Knowledge-based software design for Defense-in-Depth risk monitor system with the preliminary study for AP1000 application

MA Zhanguo[1], and YANG Ming[1]

1. *College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (mazhanguo2013@163.com, myang.heu@gmail.com)*

Abstract: A new risk monitor system was proposed not only to prevent severe accident in daily operation but also serve to mitigate the radiological hazard after severe accident consequences. The configuration of the proposed risk monitor system is the plant Defense-in-Depth (DiD) risk monitor system and the reliability monitors for the subsystems of the nuclear power plant. The software for the plant DiD risk monitor system was designed based on the object oriented module and then the knowledge-based software was developed utilizing the Unified Modeling Language (UML). Currently there are mainly two functions in the developed plant DiD risk monitor software that are knowledge-based editor which is used to model the system in a hierarchical manner and the interaction simulator that simulates the interactions between the different actors in the model. In this paper, a model for playing its behavior is called an Actor which is modeled at the top level. The passive safety AP1000 power plant was studied and the Small Break LOCA (SBLOCA) design basis accident transient is modeled using the plant DiD risk monitor software. Each plant DiD risk model for the sub system is modeled based on the simulated transient sequences. Furthermore, the simulation result is shown for the interaction between the actors which are defined in the plant risk monitor system as PLANT actor, OPERATOR actor and SUPERVISOR actor. This paper shows that it is feasible to model the nuclear power plant knowledge base using the software modeling technique. The software can make the large knowledge base for the nuclear power plant with small effort.

Keyword: risk monitor; plant Defense-in-Depth risk monitor; knowledge base small break LOCA

1 Introduction

A new risk monitor system[1] that was proposed by the authors is under development. In the proposed risk monitor system, it is designed not only to prevent severe accident in daily operation but also serve to mitigate the radiological hazard after severe accident consequences[2]. The conspicuous features of the proposed risk monitor system comparing with the existing risk monitors[3] and living PSA[4] basically lie on the following two points: (i) The range of risk is not limited to core melt accidents but includes all kinds of negative outcome events, *i.e.*, not only precursor troubles and incidents but also any types of hazard states resulting from severe accident, and (ii) The whole system of the proposed risk monitor system that was shown in Fig. 1 consists of plant Defense-in-Depth (DiD) risk monitor system and reliability monitor. The plant DiD risk monitor system predicts and valuates plausible risk state from the perspective of the whole plant, and several reliability monitors evaluates the reliability of individual subsystems to fulfill their designed function successfully under the prescribed conditions which are given by the plant DiD risk monitor system. The relationship between the both monitors was discussed [5].

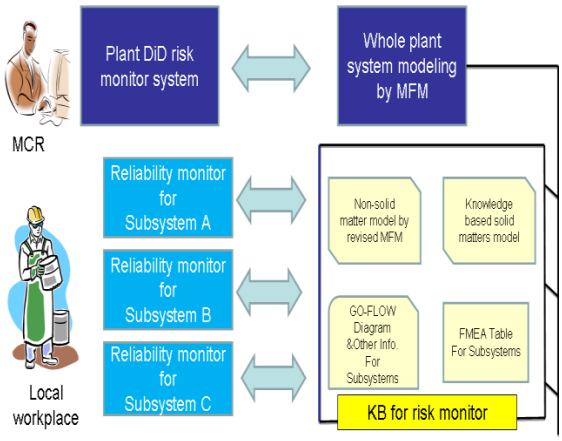

Fig. 1. The proposed risk monitor system.

Received date: June 27, 2016
(Revised date: July 11, 2016)

In Fig. 1, various Knowledge Bases (KBs) which will be used both for plant DiD risk monitor system and reliability monitors are listed up in the block which is indicated as "KB for risk monitor". The plant DiD risk monitor system will identify every potential risk state caused by any conceivable event in the plant system as a whole while events arising from common cause factors and human factors should be taken into account. Reliability evaluation for a sub-system is made by the reliability monitor by using a combination of FMEA and GO-FLOW[6]. Reliability is normally defined as the successful rate of a system's performance that will fulfill its expected function when it is requested. In the safety design of nuclear power plant (NPP), reliability of safety functions is enhanced by principles of diversity, redundancy and physical separation. The reliability monitor had been extensively studied for the safety system of conventional Pressurized Water Reactor (PWR) [7] and advanced PWR AP1000[8].

In the new risk monitor system, the risk level[2] is decided by following factors: (i) status of individual subsystems and equipment for maintaining the safety function of STOP, COOL and CONTAIN, (ii) Degree of redundancy, diversity, physical separation, (iii) Kind of initiating events, common cause factors of internal and external events, and (iv) Kind of reactor state which includes full power operation with/without online maintenance, various stage of shutdown maintenance. The example of deciding the risk level is given in Table 1.

In the new risk monitor system, the dynamic risk monitor to display the risk level changing with time for the operator in main control room is shown in Fig. 2. It can be seen that time varying risk state is displayed as a moving point (trajectory of yellow point) on TL-plane, where T is time margin until reactor becomes dangerous state and L is safety margin of various plant parameters which represent the status of three safety functions of STOP, COOL and CONTAIN. The visualization of different risk level of risk ranking is constituted by multiple sheets as defined in Table 1. The origin O of LT-plane means danger point (L_0, T_0) within a risk ranking level 0, where T_0 and L_0 mean no time margin and no safety margin to go from a risk ranking level 0 to level1. The yellow point of this dynamic risk monitor display will change in accordance with the change of DiD, that is, degree of intactness of multiple barriers as well as the three safety functions. The risk level 0 is the situation when all safety functions are intact. But even if the risk level is 0, the reliability of the plant in operation will change from time to time depending on how the redundancy, diversity and physical separation of the individual equipment and components are maintained and on the margin of plant parameters to the safety limit. In case of risk level larger than 0 where either or all safety functions will be lost, the degree of risk should be decided by evaluating by what degree the plant would be damaged based on accident phenomena and their consequences.

