 in mfs2	High flow of mass in tra5	High flow of water in RCP

The explanation sentences, derived from the set of change state in Table 5.2-1, for the counter action if the criteria for restarting the RCP is met, are given in Table 5.2-3. However, if the criteria is not met, the explanation sentences are the same in Table 5.1-5 because the RCP is still not operated. Therefore, the components influenced by the counter action are RCP and RCS, the realized components field in Table 5.2-2 represent the future plant behavior.

5.3. Identification and isolation of faulted steam generator

The MFM model related with the isolating ruptured SG operation is shown in Figure 5.3-1. The isolation of ruptured SG is represented by the control flow structure cfs5 and control function pco5. In this case, the “low volume” in sto6 is the operation condition which represents the low or no steam contained radioactive material in the turbine (objective of the system). Based on the causal reasoning of MFM, in order to make the low (no) volume in sto6, the transport function tra15 should be in low (no) flow. Therefore, the pco5 is actuated to change the state of tra16 from normal (high) flow to low (no) flow.

According to cause-effect relation and influence propagation, the change of state of tra16 will affect downstream and upstream connections and the propagate to all other function primitive and the flow structure. The states of function primitives before and after the isolation of ruptured SG or closing the MSIV are given in Table 5.3-1, which in turn the explanation sentences are generated for the counter action as can be seen in Table 5.3-2.

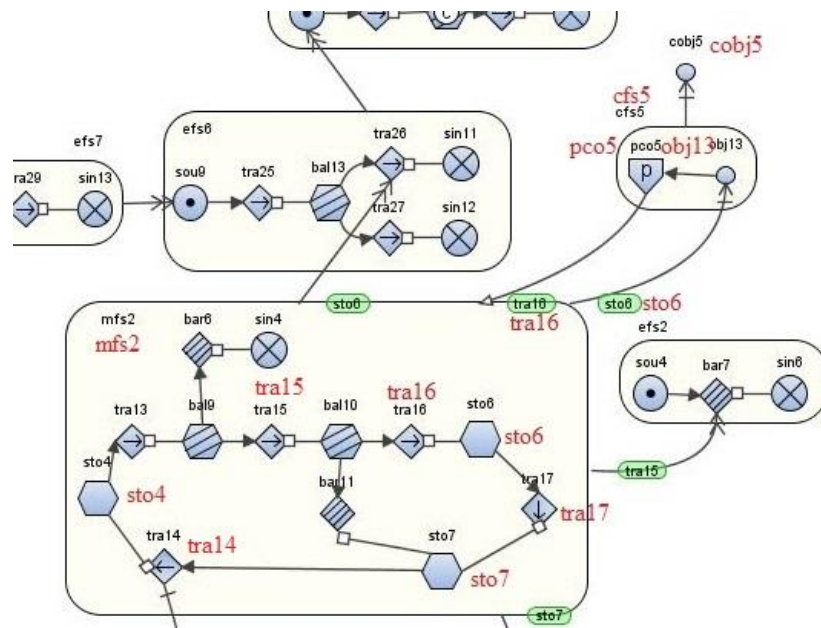


Figure 5.3-1. Part of MFM model isolation related with ruptured SG operation

Table 5.3-1. States of function primitives after isolating of ruptured SG

Counter action	Initial state	After counter action
Isolation of ruptured SG	tra15 (high flow), sto6 (high volume), sto7 (high volume), tra14 (high flow)	tra15 (no flow), sto6 (no volume), sto7 (no volume), tra14 (no flow)

Table 5.3-2. Explanation sentences of the influence of isolation of ruptured SG

Functions	MFM Model	Realized components
tra15 in mfs2	No flow of mass in tra15	No flow of steam in MSIV
sto6 in mfs2	No volume of mass in sto6	No volume of steam in turbine
sto7 in mfs2	No volume of mass in sto7	No volume of steam in condenser
tra14 in mfs2	No flow of mass in tra14	No flow of water in auxiliary feedwater system

Based on the explanation sentences, it can be derived that the MSIV, turbine, condenser and auxiliary feedwater system are the components influenced by the isolation of ruptured SG operation. In addition, the list of explanation sentences in the realized components field in Table 5.3-2 is the representation of future plant behavior caused by the counter action.

5.4. RCS cooldown using steam dump through SG PORV or steam dump valve

This step is executed after the level of faulted/intact SG has been regulated to the set point value and the safety injection (SI) has been stopped. The RCS is cooled down using steam dump through SG PORV if the condenser is not available. Otherwise, if the condenser is available, the steam dump valve is used to dump the steam. This thesis only discusses the RCS cooling down using steam dump through the steam dump valve. Figure 5.4-1 shows the MFM model related with the counter action. The counter action is modeled by the control structure cfs7 and the parameters are provided in Table 5.4-1.

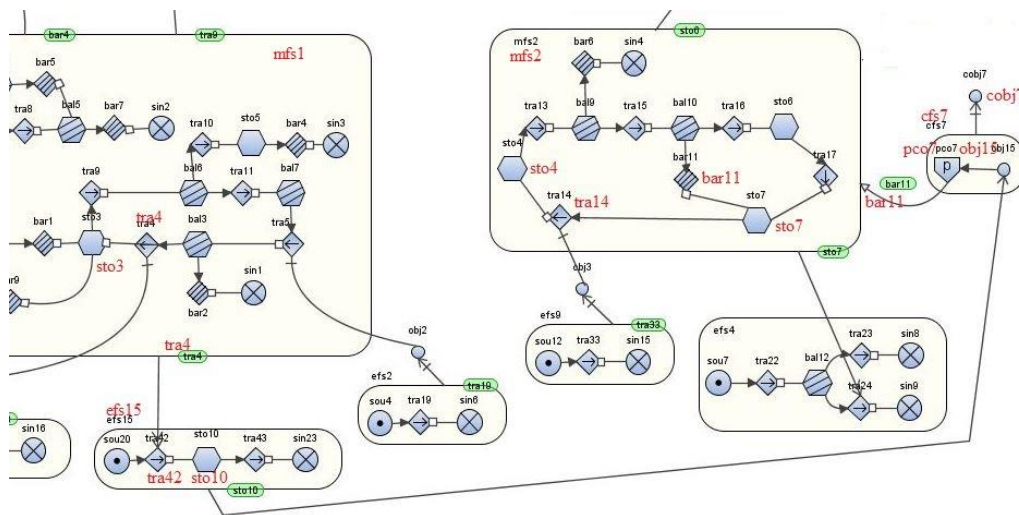


Figure 5.4-1. Part of MFM model related with RCS cooldown using steam dump valve operation

