A VALIDATION METHOD FOR EMERGENCY OPERATING PROCEDURES OF NUCLEAR POWER PLANTS BASED ON DYNAMIC MULTI-LEVEL FLOW MODELING

WEI QIN† and POONG HYUN SEONG*
Dept. of Nuclear and Quantum Engineering
Korea Advanced Institute of Science and Technology
373-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Republic of Korea
†Currently with INET, Tsinghua University, China
*To whom correspondence should be addressed. phseong@kaist.ac.kr

While emergency operating procedures (EOPs) occupy an important role in the management of various abnormal situations in nuclear power plants (NPPs), current technology for the validation of EOPs still largely depends on manual review. A validation method for EOPs of NPPs is thus proposed based on dynamic multi-level flow modeling (MFM). The MFM modeling procedure and the EOP validation procedure are developed and provided in the paper. Application of the proposed method to EOPs of an actual NPP shows that the proposed method provides an efficient means of validating EOPs. It is also found that the information on state transitions in MFM models during the management of abnormal situations is also useful for further analysis on EOPs including their optimization.

1. INTRODUCTION

Procedures in a nuclear power plant (NPP) provide instructions to guide operators in monitoring, decision making, and controlling the plant. [1] Especially in emergency situations, operators are required to simply follow the emergency operating procedures (EOPs) without diagnosing the cause of the emergency situations. This means that the quality of EOPs is one of the most decisive factors in determining the safety of the plant. However, few methods have been developed for the validation of EOPs. The review of EOPs by NPP operators is currently the most widely and commonly used method for the validation of EOPs.

Multi-level flow modeling [2] is developed for the representation of goals and functions of complex process plants, and applied to various areas such as for the development of diagnosis and planning systems for operator support in supervisory control [3-5], design of displays for supervisory control of industrial plants [6], development of dynamic operation permission systems [7,8], and the conceptual analysis and synthesis of control systems. MFM models a system by expressing it in terms of its goals and elementary functions that describe the mass, energy, and information flows in the system.

Paassen and Wieringa [9] proposed the dynamic MFM, in which the data measured from the system are used to update the state of the MFM model so that the

state of the model reflects the state of the system. In this way, the actions required to achieve the goals of a system can be determined. This property of the dynamic MFM is quite important in that it can be used for the validation and/or optimization of EOPs of NPPs. By making use of this property of the dynamic MFM, we propose a validation method for EOPs of NPPs based on dynamic Multi-level Flow Modeling (MFM).

2. THE PROPOSED METHOD

2.1 Symbols

Complex heterogeneous systems presently contain complex automated operations. MFM is proposed to describe the qualitative character of the operation of automated systems such as NPPs. MFM models a system by expressing it in terms of its goals and elementary functions, which describe the mass, energy, and information flows in the system. The relations between goals and functions, and among functions themselves, are defined. The flow functions are arranged in coherent units, which are called flow structures, and the flow functions form the means for achieving the system's goals.

In the classical MFM developed by Lind [2], symbols were defined for representing goals, basic flow functions, and relations; these are *source, sink, storage, balance,*
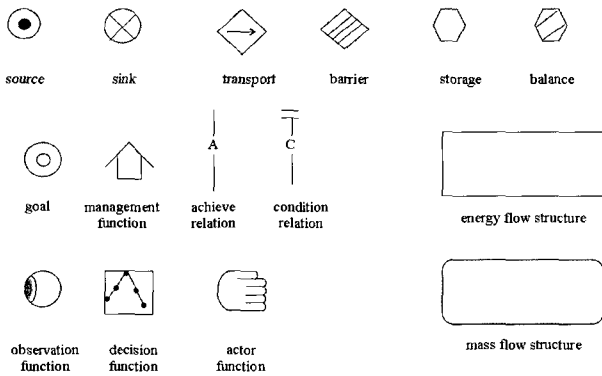
Fig. 1. Symbols used in this paper

barrier, *transport*, *goal*, *connection relation*, *condition relation*, and *achieve relation*. Each of the flow functions in MFM represents a single behavior or a specific combination of behaviors. The basic flow functions can be combined into flow structures, and the flow functions in a structure are causally related. With the introduction of the dynamic MFM by Paassen and Wieringa [9], several other symbols were added, *management function*, *observation function*, *decision function*, *actor function*, and *flow structure*. In this paper, we further divide *flow structure into mass flow structure* and *energy flow structure*, and define different symbols for two flow structures. Figure 1 shows the symbols that are used in the proposed method.

