Nuclear Engineering and Technology 50 (2018) 542–552

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

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

Original Article

Planning of alternative countermeasures for a station blackout at a boiling water reactor using multilevel flow modeling

Mengchu Song*, Akio Gofuku

Graduate School of Natural Science and Technology, Okayama University, 3-1-1, Tsushima-Naka, Kita-ku, Okayama, 700-8530 Japan

ARTICLE INFO

Article history:
Received 2 February 2018
Received in revised form
3 March 2018
Accepted 13 March 2018
Available online 23 March 2018

Keywords:
Alternative Countermeasure
Decision-Making Support
Multilevel Flow Modeling
Response Planning
Station Blackout

ABSTRACT

Operators face challenges to plan alternative countermeasures when no procedure exists to address the current plant state. A model-based approach is desired to aid operators in acquiring plant resources and deriving response plans. Multilevel flow modeling (MFM) is a functional modeling methodology that can represent intentional knowledge about systems, which is essential in response planning. This article investigates the capabilities of MFM to plan alternatives. It is concluded that MFM has a knowledge capability to represent alternative means that are designed for given ends and a reasoning capability to identify alternative functions that can causally influence the goal achievement. The second capability can be applied to find originally unassociated means to achieve a goal. This is vital in a situation where all designed means have failed. A technique of procedure synthesis can be used to express identified alternatives as a series of operations. A case of station blackout occurring at the boiling water reactor is described. An MFM model of a boiling water reactor is built according to the analysis of goals and functions. The accident situations are defined by the model, and several alternative countermeasures in terms of operating procedures are generated to achieve the goal of core cooling.

1. Introduction

The Fukushima disaster exposed an inadequate response capability [1]. The control room operators failed to carry out effective countermeasures to terminate core damage and protect barriers due to the loss of monitoring and controlling functions of plants by the serious tsunami. As for complex systems such as nuclear power plants, the cognitive task of planning plays an important role in emergency response. Planning refers to a process of developing an approach for achieving a goal [2]. In most cases, the planned response may include a complicated course of control actions. Generally, there are three potential paths for developing a response plan. The first two paths are based on written procedures or established practices. It is necessary to find the appropriate emergency operating procedures (EOPs), in which rule-based planning is the most straightforward among them. Another path is planning that involves the use of severe accident management guidelines (SAMGs), which is not a pure rule-based approach. Instead, it requires not only specific knowledge to prioritize selected high-level action candidates, but also operation skills when implementing a special high-level action. In the nuclear industry, these written procedures are prepared according to the established defense in depth concept in nuclear safety that can address multiple emergency situations [3,4]. Although the need of generating a real-time plan may be eliminated, appropriate existing procedures must be selected according to the current situations. The selection process can be both event-based and symptom-based. Accordingly, there are several techniques focusing on navigating operators, such as the computer-based procedure [5,6]. However, the Three Mile Island accident coupled with what recently occurred at Fukushima Daiichi nuclear power station (NPS) indicate that unexpected disturbances may extend beyond situations that can be addressed by existing responses such as EOP and SAMG. In other words, personnel, especially the frontline control room operators, may be required to develop alternative countermeasures based on their knowledge of the plant and situation, which is referred to as knowledge-based planning. Since no response plan can be provided, the potential support for activity of planning must be rooted in a model-based approach that can be used to identify a response means. The model should be coherent with human's mental representations of relationships within the major systems in the plant. To support the identification of effective plans, these representations are required to be [7]

---

* *Corresponding author.*
E-mail address: song.m.mif@s.okayama-u.ac.jp (M. Song).

https://doi.org/10.1016/j.net.2018.03.004

- comprehensive, showing important connections between components and systems;
- flexible so that when standard methods are unavailable, unfamiliar methods can be created; and
- detailed so that sequencing of control actions can be carefully planned.

When operators encounter a planning task, they generally consider the problem within a context of intentions, such as the purpose of a component [8]. Hence, the intentional knowledge of systems is comprehensive to humans and should be reflected in the representation that is used for planning. Functional modeling is able to describe a system's intentions by providing information about goals, functions, components, and their relationships. Multilevel flow modeling (MFM) [9,10], a functional modeling methodology, makes it possible to graphically describe this knowledge in a hierarchical structure. Another characteristic of MFM is that the abstraction level can be chosen to fit the modeling purpose, which means it can be detailed enough to generate information about operable components such as actions. MFM has been used to model action sequences for a normal operation situation [11]. Gofuku [12,13], applied the component information contained in a MFM model to generate one counteraction for an anomaly. In a previous study [14], a system was developed based on MFM to generate procedures that involved more than one operation for accident situations.

This article illustrates how MFM can be used to plan alternative countermeasures for a station blackout occurring at a boiling water reactor (BWR). First, an MFM model of the BWR is built based on analysis of goals and functions. The capabilities of MFM to represent and reason alternatives are explained. The alternatives identified by MFM can be further expressed as a series of operations based on a technique of procedure synthesis. Finally, the situations of station blackout are defined with the MFM model, and several countermeasures are generated to achieve the goal of core cooling. Limitations and future work are also discussed.

2. Modeling theory of MFM

MFM is a graphical modeling methodology that can describe goals and functions of industrial processes. The concepts of means—end and whole—part decomposition and aggregation play a fundamental role in MFM and lead to a modeling in multiple levels of abstraction. As shown in Fig. 1, a system can be described in terms of goals, functions, and physical components along the means—end relation. An end represented by a goal or high-level function can be realized by means of lower level functions or components. In the part—whole dimension, different means—end structures can be aggregated to form a complete model according to the system configurations. The modeling should not be done for each individual component but rather the behavioral interactions between them must be analyzed.

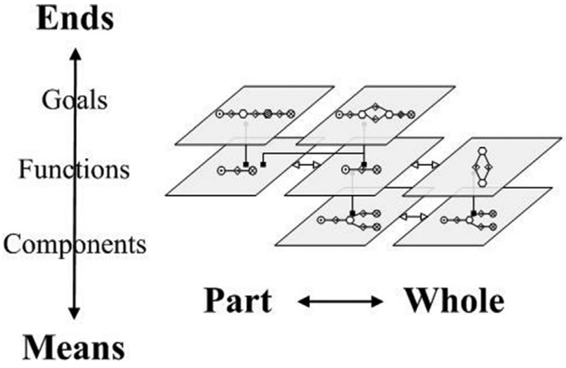


Fig. 1. Means—end and part—whole decomposition in MFM.
MFM, multilevel flow modeling.

Fig. 2 shows the basic symbols of MFM. First, the topmost ends in the model can be represented as objectives and threats, which can respectively be achieved and suppressed by functions. Since industrial processes always involve interactions between different kinds of flows, like material, energy, and information flows, a series of functional primitives are designed to describe these flows in the same abstraction level. The main primitives include source, sink, transport, barrier, storage, and balance. Separation, distribution, and conversion are special derivatives of the balance function to describe in detail different categories of balance in flows. Relations are used to connect between functions and objectives or between each individual function. One kind is influence relations, describing causal dependencies between functions. Another is the kind of means—end relations to describe purpose-related dependencies. MFM can also be used to model control systems, which have both functions and goals as an industrial process [15]. Describing control functions by MFM is based on a separate action theory, which is beyond the scope of the case in this article and will not be further discussed.