After the reactor trip and safety injection operation, the reactor is in hot shutdown condition. It means that the residual heat remains in the system and should be removed by dumping the steam from the SG in order to cooldown the RCS. In case of the condenser is available, the steam can be dumped by bypassing the turbine and opening the steam dump valve to let the steam directly flow to the condenser. In Figure 5.4-1, the temperature level of the RCS is represented by the state of sto10 in efs15 (energy flow of RCS). Therefore, the operation condition is the low volume of sto10 which is correlated with the obj15, which in turn the control function pco7 is actuated to disable the barrier function bar11. If the barrier function is disabled, it

means that the mass or energy can be transferred through the function. Therefore, it can be considered that the barrier function acts as a transport function. The states of function primitives and the explanation sentences of the influence caused by the counter action are provided in Table 5.4-1 and Table 5.4-2, respectively.

The components influenced by the counter actions are condenser, auxiliary feedwater and steam generator. In addition, one of the future plant behavior is “high volume of steam in condenser”. Other plant behaviors are provided in the realized components in Table 5.4-2.

Table 5.4-1. States of functions before and after RCS cooldown operation

Counter action	Initial state	After counter action
RCS cooldown	Bar11 (enable), sto7 (low volume), tra14 (low flow)	Bar11 (disable), sto7 (high volume), tra14 (high flow)

Table 5.4-2. Explanation sentences of influence of RCS cooldown operation

Functions	MFM Model	Realized components
Sto7 in mfs2	High volume of mass in sto7	High volume of steam in condenser
Tra14	High flow of mass in tra14	High flow of water in auxiliary feedwater
Sto4 in mfs2	High volume of water in sto4	High volume of water in SG

5.5. Applicability Evaluations

The additional information derived from the modeling of counter actions in executing the procedure step of the EOP of the SGTR accident is component influenced and future plant behavior caused by the counter actions. The additional information is presented to the operators in understandable way before they conduct the counter actions. Therefore, they will have enough knowledge about the purpose of the procedure step and the impact of their counter action related with the procedure step, which in turn it will help them to make decision and prepare for the next counter actions related with the future plant behavior.

This section discusses the applicability of the additional information. The applicability is evaluated based on the contribution to the situation awareness and reducing the human errors both omission and commission errors.

5.5.1. Contribution to Situation Awareness

As mentioned in Chapter 2 that situation awareness is the ability of operators to perceive and comprehend the information and based on those abilities, they should be able to predict the future event and prepare the next actions to anticipate the future event of the system. Regarding the prediction of the future event, this ability can be supported by the functional information because it can provide system and role of components and the system behavior.

Table 5.5-1 Contribution of additional information derived to situation awareness for SGTR accident case

Counter action	Perception	Comprehension	Projection
Reactor trip and safety injection	<ul style="list-style-type: none"> •Receive the information about the state of reactor vessel, primary side and secondary side of SG •Receive information about the state of ECCS •Receive information about the level of RCS •Receive information about the state of RCP 	<ul style="list-style-type: none"> • Understand the state and level of reactor vessel, primary side and secondary side of SG • Understand the state of the ECCS • Understand the state and level of RCS • Understand the state of RCP 	<ul style="list-style-type: none"> •Monitor the state and level of reactor vessel, primary and secondary side of SG, ECCS, RCS and RCP •Prepare for anticipate the future state of reactor vessel, state and level of SG, state and level of RCS and the state of RCP
Check RCP restart criteria	<ul style="list-style-type: none"> •Receive information about the pressurizer level •Receive information about the state of RCP •Receive information about the state and level of RCS 	<ul style="list-style-type: none"> • Understand the level of pressurizer whether to restart the RCP or not • Understand the state of RCP, whether ON or OFF • Understand the state of RCS whether supplied by the RCP or not 	<ul style="list-style-type: none"> •Monitor the pressurizer level, state of RCP and the state and level of RCS •Prepare for the next action related to the change state of the RCP and RCS
Identification and isolation of faulted SG	<ul style="list-style-type: none"> •Receive information about the ruptured SG •Receive information about isolated ruptured SG •Receive information about the state of the MSIV, turbine and condenser 	<ul style="list-style-type: none"> • Understand which SG is ruptured • Understand the state after isolation the ruptured SG • Understand the state of the secondary system 	<ul style="list-style-type: none"> •Monitor the state of isolated ruptured SG •Monitor the intact SG and secondary system •Prepare and anticipate the future state of intact SG and secondary system
RCS cool down using steam dump valve	<ul style="list-style-type: none"> •Receive the information about the state of steam dump valve which in “open position” •Receive the information about the level of steam in the condenser •Receive the information about the temperature level of the RCS 	<ul style="list-style-type: none"> • Understand that the steam will be delivered to the condenser by opening the steam dump valve • Understand the current level of dumped steam in the condenser • Understand the current temperature level of the RCS 	<ul style="list-style-type: none"> •Monitor the state of the steam dump valve, the condenser and the RCS. •Prepare for actions to anticipate the change of state of the steam dump valve, condenser and the RCS

The additional information (components influenced and future plant behavior) derived from the modeling of counter actions in executing of procedure steps discussed in previous section can be used to increase the situation awareness of operators in emergency conditions. The contributions of the functional information to the situation awareness of operators are summarized in Table 5.5-1. From the functional information provided (future plant behavior), before conducting the counter actions, operators will have clear view about the purpose of the procedure steps and the impacts of the counter actions. Then, by having the information, operators should aware and monitor the components influenced and the plant behavior affected by the counter actions.

An example of counter actions with lack of situation awareness is the accident happened during the mitigation of SGTR accident of Point Beach Unit 1 in 1975 [64]. In the mitigation of the accident, the operators were slow to recognize the occurrence of steam generator tube rupture, slow to start the load reduction and slow to isolate the rupture steam generator. The above situation can be minimized if operators are aware about the situation of the plant. The situation awareness can be increased by providing the additional information, especially the future plant behavior, as summarized in Table 5.5-1.