2.2 Modeling procedure

The modeling procedure of the proposed method is as follows:

1. The top goal of a system is first identified. In heterogeneous systems, various operational modes may exist under different operational circumstances. Therefore, for the same heterogeneous system, there could be various MFM models with different top goals.

2. The necessary functions to achieve the top goal are represented using predefined flow functions. The *flow functions* will be encapsulated into one or several flow structures. Inside each flow structure, all the flow functions work upon the same energy or mass flow. A flow function in a flow structure contributing mainly to the achievement of a higher level goal is connected to the goal with an *achieve* relation.

3. The subgoals necessary for the achievement of the functions in higher level flow structures are identified and then connected to the corresponding functions with a *condition* relation. This is an iterative process until the target system is fully decomposed into basic flow functions whose operational characters can be obtained from solid data. At this point, the model has a multi-level property.

4. Two sets of meaningful states are defined, one for the goals and one for the flow functions. The flow functions and goals are not only logical concepts, but they have physical representations in real systems. The states of the flow functions and goals should be definable from the real-time data of a real system or simulator. MFM models constitute a kind of logical and physical decomposition of a system, and as such the system is decomposed by the means-end logic. The models describe the interrelationships and mechanisms in the target system.

5. During the real time operation of the target system, the real-time data are measured from the target system, and then fed to the MFM model to update the states of the goals and flow functions in the model. In this way, the dynamic model reflects the states of the system in real time.

2.3 EOP Validation Process

The process for validating EOPs consists of the following procedures:

1. A MFM model is developed following the procedure described in Section 2.2 for an abnormal situation in an NPP such as a loss of coolant accident (LOCA), a steam generator tube rupture accident (SGTR), or a steam line break (SLB).

2. A simulator simulates the abnormal situation, and the plant parameter data are collected in real time to determine and update the states of the goals and flow functions in the MFM model.

3. The state transitions of the NPP during the abnormal situation are recorded to validate the operators' actions specified in EOPs. EOPs should be correctly functioning to guide the operators during the abnormal situations in order to reduce the impact of the abnormal situation and eventually cool down the reactor. The NPP system should have experienced a series of state transitions during the abnormal situation for the achievement of the overall goal. The states of all the components should be within permitted operating conditions and fulfill the system requirements of the NPP as well as regulatory codes and standards.

3. AN EXAMPLE

3.1 Configuration of Simulator, EOPs, and MFM model

As an example, the validation procedure is applied to the validation of EOPs of a pressurized water reactor (PWR) NPP under an SGTR accident. The fully-implicit safety analysis-2 (FISA-2) simulator, which is a simulator for a Westinghouse 600MWe-type PWR NPP, is used for the simulation of the SGTR accident. The workstation version of the simulator (FISA-2/WS) was

developed by Seok et al. [10-11] in 1992 and the personal computer (PC) version (FISA-2/PC) was developed by Sim et al. [12] in 2002. The simulator was used for the experimental verification of various previous studies such as modeling the information processing of NPP operators [13] and development of an automated operating procedure system [14]. The EOPs of a Westinghouse 600MWe-type PWR NPP, Kori unit 2, implemented in a computerized procedure system ImPRO developed by Jung et al.[15], are used as the target EOPs subject to validation. The MFM model for the management of an SGTR accident developed by Gofuku et al. [7,8] is used as the MFM model. In the MFM model, the cooling of the reactor is modeled as the top goal to prevent radioactive release to the environment, since the nuclear reactor is assumed to be automatically tripped by the plant protection system (PPS), and the cooling of the reactor becomes the most important concern in the management of an SGTR accident. Figure 2 shows the MFM model. The definitions of goals, flow functions, and structures used in the MFM model are summarized in Table 1, Table 2, and Table 3, respectively. Several important goals and states are also identified and summarized in Table 4 and Table 5, respectively.