To summarize, MFM has features that can satisfy the requirements of representation for planning described in the Introduction: (1) intentional knowledge represented by MFM is coherent with the process of comprehending systems and their relationships, (2) MFM is flexible because it is a common modeling strategy that shows basic knowledge of systems with explicit symbols, which makes it possible to derive various useful information, and (3) the level of abstractions can be selected to fit the modeling purpose. Moreover, MFM also can be used for reasoning about causes and consequence, which will be the foundation of this study that leads to the generation of countermeasures.

3. Functional modeling of BWR

3.1. BWR and its operational objectives

A BWR is a kind of light-water reactor. Fig. 3 shows the system configuration of a General Electric (GE)-type BWR, which is same as Units 2 to 5 of the Fukushima Daiichi NPS [16]. The BWR has only one single power cycle, in which steam is directly produced through the reactor core to drive the turbine generator. There are various auxiliary systems that are designed to maintain normal operation and to ensure the plant's safety during accidents.

The operational objectives of the plant should first be identified in modeling of a system. There are two categories of objectives that need to be achieved in the operation of the BWR. One is for normal operation and the other comprises safety goals for emergency situations. The major objectives that will be shown in the MFM model are summarized in Table 1. Note that objectives in MFM are goals that are directly related to operational parameters of flow functions, such as power corresponding to the flow rate of the heat transfer function. They could be subgoals of goals that are not represented in the model; for example, *obj7* can be treated as a subgoal of the goal of protecting barriers.

3.2. Flow functions of reactor pressure vessel and primary containment vessel

The MFM model of the BWR is shown in Fig. 4. From the objectives, two major flow structures (energy flow structure *efs3* and mass flow structure *mfs1*) are directly identified, and they

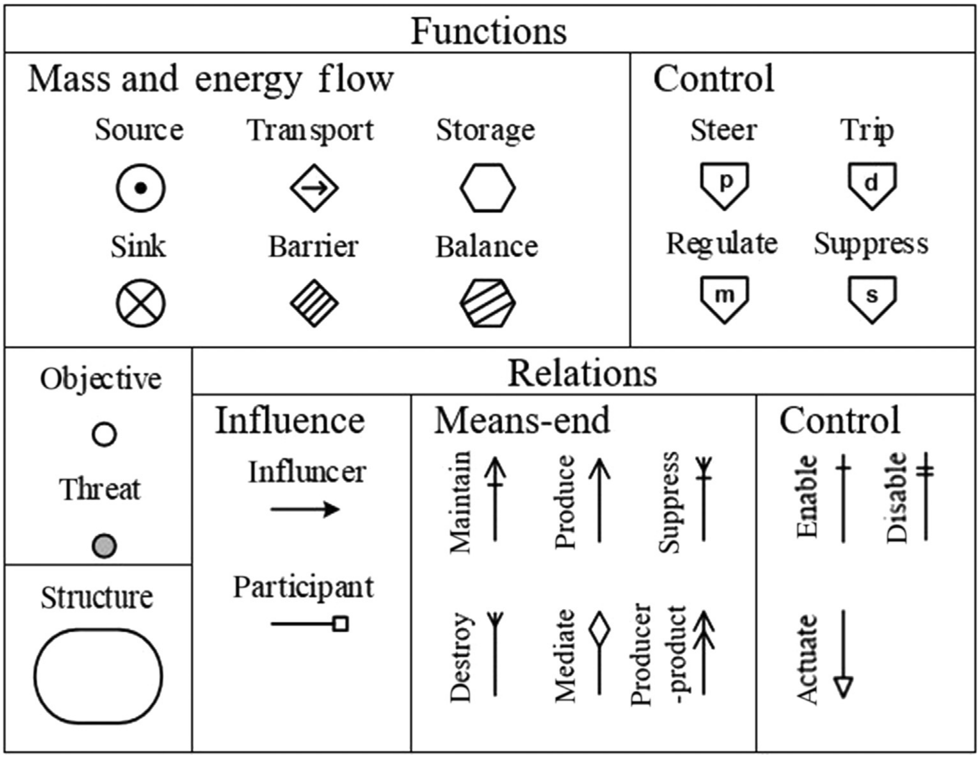


Fig. 2. MFM symbols.
MFM, multilevel flow modeling.

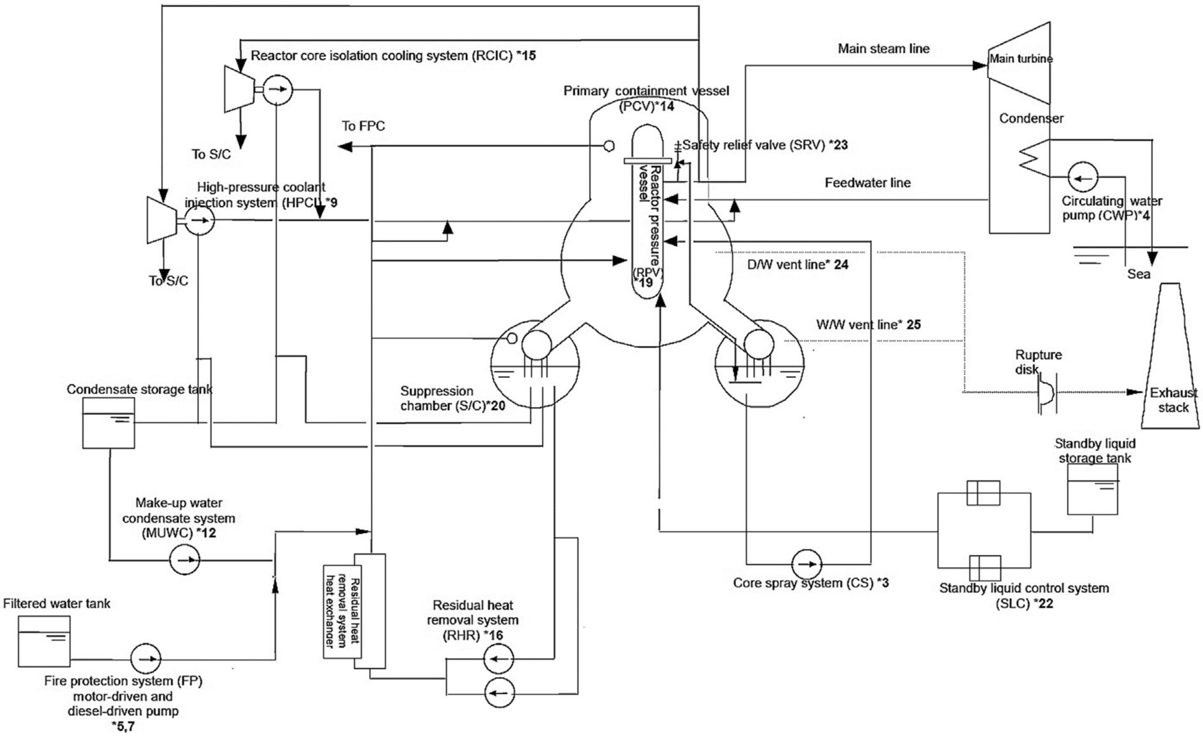


Fig. 3. The system configuration of a BWR plant (valves are not shown).
BWR, boiling water reactor; D/W, dry well; W/W, wet well.

describe energy and mass flow functions within the reactor pressure vessel (RPV) and primary containment vessel (PCV). Table 2 lists the major functions and their correspondence to possible components or systems. Functions that can contribute to the objectives in Table 1 are also indicated. Note that there may be some functions in high level abstraction that cannot directly correspond to some components. In *efs3*, the reactor core provides the energy source (*sou4*) for the whole energy transfer in

Table 1
Major operational objectives of BWR.