In the case of identification of the accident, it can be derived from the impact of the reactor trip and safety injection operation to the state of RCS, state and level of SG both primary and secondary side and also the state of RCP. Because the secondary side of the SG is also impacted by the operation action, operators should monitor the radiation level in the SG blowdown line. The ruptured SG can be identified by the high level of radioactive in the SG blowdown line. By having this information, it will make it faster for operators to identify the SGTR accident and to isolate the ruptured SG.

5.5.2. Contribution to Reduce Human Errors

Investigations related with the cause of the accidents especially in nuclear plants found that besides the technical factors, such as system malfunction caused by ageing of components, human errors also contribute to the accidents. It is found

in the United states, among the 180 significant events, 48% of them were caused by human errors [65]. Some efforts have been conducted to reduce the potential of human errors such as providing training program and improving the human machine interfaces including improved interfaces and operator support systems.

Regarding the action conducted by operators, human errors can be divided into omission error and commission error. In case of mitigating accident of nuclear power plant following the instruction of the EOP, the omission error can be happened if operators omit or skip some important procedure steps for any reasons. First, because of the complexity of the procedure steps which cause operators difficult to understand the purpose of the procedure step. As their mitigation tasks are limited by time, then they decide to skip the procedure step. This behavior will make them fail to mitigate the accident and endanger the plant condition.

On the other hand, the commission error related to a mistake that consists of doing something wrong. CBPs with complex and ambiguous instructions will cause operators difficult to understand the purpose of the procedure step which in turn they may make wrong decisions and take the wrong counter actions. In addition, it is also happened if the CBPs has lack of information.

The above problems can be solved by providing the additional information to the CBP. The additional information provides the objective of the procedure step as well as the components influenced, and future plant behavior caused by the counter actions. By providing the additional information, operators will have clear view about what will happen in the plant and enough knowledge to do the counter action. Therefore, they will not skip or omit some procedure steps and the potential of omission error will be reduced. Otherwise, by having enough knowledge about the procedure step, it will help operators to make correct decision and counter actions. Therefore, the incident caused by the commission error will be reduced.

Chapter 6

6. Preliminary Design of CBP User Interface with the Desirable Feature

6.1. Process of Displaying the Additional Information

This chapter discusses the preliminary design of the CBP user interface with the desirable feature. The desirable feature is the additional information: components influenced and future plant behavior. As the purpose of the study is to derive the proposed a CBP with the additional information feature, therefore in the preliminary design of the CBP, the focus only on displaying the additional information to the CBP user interface. In other words, the detail instruction of the procedure steps such as components to be controlled, parameter required to control the components and how to take the actions including the plant status will not be considered.

In the preliminary design, the CBP has feature of displaying the additional information each time operators click on a specific procedure step. Benefits of this feature, before operator taking the counter actions, they will have clear view and understanding as well as knowledge about the purpose of the procedure step, the impact of their counter actions. Consequently, they will monitor the state of the influenced components and the plant behavior. Moreover, they will prepare for the actions related with the change of influenced components and anticipate the future plant behavior.

As the preliminary design, the process of deriving the additional information and extracting the additional information to the CBP user interface is manually conducted. The process of deriving the additional information from the MFM mode is investigated manually using cause-effect relation and influence propagation (in hand investigation). The additional information, including objective of the procedure step, components influenced, and future plant behavior derived from the investigation is expressed in explanation sentences in order to make it easier for operators to understand the information. Then, the explanation sentences are collected separately based on the procedure steps. For example, the explanation sentences of a group of “Identification and isolation of ruptured SG” will be as provided in the Table 6.1-1.

Table 6.1-1. Group of explanation sentences for isolate ruptured SG

Objectives	To isolate the ruptured SG
Components influenced	MSIV, turbine, condenser, auxiliary feedwater
Future plant behavior	No flow of steam in MSIV No volume of steam in turbine No volume of steam in condenser No flow of water in auxiliary feedwater system

Finally, the explanation sentences are extracted to the CBP user interface and displayed to the operators in understandable way each time the select on a specific procedure step. Figure 6.1-1 summarized the process of deriving and displaying the additional information to the CBP user interface.

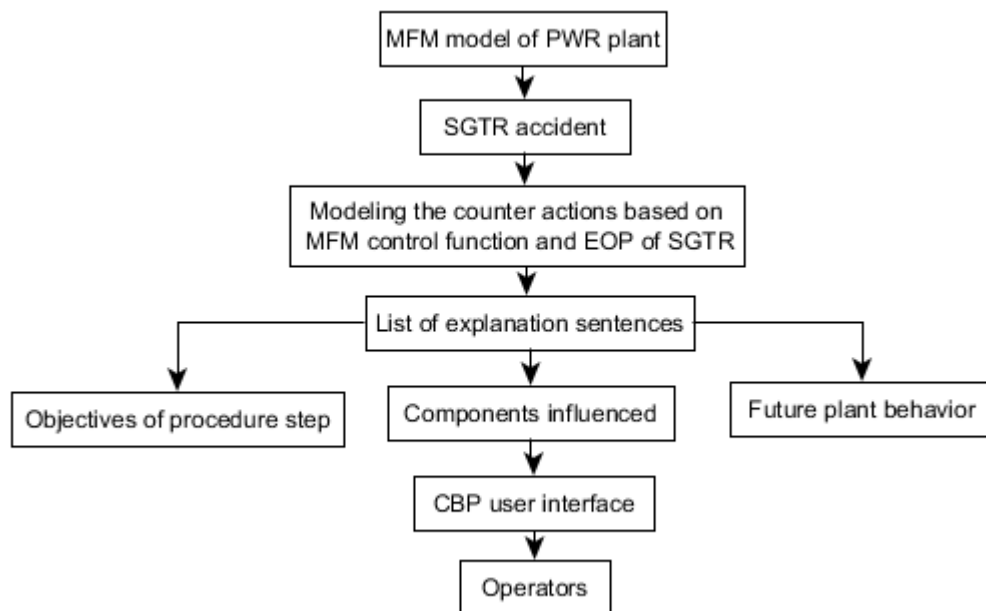


Figure 6.1-1. Process of displaying additional information to the CBP user interface

In the future works, the process of deriving the additional information from the MFM model and displaying the additional information will be conducted automatically. It means that each time users or operators click on a specific procedure step, it will execute the program to derive the additional information from the MFM model. Then, the additional information in the form of explanation sentences will be displayed on the additional information field on the CBP user interface.