Table 1. Definitions of goals

Symbol	Description
Go1	Cooling the reactor
Go2	Circulation of primary coolant
Go3	Establishing heat removal
Go4	Maintaining primary coolant
Go5	Pumping primary coolant
Go6	Maintaining subcooling
Go7	Maintaining primary pressure > secondary pressure
Go8	Generating steam
Go9	Establishing steam flow
Go10	Bypassing steam
Go11	Maintaining feedwater

Table 2. Definitions of flow functions

Symbol	Description
So1	Heat generation by nuclear reaction
So2	ECCS coolant tank
So3	RCS pump electrical source
So4	Charging coolant tank
So5	Spray water tank
So7	Pressurizer heater electrical source
So8	Heat from primary coolant
So9	Heat from SGTR flow
So10	Feedwater and auxiliary feedwater
So11	SGTR flow
So12	Feedwater pump electrical source
Tr1	Transfer heat from reactor core
Tr2	Transfer heat by primary coolant
Tr3	Pumping primary coolant to reactor core
Tr4	Primary coolant flowing through SGTR
Tr5	Transport ECC coolant
Tr7	Transport charging flow to primary loop
Tr10	Transport pressurizer vapor through PORV
Tr12	Transfer heat from primary coolant to SG feedwater
Tr13	Transfer heat from SGTR flow to SG feedwater
Tr14	Relief heat from SG through MSRV
Tr15	Transport heat from SG to turbine
Tr17	Bypassing heat to condenser
Tr21	Transport feedwater to SG
Tr22	SGTR flow flowing into SG
Tr23	Transport steam from SG to turbine
Tr24	Relief steam from SG through MSRV
Tr25	Bypassing steam to condenser
Si1	Removal of heat from primary loop
Si6	Injection of ECC coolant
Si21	Spray into pressurizer
St1	Primary coolant cold leg
St2	Primary coolant hot leg
St3	Charging and letdown tank
St4	SG to store heat
St5	Condenser
St6	SG to store feedwater
Br1	Steam pipe to transport steam heat
Br2	Turbine to exchange heat to kinetic energy
Br3	Steam pipe to transport steam
Br4	Turbine

Table 3. Definitions of structures

Symbol	Description
S1	NPP system
S2	Primary loop
S3	ECCS
S4	RCP
S5	CVCS
S6	Pressurizer spray
S7	Pressurizer PORV and SV
S8	Pressurizer heater
S9	Secondary loop and turbine system
S10	Secondary loop and turbine system
S11	Feedwater and auxiliary feedwater system

Table 4. Several important functions

Function	Plant parameters corresponding to flow functions
So1	Core power level
Si21	Pressurizer spray valve
Tr10	Primary system PORV (power-operated relief valve)
Si3	SGTR flow rate
So9	SGTR flow rate
So11	SGTR flow rate
Si6	ECCS (emergency core cooling system) flow rate
Si10	RCS pump flow rate
St1	Flow rate of primary cooling
Si105	Feed water flow rate
St4	SG power
Tr25	Steam bypass flow rate
Tr23	MSIV (main steam isolation valve) parameter
St6	Steam flow rate
Tr24	Main steam relief valve flow rate
Br2	Turbine power

3.3 States of Goals and Functions

The definitions for the states of goals and flow functions, and the rules for determining the states of goals and flow functions follow the definitions by Paassen and Wieringa [9]. Three states of goals are defined as follows:

Immediate achievement : This means that at the present time the goal is achieved, because the criteria for goal achievement, for example, a specific flow rate, are met. It does not necessarily mean that the goal will retain the achieved state in the near future.

Future achievement : This means that the goal will be or will remain achieved (as in immediate achievement) within some foreseeable future. The time span considered for this depends on the dynamics of the system. This aspect of achievement is of interest to the agent (whether human or automation) that manages the flow functions in the structure. A lack of future achievement indicates that a management action is due; either a human operator or automation should influence the flow functions in such a way that the goal will remain achieved in the foreseeable future. However, future achievement of goals does not mean that agents as operators are not required to make any operation until goals turn into immediate achievement. Future achievement of goals means that under the condition that agents strictly follow the remaining steps of EOPs, goals can be in the state of future achievement.