Table 1. Risk level in the risk monitor system

Risk level	Stop	Cool	Contain	Possibility of severe accident
0	1	1	1	No risk safety shutdown, cooled and no release
1	1	1	0	No severe accident phenomena, but some problem in containment
2	1	0	1	Loss of not so serious cooling function, safety shutdown, but cooling failed but no release
3	1	0	0	Serious severe accident possible safety shutdown, but both cooling and contain function failed
3	0	1	1	Severe accident may be suppressed by engineering safety feature function, shutdown failed but cooling and no release
3	0	1	0	Some contain function failed shutdown failed, cooled but released
4	0	0	1	Serious though severe accident phenomena occur because containment function succeeded shutdown failed, cooling failed but no release
5	0	0	0	Worst severe accident because all safety functions failed

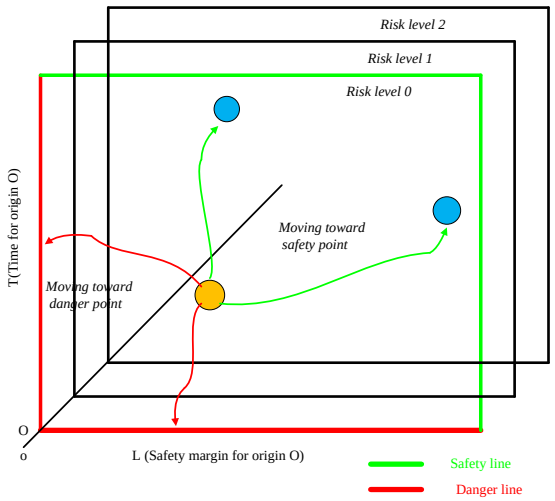

Fig. 2. Visualization of dynamic changing risk.

As one of the two layers of the proposed risk monitor system, the reliability monitor system is studied using the GO-FLOW and FMEA. But the plant DiD risk monitor system which is the user interface for the operators as the other layer should be designed and developed. In the authors' proposal, the plant DiD risk monitor system can build up the knowledge base for the NPPs including the successful scenarios and the failure scenarios for each subsystems. The plant DiD risk monitor system can monitor the functions of the subsystems in the NPPs and inform operators the plant state. In case of accident, the plant DiD risk monitor system can help the operator to make the correct action to mitigate the impact of the accident. So that the plant DiD risk monitor system can help the operator to monitor the plant systems and relieve the operators' work load.

This paper focuses on the software design and development for the plant DiD risk monitor system and the application demonstration for the AP1000 plant SBLOCA transient. As a part of the new risk monitor system, the software can model the plant systems in the state manner. The remaining of this paper is organized as following: Section 2 presents the software design for the DiD risk monitor system. Section 3 presents the developed software for the plant DiD risk monitor system. Section 4 presents the application in passive safety AP1000 of the plant DiD risk monitor system in the SBLOCA scenario to demonstrate the main function of the software. The conclusions and future work are given in Section 5.

2 Software design for the plant DiD risk monitor system

Based on the study[1]-[5] to the proposed risk monitor system, the following requirements from (A) to (D) are summarized and they are utilized as the basis of integrated functional modeling method to design the plant DiD risk monitor system.

(A) State transition diagram

This is to be realized as object-oriented modules for the abstracted state transition of machine and plant system by the principle of machine, where the following conditions should be equipped:

(i) Relation between original state, external input or disturbance and outcome state should be semantically described.
(ii) The state transition will be caused by either autonomous machine behavior or human-machine interaction. Then trigger condition of state transition should be described.
(iii) Each state should assign both the risk level and the degree of risk defined in Table 1. The risk level distinguishes the risk state in accordance with whether or not three safety functions of STOP, COOL and CONTAIN are maintained, while the degree of risk gives quantitative risk state by appropriate computational method.

(B) Basic task element diagram

This is also to be realized as object-oriented modules for individual basic task elements seen in the related procedure or guidelines, where the following conditions should be equipped:

(i) Name; explain its meaning
(ii) Action; what to see and by what way to judge
(iii) Means; what to do for which by what way
(iv) Right outcome; what's target result by what criterion to judge as right and what to do next
(v) Unwanted outcome; what will be the said states and what to do next.

(C) Composite task element diagram

The tasks performed either by machine or human are normally the combination of many elementary tasks, and those elementary tasks are described by basic task element diagram. If the composite task element is represented by the same form of the elementary task element, this composite task element can be also utilized as a basic task element. To sum up, the composite task element will be generated by the combination of individual basic task elements, where the following conditions should consider:

(i) Name; explain its meaning of the composite task
(ii) Method of how to synthesize the composite task from the selected basic task elements.

Additional parameters are needed by the synthesis of selected elemental tasks which originally have the following parameters:

(i) Action: what to see and by what way to judge
(ii) Means: what to do for which by what way

(iii) Right outcome; what's target result by what criterion to judge as right and what to do next
(iv) Unwanted outcome; what will be the said states and what to do next.

(D) User interface of plant DiD risk monitor software

There are at least two different subjects for developing the user interface of plant DiD risk monitor system. They are:

(i) User interface 1 for knowledge base management to register, update and delete various kinds of diagrams as mentioned in (A), (B) and (C), and
(ii) User interface 2 for analyzing various aspect of risk problem on the target plant system in a certain analysis scenario

Following the requirements, the basic idea of knowledge-based software for the plant DiD risk monitor system can be summarized as:

(i) essential information of human-machine interaction to manage the plant condition in any given accident scenario can be represented by the software modeling of versatile state transitions,
(ii) mutual interaction between the different states can be generated by simulating the behavior of different actors of plant, operator and supervisor,
(iii) whether or not the outcome of any interaction would be desirable, and
(iv) what would be the causes to bring undesirable outcome should be analyzed by the interactive simulation of different actors by using the software of the plant DiD risk monitor system.