6.2. Design of the CBP User Interface

The design of the proposed CBP with the desirable feature is based on the standard, the requirements of the representation of CBP user interface and also considering human factor engineering. Literature [21] mentions some requirements for the representation of the CBP user interface which are used in this study. Based on the requirements, the presentation of the CBP should include identification; basic steps; warning, caution and notes; lists; organizations; and formatting and screen layout. In addition, the CBP user interface should provide functionality for monitoring operator actions, planning and implementation and support for path monitoring and navigation.

The identification of procedures involves the procedure title, procedure number, revision and date, high level objective and their category. Procedures are represented in basic steps which composed of verbs and direct objects. Warning, caution and notes which qualifies the required actions and decision, can be used to support the performance of a procedure. Lists formats are frequently used to present groups of items of actions, conditions, components, criteria and systems. Organization of procedure is one of important aspect of the CBP user interface because it is related with the successfulness of operators in using the CBP. Finally, because of the limitation of visual display units, the procedure should be presented in convenience way whether in the flowchart-based format or text-based format or combination of flowchart-based and text-based format.

Figure 6.2-1 shows the draft of layout of the presentation of the CBP user interface by considering the above requirements. Then the design of the CBP user interface with the additional information feature is provided in Figure 6.2-2. The figure is the initial display of the CBP before users or operators select a procedure step. After the operators click on a specific procedure step, the presentation of the CBP user interface is given in Figure 6.2-3. It can be seen that the additional information related with the impact of the counter actions is displayed on the additional information field of the CBP user interface. In addition, the CBP user interface also has a feature in which when the procedure step has been selected, the color of the procedure of step will be changed. In this case, the color is changed to green. The purpose of the color marking is to

remind the operators of their current position on the procedure step. In addition, it can be used to let other operators know the current actions of mitigating the accident.