Soundness of achievement : When the achievement for a goal is sound, there is proper support for achieving and maintaining that goal. This means the functions needed to achieve the goal do exist and may be used. However, at present time, they are not functioning to

achieve the goal.

Two states for flow functions are defined as follows:

Enabled : A function is ready to be integrated with the other functions, but not necessarily working.

Established : A flow function that is functioning in a desired manner supports the achievement of a goal.

Three rules are defined to determine the states of flow functions.

Rule 1. A flow function is enabled when, aside from the question of whether it has material to deliver or capacity to receive material, it has the full potential to contribute to the achievement of the goals it supports. This rule works based on the functional integrity of the flow functions.

Rule 2. A flow function is established when it is functioning in such a manner that the goals that are being supported will be achieved within a reasonable time span. This rule works rather indirectly on the goals' attributes and states than on the flow functions' attributes themselves. When we consider the state of a flow function, which directly supports a goal with an achieving relationship, we can consider the state of the goal. If the state of the goal is immediate achievement, and only if the immediate achievement state of the goal is the necessary and sufficient condition of the established state of the flow function, we can determine that the state of the flow function is established. This works in exactly the same manner as the future achievement state of the goal. If the flow function's state cannot be determined by this rule, it is necessary to proceed to Rule 3.

Rule 3. A flow function is established when it is enabled and its material quantities and material qualities are within the bounds required for future establishment of the flow functions with an achieving role. This rule works directly on the attributes of the flow functions. Hence, the design specification data of the components corresponding to the flow functions must be utilized to use this rule.

3.4 Result of Simulation

During the experiments in the present study, an NPP operational condition is provided by a FISA-2/PC simulator. The operator was instructed by ImPRO to control the FISA-2/PC simulator under a SGTR accident. The following are the EOPs for the SGTR situation that is used in ImPRO.

Step 1 : Confirm the entry condition for SGTR

Step 2 : Check SFSC and execute radiation procedure

Step 3 : Check pressurizer pressure for SIAS (safety injection actuation signal)

Step 4 : Check RCP (reactor coolant pump) operation limit

Step 5 : Maintain RCS (reactor coolant system) below 287°C and 82 kg/cm²

Step 6 : Identify and isolate ruptured SG (steam generator)

Step 7 : LPSI (low pressure safety injection) pump

operation

During the SGTR accident consequences, plant parameter data generated by FISA-2/PC determine the states of the flow functions and goals in the MFM model. We compare the data obtained from the simulator under a normal situation and those obtained under the SGTR situation. If the two values compared are equivalent within 2% error, based on Rule 3, we determine that the flow function is established. When Rule 2 can be applied, we determine the state of the flow function based on the state of the goal, which is supported by the flow function. As the results of the simulation, the states of the MFM model during the operation of ImPRO on the FISA-2/PC simulator are captured. In Figure 3, Figure 4, and Figure 5, the states of the MFM model are shown for three transient moments after step 3, step 5, and step 7 have been executed in the SGTR procedure of ImPRO. Table 6 and Table 7 summarize how the performance of Step 5 and Step 7 by operators changes the states of the MFM, respectively.

In conventional static MFM models, it is generally expected that the states of goals are determined by the states of flow functions. However, in dynamic MFM models, we believe that some time delay should also be considered, and therefore the change of states of flow functions sometimes do not directly change the states of goals. For example, in Figures 3 through 5, the state of

Go1 changes from *future achievement* to *immediate achievement*, even though the state of *Tr2* remains *established*. This time delay is also due to the limitations of the definitions of the states of flow functions. In this paper, the *enabled* state of a flow function means that the flow function is ready to support the achievement of a goal, and the *established* state of a flow function means that the flow function is supporting the achievement of a goal. This means that the *established* state of *Tr2* merely indicates that Tr2 is working correctly to support the achievement of *Go1*. It does not necessarily mean that the *Go1* is achieved. Therefore, in dynamic MFM models, the change of the states of flow functions does not necessarily equate with the change of the states of goals.