Category	Number	Descriptions
Category 1 (normal)	obj1	Maintain electrical power production.
	obj2	Maintain heat production of the reactor core.
	obj3	Maintain water level in RPV.
	obj4	Maintain the average temperature/pressure in RPV.
Category 2 (emergency)	obj5	Produce increase of the heat transfer from the reactor core.
	obj6	Produce decrease of the average temperature/pressure in RPV.
	obj7	Produce increase of the heat transfer from PCV.

BWR, boiling water reactor; PCV, primary containment vessel; RPV, reactor pressure vessel.

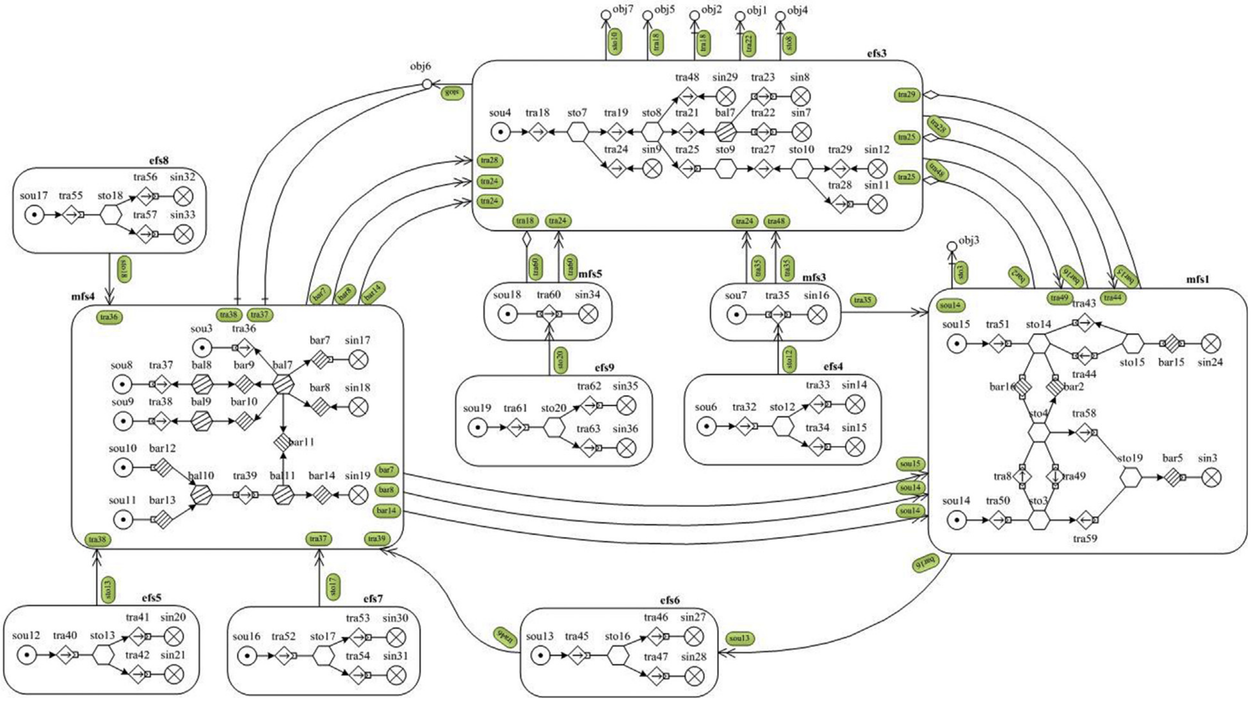


Fig. 4. MFM model of BWR.
BWR, boiling water reactor; MFM, multilevel flow modeling.

the plant. Normally, the source is generated by the fission reaction in the nuclear materials, whose potential of energy output can be controlled by the insertion and withdrawal of control rods. While in an emergency, considering that the reactor has been shut down, the energy source comes from the heat released as a result of radioactive decay, a process that cannot be controlled. There are five energy sinks identified for heat transfer. *Sin9* indicates that the heat stored in the coolant is partially consumed by injected additional coolant. *Sin29* is used to explain the heat transfer from steam to water in the process of condensation caused by spray. During normal operation, *sin7* and *sin8* indicate that some energy in steam is applied to drive the turbine generator, and the rest is transferred to the sea in a condenser. In addition, the steam energy that may be released in the PCV can be consumed by spray (*tra28*) or released to the environment via the venting system (*tra29*).

The mass flow structure *mfs1* describes the material transfer in the major part of the BWR plant. The model is constructed according to the process between several storage functions. First, *sto3*, *sto4*, and *sto19*, representing coolant in the RPV, steam in the RPV, and water in the condenser, comprise the major power cycle of the BWR. The steam can be released to the suppression chamber (*sto14*) by opening safety relief valves or stop valves of HPCI or RCIC. The closed valves are modeled with barrier functions (*bar2* and *bar16*). *Sto15* represents the steam and other gas that may be released into the wet well (W/W) and dry well (D/W) of the PCV. The steam can be finally released to the environment through the venting systems (*bar15*). Source functions *sou14* and *sou15* represent the water sources for core and containment injection, respectively. There is only one objective directly related to *mfs1*, maintaining the water level in the RPV, which is contributed by the state of coolant storage function *sto3*.

As shown in Fig. 4, *mfs1* and *efs3* are interrelated by some means–end relations: (1) *bar2* in *mfs1* is connected with *tra25* in *efs3* with a mediate relation, that is, because *bar2* in a state of leak means steam releases to PCV, which at the same the time means a process of energy transfer; (2) a produce–product relation connecting *tra48* in *efs3* and *tra49* in *mfs1* indicates a process of condensation in RPV when the energy in steam transferring to spray water (*tra48*) results in the steam being condensed to water (*tra49*); (3) the mediate relation of *bar16*–*tra25*, the relation of mass–energy transfer, represented using the principle of 1; (4) the produce–product relation of *tra28*–*tra44*, the process of condensation in the PCV, same as 2; and (5) the mediate relation of *bar15*–*tra29*, the mass–energy transfer of the process of PCV venting.

Table 2
Major functions in RPV and PCV.

