Functional information in operator support systems

GOFUKU Akio[1], and INOUE Takahisa[1]

1. *Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-Naka, Kita-ku, Okayama 700-8530, Japan (fukuchan@sys.okayama-u.ac.jp)*

Abstract: One of important roles of operators in the operation of nuclear power plants is to take suitable counteractions in an abnormal plant condition. It is important to share functional information of components between operator support systems and operators in a main control room equipping with a fourth generation control panel because functional information expresses the role of a component in a system and the information can be used to find an alternative measure in an abnormal plant condition. A technique to generate emergency counter-operation procedures based on Multilevel Flow Modeling （MFM） of a target system is introduced. The technique will be a promising technique to take counteractions resiliently. Its applicability is confirmed through case studies for a PWR plant to derive counter operation procedures in several accidental situations that counter procedures what are called accident managements (AMs) are prepared.

Keyword: operator support; functional model; Multilevel Flow Modeling; pressurized water reactor; counter operation procedure

1 Introduction

The role of operators in plant operation are to control plant condition according to operation plan, to monitor plant conditions, especially to detect the occurrence of an anomaly, and to take suitable counter actions in an abnormal plant condition. The situation awareness[1] is important in the tasks of operators. The situation awareness is composed of 1) suspecting that something happens, 2) identifying the anomaly cause, and 3) predicting future plant behavior.

A newly constructed nuclear power plant equips with a fourth generation control panel. The panel utilizes an integrated display of measurements and operation information by the recent advancement of information and interface technologies. The outline of plant condition is displayed in a large screen to share important information of plant conditions among operators. For operators, CRT-based operation terminals are installed to give flexible ways of monitoring plant conditions and taking operation actions. In addition, some functions of automatic check of monitoring and confirming operator actions by computers installed in the control panel.

The operation style of operators is said to change from manual control to cognitive control through supervisory control by the introduction of advanced automated systems and intelligent systems. Autonomous intelligent systems support operators by taking automated operation procedure and operators select a suitable operation strategy. Plant instrumentation signals are processed to give meaningful information for operators by integrating measurements from instrumentation and control systems relevant to operations. A human-machine joint system to accomplish common goals of operators and automated systems is investigated from the viewpoints that operators can maintain their skill in monitoring and operating plants.

Lessons learned from Fukushima-Daiichi accidents caused by the serious tsunami include the necessity and importance that operators and field staff in a plant site should have the abilities to behave autonomously and to decide suitable counter actions in order to recover resiliently plant condition or at least not to have serious damage.

This article first introduces the concepts for achieving the safety of nuclear power plants, summarizes the types of information sharing and proposing the idea of co-operator to support operators. Then, the article emphasizes the importance to use functional information in the operation of nuclear power plants. It also introduces a technique to derive plausible

Received date: March 2, 2016
(Revised date: March 21, 2016)

counter operation procedure that the authors have studied.

2 Concepts for the safety of nuclear power plants and operator support

2.1 Defense in depth

"Defense in depth"[2] is one of the concepts to achieve the safety of nuclear power plants. The concept is applied especially in the design phase of nuclear power plants. The principal idea of "Defense in depth" is to keep the safety of a system by multiple protection layers even if several layers don't work well.

Generally, "Defense in depth" is realized by five layers in nuclear power plants[2]. The layers enable to respond to an anomaly and failure and to reduce the influence of an accident.

First layer: Preventing the occurrences of anomalies and failures (preparing to prevent the occurrence of a disturbance).
Second layer: Preventing the development of an anomaly and failure to an accident (preparing to reduce the influence of a disturbance to plant components).
Third layer: Mitigating the affects of accident (preparing to avoid the release of radioactive substances even if serious failures have occurred in plant components)
Fourth layer: Taking measures to an accident that exceeds design criteria (preparing to avoid the considerable release of radioactive substances even if core damage have happened).
Fifth layer: Taking measures to protect the public and the environment (preparing to suppress public exposure of radioactivity even if serious release of radioactive substances have happened).