In Figures 3 through 5, some flow functions are uncolored. Because the FISA-2/PC simulator that is used in the experiment is a compact simulator of nuclear power plants while the MFM model used in the experiment is a somewhat detailed model for an SGTR accident in nuclear power plants, some parameters that are necessary to determine the states of the flow functions in the MFM model could not be obtained from the simulator. The states of those flow functions are uncolored. In practice, this is not an obstacle to the efficiency of the model. In each flow structure, the flow functions are functioning on the same physical or energy

Table 6. Change of the states of goals and flow functions by the performance of Step 5

Goal / Flow function	Description	State after Step 3	State after Step 5
Si6	Injection of ECC coolant	Enabled	Established
Si21	Spray into pressurizer	Enabled	Established
Tr10	Transport pressurizer vapor through PORV	Enabled	Established
Si36		Established	Enabled

Table 7. Change of the states of goals and flow functions by the performance of Step 7

| Goal / Flow function	Description	State after Step 5	State after Step 7
Go1	Cooling the reactor	Future achievement	Immediate achievement
Go7	Maintaining primary pressure > secondary pressure	Immediate achievement	Soundness of achievement
Go9	Establishing steam flow	Immediate achievement	Soundness of achievement
Go10	Bypassing steam	Immediate achievement	Soundness of achievement
Si6	Injection of ECC coolant	Established	Enabled
So9	Heat from SGTR flow	Established	Enabled
Tr4	Primary coolant flowing through SGTR	Established	Enabled
Tr14	Relief heat from SG through MSRVa	Enabled	Established
Tr15	Transport heat from SG to turbine	Established	Enabled
Tr17	Bypassing heat to condenser	Established	Enabled
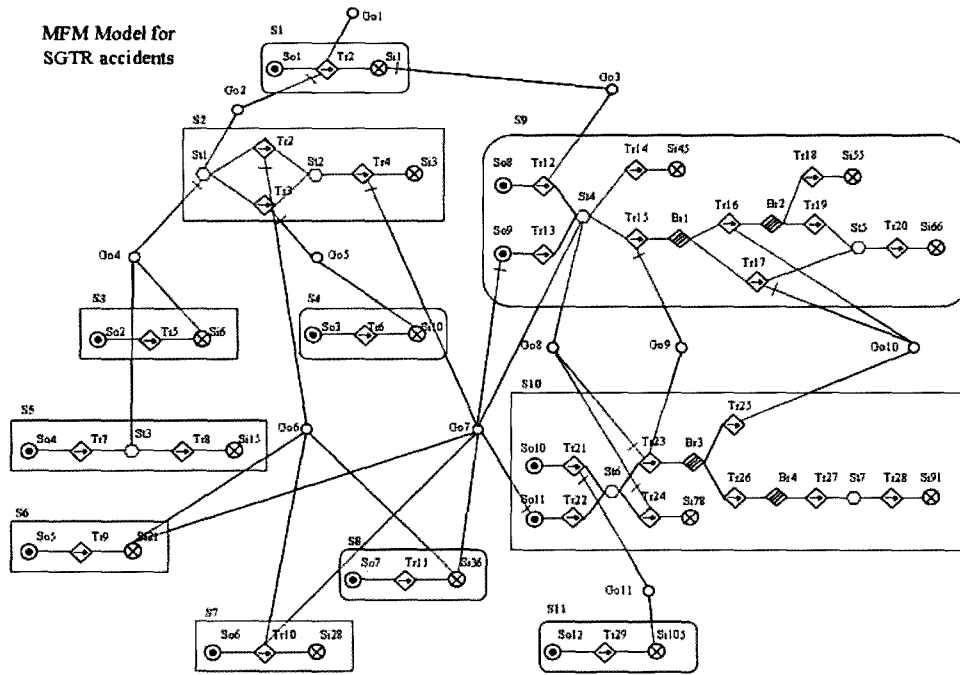
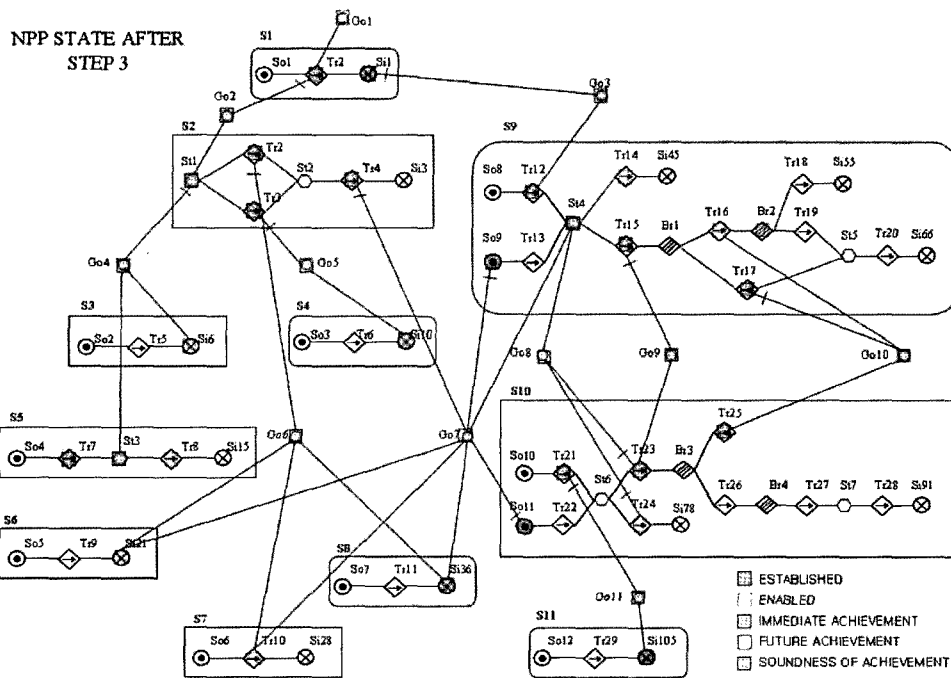Fig. 2. An MFM model for NPPs under an SGTR accident