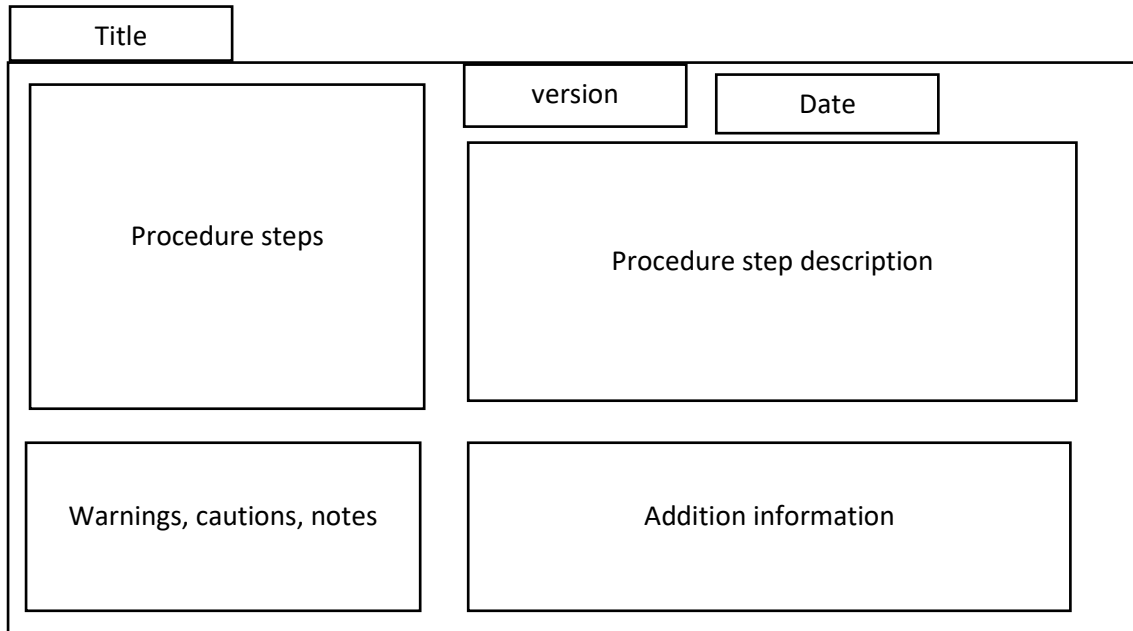


Figure 6.2-1. Draft of layout of the CBP user interface

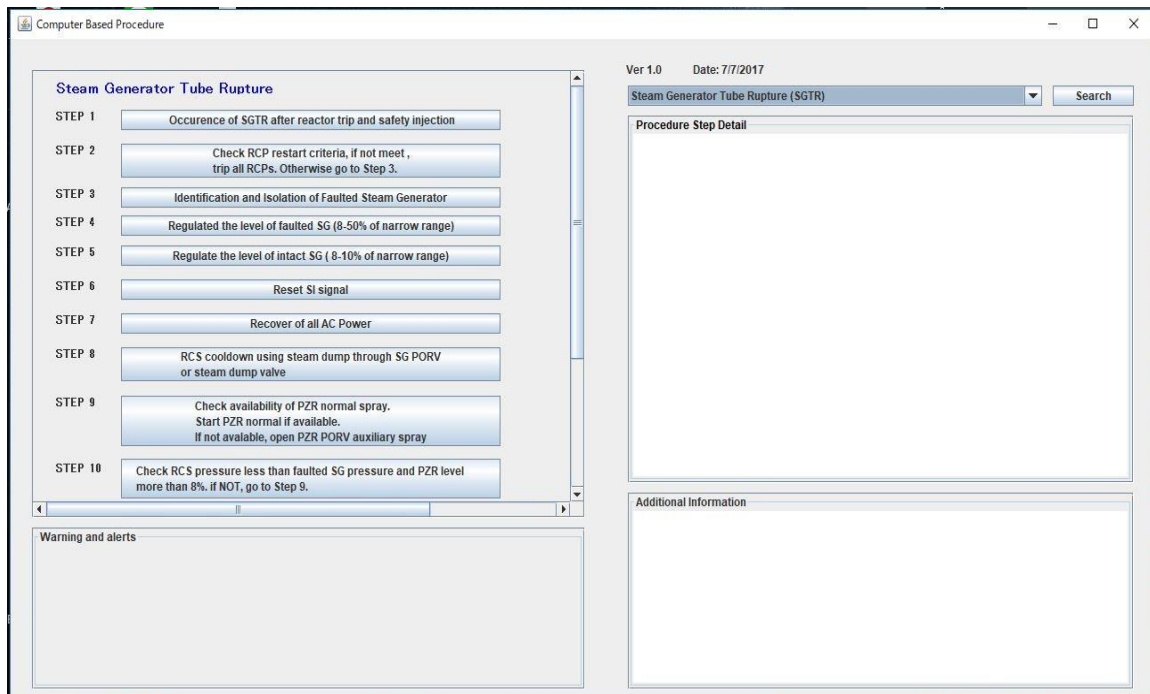


Figure 6.2-2. The initial display of the CBP user interface

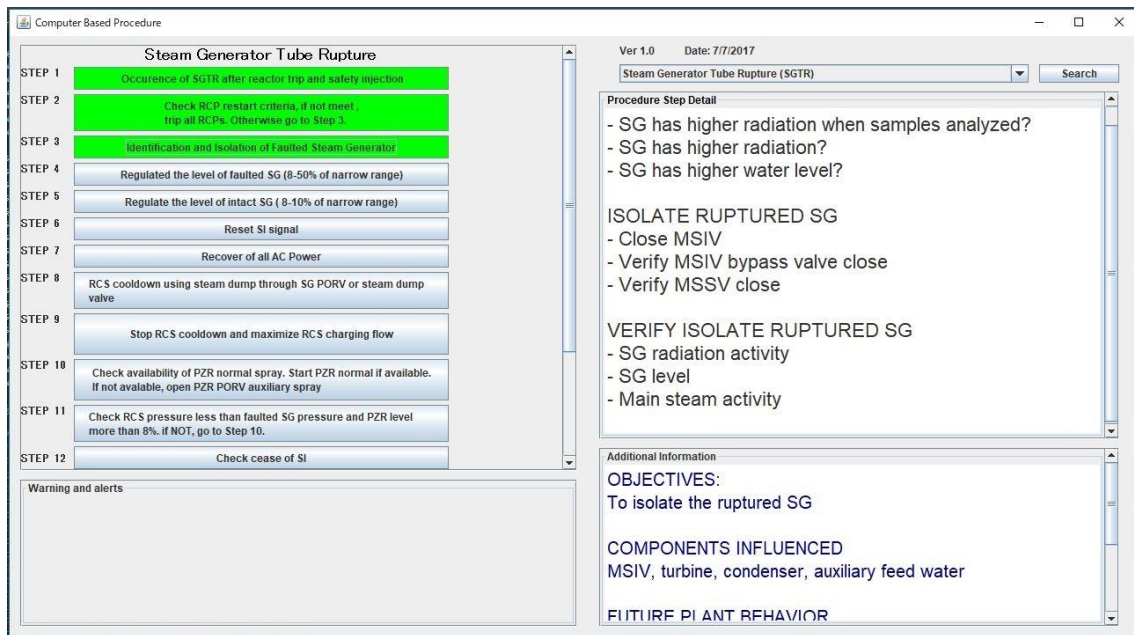


Figure 6.2-3. Displaying the additional information on the CBP user interface

To conclude, the preliminary design of the proposed CBP user interface with the desirable feature can be used as a basic idea to design the complete CBP user interface involving the detail description of procedure steps, plant status, and other useful features which increase the usability of the CBP and reduce the possibility of human error when using the CBP in mitigating the accident. Furthermore, in the future, the CBP user interface with the desirable features can be implemented in real plants.

6.3. Evaluation of the Design of the CBP User Interface

As a proposed design, the CBP user interface should be evaluated. The evaluation study will be conducted as an objective assessment of the proposed CBP prototype. The purpose of the evaluation study is to derive the inputs and recommendations of on how to improve the functionality and the user interface of the proposed CBP. In addition, it is also intended to increase the usability of the CBP. This section discusses on how to evaluate the proposed CBP user interface.

Evaluation materials

The evaluation study uses the proposed CBP user interface with the additional information, CBP user interface without the additional information, and some questioners which participants should respond related with the usage of the CBP.

Participants

The participants can be students from nuclear engineering department or workers of nuclear power plants/research institutes.

Evaluation methods

Figure 6.3-1 shows the method to evaluate the proposed CBP user interface. There are two aspects that will be assessed through the evaluation: the functionality and the usability of the CBP user interface. The functionality of the CBP user interface can be assessed by providing the participants with the two types of CBP, which are CBP with the additional information and without additional information.

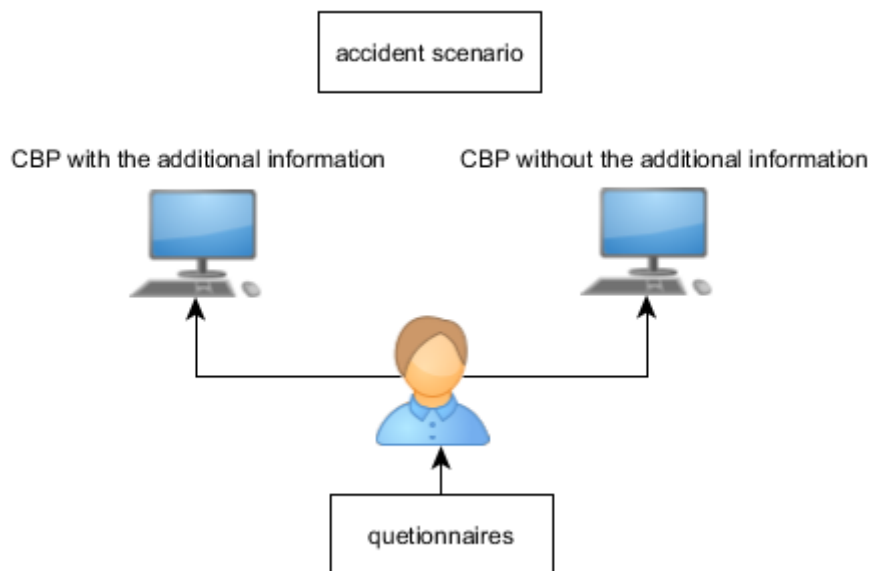


Figure 6.3-1. Method to evaluate the proposed CBP user interface

In the initial phase of the evaluation, participants will be given an accident scenario and they are asked to use both the CBP how to mitigate the accident and should take more

consideration to the impact of the counter actions. In the end of the tasks, participants will be given some questions related with their activities using the both CBPs. Such questions will be “which CBPs more appropriate to mitigate the accident?” or “which CBP do you prefer to use? Give the reasons” or other questions related with the functionalities of the CBP.

