18th International Conference on Structural Mechanics in Reactor Technology (SMiRT 18)
Beijing, China, August 7-12, 2005
SMiRT18-O02-8

SYSTEM VALIDATION OF COMPUTERIZED PROCEDURE SYSTEM BASED ON MULTI-LEVEL FLOW MODELING

Wei Qin*， Liangju Zhang
Institute of Nuclear and New Energy Technology, Tsinghua University
Phone: 010-62784832
E-mail: philipqinwei98@mails.tsinghua.edu.cn

ABSTRACT
Computerized Procedure System (CPS) has been developed in Nuclear Power Plant (NPP) Instrumentation and Control (I&C) system. As part of CPS, emergency operating procedures (EOPs) take such an important role in the management of various abnormal situations in nuclear power plants, current technology for the validation of EOPs still largely depends on manual review. In this sense, a validation method for EOPs of NPPs is 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. The application of the proposed method to EOPs of an actual NPP shows that the proposed method provides an efficient way for 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 such as optimization of EOPs.

Keywords: multilevel flow modeling, emergency operating procedure, simulator, validation, nuclear power plant

1. INTRODUCTION

Procedures in a nuclear power plant (NPP) provide instructions to guide operators in monitoring, decision making, and controlling the plant (O'Hara, 2002). 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 that determine the safety of the plant. But, 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 (Lind, 1994) 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 (Fang, 1994), (Larsson, 2002), (Petersen, 2000), design of displays for supervisory control of industrial plant (M. Lind, 1999), 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 (Paassen, 1999) 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, what actions are required to achieve the goals of a system can be determined. This property of 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 dynamics 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 nowadays contain complex automated operations. MFM is proposed to describe qualitative characters of the operation of automated systems such as NPPs. 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. 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 (Lind, 1994), symbols were defined for representing goals, basic flow functions, and relations, which are *source*, *sink, storage*, *balance*, *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. The flow functions are arranged in coherent units, called flow structures, these flow functions form the means for achieving the system's goals. Classified by mass and energy flow functions, the structure can be categorized into mass flow structures and energy flow structures. Figure 1 shows the symbols that are used in the proposed method.