Fig. 3. States of the MFM model for NPPs under an SGTR accident after step 3 of EOPs
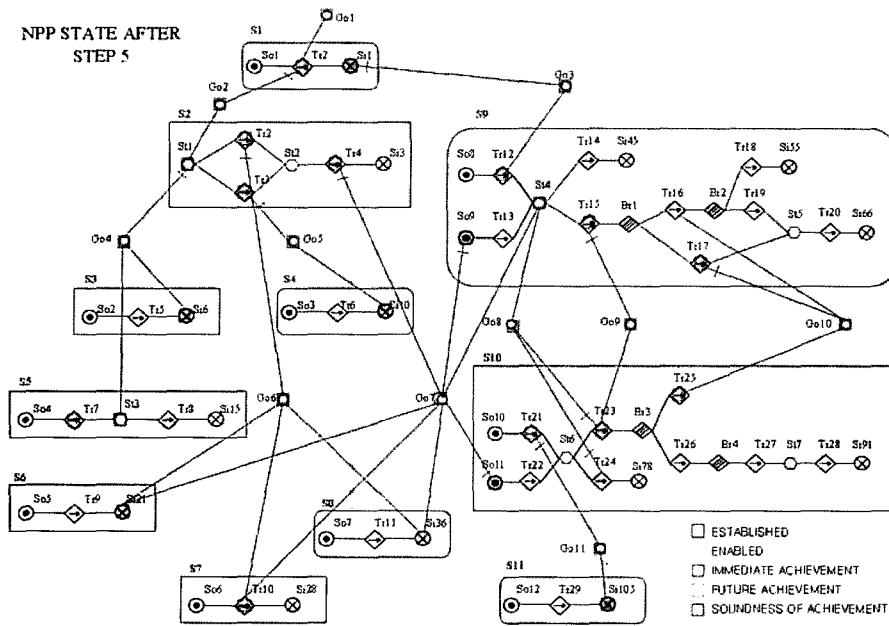
Fig. 4. States of the MFM model for NPPs under an SGTR accident after step 5 of EOPs
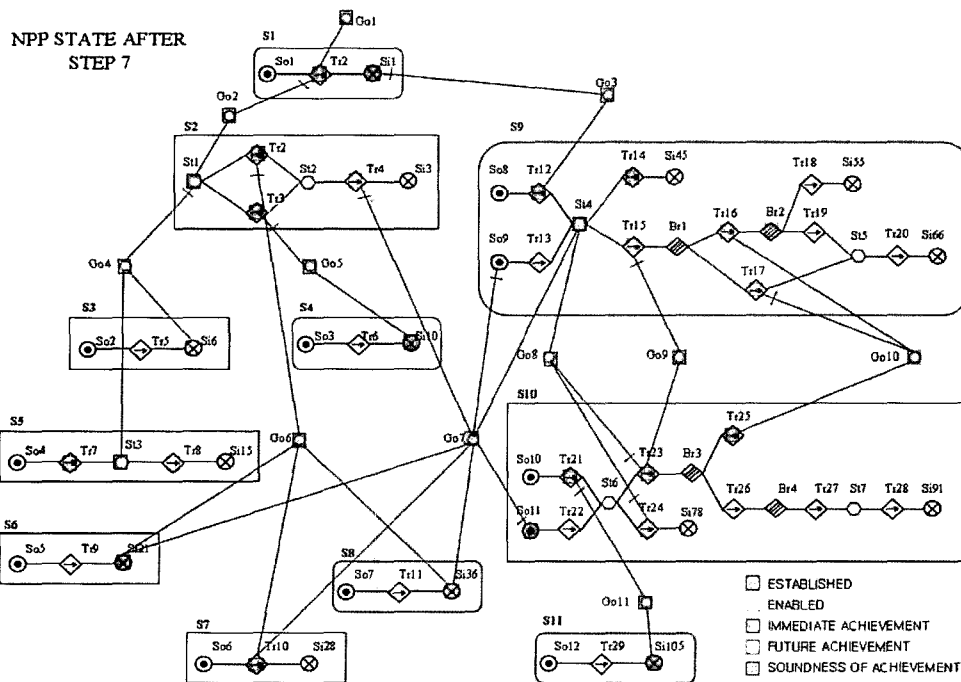