The DiD risk monitor system designed to realize the above ideas consists of three subsystems:

(i) Knowledge-base editor,

All knowledge bases (State transition charts, Basic task elements, and Composite task elements) will be represented by State Chart Diagrams that is created using the knowledge-base editor.

(ii) Interaction simulator, and

Plant actor defined by State Chart Diagram will conduct on accident simulation, and both the operator and shift supervisor also defined by State Chart Diagram will conduct on plant monitoring and control. It is possible to conduct various different simulations by setting different input condition to both actors of plant and human operators.

(iii) Interaction analyzer.

By using the simulation results of interaction between human and machine, it becomes possible to find problems in the procedure and to propose effective countermeasures to improve the human factors issues. The interaction analyzer is a sort of application software system for specific purpose by utilizing the interaction simulator result with appropriate knowledge-bases constructed by the knowledge-base editor. In section 4, both the knowledge-base editor and interaction simulator are explained with the SBLOCA scenario in AP1000 plant which was given in the research paper [9].

3 The plant DiD risk monitor system software development

3.1 Knowledge-base editor

The plant DiD risk monitor system has three categories of the knowledge-base: state transition diagram, basic task element, and composite task element, in order to simulate specific human-machine interaction. In the area of software engineering, any knowledge-base information can be modeled by "State Chart Diagram" as defined in Unified Modeling Language (UML) Ver. 2.0[10].

The Knowledge-based editor was developed as a plug-in of Integrated Development Environment "Eclipse"[11] with the use of Graphical Editing Framework "GEF"[12]. Those software modules and the libraries only depend on Java, an object oriented programming language which does not depend on any platforms, and therefore software system of DiD risk monitor to be developed on those software environment can be installed on any Windows-PC or Macintosh-PC.

The knowledge-based editor mainly has three functions:

(i) Describe basic task element diagram,
(ii) Describe composite task element diagram, and
(iii) Describe system status change condition.

The system is designed in the hierarchical structure. The basic task element diagram is used when the user is editing one of the basic task elements of

human-machine interaction by the form of "State Chart Diagram". The composite task element diagram acts as the upper level of the basic task element diagram. The composite task element diagram can also be used as the element in its upper level models. The AND and OR logics can model the machine status working logical condition.

Figure 3 is the snapshot of the knowledge-base editor, in which a canvas in the center of the screen shows "State Chart Diagram" during its editing. The users can drag and drop a state, a label and so on, by selecting it from the right side area named "Components" and dragging into the canvas. A “transition line” between the states can be drawn by Connection tool in the upper-right area named “Palette”. The role of transition line is to connect a source state to the target state by an arrow line. It also holds several event handlers to make this state transition. When a certain event is generated, then the handler for this event makes the state transition to execute the script which is defined as the action of this event handler. The users can write command sequences in Java style program as the action.

Concretely, the users can define the following 4 types of events and its handlers:

(i) Actor External Event: The generated event can be handled by the other actors. For example, the plant actor generates an alarm by itself as an "Actor External Event". Other actors like an operator and a supervisor handle this event as reaction to the occurred alarm. The operator actor generates an "Actor External Event" which means operator's action in the plant actor. The plant actor reacts with the operation action by handling this event. Therefore, the interaction among actors is simulated by sending and handling the "Actor External Events". Event generator, generated place and the meaning of the event used in example simulation are summarized in Table 2.

(ii) Actor Internal Event: An actor can generate the event to handle by himself/herself.

(iii) Primary Event: The state becomes active or inactive, and the events (OnEntry/OnExit) are generated by the system automatically. The users can define the action scripts to be executed in that timing. These events are named "Primary Events".

(iv) Timer Event: The event is generated after its pre-defined duration time.

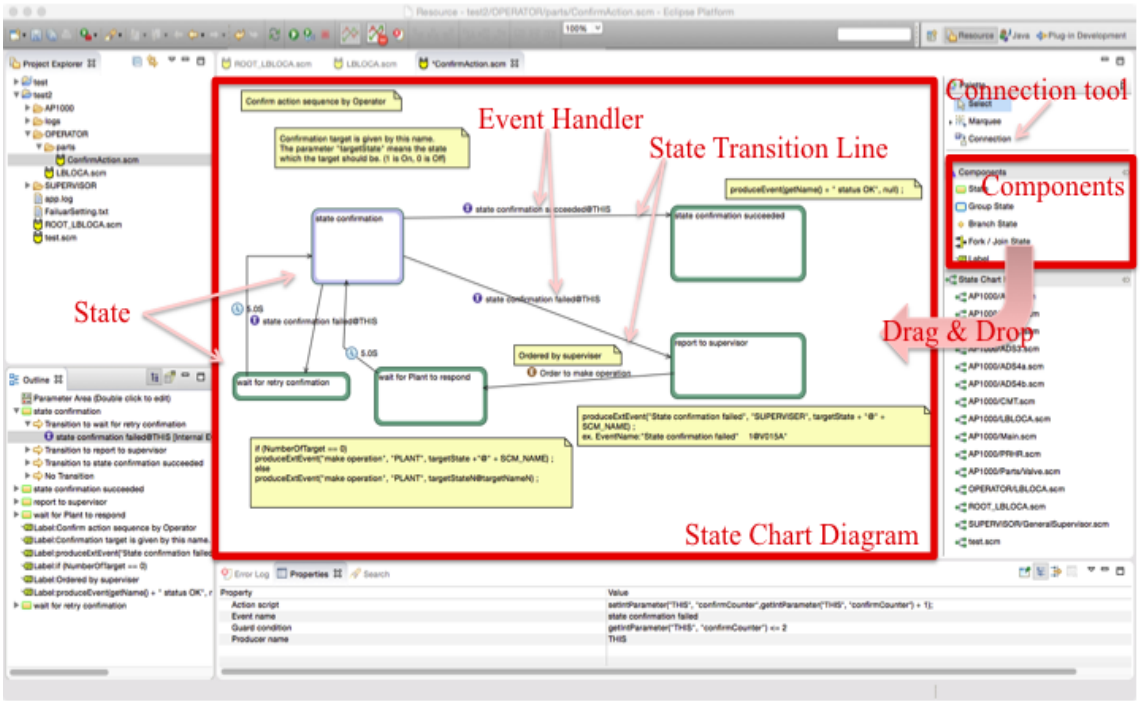

Fig. 3. The knowledge-base editor.