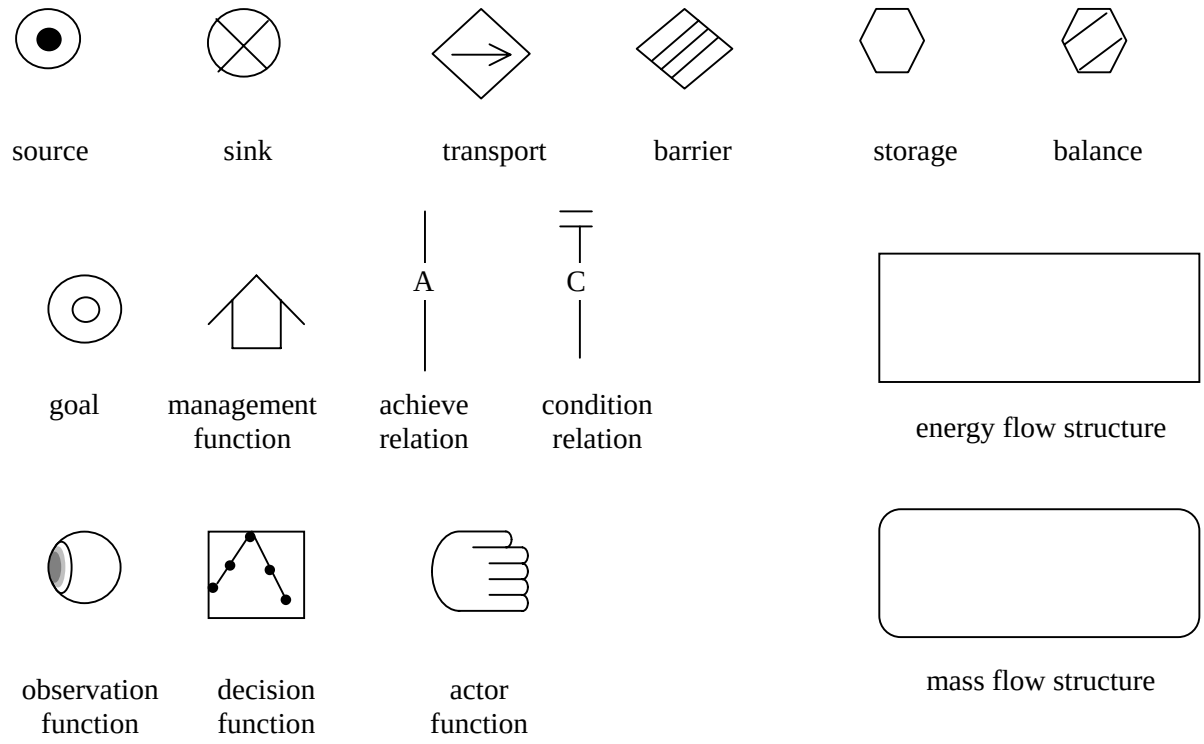

Figure 1 Symbols used in this paper

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, there could be various operational modes under different operational circumstances with different top goals. 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 are working 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 representation in real systems. The states of the flow functions and goals should be able to be defined from the real-time data of a real system or simulator. In fact, MFM models are a kind of logical and physical decomposition of a system, and therefore the system is decomposed by the means-end logic. The models are describing interrelationship 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 is simulating the abnormal situation, and operators will handle the abnormal situation guided by EOPs, at the same time 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 simulated 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 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 towards 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 Westinghouse 600MWe-type PWR NPP, is used for the simulation of the SGTR accident. The EOPs implemented in a computerized procedure system ImPRO (Jung, 2004) are used as the target EOPs subject to validation. The MFM model for the management of an SGTR accident developed by Gofuku et al. (Gofuku, Ohi, 2003), (Gofuku, Ozaki, 2003) 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, and 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.

3.2 States of Goals and Functions

The definitions for the states of goals and flow functions, and the rule for determining the states of goals and flow functions follow the definitions by Paassen and Wieringa (Paassen, 1999). 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 goal is going to retain achieved 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 automaton) 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 automaton should influence the flow functions in such a way that the goal will remain achieved in the foreseeable future. But, future achievement of goals does not mean that agents as operators are not required to make any operation until goals turn into immediate achievement. 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 a proper support for achieving and

maintaining that goal. That means the functions needed to achieve the goal do exist and may be used. But at present time, they are not functioning to achieve the goal.
Two states for flow functions are defined as follows