Fig. 5. States of the MFM model for NPPs under an SGTR accident after step 7 of EOPs

flow, and thus flow functions within a flow structure are causally related, and the key flow functions to achieve the goal or subgoal in the model are determined. Therefore, it is concluded that the uncolored flow functions do not have significant impact on the determination of the states of important goals in the MFM model. We believe that if full-scope simulators of nuclear power plants are used for the validation of EOPs, the states of all flow functions and goals can be determined.

As shown in Figure 5, by the completion of the EOPs for an SGTR accident implemented in ImPRO, the top goal in the MFM model for the NPP under the SGTR accident, *cooling of the reactor*, has been achieved. This means that the EOPs successfully guide the NPP operators to the top goal of the MFM model, *cooling of the reactor*, and the MFM model used in the experiment provided sufficient information for the validation of the EOPs. Therefore, we conclude that the EOPs that we used are valid, and MFM models can be used for the validation of EOPs. For further analysis, NPP operational experts can fully utilize the state transition information to analyze the performance of EOPs during the SGTR accident consequences.

By using the proposed validation method, we can analyze the transitions of the states of the goals and flow functions in MFM models in various abnormal situations. The analysis will also be helpful in discovering the impact of a certain series of actions/checks upon the system under a certain operational mode such as a SGTR accident situation. Through application of the dynamic MFM models, we can also illustrate the state transition processes of NPPs in various situations.

3.5 Discussion

While it is concluded that the proposed method is quite useful for the validation of EOPs, there are several points that should be noted. Because NPP is a complex heterogeneous system upon which EOPs are working, there is wide range of requirements about EOPs to follow in different levels and with different foci. However, MFM models a system based on a specific operational mode, and thus it models the system beginning from a top goal, which is the most critical concern under that operation mode. The most direct information provided by dynamic MFM validation approach is the states of the top goal. Although MFM can record the state transitions of every flow function and goal during the accident, in order to validate EOPs related to other aspects of NPP system requirements, there must be further analysis of recoded data to establish validation.

For the proposed validation method to be used in real validation of EOPs, the proposed method should be implemented into the online procedure performance monitoring and diagnosis system in full-scope simulators of NPPs. This system has an interface with the full-scope simulators and hence it can obtain sufficient plant data in

real time. This system has MFM models under different operation modes and can update MFM models with the simulation data automatically. The state of every flow function and goal can be independently monitored and displayed to assist in the validation of EOPs.