3.2 The hierarchical design of the software

The software is designed that the system can be modeled in hierarchical manner. There is no required limitation for the hierarchical levels. That is to say the models can be designed in any hierarchical level according to the actual system. The top level is the actor level and the following level is the main function or sub systems in corresponding actor. Then the last level is the detailed devices for each system.

In the AP1000 example system models in section 4, there are three actors in the top level model that are OPERATOR actor, PLANT actor, and SUPERVISOR actor. For OPERATOR actor and SUPERVISOR actor, there are two levels shown as Fig. 4. The second level of the OPERATOR actor is the operator's confirmation information for each system, the operation to the system and the report to the supervisor about the system status. The second level of the SUPERVISOR is the orders to the operator from the supervisor.

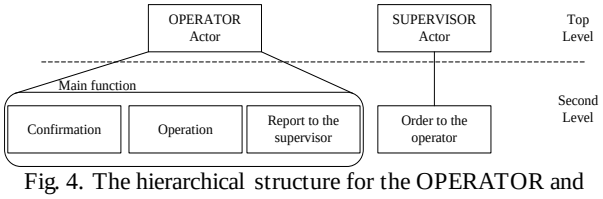

Fig. 4. The hierarchical structure for the OPERATOR and SUPERVISOR actors.

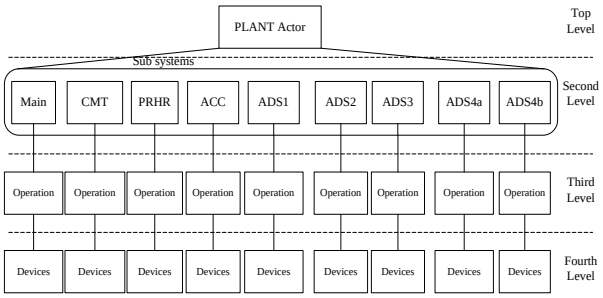

Fig. 5. The hierarchical structure for the PLANT actor.

For the PLANT actor, there are four levels shown as Fig. 5. In the second level, it models the sub systems that are designed to cope with the SBLOCA accidents. In the third level, the operations such as open or close to the sub systems are modeled. And in the fourth level, the devices in each sub systems are modeled such as the valves.

3.3 Interaction Simulator

Once users converts all knowledge-base information for a given accident scenario into a set of "State Chart Diagrams", the users can execute the interaction simulation among actors by activating the interaction simulator. The result of the interaction simulation is given in the time sequential log file where generated "Actor External Events", executed Log commands and Failure commands are recorded. The generated "Actor External Events" are the sequence of actor's action where the events are recorded by classifying into three types of action as shown in Table 2. The commands are written in the action of the event handler and executed on handling the event. Log command is used for recording any text into the log file. The user can use it for recording significant plant situation, an important operator judgment and so on. The failure command is used for simulating failures committed by actors.

Table 2. Actor External Event and its meaning

Event generated by	Event generated in (Place)	Type of the action
PLANT actor	PLANT actor	Alarm
OPERATOR actor	PLANT actor	Operation to the plant
OPERATOR actor	SUPERVISOR actor	Report to the supervisor
SUPERVISOR actor	OPERATOR actor	Oder to the operator

4 The plant DiD risk monitor software application in AP1000

4.1 AP1000 single loop model in the SBLOCA scenario

The target system is the passive core cooling system (PXS) in the AP1000 NPPs. Figure 6 gives the single loop model of the PXS during the SBLOCA accident. The SBLOCA break is 10-inch cold leg break as shown in Fig. 6. Derivation of timing charts which describe how the individual components will start and stop by the condition of plant parameters is indicated in the Fig. 7 and Table 3. These figures and tables are summarized from published safety analysis report of AP1000.

In the first place, it is explained why AP1000 is selected as the example system. Basically, the AP1000 employs passive safety systems to improve the plant safety while reducing the number of active safety systems. The major reason of adopting many passive safety systems is to decrease the possibility of hardware failure and human error.

Furthermore, the authors of this paper have developed the reliability monitor for safety system of AP1000 to evaluate its reliability in the event of loss-of-coolant accident (LOCA) with comparing that of conventional PWR[7]. The last is that the passive PRHR, CMT and ADS systems are key safety systems designed to mitigate the SBLOCA.