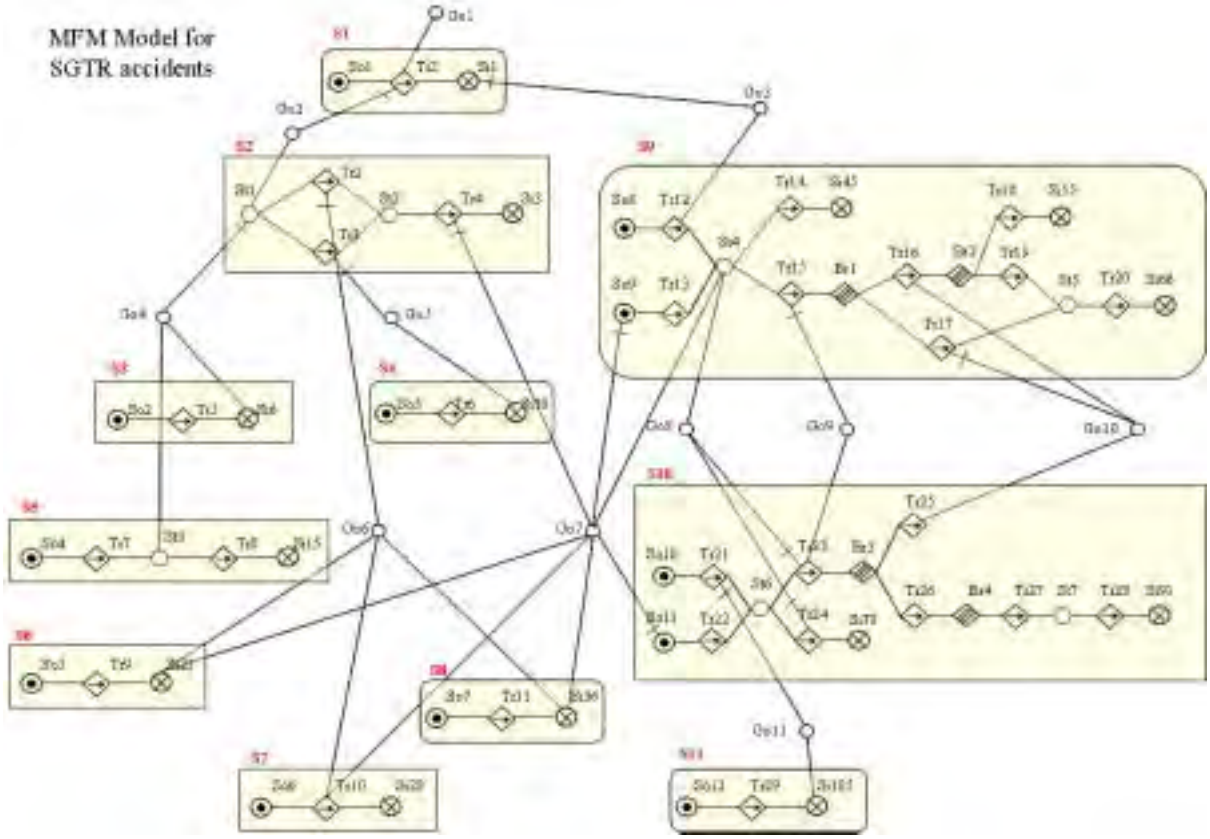

Figure 2 An MFM model for NPPs under an SGTR accident [7,8]

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 1 Definitions of goals

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 2 Definitions of flow functions

Structure	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 3 Definitions of structures

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

Table 4 Several important functions

Goal	Plant parameters corresponding to goals
Go4	Primary pressure
Go7	Secondary pressure
Go6	Subcooling
Go8	SG pressure

Table 5 Several important goals

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 achieving relationship, we can consider the state of the goal. If the state of the goal is immediate achievement, and only if 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 exactly the same way for the future achievement state of the goal. If the flow function's state cannot be determined by this rule, we have to go 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. So the design specification data of the components corresponding to the flow functions must be utilized to use this rule.
Transactions of states of the flow functions in the MFM model are based on plant parameters obtained from the simulator FISA-2/PC. The data obtained from the simulator under normal situation and those obtained under SGTR situation are compared. If the two values compared are equivalent within 2% error, based on Rule 3, It is determined that the flow function is established; or, based on Rule 2, state of the flow function is determined based on state of the goal which is achieved by the flow structure consisted of this flow function.

3.3 Result of Simulation

During the experiments of the authors, an NPP operational condition is provided by a simulator. The operator was instructed by ImPRO to control the simulator under the accident of SGTR. During the accident SGTR consequence, plant parameter data generated by simulator will determine the states of the flow functions and goals in the MFM model. As the results of the simulation, the states of the MFM model during the operation of ImPRO on the simulator are captured. In Figure 3, Figure 4 and Figure 5, the states of the MFM model is shown for three transient moments after step 3, step 5 and step 7 have been executed in the SGTR procedure of ImPRO. In Figure 3, Figure 4, and Figure 5, it can be found that some flow functions are uncolored. Because the simulator that is used in the experiment is a compact simulator of nuclear power plants while the MFM model used in the experiment is 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 remain as uncolored. Actually, that cannot be an obstacle to the efficiency of the model, in each flow structure, the flow functions are functioning on the same physical or energy flow, so 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, so from the analysis on the impact of the uncolored flow functions, 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 think 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. It 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 states transitions information to analyze the performance of EOPs during the SGTR accident consequence.
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 be also helpful discovering the impact of a certain series of actions/checks upon the system under a certain operational mode like the SGTR accident situation. By the application of the dynamic MFM models, we can also illustrate the state transition processes of NPPs in various situations.