Structure	Function	Component/system	Descriptions	Objective contributed
efs3	sou4	Reactor core	Heat resource in the reactor core	
	tra18		Heat transfer from core to coolant	obj2/obj5
	sto7	RPV	Heat in the coolant	
	tra24		Heat consume by additional coolant	
	sto8	RPV	Heat in the steam in RPV	obj4/obj6
	tra22		Heat transfer for power production	obj1
	tra48		Condensation in RPV	
	sto9	PCV suppression chamber	Heat in the suppression chamber	
	sto10	PCV D/W or W/W	Heat in the steam in PCV	obj7
	tra28		Condensation in PCV	
	tra29		Energy release via venting path	
mfs1	sto3	RPV	Coolant storage in RPV	obj3
	sto4	RPV	Steam storage in RPV	
	tra58	Main steam lines/turbine	Steam transports from RPV to condenser	
	sto19	Condenser	Water storage in condenser	
	bar5		Isolation between condenser water and sea water	
	sin3		Sea	
	tra59	feedwater line	Water transfer in feedwater line	
	bar2	SRV	Steam isolation by SRV	
	bar16	steam stop valves of RCIC/HPCI	Steam isolation by steam stop valves of RCIC/HPCI	
	sto14	PCV suppression chamber	Water in the suppression chamber	
	sto15	PCV D/W or W/W	Steam in PCV	
	bar15	Venting valves	Steam isolation by venting valves	
	sin24		Environment	
	sou14		Sources of core injection	
	sou15		Sources of containment injection	

D/W, dry well; HPCI, high pressure coolant injection; PCV, primary containment vessel; RCIC, reactor core isolation cooling; RPV, reactor pressure vessel; SRV, safety relief valve; W/W, wet well.

3.3. *Modeling of the auxiliary systems*

The other functional structures in the model describe auxiliary systems of the BWR. Table 3 lists the major functions and their possible corresponding components or systems. *Mfs3* models the water transfer of the independent core spray (CS) in a high abstraction level, with only a source, a transport, and a sink function to describe the basic injection process. Two produce–product relations connect *mfs3* with *efs1* because *tra35* can cause both condensation of steam and heat consumption of coolant in the RPV. Because *tra35* is also one of the reasons that *sou14* in *mfs1* becomes available, a produce–product relation between them is also modeled. *Mfs5* represents the independent standby liquid control (SLC) with the same level of *mfs3*. Besides that *tra60* in *mfs5* contributes to heat consumption in that RPV, it has a function as a control system capable of shutting the reactor down. Hence, *tra60* is also connected to *tra18* with a mediate relation, and this indicates that by injecting boron water, heat release of the nuclear core can be controlled.

Mfs4 represents a special category of safety systems that may be involved in a pipeline connection between each other. For instance, the make-up water (condensate) (MUWC) and the fire protection (FP) are connected with the residual heat removal (RHR) at the pipelines between the heat exchanger and the low-pressure injection inlets to the RPV and the PCV. Another example of a system connection can also be found for the RHR: it is connected with the RCIC or the HPCI. The detailed correspondences between functions and components in *mfs4* are shown in Table 3. Note that, considering RCIC and HPCI are modeled to represent a category of injection system with the same resources and same kind of components, namely the turbine-driven system, they are modeled using the identical series of functions.

In addition, *efs4-9* describe the essential means for some transfer functions realized by pumps in the auxiliary systems, i.e., energy conversion from other energy (electrical power except for *efs6*, which is steam for RCIC/HPCI pump) to rotational energy of the pumps.

Table 3
Major functions of auxiliary systems.

Structure	Function	Component/system
mfs3	sou7	Suppression chamber
	tra35	CS pump
mfs4	sou3	Suppression pool
	tra36	RHR pumps
	sou8	Filtered water tank
	tra37	FP pump
	bar9	FP valve
	sou9	Condensate storage tank
	tra38	MUWC pump
	bar10	MUWC valve
	bar7	Containment spray valve
	bar8	Low-pressure injection valve
	bar11	Connection valve
	sou10	Condensate storage tank
	sou11	Suppression pool
	tra39	RCIC/HPCI pump
	bar12-14	RCIC/HPCI valves
mfs5	sou18	Standby liquid storage tank
	tra60	SLC pumps

CS, core spray; FP, fire protection; HPCI, high pressure coolant injection; MUWC, make-up water (condensate); RCIC, reactor core isolation cooling; RHR, residual heat removal; SLC, standby liquid control.

4. Alternative representation in MFM

Most systems have the design feature of many-to-many mappings of means–end, as represented in MFM, which means the same end can be realized by many alternative means, and meanwhile a means can achieve several ends at the same time. Fig. 5 shows a structure of means and ends that includes many-to-many mapping. There are three ends, Q_1, Q_2, and Q_3, which can be objectives or functions in a high abstraction level. For each end, there are several means, i.e., functions or components. Each mean may be also realized by several means in lower levels. Note that the AND/OR graph notations in the figure suggest a distinction when reading from ends toward means. AND means an end requires several means to be satisfied at the same time for its realization, while OR means that the end can be realized by any of means represented in lower level.

All the means–end relationships that have been considered in system design can be represented by MFM many-to-many mapping, which thereby provides an approach to search available alternative means to achieve given ends when some means may be unavailable. As shown in Fig. 5, when P_2 and P_4 fail, P_3 becomes the only means that can realize Q_2. Moreover, if R_1 is available, there are also two alternative means, R_2 or R_3, to finally achieve Q_2.

Cases can be also found in the BWR model in Fig. 4, for example, *tra24* in *efs3*, which represents the heat consume function realized by additional coolant. *Tra24* is connected with *tra35* in *mfs3*, *tra60* in *mfs5*, and *bar8* and *bar14* in *mfs4* in lower levels, which represents the injection function of CS, SLC, low pressure coolant injection (LPCI), and RCIC/HPCI, respectively. Moreover, although the component level is not directly represented in the model, the MFM model implies the alternative components for a given function. For instance, *tra39* in *mfs4* is used to describe the pumping function realized by two steam-driven injection systems, namely, RCIC and HPCI.

5. Alternative identification by causal reasoning of MFM

The means should not only be used by the agent (component) with the intention of achieving an end, as shown in the many-to-many mappings of MFM but also should be able to produce the end; this indicates means can causally influence the achievement of the end by changing states. In addition, means for different ends in the same part–whole level are also causally related [10,12,17]. Thus, with these two causal aspects of MFM, means that may be previously unassociated can be identified because they can produce the achievement of given ends as a regulated means does. This is very important when considering alternatives for unexpected situations, where designed means may become unavailable. A typical example is shown in the mitigation of the Fukushima accident, where the FP system was used as a means of core injection. In MFM, this kind of alternative can be searched using causal reasoning.

MFM defines some qualitative states for functional primitives to explain how far the performance of a function deviated from the desired norm, such as high or low state of a transport function. Gofuku [13,18] defined the cause–effect relations of states between each two connected primitives in the model as the influence propagation rules. Zhang [19] recently updated the rules to make it possible to analyze the casualties for a set of current MFM primitives. Table 4 shows examples of two categories of rules, namely part–whole and means–end rules. As we can see from the table, there are two possible situations where the influences cannot be propagated. One is considered when reasoning cause-consequence between a transport function and a nontransport function such as storage, which are connected by a participant relation (there is a box on the relation at the transport-side), which means that the nontransport function cannot influence the state of the other function but only passively receive or deliver the flow. Another situation results from the asymmetrical feature of the means–end relation, which means the existence of an objective or a function in the upper level is conditional on the existence of the main function (the function that directly contributes to realizing objective or upper-level function), but not the reverse [10]. Hence, the state change of an objective or a function cannot be propagated to its main function.