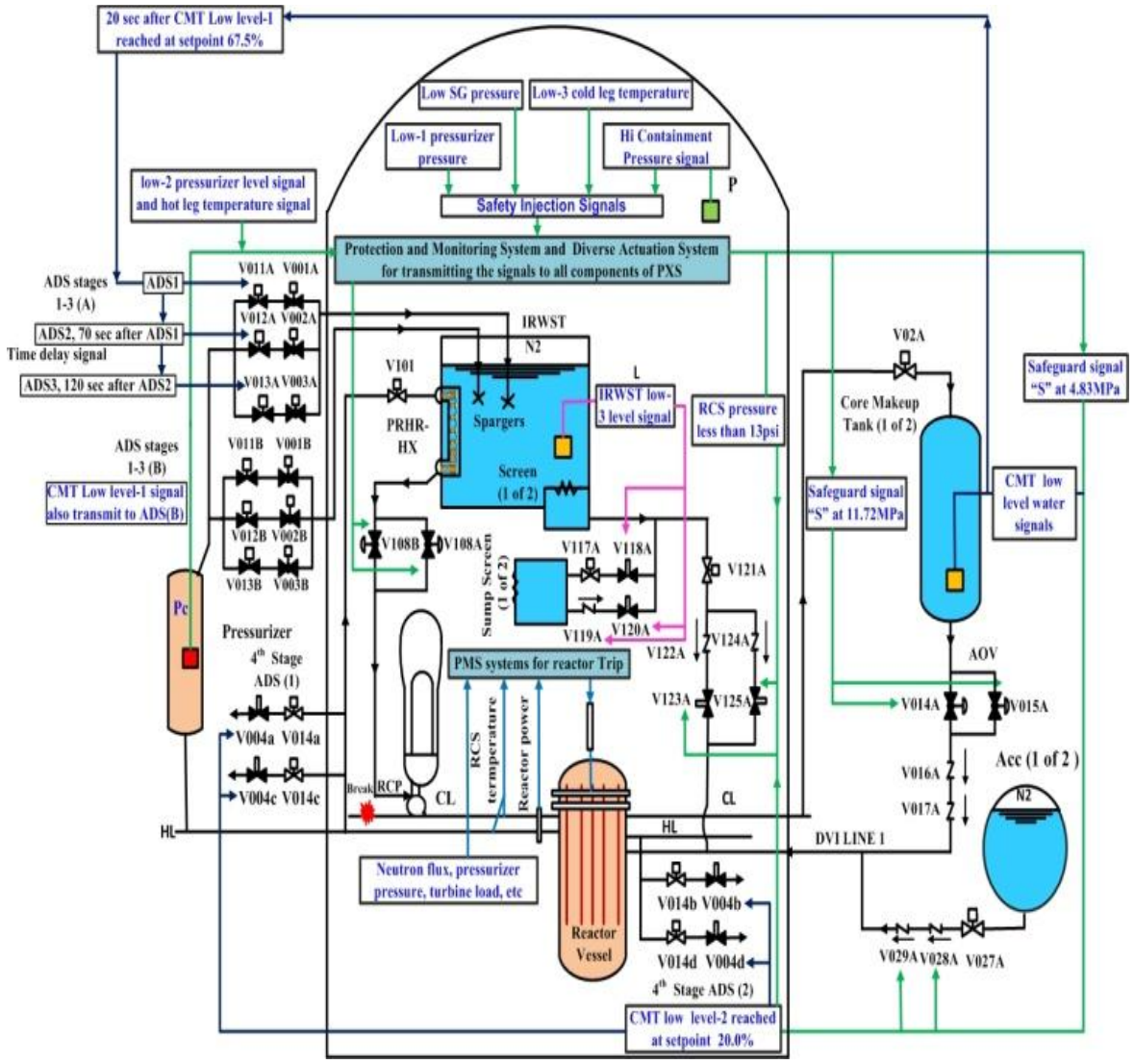

Fig. 6. Single loop model of PXS of AP1000[7].

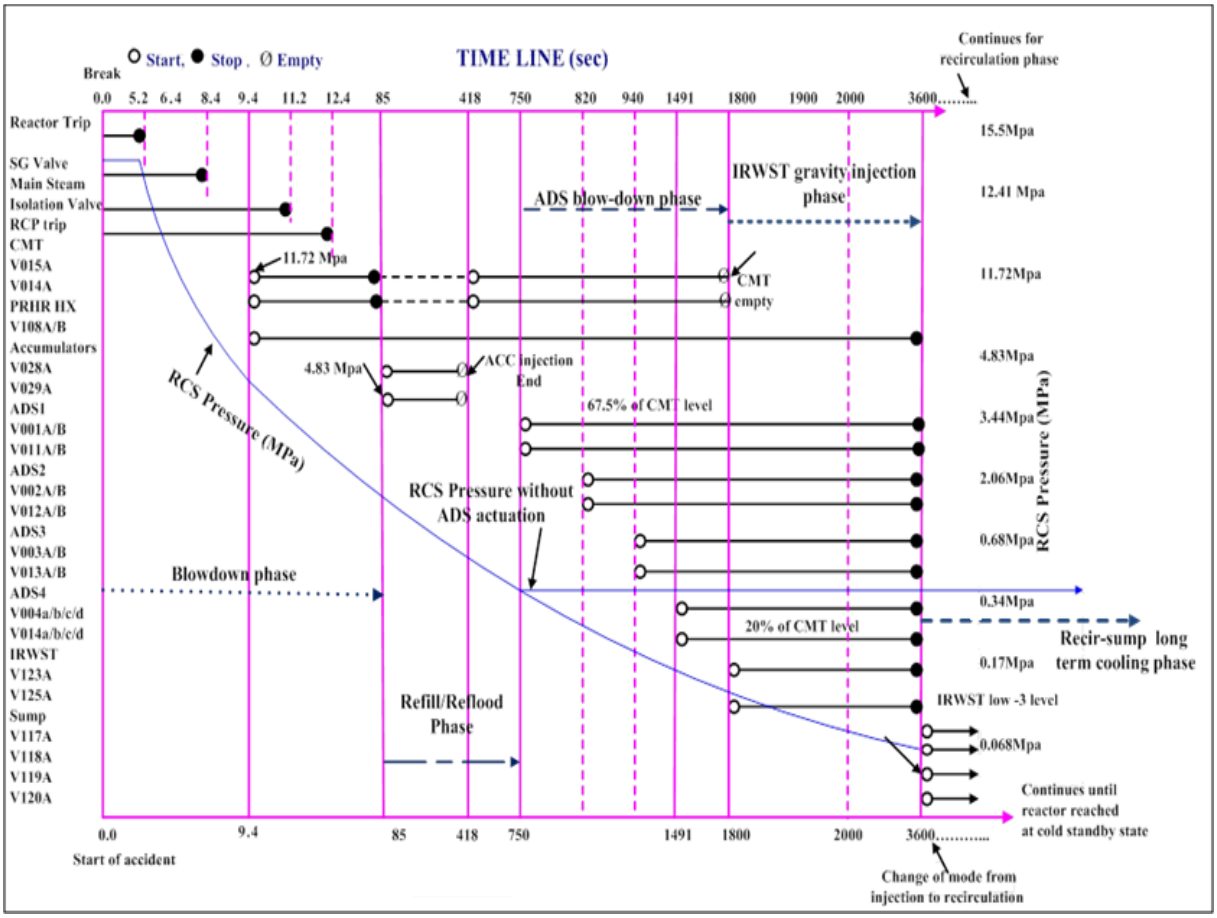

Fig. 7. Transient sequence behavior of PXS system of AP1000 during SBLOCA[7].