2.2 Resilience engineering

Resilience engineering[3, 4] focuses on how humans respond to a thread flexibly and how humans recover the damaged system in an early stage of the happening of a disturbance. For example, if an uncontrollable disturbance (*i.e.* natural disaster) happens, human operators try to keep system's stability by avoiding, absorbing the influence of the disturbance, and recovering from an abnormal situation rapidly. There are four abilities to make a system/organization resilient: 1) monitor, 2) respond, 3) anticipate, and 4) learn.

2.3 Information sharing

Information sharing is important in the operation of nuclear power plants because the operation is conducted by an operator team and automated systems. There are three types of information sharing.

The first is the information sharing among operators. Operation information in normal operating conditions is shared to succeed efficiently the operation task at a shift change. The information of a troublesome component may contribute to detect an anomaly in an early stage. The operation know-how of skilled operators can be succeeded smoothly to young operators by information sharing through on-the-job training. To share the information of plant condition in an abnormal plant condition will contribute to increase the quality of effective information for counter actions and to avoid cognitive narrow path in making a decision.

The second type of information sharing is the one between operators and operation support systems. Not only the information of plant condition but also the knowledge and information necessary for inferring plant condition and making a decision should be shared.

The third type is the information sharing among plant designers, operators and maintenance workers. This type seems not to be considered in the operation and maintenance of nuclear power plants but is considered to be important as much as the other types of information sharing. Sharing design information will contribute to take suitable counter actions in an abnormal situation because operators can understand the roles of components and parts of a plant and the operation conditions supposed in designing a plant. To share the maintenance information will also contribute to detect early an anomaly and/or anomaly cause by suitable and effective plant monitoring.

2.4 Co-operator

The authors propose the concept of co-operator[5] that a near future operator support system behaves as an

intelligent software agent by supporting the situation awareness of operators to increase the safety and reliability of a plant that is operated by fewer operators. The co-operator monitors plant condition and supports plant control by operators using plant knowledge and the knowledge related with diagnosis and operation. It mutually interacts with operators to exchange and indicates useful information. The expected roles of the co-operator are subordinate to accurately execute tasks requested by operators, partner to share operation tasks, and adviser to give useful knowledge for operators.

There are several topics for developing a co-operator. Because the co-operator is an intelligent software agent, monitoring plant condition based on different viewpoints from those of operators is important as well as monitoring based on the same viewpoints as those of operators. Moderate back up of the errors made by operators will be useful to reduce human errors of operators. The concept of dynamic operation permission[6] is an example. The third topic is to generate easy understandable explanation of processes and conditions of reasoning made by co-operator and to display through efficient interaction with operators. The fourth topic is also important but difficult to develop. It is to understand the intentions of operators in taking operation actions. More technological advancements in especially artificial intelligence and human interface are necessary.

3 Function and functional model

3.1 Function

An artifact is designed under designers' intention. The intention can be expressed in terms of goals, purposes, expected behaviors, effects, and so on. An artifact has a main goal that is most important description of designers' intention. Components and parts in a system have some roles to realize the main goal and they are combined hierarchically to form a specific structure. The roles are often expressed in terms of functions. Therefore, functions can be modeled in a hierarchical way.

The characteristics of functions are as follows:

1) functions are in high abstraction level, and
2) a function explains that why a component exists in a system[7].

A function may be realized by different components. For example, the pressure of a vessel with steam and water decreases by condensing the steam. The depressurization can also be realized by extracting some steam and/or water from the vessel. Furthermore, a component may have behaviors that are not recognized as functions in the original design but may be recognized as functions in abnormal conditions[8].

There are advantageous features in a functional model that expresses functions of system components and parts. Roles and purposes are correlated with system behavior. Causal relations are represented. A functional modeling framework has hierarchical modeling capability. A function is described by a linguistic representation. However, a functional model usually does not express quantitative information. It may be difficult to change a functional model when the function of a system or a component changes.