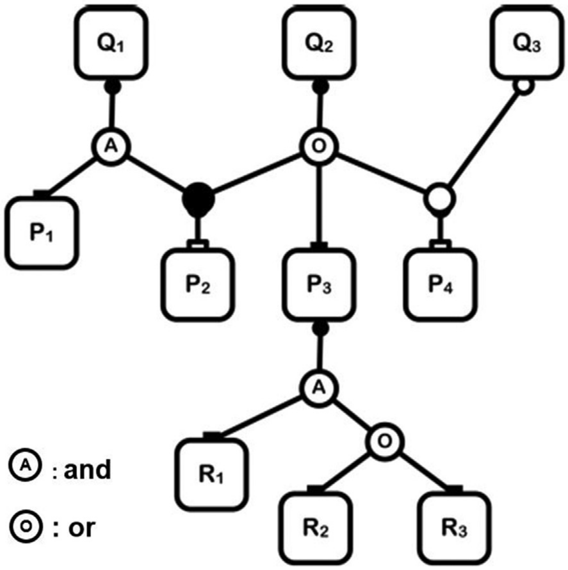


Fig. 5. A structure of means and ends in MFM.
MFM, multilevel flow modeling.

By applying the influence propagation rules, a function with state change can propagate its influence on the other functions along different paths in the model. If necessary, by reversely using the rules, state changes of functions can be inferred as possible causes for a known consequence, which may be evidence observed in the system or an assumed condition. The example in Fig. 6 is used to briefly illustrate how a successful path that is not originally considered to achieve an end can be identified using MFM reasoning. One of the designed functions of RHR is to achieve core injection (P_1-Q_1), and FP is intended for fire protection (P_2-Q_2). By matching appropriate influence propagation rules, it can be found that a state change of functions in P_2 can affect the state of functions in P_1, which finally causes the achievement of Q_1.

6. Synthesis of alternative procedures

In terms of MFM, response planning can be defined as a process of matching a goal state to be achieved with available functions and their specific states. To reach the goal state, the means of some control inputs, i.e., operations, are required to change the states of specific parts of the plant, normally some operable components. In the previous study [14], it has been investigated that MFM can be used to synthesize a sequence of operations on components, that is, the operating procedure to achieve a system goal. In this article, applying the technique of procedure synthesis to transfer the alternative means proposed in Sections 4 and 5 into operating procedures is considered.

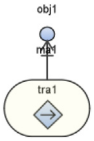
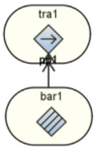
6.1. Prerequisites

Although MFM describes intentional knowledge about components, the component level is not directly reflected in the model. If the component information, such as operations, is something desired to be derived from an MFM model, the relationships between functions, states, and components should be established before reasoning. Hence, the following vector format is defined to describe essential information, including components of each functional primitive x in an MFM model,

$$\overrightarrow{V}(x) = (P(x), f_u(x), f_d(x), S(x), A(x), Com(x), O(x), Con(O(x))). \tag{1}$$

where $P(x)$ is the basic primitive in MFM, i.e., objective, source, sink, transport, barrier, balance, or storage. $f_u(x)$ and $f_d(x)$ are the primitives connected upstream and downstream of x in an MFM model,

Table 4
Examples of influence propagations rules.

Category	Pattern	Cause	Consequence
Part-whole		sto1 high volume/low volume	tra1 high flow/low flow
		tra1 high flow/low flow	sto1 low volume/high volume
		tra1 high flow/low flow	sto1 high volume/low volume
		sto1 high volume/low volume	no consequence
Means-end		tra1 high flow/low flow (state 1)	obj1 true (high)/true (low)
		tra1 no flow (state 2)	obj1 false
		obj1 true/false	no consequence
		bar1 leak	tra1 high flow
		bar1 normal	tra1 no flow
		tra1 high flow/low flow	no consequence

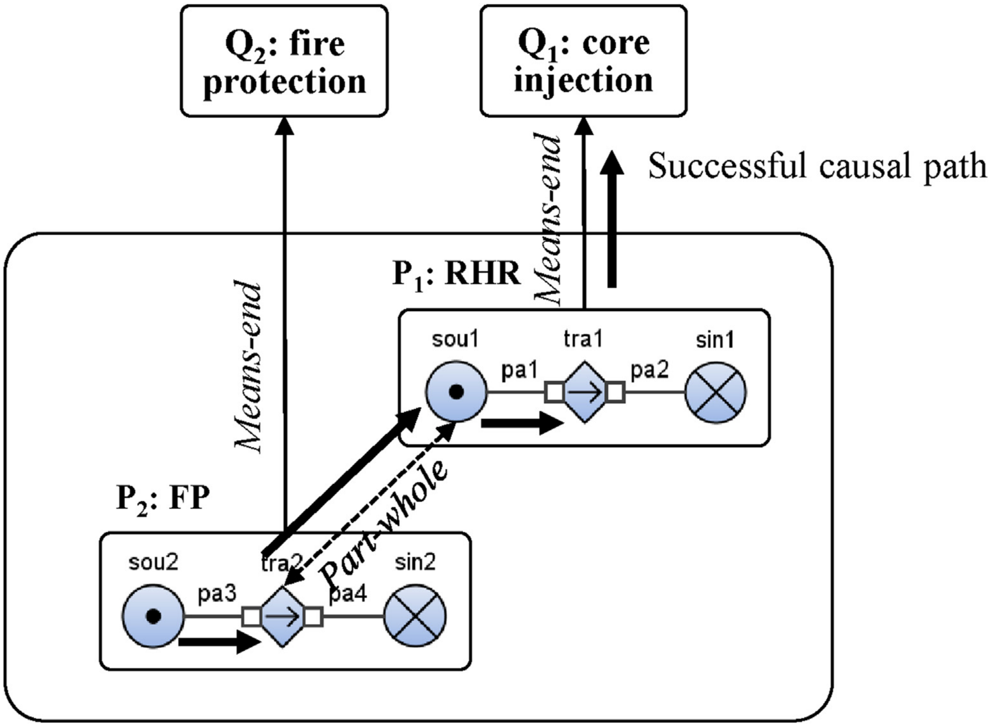


Fig. 6. Identification of a successful causal path.

respectively. $S(x)$ is the state. $A(x)$ is used to judge whether the primitive is available or not. $Com(x)$ is the component that corresponds to x. $O(x)$ represents a possible operation on $Com(x)$. $Con(O(x))$ represents the conditions that should be satisfied before the execution of $O(x)$. In other words, $O(x)$ cannot realize its intention, namely changing the state of function without satisfactions of conditions. $Con(O(x))$ can be represented as

$$Con(O(x)) = (f_{con}(x), S(f_{con}(x))). \tag{2}$$

This means that the condition can be the state of some primitives in the MFM model.