Table 3. Time sequences of SBLOCA DBA in AP1000 and related actuation signal conditions[13][14]

Activation systems	Phases of LOCA (injection and recirculation phases)		Detecting device	Actuation signals of RPS, PXS and PCCS	Time (sec) from LOCA	Components to be used for actuation in different phases
Reactor Protection system	Blow-down phase	Reactor scram (reactor trip)	Pressure sensors and temperature sensors	Hi-neutron flux, low coolant flow, over temperature. RCS 12.41Mpa,	5.2 sec	Reactor trip switchgear breakers.
		Safeguard signal "S"		RCS 11.72 MPa	6.4 sec	Safety actuation system
		Steam generator feedwater		After trip signals	8.4 sec	Feedwater control valve close
Passive Core cooling system		CMT injection system	RCS pressure sensor in pressurizer	Low-2 pressurizer pressure, safety injection signals, safeguard S signal at 11.72Mpa	9.4 to 85 sec	CMTs tanks, valves V014A to V017A
		PRHR system			9.4 to 3600 sec	PRHR-HX, V108A/B, V101
		Main steam isolation		After "S" signal	11.2sec	Isolation valves start to close
		RCP trip		After "S" signal	12.4sec	Pump trip
	Re-fill/ Reflood Phase	Accumulator start which stop CMT injection	RCS pressure sensor	S signal at 4.83Mpa RCS pressure	85 to 418 sec	ACC Tank, valves V027A to V029A
		CMT start again after Acc empty	Certain RCS pressure value	Accumulator empty signal	418 to 1800	CMTs tanks, V014A to V017A
	ADS blow-down Phase	ADS stage 1 (A/B)	CMT water level sensor	20sec after 67.5% liquid volume fraction in CMT	750 to 3600 sec	ADS 1, V001A/B, V011A/B
		ADS stage 2 (A/B)	Time delay timers	70sec after ADS-1 actuation	820 to 3600 sec	ADS2,V002A/B, V012A/B
		ADS stage 3 (A/B)	Time delay timers	120sec after ADS-2 actuation	940 to 3600 sec	ADS3,V003A/B, V013A/B

		ADS stage 4 (a/b/c/d)	Time delay timers	20.0% liquid volume fraction in CMT and 551sec after ADS3 actuate	1491 to 3600 sec	ADS 4, V004a/b/c/d, V014a/b/c/d
	IRWST injection phase	IRWST gravity injection lines flow	RCS pressure & CMT water level sensor	RCS pressure less than 89.6 KPa/13psi plus containment pressure	1800 to 3600 sec	IRWST tank, IRWST screen1, V121A to V125A
	Recirculation sump phase	Recirculation injection lines flow	IRWST low level water sensor	IRWST low-3 level signal	3600 to 6000sec	Sump, recirculation screen 1, V117A, to V120A
Passive containment cooling system	Containment cooling	Natural circulation of Air with water spray	Containment's temperature and Pressure sensors	Hi-2 containment pressure signal59psig, Hi containment temperature	30 sec to 72 hours after LOCA	PCCWST, V001A/B/C, V002A/B/C

For the operator, it is important to recognize what accident is happen. Unfortunately, the operators cannot always recognize the accident based on the process parameters. In order to demonstrate the developed software function, it is assumed that the operator successfully recognize that the SBLOCA has happened. In AP1000, there is no need of the active human operations during the SBLOCA accident but the operator need to confirm the status. So the operator confirmation is modeled as the interaction between the OPERATOR and the PLANT actors. In the Fig. 8 gives the task transition diagram for SBLOCA. The task transition of the plant safety systems will start by the occurrence of small break in primary loop followed by the sequence of automatic actions of reactor protection system (No.1) and then passive core cooling system (No.2), in order to settle the plant process to the successful cold stand by state (No.4) and then to cold shutdown by state (No.6), while passive containment cooling system (No.3) to assure no external FP release (No.5). These successful scenarios to protect the plant are so called "Third defense layer" of NPP. But failures of No.1 and No.2 may lead to "core melt accident". Therefore, "Fourth defense layer" will have to be introduced in order NOT to develop the core melt accident into more serious stage of severe accent. On the other hand, the failure of No.3 will lead to "FP release to the environment". And offsite emergency measures to cope with radioactive release to the environment will be "Fifth defense layer".

The example configuration of plant operators and communications rules between each other are illustrated in Fig. 9 which is modeled as the configuration of actors in the plant.

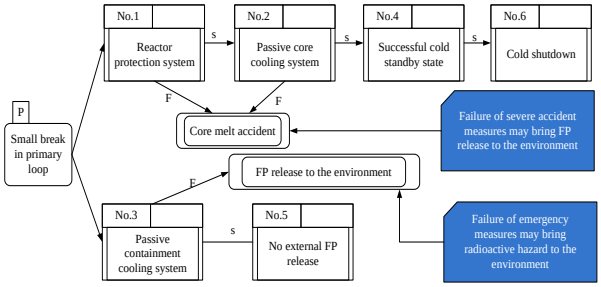

Fig. 8. Task transition diagram of AP1000 for SBLOCA.

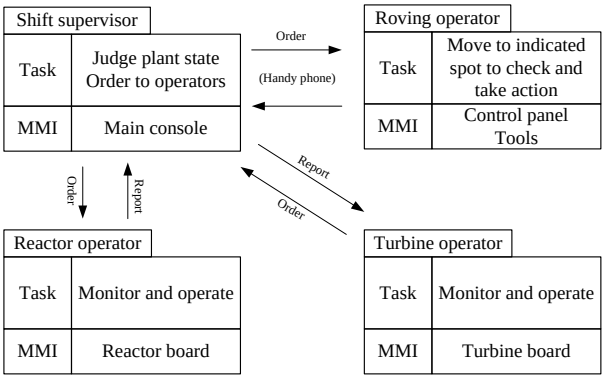

Fig. 9. Example operators configuration and communication path diagram.