As described above, functional information of components is important to design large-scale complex systems such as nuclear power plants. The information on functions of components of a nuclear power plant is considered to be important and helpful for operators in operation, especially in the case of abnormal situation. However, functional information seems not to be used in the current plant operation.

3.2 Multilevel Flow Modeling

Multilevel Flow Modeling (MFM)[9-11] is a methodology to model an engineering system from the standpoint of means and goals. It represents a system along two dimensions of means-end and whole-part dimensions. The distinctive feature of MFM is to use a set of primitive function concepts to represent system goals, functions, and their relations in a graphical way. Figure 1 shows the symbols of current MFM[11].

The roles of systems and components are represented by "objective" and "threat" of the figure. System functions are represented by a set of mass, energy, activity, and information flow structures. The functions and their relations of a part of a system are represented by the symbols in a flow structure. Each function is connected by a relation symbol of "influence". Relations between primitive functions

and "targets" are represented by a relation symbol in "means-end" and "control".

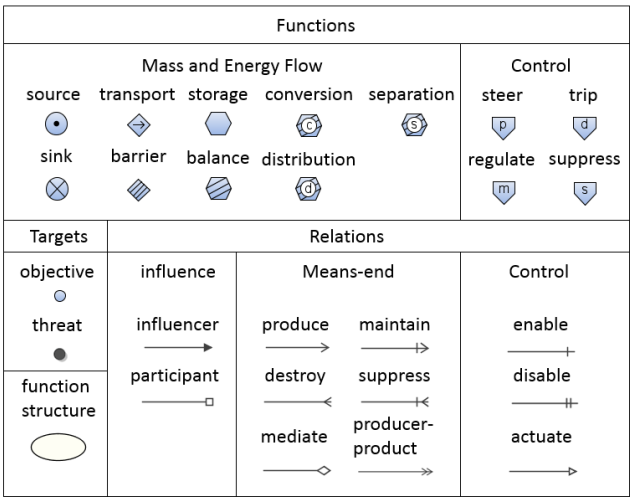
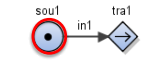
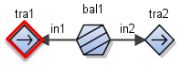


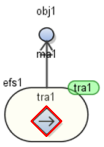
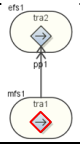
Fig. 1 Symbols of MFM[11].

Table 1 Examples of the influence propagation rules

(a) Rules for the relations among functions

Pattern	Cause	Consequence	
	sou1	tra1	
	High output F	High F	
	Low output F	Low F	
	tra1	bal1	tra2
	High F	Leak	Normal
		Normal	High F
	Low F	Fill	Normal
		Normal	Low F

(b) Rules between function structure and objective

Pattern	Cause	Consequence
	tra1	obj1
	High F	True (high)
	Low F	True (low)
	Not function	False
	tra1	tra2
	High F	High F
	Low F	Low F

3.3 Causal inference based on MFM model

The relations between objectives (goals) and flow structures in an MFM model express necessity and condition relations. The relations between two functional symbols in a flow structure express mass or energy balances between the two components or parts that realize the functions. From these modeling features, the relations in an MFM model are considered to represent causalities.

The authors studied a causality inference technique[12] based on an MFM model for the old set of MFM symbols. Recently, Zhang, *et al.*[13] and the authors[14] derive causality inference rules for the new set of MFM symbols shown in Fig. 1.

Some of influence propagation rules are shown in Table 1. For example, the upper pattern of the rules shown in Table 1 (a) indicates that if provided flow by a source function increases (a source state changes to "high output flow"), then transported flow by the downstream transport function will increase (transport state changes to "high flow"). On the other hand, if provided flow decreases (source state changes to "low output flow"), then transported flow will decrease (transport state will be "low flow").

4 Technique to generate counter operation procedures

4.1 Background

It is important to suppose a variety of accidents and to prepare in advance efficient measures in order to minimize the damage in the happening of an accident. Basically operators are asked to take measures following operation procedures. However, there might happen an abnormal situation that is not supposed due to the troubles of back up systems and safety systems. Therefore, it is desirable to support operators in such a situation as well as to suppose abnormal situations and to prepare counter measures for them as many as possible.