In the future phase of evaluation, participants will be given a task to mitigate an accident using the two types of CBP. In this evaluation, besides giving some questions in the end of assessment, the time of operators completing the counter actions using the both CBPs will be recorded and compared.

In case of usability evaluation of the proposed CBP, operators should respond to some questionnaires related the representation of the CBP. As an example, some survey about the suitability of the device such as the screen size and display brightness will be asked to the participants. In addition, participants will be asked related with the interface and how the participants use the functions and features in the CBP interface as well as their feeling while using the CBP. Besides the questions and the survey, participants should give some suggestion and recommendations in order to improve the functionalities and the usability of the proposed CBP.

7. Conclusions and Future Works

Currently, most of modern main control rooms of nuclear power plants are equipped with the advanced human machine interfaces and operator support systems including computer-based procedures (CBPs). CBPs provide some features and offer benefits compare with the paper-based procedures. Information is provided more dynamic in CBPs and there is a link to connect to other procedures easily.

The design of the CBPs should refer to the related standard and consider the human factor engineering to prevent the human error in using the CBPs. This study proposes a CBP with the desirable feature by adding the additional information in order to increase the usability of the CBP. In addition, it is also intended to increase the situation awareness of the operators. The additional information is components influenced and future plant behavior as the impact of the counter actions of operators in mitigating the accident following the instruction in procedure step of the EOP.

The method to derive the additional information is by applying an SGTR accident to the MFM model of PWR plant. The counter actions are modeled by the MFM control functions. The investigation to derive the information about the components influenced and future plant behavior is conducted based on cause-effect relation and influence propagation. Future plant behavior is useful information and help operators to understand the plant state and anticipate the future events. It will increase the situation awareness of operators and then minimize the human errors caused by operators' actions especially in an emergency condition. The additional information is applicable to increase the situation awareness and to reduce the human errors considering the mitigation of SGTR accident in the past with the lack of situation awareness.

Contributions

The results of the study, such as the additional information of the impact the counter actions in mitigating an accident, have contributions to the increasing of the situation awareness of operators by supporting the achievements of perception, comprehension and projection abilities. In addition, it also contributes to reduce the potential of human errors caused by the counter actions both errors of omission and errors of commission.

Furthermore, the technical contribution of the study is the extension of the implementation of MFM modeling methodology. First, this study proposes the application of MFM control function model the counteractions (automatic or operator action) of executing the procedure step of an EOP. The counter action (represented by an MFM control function) is actuated based on the operation condition and objective of the system to produce a new state of a function primitive by changing the state of a function primitive (a controlled component). Second, this study also proposes some new states of definition of MFM model which are suitable for the analysis of the impact of the counter actions based on cause-effect and influence propagation rules. Furthermore, this study also enhances the benefit of MFM modeling methodology for causal reasoning analysis.

Future Works

Future works include the investigation of modeling the counter action to other procedure steps in the EOP and the development of a technique to explain the effects and side effects of counter operations in understandable way for operators. In addition, develop the CBP user interface with the additional information feature which the information is gathered automatically from the MFM model.

Moreover, the proposed CBP user interface with the desirable feature (additional information) will be evaluated by the real operators in order to validate the design and to increase the usability and the functionality of the CBP. It is expected that by providing the additional information related with the functions of components and future plant behavior will reduce the commission errors of operators because operators will understand the intention of counter actions, especially in an emergency condition.

References

- [1] Oxstrand, J., Le Blanc, K., Filkstad, C., Evaluation of Revised Computer-Based Procedure System Prototype, Idaho National Laboratory External Report, January, 2013; Idaho, US.
- [2] Seong, P. H., Kang, H. G., Na, M. G. Kim, J. H., Heo, G., and Y. Jung, Advanced MMIS toward Substantial Reduction in Human Errors in NPPs, Nucl. Eng. Technol., 2013; 45(2), pp. 125–140. DOI: 10.5516/NET.04.2013.700
- [3] Suryono, T.J, and Gofuku, A, The Desirable Features of Computer Based Emergency Operating Procedure for Nuclear Power Operation, IFAC-PapersOnLine, 2016; 49(19), pp. 403–407. DOI: 10.1016/j.ifacol.2016.10.599
- [4] Lind, M., Modeling goals and functions of complex plant, Appl. Artif. Intell. Int. J., 1994; 8(2), pp. 259–283.
- [5] Lind, M., An Overview of Multilevel Flow Modeling, Nucl. Saf. Simul, 2003, 4(3), pp. 4–9.
- [6] Lee, S.H, Kim, K, Kim, H.J, and Eun, Y.S., Analyses of SGTR accident with mihama unit experience, J Korean Nucl Society, 1994, 26(1). pp. 41–53.
- [7] Gofuku, A, Applications of MFM to intelligent systems for supporting plant operators and designers : function-based inference techniques, Nucl. Saf.Simul., 2011, 2(3), pp. 235–245.
- [8] Walton, N.V, and McCall, D.B, Development and review of plant specific emergency operating procedures, Safety ReportSeries N.48, 2006, IAEA, Vienna, Austria.
- [9] Park, J, and Jung, W., A study on the validity of a task complexity measure for emergency operating procedures of nuclear power plants-Comparing task complexity scores with two sets of operator response time data obtained under a simulated SGTR, Reliab. Eng. Syst. Saf., 2008, 93(4), pp. 557–566. DOI: 10.1016/j.res.2007.02.002
- [10] Xu, S., Song, F., Li, Z. Zhao, Q., Luo, W., He, X., and Salvendy, G., An ergonomics study of computerized emergency operating procedures: Presentation style, task complexity, and training level, Reliab. Eng. Syst. Saf., 2008, 93(10), pp. 1500–1511. DOI: 10.1016/j.res.2007.09.006