The operations in the plant can be classified into three categories [11]. The first is the on/off type, which marks a qualitative shift in the state. The second is the adjustment type to change the quantitative state after the qualitative state has been established, which always deals with the tuning of the plant state. The last category of operations involves actions on the automatic controller, for instance, to establish linkages of multiple components. The last two categories are common in the normal operations, while the first is common in the start-up tasks and emergencies, both of which require establishing or stopping some material or energy flows. Considering the application to accidents, the approach for the moment defines state correspondence of function-component for on/off-type operations. If other types of operations are observed in other cases, similar correspondences should be defined. Two kinds of on/off-type operation can be found in the BWR case of this paper. One is operation for the isolation valves. In the MFM model of Fig. 4, the valves are modeled as barrier functions, whose state can be changed by opening or closing the valves. Another kind of operation is to start or stop a pump, which is represented as a transport function. Tables 5 and 6 show the relations between states of function, components, and required operation, for valves and pumps, respectively. For example, if a barrier function is required to be in a state of leak, opening the corresponding valve is necessary. Because the pump is considered with only two states, on and off, which means that there is no other operation than starting or stopping. It is thereby assumed that when the reasoning result requires a transport function to be in a high-flow state, the operation of starting is considered, while for the state of low flow or no flow, stopping the pump should be considered.

6.2. *Algorithm*

The flow chart of procedure generation is shown in Fig. 7. The details of the algorithm are proposed in the study by Gofuku et al. [14]. In the first step, the unavailable functions in the model should be defined according to the situation in accidents. A goal that can correspond to an objective is then set, and the causes that can realize the objective are inferred by matching appropriate influence propagation rules. The goal must be the most relevant to the current state, but the determining process is beyond the range of this article. The causes are iteratively reasoned along available functions in the model until the found state change of some function can be achieved by an operation. After checking conditions for this operation, a new goal may be defined, which requires searching other operations to achieve it. Thus, there will be a series of operations that are found to achieve a set goal, which is referred to as a procedure. Although some situations may require operations being executed nearly in parallel, to synthesize the operations in a sequence, the method defines that the latter found operation should be arranged before the former in a procedure.

7. Applications

In this part, the above method will be used to plan alternative countermeasures for the station blackout (SBO). SBO refers to an accident initiated by the loss of both off-site and on-site power systems, to be specific, in nuclear power plants, the electrical grids, and emergency diesel generators, with the result that the alternating current power cannot be maintained for core cooling and other safety functions in a shutdown situation [20]. It should be emphasized that the SBO situation in this article is not completely identical with the situation in the Fukushima Daiichi NPS because there is an underlying assumption that the critical support systems for control such as direct current power are available, while in the Fukushima accident it failed. Moreover, the failures of the stationary diesels that can supply power for MUWC and FP as occurred in the Fukushima accident are not considered. Hence, only a common defined SBO situation is analyzed in the current article. In this section, the unavailable functions in the accident will be first defined, and then several alternative countermeasures in terms of operating procedures are generated for the goal of core cooling.

Table 5
Correspondence of barrier valve.

State	Function	Component	Operation
State-1	Normal	Closed	Closing
State-2	Leak	Opened	Opening

Table 6
Correspondence of transport pump.

State	Function	Component	Operation
State-1	Low/no flow	Stopped	Stopping
State-2	High flow	Operated	Starting

7.1. *Defining unavailable functions*

Since SBO is an emergency, the objectives maintained in normal operation naturally become invalid. The unavailable functions include the flow functions of the main steam lines, feedwater line, SLC, CS, and RHR. In the study, an independent failure is also assumed for the steam-driven injection system RCIC and HPCI. Table 7 lists the unavailable objectives, functions, or structures during the accident situation supposed in this study.

7.2. *Generation of alternative countermeasures*

The goal of core cooling is assumed for generating alternative countermeasures. To achieve this, objective *obj5*, namely to produce an increase of the heat transfer from the reactor core, is specified as a trigger to find essential operations that can result in the goal. In Fig. 8, the functional flows that are emphasized by a sequence of arrows are used to illustrate how a procedure can be derived from an objective. First, by matching several predefined influence propagation rules, it is found that *bar8* in *mfs4* with a leak state can cause the state of *obj5* to change to true. Although this state can be realized by opening some valves, the condition that upstream provides the materials must be satisfied in advance. An operation is thereby found to be executed prior to the previous operation. Based on a similar mechanism, two more operations can be derived. Table 8 shows the process of deriving a procedure using the algorithm.

As shown in Table 9, including the procedure in the above-mentioned example, five different procedures are generated for the goal of core cooling in the situation of SBO. There are four means designed for cooling the core by injecting additional coolant by RHR, RCIC, CS, and SLC, respectively. As shown in the MFM model, those means are represented by the principle of many-to-many mappings. During an accident, however, all of them fail due to loss of power and the posited failures. The first four procedures in Table 9 indicate how to enable previously failed injection with alternative systems, i.e., FP and MUWC, which are originally intended for other purposes, but depressurization of the reactor with the operation of opening SRVs is required. Hence, both many-to-many principle and causal reasoning of MFM contribute to deriving these procedures. The last procedure shows that the single operation of opening SRVs also influences core cooling by releasing some energy in the RPV, which is directly derived using causal reasoning.

8. Discussion

The approach based on MFM provides a systemic way to identify components available in accidents that can be used to achieve a response goal. The results shown in the BWR case indicate that some systems that are not originally intended for the current purpose, such as the FP for core injection, can be derived as countermeasures. This is vital when most designed measures become unavailable. Since the occurrence of the Fukushima accident, it has been reflected that the accident management should consider the