4. CONCLUSIONS

In this paper, a validation method for EOPs of NPPs is proposed based on dynamic MFM. The MFM modeling procedure and the EOP validation procedure is provided in the paper. MFM models describes 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 the real NPPs or simulators. The flow functions and goals are not only logical concepts but they 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, and this is usually done through NPP I&C system.

REFERENCES

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

Washington D.C.,
[2] M. Lind, (1994), Modeling goals and functions of complex industrial plant, Applied Artificial Intelligence, Vol.8, No.2, pp.259-283
[3] M. Fang, (1994), MFM Model Based Diagnosis and Implementation, Department of Automation, 94-D-712, Technical University of Denmark
[4] J. E. Larsson, (2002), Diagnostic reasoning based on means-end models: experiences and future prospects, Knowledge-Based Systems, vol.15, pp.103-110
[5] J. Petersen, (2000), Causal reasoning based on MFM, Proceedings of Cognitive Systems Engineering in Process Control 2000 (CSEPC2000), pp.36-43, Taejon, Korea
[6] M. Lind, (1999), Plant modeling for human supervisory control, Transactions of the institute of measurement and control, vol.21, No.4/5, pp.171-180
[7] A. Gofuku, T. Ohi, K. Ito, (2003), 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
[8] Gofuku, Y. Ozaki, K. Ito, (2003), A dynamic operation permission system for pressurized water reactor plants, Proceedings of 2002 international symposium on the future I&C for NPP (ISOFIC2002), pp.360-365, Seoul, Korea
[9] M.M. van Paassen, P. A. Wieringa, (1999), Reasoning with multilevel flow models, Reliability engineering and system safety, vol.64, pp.151-165
[10] Y. Jung, P. H. Seong, M. C. Kim, (2004), 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