4.2 The plant DiD risk model of the AP1000

The plant DiD risk model is modeled for the systems with the assumption and procedure in section 4.1. In the current model, the knowledge base is modeled for the successful scenario than the failure scenario knowledge base. Fig. 10 gives the top "State Chart Diagram" of the plant. In the configuration, there are three actors as OPERATOR actor, PLANT actor and SUPERVISOR actor. The "State Chart Diagram" is designed in the hierarchical manner. Fig. 10 also shows the hierarchical decomposition of the plant actor by "State Chart Diagram". For each subsystem, there are several devices in the subsystem diagram and each system performs its safety function during the SBLOCA accident.

For example, the "State Chart Diagram" in Fig. 11 models Passive Residual Heat Removal (PRHR) system. After 3 seconds delay, the system works when one of the valves named "V108A" or "V108B" is opened and the valve named "V101" is opened. The "State Chart Diagram" in Fig. 11 models the condition mentioned above. Those icons labeled as V108A, V108B and V101 are associated to other "State Chart Diagram" which models the function of a general valve. An "AND" condition is expressed as Join pseudo states. An "OR" condition is expressed as that both conditions of the "OPEN V108A" and "OPEN V108B" can make transition to the join pseudo state. By these ways, "State Chart Diagram" can model these logical conditions easily for the system status. The PHRH system is always working to remove the heat during the accident.

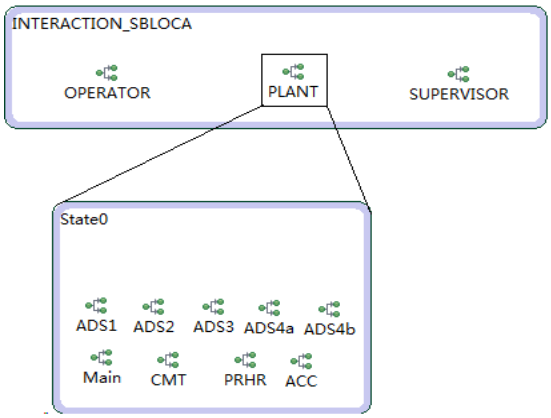

Fig. 10. The top and hierarchical diagram for the AP1000.

Figure 12 provides the detailed diagram for the plant actor "Main" icon in Fig. 10, where the details of all the transient sequence in the Fig. 7 are modeled by "State Chart Diagram". After the pre-determined time delay, the corresponding state is executed then the internal or external event is generated to run the corresponding safety system to cope with SBLOCA accident. At the same time, the decrease of reactor pressure is described in each state.

Figure 13 shows an operator's knowledge-base to cope with reactor trip. This diagram shows that the operator's ordinary state is in idling state, but the reactor trip event or safeguard signal event will occur. Then Steam Generator (SG) feed water stop event, Main steam isolation or RCS pump trip event will follow. The operator will confirm that the plant works properly against each of the alarms. A vertical bar on the left side of Fig. 13 is a fork pseudo state, expressing the branch to parallel processing. This figure shows that these three processes should be processed in parallel, not in sequence. In this case, these three processes for each of the three events should be processed in parallel. Each of the states named "confirm SG water stop", "confirm Main steam isolation" and "confirm RCS pump trip" hold an icon. These icons are all associated to the corresponding "State Chart Diagram". The name below each icon is the target machine name that is given to the "State Chart Diagram" as a variable. A vertical bar on the right side of Fig. 13 is a join pseudo state, expressing the merge to single processing and waiting for all parallel processing connecting to the join state to finish. Then the following diagrams will model the operator to confirm other safety systems.

In the Fig. 14, this diagram shows the operator behavior of getting the status of the machine and comparing the status with the required status such as to confirm whether the reactor coolant pump trip or not. The actual status is set by the Plant actor and the desired status is set by the Operator actor. If the status is matched, it generates an internal event and the upper diagram handles this event and proceeds to the next step. If the status doesn't match, the operator retries the status confirmation to cope with delaying the status change, and reports to the supervisor that the confirmation is failed. After a certain order is given by the supervisor, the operator makes operation against the plant and retries status confirmation repeatedly.

Figure 15 is the model for the supervisor interaction with the operator. In this diagram, the group state is used as the two states have the same event. Normally, the supervisor is in idle state. But if the operator reports that the state confirmation failed, the supervisor will order the operator to make some operation and the supervisor gives up without any order to the operator after several times.

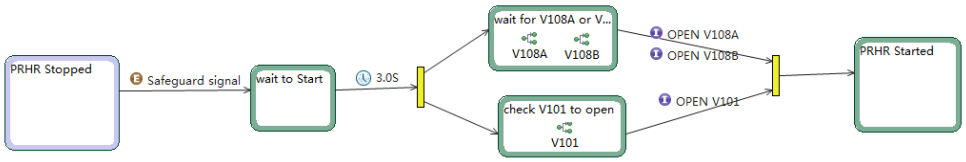

Fig. 11. The detailed diagram for PRHR in the plant actor.