One of techniques to support operators is to generate plausible operation procedure for an emergency situation. The technique can strengthen the third and fourth layers of "Defense in depth". Operation procedures using the components that have the same function as that of failed component will help operators to take suitable counter actions resiliently.

4.2 Outline of the algorithm to generate operation procedures based on an MFM model

The principal idea of generating procedures for emergency response is to find a series of operations to realize a safety goal considered in an emergency

situation by using the components that are not originally equipped for the safety goal but have the functions to achieve it. From this point, a functional model plays a key role of finding counter operations. The technique uses the MFM model of a target system. Influence propagation rules are applied to estimate the effects of an operation on the future plant condition and behavior. The data of the conditions for each operation are also used because usually some conditions should be satisfied before taking an operation.

Figure 2 shows the flow chart of the algorithm to generate an operation procedure to mitigate the influence by an unexpected anomalous situation. First, the MFM model of a target system is modified by changing the functions in the MFM model corresponding to the failed components by the occurrence of an abnormal situation in Step 1. The function changed is supposed not to recover to the normal condition. In Step 2, a safety goal is set to reduce the damage or influence of the abnormal situation. The selection of safety goal is made by operators. Then, in Step 3 the safety goal is re-described by changing the viewpoint of goal description for searching the objectives represented in the MFM model. Objectives to match the safety goal or re-described safety goals are searched in Step 4.

The influence propagation is made using reversely influence propagation rules from the objective that matches the safety goal or re-described safety goals in Step 5. The plant behaviors and operations that can contribute to achieve the safety goal may be found. They are considered as the candidates of operations. In Step 6, the conditions of each operation candidate are checked if the operation candidate can be taken without any condition. If there is a certain condition for the operation, the condition is set as the safety goal and the control of executing the algorithm returns to Step 3. The loop is repeated until a first operation that can be taken without any condition for each operation candidate is found.

Finally, a series of operations found are reversely ordered considering the conditions of operations in Step 7. The reordered operations form an operation procedure.

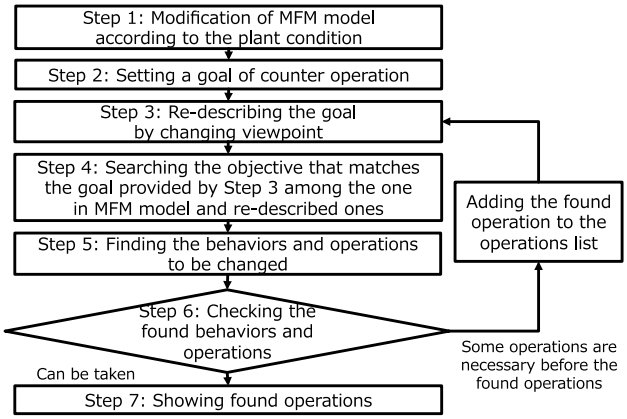


Fig. 2 Flow chart of operation procedure generation algorithm.

4.3 Applicability evaluation

In order to confirm the applicability of the technique to generate plausible operation procedures, an MFM model for a PWR plant is constructed as shown in Fig. 3. The model represents functions and their relations of the major systems and some safety systems of a PWR plant such as the primary system, the secondary system, the turbine bypass system, the residual heat removal system, the internal spray system, and the fire protection system.

Three severe accidental situations of a PWR plant are considered. They are loss of coolant accident (LOCA) cases after the detection of partial core damage with the conditions such that (A) the Emergency Core Cooling System (ECCS) and main steam relief valve fail to initiate, (B) the residual heat removal system does not work, and (C) internal spray system fails to initiate. The real Japanese PWRs prepare counter procedures what are called accident managements (AMs)[15] for the situations using suitable components that are originally equipped for other purposes: "Using turbine bypass system" for the case A, "Alternative recirculation" for the case B and "Water injection into a reactor containment" for the case C.