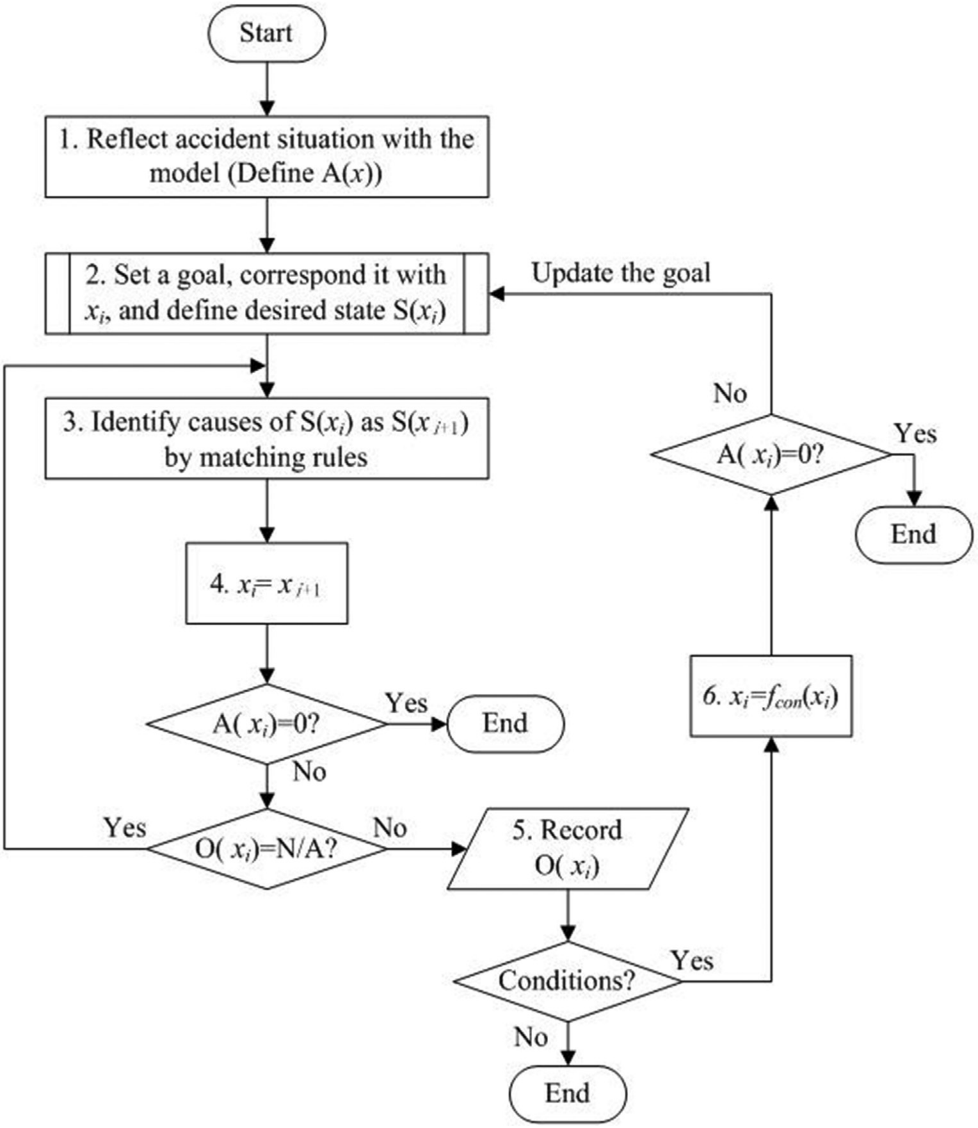


Fig. 7. The flow chart of procedure generation.

full design capabilities of the plant, including the possible use of systems beyond their originally intended functions and measures to attain flexibility of functions [16], [21]. Thus, the study can be applied to supplement existing responses such as EOPs and SAMGs. On the one hand, more anomalous situations can be covered by assuming different sets of unavailable functions in the MFM model. On the other hand, the method can improve the diversity in preparation of the same situation, which will make the response plans more robust and the plant more resilient.

Table 7
Unavailable MFM primitives during the supposed accident situation.

Primitives	Plant state that leads to the unavailability
obj1~4	SBO
tra58/tra21	SBO
tra59	SBO
tra35/efs4/tra48	SBO
tra60/efs9	SBO
tra36/efs8	SBO
tra39/efs6/bar16	Supposed failures of RCIC/HPCI
efs4	SBO
efs6	Supposed failures of RCIC/HPCI
efs8	SBO
efs9	SBO

HPCI, high pressure coolant injection; MFM, multilevel flow modeling; RCIC, reactor core isolation cooling; SBO, station blackout.

Although multiple procedures are generated, they may not be as complete as an EOP that can be directly executed. One reason is each component considered in the MFM model is generally treated as one entity to only reflect the attention that is normally required during operations. For instance, a pump is composed of a motor, a propeller, and other subcomponents, which means operators have to coordinate different kinds of operations for a task of starting the pump. It is, however, only represented by a transport function with only single defined operation. It might be resolved by extending the knowledge to lower level functions implied in each operable function in the MFM model. Another limit comes from insufficient consideration of operational conditions. The condition of each operation is only assumed as a particular function state. The operations, however, may have multiple conditions that must be satisfied before, which further requires that operations derived from different conditions be arranged into a sequence. In the future, it will be necessary to improve the algorithm of procedure

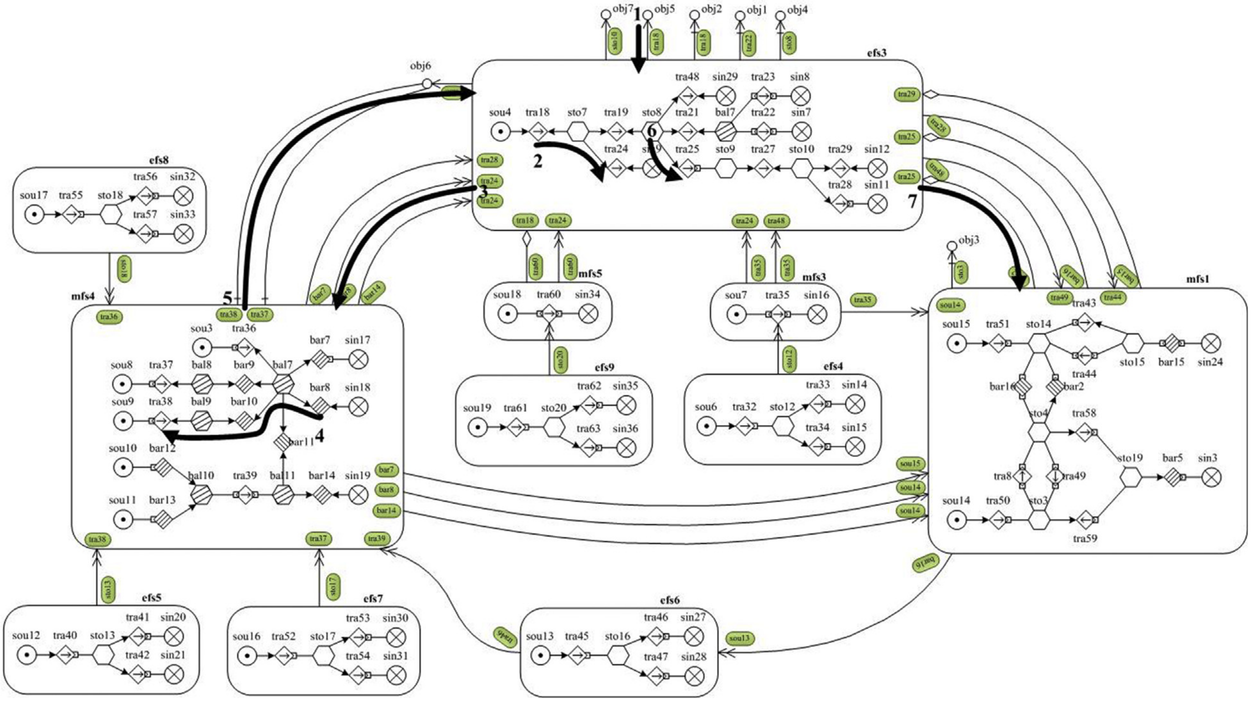


Fig. 8. Reasoning process in the MFM model.
MFM, multilevel flow modeling.

Table 8
Process of deriving a procedure.

Step in algorithm	Primitive	Desired state	Operation
2	obj5	True (high)	
3	tra18	High flow	
3	sto7	Low volume	
3	tra24	High flow	
3→5	bar8	Leak	Open valve
6→2→5	bar10	Leak	Open valve
6→2→5	tra38	High flow	Start pump
6→2	obj6	True (low)	
3	sto8	Low volume	
3	tra25	High flow	
3→5	bar2	Leak	Open valve

synthesis to address the possible priority of conditions. To address the above two limits, detailed information about components might be necessary.