4. CONCLUSIONS

In this paper, a validation method for EOPs of NPPs is proposed based on dynamic MFM. The MFM procedure and the EOP validation procedure are provided in the paper. MFM models describe the goals and functions of NPPs, and the application of dynamic MFM provides a method for representing the states of NPPs based on the real-time data from real NPPs or simulators. The flow functions and goals are not only logical concepts but also have physical representation in the real system. From the measurement of the physical representations of goals and flow functions, solid data can be physically obtained. This is usually done through the NPP I&C system.

As an application, the proposed method is applied to the EOPs of an actual nuclear power plant. The experimental facility consists of EOPs of a Westinghouse 600MWe-type NPP, a simulator for that type of NPP, and the MFM model for an SGTR accident. The state transitions of the simulator during the SGTR accident are recorded to validate the EOPs for the management of SGTR accidents. The results indicate that it is possible to make some assessment of the impact of a certain series of actions/checks upon the system under a certain operational duration.

It is expected that the procedure validation based on dynamic MFM can be implemented as a product of the online procedure performance monitoring and diagnosis system in real NPPs. These approaches will make the activities for the validation of EOPs more instructive and productive.

Acknowledgement

REFERENCES

[1] J. M. O'Hara, J. C. Higgins, W. F. Stubler, J. Kramer, Computer-based Procedure Systems: Technical Basis and Human factors review guidance, NUREG/CR-6634, U.S. Nuclear Regulatory Commission, Washington D.C., 2002

[2] M. Lind, Modeling goals and functions of complex industrial plant, Applied Artificial Intelligence, Vol.8, No.2, pp.259-283, 1994

[3] M. Fang, MFM Model Based Diagnosis and Implementation, Department of Automation, 94-D-712, Technical University of Denmark, 1994

[4] J. E. Larsson, Diagnostic reasoning based on means-end

models: experiences and future prospects, Knowledge-Based Systems, vol.15, pp.103-110, 2002

[5] J. Petersen, Causal reasoning based on MFM, Proceedings of Cognitive Systems Engineering in Process Control 2000 (CSEPC2000), pp.36-43, Taejon, Korea, 2000

[6] M. Lind, Plant modeling for human supervisory control, Transactions of the institute of measurement and control, vol.21, No.4/5, pp.171-180, 1999

[7] A. Gofuku, T. Ohi, K. Ito, Development of a dynamic operation permission system, Proceedings 2003 CUP workshop on advanced I&C systems for NPP operation and maintenance, pp.71-78, Aomori, Japan, 2003

[8] A. Gofuku, Y. Ozaki, K. Ito, A dynamic operation permissi-on system for pressurized water reactor plants, Proceedings of 2002 international symposium on the future I&C for NPP (ISOFIC2002), pp.360-365, Seoul, Korea, 2003

[9] M.M. van Paassen, P. A. Wieringa, Reasoning with multilevel flow models, Reliability engineering and system safety, vol.64, pp.151-165, 1999

[10] H. Seok, H. C. NO, S. J. CHO et al., Development of software for the microsimulator for the Kori nuclear power plant unit 2 - user manual, Korea Electric Power Co.,

KRC-90N-J07, 1992

[11] H. Seok, H. C. NO, S. J. CHO et al., Development of software for the microsimulator for the Kori nuclear power plant unit 2, Nuclear technology, vol.106, no.3, pp.384-396, 1994

[12] Y. R. Sim, M. G. Na, H. C. No, Development of a small-scale simulator for designing advanced control algorithms at nuclear power plants, Proceeding of KNS autumn meeting, Yongpyeong, Korea, 2002

[13] J. H. Kim, S. J. Lee, P. H. Seong, Investigation on applicability of information theory to prediction of operator performance in diagnosis tasks at nuclear power plants, IEEE transactions on nuclear science, vol.50, no.4, pp,1238-1252, 2003

[14] Seung Jun Lee and Poong Hyun Seong, "Development of an Automated Operating Procedure System using Fuzzy Colored Petri Nets for Nuclear Power Plants," Annals of Nuclear Energy, 2003, Vol. 31, No. 8, pp. 243~250.

[15] Y. Jung, P. H. Seong, M. C. Kim, A model for computerized procedures based on a flowchart and success logic tree, Reliability engineering and system safety, vol.83, no.3, pp.351-362, 2004