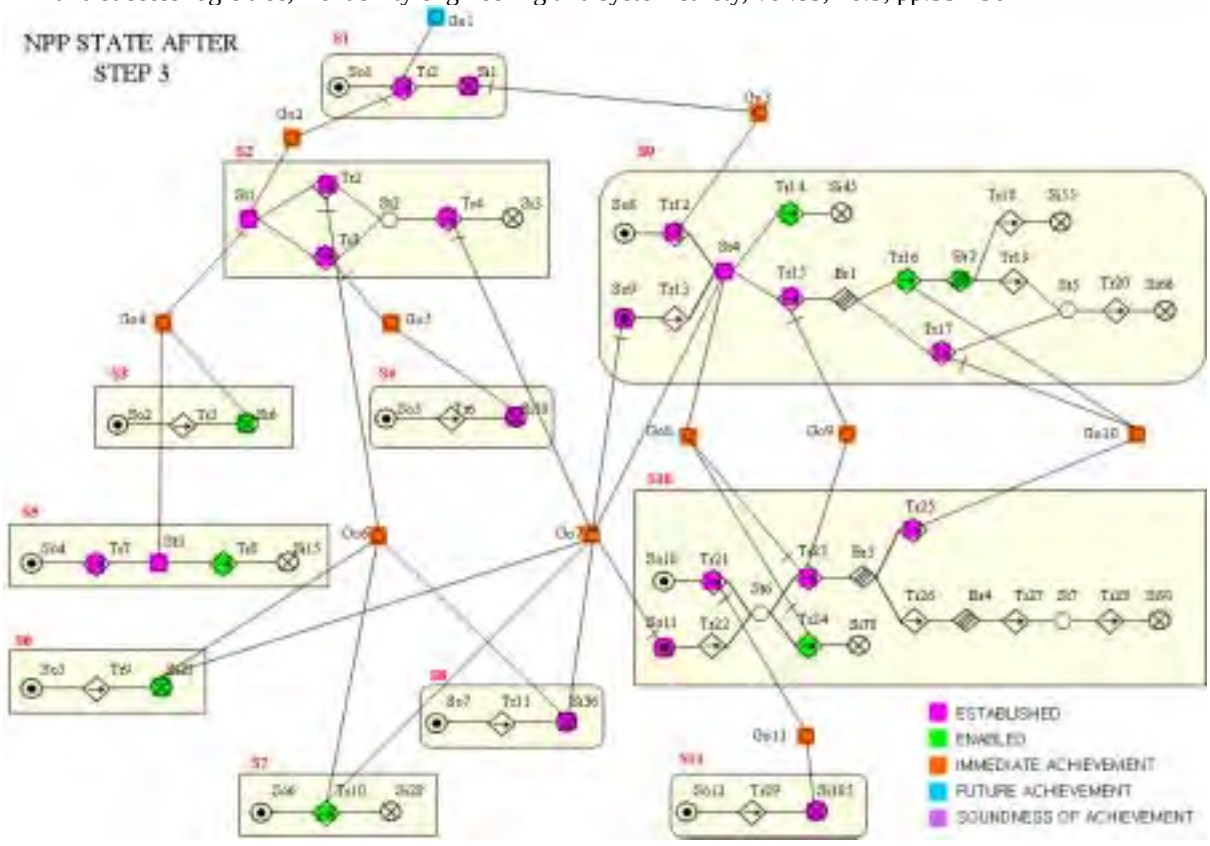

Figure 3 States of the MFM model for NPPs under an SGTR accident after step 3 of EOPs

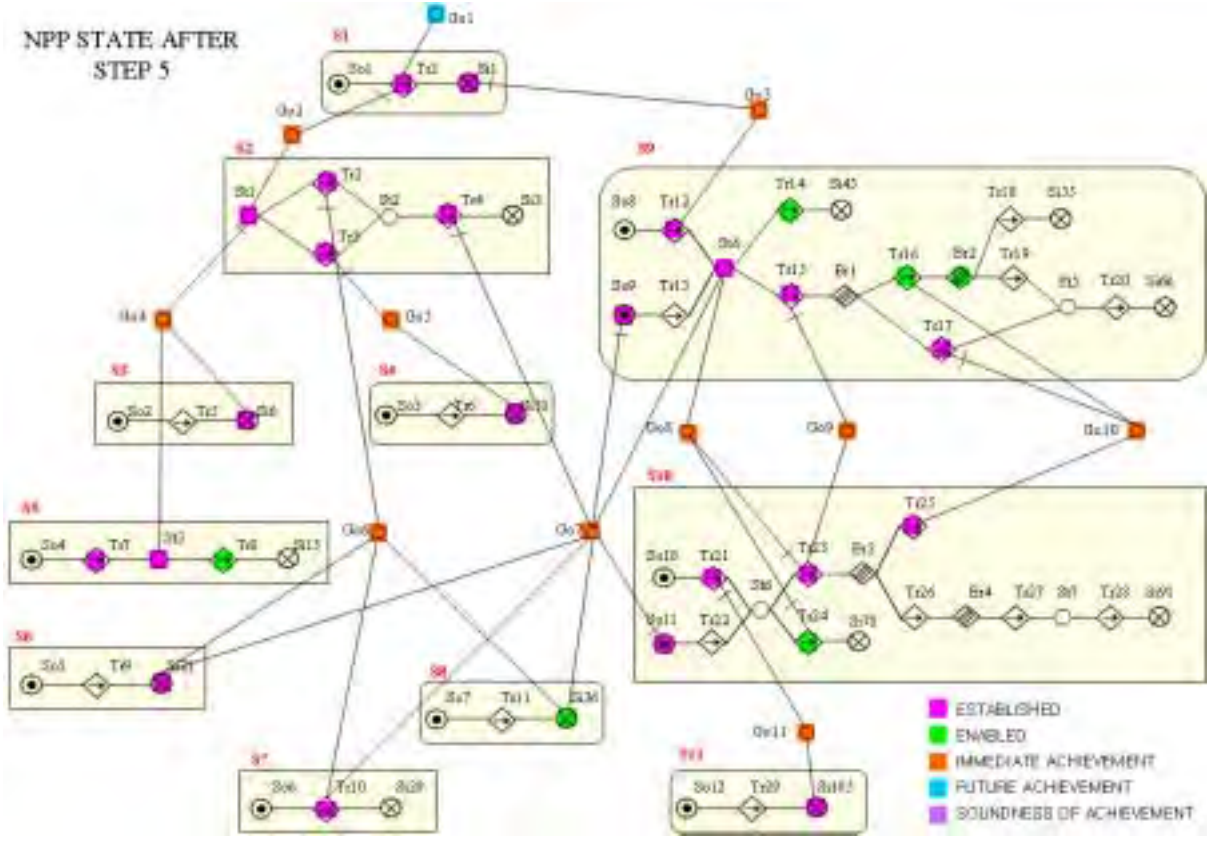

Figure 4 States of the MFM model for NPPs under an SGTR accident after step 5 of EOPs