- [11] Hong, J.H., Lee, M.S., and Hwang, D.H., Computerized procedure system for the APR1400 simulator, Nucl. Eng. Des., 2009, 239(12), pp. 3092–3104. DOI: nucengdes.2009.09.024
- [12] Boring, R.L, and Gertman, D.I, Human Reliability Analysis for Computerized Procedures Human Factors and Ergonomics, Proc. Human Factors and Ergonomics Society 55th Annual Meeting, September, 2011, pp. 1720-1724. DOI: 10.1177/1071181311551357
- [13] Lipner, M.H, and Kerch, S.P, Operational benefits of an advanced computerized procedures system, Nucl. Sci. Symp. Med. Imaging Conf. 1994., 1994 IEEE Conf. Rec., 1994, 3, pp. 1068–1072.
- [14] Converse, S.A., Evaluation of the Computerized Procedures Manual II (COMPMA II), NUREG/CR-6398, Nuclear Regulatory Commission, 1995, Washington, DC, US.
- [15] Pirus, D, and Chambon, Y, The computerised procedures for the French N4 series, Proc. 1997 IEEE Sixth Conference on Human Factors and Power Plants, 1997, June 8-13, Orlando, Florida, U.S, pp. 3–9. DOI: 10.1109/HFPP.1997.624836
- [16] Jung, Y., Seong, P.H., and Kim, M.C., A model for computerized procedures based on flowcharts and success logic trees, Reliab. Eng. Syst. Saf., 2004, 83(3), pp. 351–362. DOI: 10.1016/j.res.2003.10.012
- [17] De Oliveira, M.V., Bruno, D.S., De Carvalho, P.V.R., and Grecco, C.H.S, Applying Computer-based Procedures in Nuclear Power Plants, International Nuclear Atlantic Conference-INAC 2009, Brazil.
- [18] Seong, P.H., Kang, H.G., Na, H.G., Kim, J.H., Heo, G and Jung, Y., Advanced MMIS toward substantial reduction in human errors in NPPs, Nucl. Eng. Technol., 2013, 45(2), pp. 125–140. DOI: 10.5516/NET.04.2013.700
- [19] O’Hara, J.M., Higgins, J., and Stubler, W., Computerization of Nuclear Power Plant Emergency Operating Procedures, Proc. Hum. Factors Ergon. Soc. Annu. Meet., 2000, 44(22), pp. 819–822.
- [20] IEC Standard, “IEC 62646. Nuclear power plants - control rooms - Computer-based procedures.” International Electrotechnical Commissions, Geneva, 2012.

- [21] O'Hara, J. Higgins, J., Stibler, W, and Kramer, J., Computer-based procedure systems: technical basis and human factors review guidance, NUREG/CR-6634, US Nuclear Regulatory Commission, 2000.
- [22] IAEA, Operator support systems in nuclear power plants, Proceeding of a Specialists Meeting, May 17–21, 1993, Moscow, Russian Federation.
- [23] Lee, S.J, and Seong, P.H., Design of an Integrated Operator Support System for Advanced NPP MCRs: Issues and Perspectives, In: Yoshikawa H., Zhang Z. (eds) Progress of Nuclear Safety for Symbiosis and Sustainability. 2014, Springer, Tokyo pp. 11–27. DOI: 10.1007/978-4-431-54610-8_2
- [24] Gofuku, A., and Sato, T., Development of a dynamic operation permission agent for preventing commission errors of operators, Proceedings of Second International Conference on Innovative Computing, Information and Control; 2007 Sept 5–7; Kumamoto, Japan: IEEE, 2007,p.108
- [25] Niwa, Y., Takahashi, M., and Kitamura, M., The Design of Human – Machine Interface for Accident Support in Nuclear Power Plants, Cognition, Technology & Work, 3(3), pp. 161–176, 2001. DOI: 10.1007/PL00011531
- [26] Flin, R. H. , O'Connor, P., and Crichton, M., Safety at the sharp end - a guide to non-technical skills. Boca Raton, Florida, U.S: CRC Press Taylor & Francis Group, 2008.
- [27] Endsley, M. R. , Toward a Theory of Situation Awareness in Dynamic Systems, J. Hum. Factors Ergon. Soc., 1995, 37(1), pp. 32–64.
- [28] Lee, H.C, and Seong, P.H, A computational model for evaluating the effects of attention, memory, and mental models on situation assessment of nuclear power plant operators, Reliab. Eng. Syst. Saf., 2009, 94(11), pp. 1796–1805. DOI: 10.1016/j.res.2009.05.012
- [29] Chen, Y., Gao, Q. , Song, F., Li,, and Wang, Y, Procedure and information displays in advanced nuclear control rooms : experimental evaluation of an integrated design, Ergonomics, 2017, 60(8). DOI: 10.1080/00140139.2017.1288929
- [30] Reinerman-Jones, L., Guznov, S., Tyson, J., D'Agostino, A., and Hughes,N., Workload, Situation Awareness, and Teamwork, 2015, U.S. Nuclear Regulatory Commission, Washington, D.C, U.S.

- [31] Hallbert, B., Sebok, A., and Morrisseau, D., A study of control room staffing levels for advanced reactors, NUREG/A-0137, Nuclear Regulatory Commisiion, 2000, Washinton, D.C, U.S.
- [32] Hollnagel, E., Pariès, J., Woods, D., and Wreathall, J., Resilience Engineering in Practice: a guidebook. 20011, Ashgate, U.K.
- [33] Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D., Ladva, D., Rafferty, L., and Young, M., Measuring Situation Awareness in complex systems: Comparison of measures study, *Int. J. Ind. Ergon.*, 2009, 39(3), pp. 490–500. DOI: 10.1016/j.ergon.2008.10.010
- [34] Durso, F.T., Hackworth, C.A., and Truitt, T.R., Situation Awareness As a Predictor of Performance in En Route Air Traffic Controllers., *Air Traffic Control Q.*, 199, 6(1), pp. 1–20.
- [35] Hollnagel, E, Wears, R, and Braithwaite, J., From safety-I to safety-II: a white paper, 2015, The Resilient Health Care Net: Published simultaneously by the University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia. pp. 1–32.
- [36] Hollnagel, E., From Safety-I to Safety-II: A brief introduction to resilience engineering. Available: <http://safetysynthesis.com/onewebmedia/Introduction%20to%20S-I%20and%20S-II.pdf>
- [37] Hollnagel, E., From protection to resilience : Changing views on how to achieve safety, 8th International Symposium of the Australian Aviation Psychology Association, Apr 2008, Sydney, Australia.
- [38] Flin, R.H., O'Connor, P., and Crichton, M., Safety at the Sharp End: A Guide to Non-technical Skills. Ashgate, 2008.
- [39] Hollnagel, E, Resilience Engineering: building a culture of reslilience, 2013. Avaialable: http://www.ptil.no/getfile.php/1325150/PDF/Seminar%202013/Integrerte%20operasjoner/Hollnagel_RIO_presentation.pdf.
- [40] Gustavsson, P., Resilience and Procedure Use in the Training of Nuclear Power Plant Operating Crews, Master Thesis, 2011, Linkoping University, Sweden.