Table 4 shows the derived operation procedures and AM for the case C. As shown in the table, the same procedure as AM is successfully derived by the proposed algorithm based on the constructed MFM model. Moreover, the proposed algorithm derives some other candidates of operation procedures. These operation procedures are considered to be effective to reduce the negative influence due to the accidental situations.

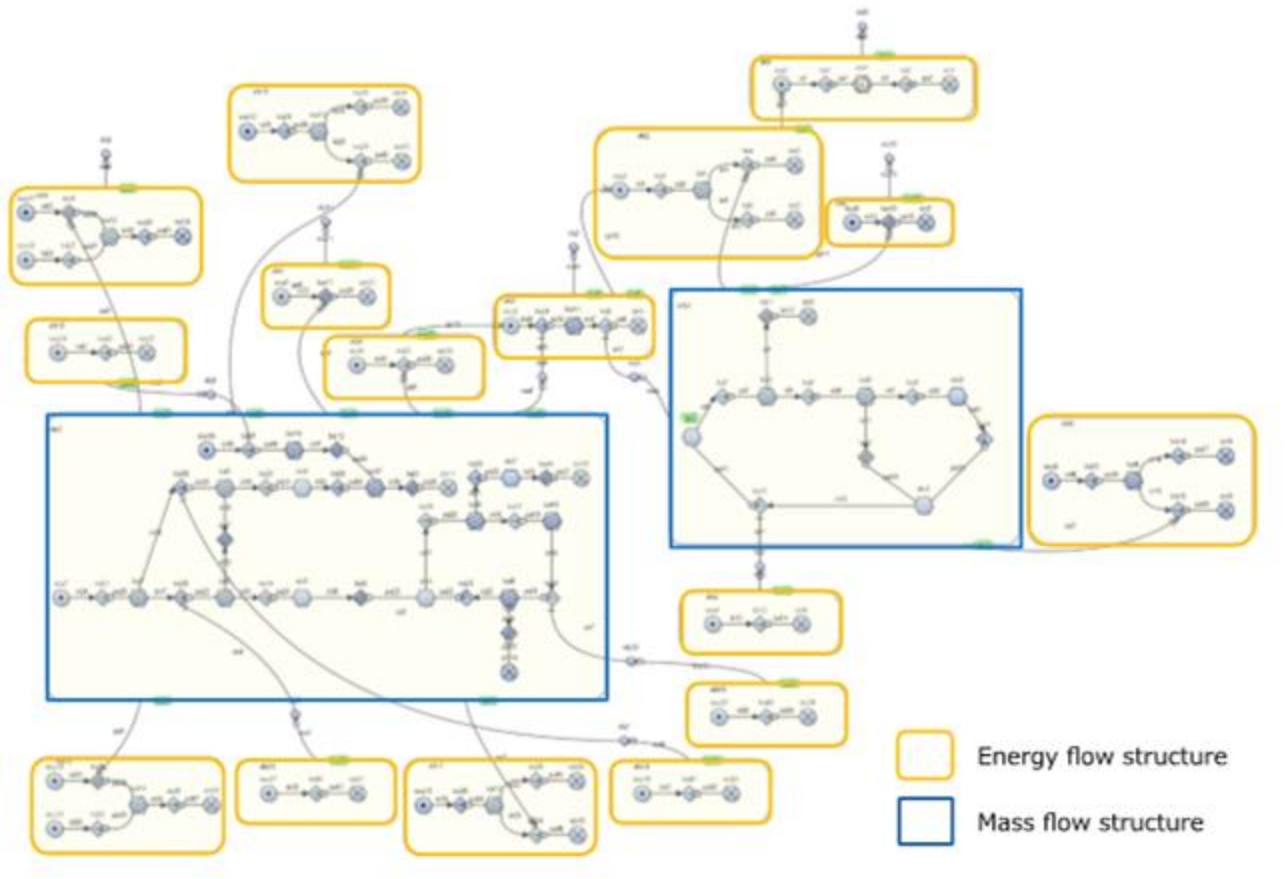


Fig. 3 MFM model of a PWR plant.