Obviously, the countermeasures are derived from a viewpoint of positive effect, namely a response goal. The negative consequences are thereby implicit. It is necessary for the decision-maker to evaluate response plans, not only the possible consequences on the other components but also how readily the plan can be implemented, which will aid people in making the final decision. A study [22] has investigated some criteria of plan evaluation. In addition, to precisely evaluate the response plans, the quantitative information, such as volume of a tank to indicate how long the core injection can be maintained, may be further required. Since MFM is a qualitative modeling method, being unable to describe and reason quantitative knowledge is an intrinsic limitation. In the future, therefore, other techniques may be essential to provide quantitative consequences of the generated plans.

9. Conclusions

The article has investigated two capabilities of a functional modeling methodology called multilevel flow modeling to plan alternative countermeasures for accidents. A special concern is the situations where no response plan exists to address the current plant state. One is a knowledge capability, namely a model that describes the intentions of systems and components that may be applied as essential resources in a response. The alternative means designed to achieve a given end can be chosen from the many-to-many mappings in MFM. Another capability is a causal reasoning function of MFM, by which a state change of an originally unassociated function might be identified as an alternative means to realize the goal of countermeasures. The alternatives can be formulated as countermeasures with a series of operations using a technique of procedure synthesis. An application to a station blackout with failure of some components at a BWR is described. The intentional knowledge of BWR is represented by an MFM

Table 9
Generated procedures for the goal of core cooling.

Step	Procedure 1	Procedure 2	Procedure 3	Procedure 4	Procedure 5
1	Open SRVs (bar2)	Open SRVs (bar2)	Open SRVs (bar2)	Open SRVs (bar2)	Open SRVs (bar2)
2	Start MUWC pump (tra38)	Start FP pump (tra37)	Start FP pump (tra37)	Start MUWC pump (tra38)	
3	Open MUWC valve (bar10)	Open FP valve (bar9)	Open FP valve (bar9)	Open MUWC valve (bar10)	
4	Open low-pressure injection valve (bar8)	Open low-pressure injection valve (bar8)	Open connection valve (bar11)	Open connection valve (bar11)	
5			Open RCIC injection valve (bar14)	Open RCIC injection valve (bar14)	

FP, fire protection; MUWC, make-up water (condensate); RCIC, reactor core isolation cooling; SRV, safety relief valve.

model. The failed functions are then defined, and several operating procedures using available functions are generated to achieve the goal of core cooling. The weakness of the current version of the proposed technique and future works are also discussed.

Conflict of interest

The authors declare no conflicts of interest.

Acknowledgments

A part of the results of this study was obtained by the support of Japan Society for the Promotion of Science (JSPS) [KAKENHI grant number 16H03136] and CHUBU Electric Power Co., Inc. in Japan.

Abbreviations

AC	Alternating Current
BWR	Boiling Water Reactor
CBP	Computer-Based Procedure
CS	Core Spray
DC	Direct Current
D/W	Dry Well
EOP	Emergency Operating procedure
FP	Fire Protection
HLA	High-Level Action
HPCI	High Pressure Coolant Injection
MFM	Multilevel Flow Modeling
MUWC	Make-Up Water (Condensate)
NPS	Nuclear Power Station
PCV	Primary Containment Vessel
RCIC	Reactor Core Isolation Cooling
RHR	Residual Heat Removal
RPV	Reactor Pressure Vessel
SAMG	Severe Accident Management Guideline
SBO	Station Blackout
SLC	Standby Liquid Control
SRV	Safety Relief Valve
W/W	Wet Well

Appendix A. Supplementary data

Supplementary data related to this article can be found at https://doi.org/10.1016/j.net.2018.03.004.

References

[1] E. Hollnagel, Y. Fujita, The Fukushima disaster-systemic failures as the lack of resilience, Nucl. Eng. Technol. 45 (2013) 13–20.

[2] W.F. Stubler, J.M. O'Hara, J.C. Higgins, J. Kramer, Human Systems Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance, NUREG/CR-6637, U.S. Nuclear Regulatory Commission, Washington, DC, 2000.

[3] IAEA, Defence in Depth in Nuclear Safety, IAEA, Vienna, 1996.

[4] IAEA, Implementation of Accident Management Programmes in Nuclear Power Plants – Safety Reports Series No. 32, IAEA, Vienna, 2004.

[5] S.J. Lee, P.H. Seong, Development of an integrated decision support system to aid cognitive activities of operators, Nucl. Eng. Technol. 39 (2007) 703–716.

[6] R.L. Boring, K.D. Thomas, T.A. Ulrich, R.T. Lew, Computerized operator support systems to aid decision making in nuclear power plants, Procedia Manuf. 3 (2015) 5261–5268.

[7] R.J. Mumaw, D. Swatzler, E.M. Roth, W.A. Thomas, Cognitive Skill Training for Nuclear Power Plant Operational Decision Making, NUREG/CR-6126, U.S. Nuclear Regulatory Commission, Washington, DC, 1994.

[8] M. Lind, M.N. Larsen, Planning support and the intentionality of dynamic environments, in: Expert. Technol. Cogn. Human-Computer Coop., L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 1995, pp. 255–278.

[9] M. Lind, Modeling goals and functions of complex industrial plants, Appl. Artif. Intell. 8 (1994) 259–283.

[10] M. Lind, An introduction to multilevel flow modeling, Nucl. Saf. Simul. 2 (2011) 22–32.

[11] M.N. Larsen, Modelling Start-up Tasks Using Functional Models, The Technical University of Denmark, 1993.

[12] A. Gofuku, K. Adachi, Y. Tanaka, Finding out counter actions in an anomalous plant situation based on functions and behavior, Trans. Inst. Syst. Control Inf. Eng. 11 (1998) 458–465.

[13] A. Gofuku, Application of a derivation technique of possible counter actions to an oil refinery plant, in: Proc. 4th IJCAI Work. Eng. Probl. Qual. Reason, 1999, pp. 77–83.

[14] A. Gofuku, T. Inoue, T. Sugihara, A technique to generate plausible counter-operation procedures for an emergency situation based on a model expressing functions of components, J. Nucl. Sci. Technol. 54 (2017) 578–588.

[15] M. Lind, Control functions in MFM: basic principles, Nucl. Saf. Simul. 2 (2011), 132–129.

[16] TEPCO, Fukushima Nuclear Accident Analysis Report, Tokyo Electric Power Company, Inc., Tokyo, 2012. http://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0104.pdf.

[17] M. Lind, X. Zhang, Applying functional modeling for accident management of nuclear power plant, Proc. ISOFIC/ISSNP 2014 (5) (2014) 1–10.

[18] A. Gofuku, Applications of MFM to intelligent systems for supporting plant operators and designers: function-based inference techniques, Nucl. Saf. Simul. 2 (2011) 235–246.

[19] X. Zhang, M. Lind, O. Ravn, in: Consequence Reasoning in Multilevel Flow Modelling, IFAC Proc, 12, 2013, pp. 187–194.

[20] S.A. Hodge, J.C. Cleveland, T.S. Kress, M. Petek, Identification and Assessment of BWR In-vessel Severe Accident Mitigation Strategies, 1992.

[21] IAEA, The Fukushima Daiichi Accident Report by the Director General, IAEA, Vienna, 2015.

[22] T. Inoue, A. Gofuku, A technique to prioritize plausible counter operation procedures in an accidental situation of plants, in: 8th Int. Symp. Symbiotic Nucl. Power Syst. 21st Century, 2016.