- [41] Hollnagel, E and Fujita, Y, The Fukushima disaster-systemic failures as the lack of resilience, Nucl. Eng. Technol., 2013, 45(1), pp. 13–20. DOI: 10.5516/NET.03.2011.078
- [42] Hollnagel, E., Time and time again, Theor. Issues Ergon. Sci., 2002, 3(2), pp. 143–158.
- [43] Corcoran, W.R., Finnicum, D.J., Hubbard, F.R., Musick, C.R. and Walzer, P.F., The operator's role and safety functions, pp. 290–305. Available: http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/12/605/12605058.pdf
- [44] Gofuku, A and Tanaka, Y, Display of diagnostic information from multiple viewpoints in an anomalous situation of complex plants, Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (IEEE SMC '99); 1999 Oct 12 -15; Tokyo, Japan. IEEE, 1999; p. 642–647.
- [45] Lind, M., Control functions in MFM : basic principles, Nucl. Saf. Simul., 2011, 2(2), pp. 132–129.
- [46] Lind, M., An introduction to multilevel flow modeling, Nucl. Saf. Simul, 2(1), 2011, pp. 22–32.
- [47] Lind, M., Yoshikawa, H., Jørgensen, S.B., Ming, Y., Tamayama, K., and Okusa, K, Multilevel flow modeling of monju nuclear power plant, Nucl. Saf. Simul., 2011, 2(3), pp. 274–284.
- [48] Larsson, J.E., Knowledge-based methods for control systems [dissertation]. Lund: Lund Institute of Technology; 1992.
- [49] Larsson, J.E., Diagnosis based on explicit means-end models, Artif. Intell., 1996, 80, pp. 29–93.
- [50] Gofuku, A., Multi-level flow modeling and its applications, Nucl. Saf. Simul., 2014, 5(4), pp. 3–7.
- [51] Larsson, J.E., Diagnostic reasoning based on means-end models: experiences and future prospects, Knowledge-Based Syst., 2002, 15(1–2), pp. 103–110.
- [52] Petersen J. Causal reasoning based on MFM. In: Proceedings of Conference on Cognitive System Engineering in Process Control (CSEPC); 2000 Nov 22-25; Tae-jeon, Korea. p. 36–43.

- [53] Gofuku A, Sato T. Dynamic operation permission system for oil refinery plants. In: International Conference of Networking, Sensing and Control; 2009, Mar 26–29; Okayama, Japan, IEEE, 2009. p. 746–751.
- [54] Zhou, Y, Yoshikawa, H, Wu, W, Yang, M and Ishii, H, Modeling Goals and Functions of Micro Gas Turbine System by Multilevel Flow Models, *Inf. Media tech.*, 2006, 1, pp. 963–972.
- [55] Zhang, X, Ravn, O and Lind, M, Assessing Operational Situations, PhD Dissertation, Technical University of Denmark, Department of Electrical Engineering, 2015.
- [56] Lind M and Zhang, X., Functional Modelling for Fault Diagnosis and its Applications for NPP, *Nucl. Eng. Technol.*, 2014, 46(6), pp. 753–772. DOI: 10.5516/NET.04.2014.721
- [57] Zhang, X., Lind, M., and Ravn, O., Consequence reasoning in multilevel flow modelling, *IFAC Proc. Vol.*, 2013, 46(15), pp. 187–194. DOI: /10.3182/20130811-5-US-2037.00028
- [58] Lind, M, Means and ends of control, *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, 2004, 1, pp. 833–840. DOI: 10.1109/ICSMC.2004.1398406
- [59] Heussen, K, Saleem, A and Lind, M, Control architecture of power systems: Modeling of purpose and function, 2009 IEEE Power Energy Soc. Gen. Meet., 2009, 26-30 July, Calgary, Canada, pp. 1-8. DOI: 10.1109/PES.2009.5275963
- [60] Inoue, T and Gofuku. A, A technique to prioritize plausible counter operation procedures in an accidental situation of plants, *Nucl. Saf. Simul*, 2016, 7(2), pp. 144-152.
- [61] Kondo, S, Lessons learned for PSA from the SGTR incident at Mihama, unit 2, in 1991, *Reliab. Eng. Syst. Saf.*, 1994, 45(1–2), pp. 57–65. DOI: 10.1016/0951-8320(94)90076-0
- [62] Suryono, T.J and Gofuku. A, Investigation of Functional Information Display on Computer-based Emergency Operating Procedure,” *Proc. ISSNIP 2016.*, 8th International Symposium on Symbiotic Nuclear Power System for 21st Century, 2016, 26-28 September, Chengdu, China.

- [63] Suryono, T.J., and Gofuku, A., Techniques to derive additional information of operation actions for computer-based operating procedure, *J. Nucl. Sci. Technol.*, 2018, 55(6), pp. 672–683. DOI: 10.1080/00223131.2018.1428122
- [64] Suryono, T.J., and Gofuku, A, Functional information of system components influenced by operators' actions on emergency operating procedure, *Procs. 2017 25th Intl. Conf. Nucl. Eng (ICONE25)*, pp. 1–10.
- [65] MacDonald, P.E., Shah, V.N, Ward, L.W., and Ellison, P.G., Steam Generator Tube Failures, NUREG/CR-6365, Nuclear Regulatory Commission, 1996.
- [66] Seong, P.H., and Shin, S., Design of an integrated operator support system for advanced NPP MCRs: issues and perspectives,” in H. Yoshikawa and Z. Zhang (eds), *Progress of Nuclear Safety for Symbiosis and Sustainability: Advanced Digital Instrumentation, Control and Information System for Nuclear Power Plants*, 2014, pp. 11–27.