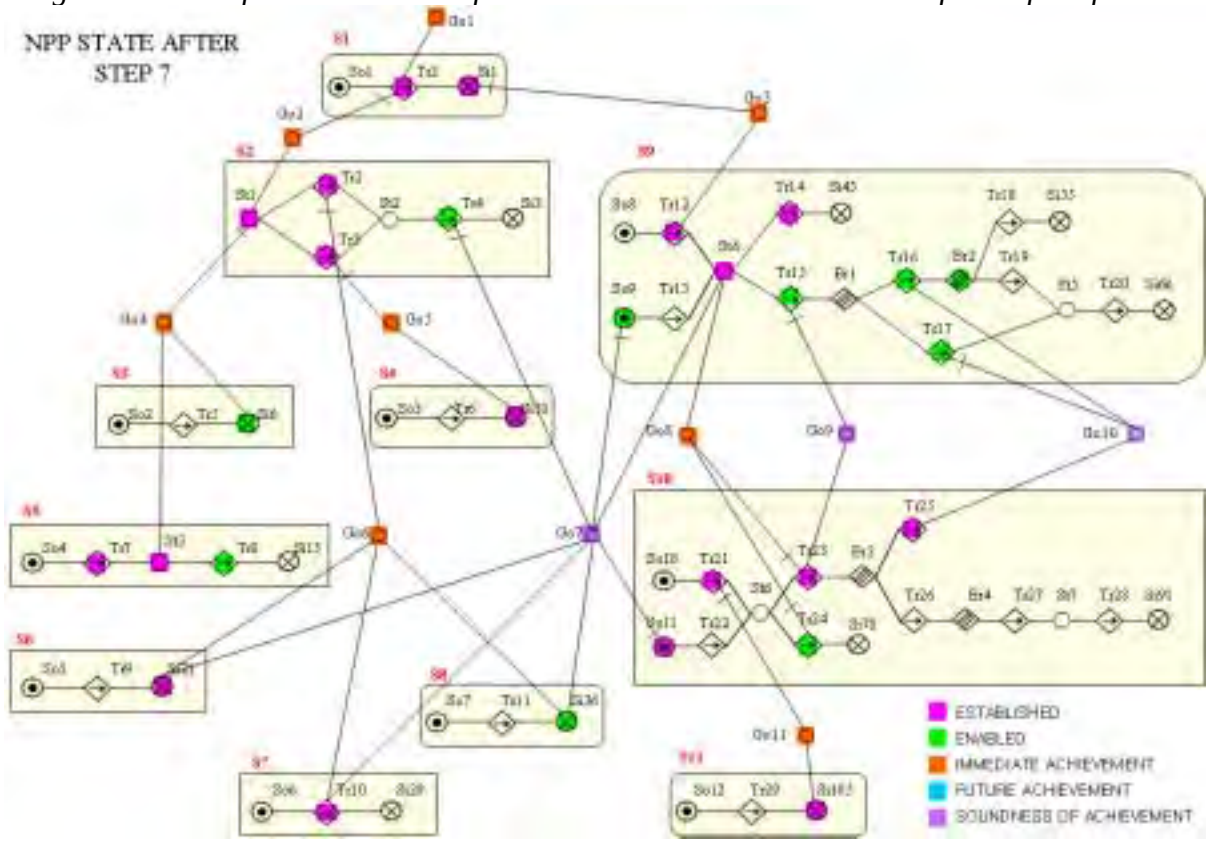

Figure 5 States of the MFM model for NPPs under an SGTR accident after step 7 of EOPs