Table 4 Comparison between derived operation procedures and AM for Situation B

	Generated procedures	AM
a	1. Opening MSIV 2. Opening TBV	
b	1. Opening tie-line valve 2. Opening residual heat removal valve	1. Opening tie-line valve 2. Opening residual heat removal system valve (Alternative recirculation)
c	1. Opening PRV	
d	1. Opening MSRV	

6 Conclusions

One of important roles of operators in plant operation is to take suitable counter actions in an abnormal plant condition. The article emphasizes the importance of information sharing between operator support systems and operators. The article also points out the importance to use functional information in taking resiliently counter actions and introduces a technique to generate emergency counter operation procedures based on the MFM model of a target system.

By applying the technique to generate operation procedures in several accidental situations of a PWR plant and comparing the derived operation procedures with AMs for PWR plants, it is concluded that the technique is able to produce suitable candidates of operation procedures.

Future works include the implementation of the proposed technique and the development of a technique to estimate the quantitative effects of the derived operation procedures for selecting most effective counter operation procedure.

References

[1] ENDSLEY, M. R.: Toward a theory of situation awareness in dynamic systems, Human Factors, 1995, 37 (1): 32-64.

[2] INSAG: Defence in depth in nuclear safety, INSAG-10, IAEA, 1996.

[3] HOLLNAGEL, E., WOODS, D. D., and LEVENSON, N.: Resilience engineering: Concepts and percepts, Ashgate Publishing Ltd., 2006.

[4] HOLLNAGEL, E., PARIES, J., WOODS, D. D., and WREATHALL, J., Resilience engineering in practice: A guidebook, Ashgate Publishing Ltd., 2011.

[5] GOFUKU, A.: Support systems of plant operators and designers by function-based inference techniques based on MFM models, International Journal of Nuclear Safety and Simulation, 2011, 2 (4): 327-338.

[6] GOFUKU, A., and SATO T.: Dynamic operation permission system for oil refinery plants, The International Journal of Intelligent Control and Systems, 2009, 14 (2): 149- 157.

[7] AAAI, AAAI-93 workshops summary reports, AI Magazine, 1993, 15 (1): 63-66.

[8] GOFUKU A.: Deriving behaviour of an engineering system from a functional model, Journal of the Japanese Society for Artificial Intelligence, 1996, 11 (1): 112-120. (In Japanese)

[9] LIND, M.: Representing goals and functions of complex systems - an introduction to multilevel flow modeling, Institute of Automatic Control Systems, Technical University of Denmark, Report No. 90-D-381, 1990.

[10] LIND, M.: An introduction of multilevel flow modeling, International Journal of Nuclear Safety and Simulation, 2011, 2 (1): 22-32.

[11] LIND, M.: Control functions in MFM: basic principles, International Journal of Nuclear Safety and Simulation, 2011, 2 (2):132-139.

[12] GOFUKU A., ADACHI K., and TANAKA Y.: Finding out counter actions in an anomalous plant situation based on functions and behavior, *Transactions of The Institute of Systems, Control and Information Engineers*, 1998, 11 (8), 458-465 (in Japanese).

[13] LIND, M., and ZHANG, X.: Functional modeling for fault diagnosis and its application for NPP, Nuclear Engineering and Technology, 2014, 46 (6): 753-772.

[14] INOUE, T., GOFUKU, A., and SUGIHARA, T.: A technique to generate plausible operation procedure for an emergency situation based on a functional model, Proc. of International Symposium on Socially and Technically Symbiotic Syst-ems 2015 and International Symposium on Symbiotic Nuclear Power Systems 2015, 2015: 437-443.

[15] The Japan Atomic Power Company, Overview of protecting measures that were established in AM examination report and AM maintenance report, Available: http://www.meti.go.jp/press/2012/04/20120419002/20120419002-6.pdf. [Access date: 2016. 2. 27]. (In Japanese)