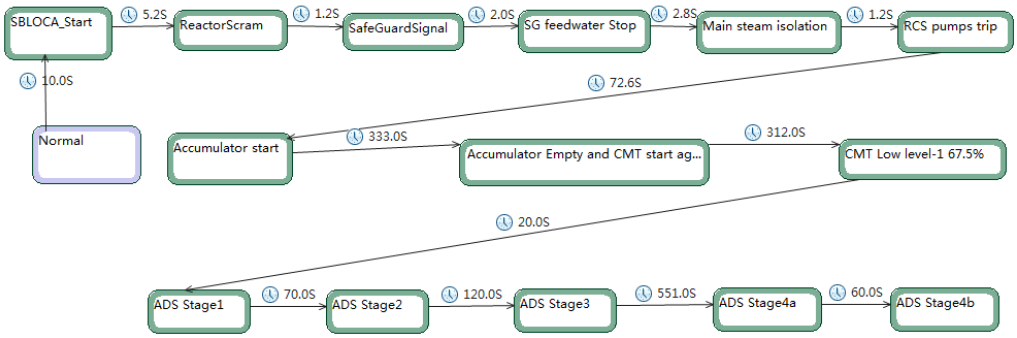

Fig. 12. The detailed diagram for "Main" in plant actor.

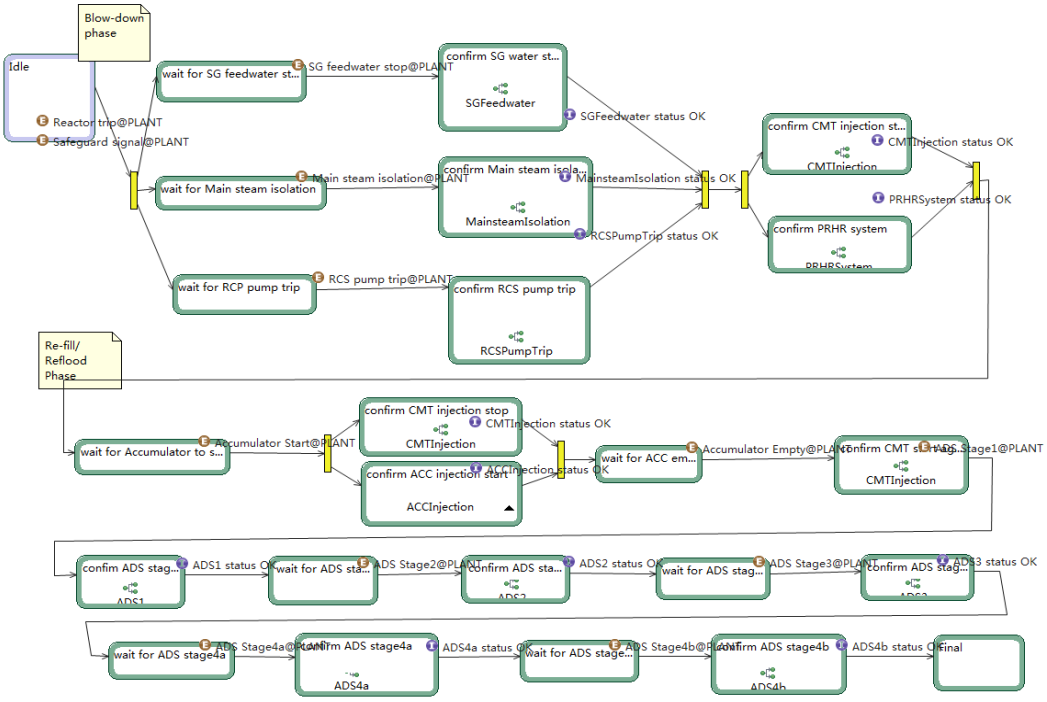

Fig. 13. The detailed diagram for the operator actor.

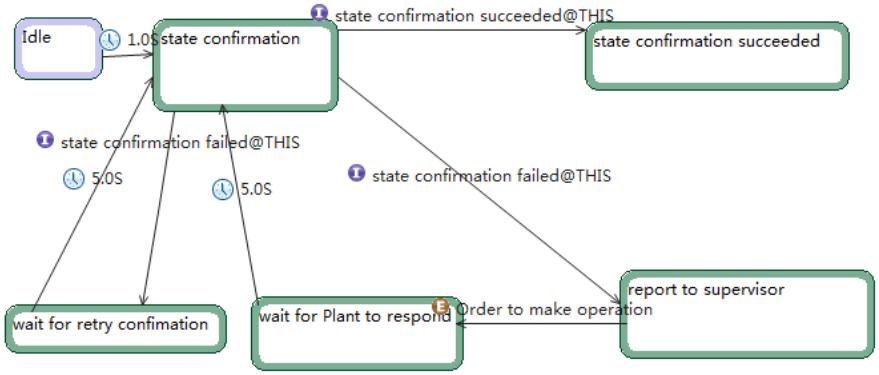

Fig. 14. The detailed diagram for the confirm action.

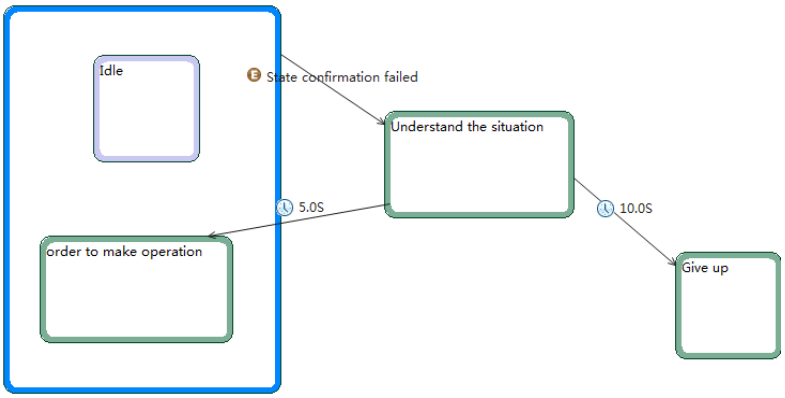

Fig. 15. The detailed diagram for the supervisor actor.

4.3 The AP1000 model simulation results in the plant DiD risk monitor system

The interactions among the different actors such as between the supervisor and the operator are given as the time sequential log. Figure 16 gives the interaction simulation result among the actors. In the simulation results they can be easily got that the service of the safety system as the PLANT actor, the action to the PLANT actor and the report to the SUPERVISOR actor from the OPERATOR actor and the order to the OPERATOR actor from the SUPERVISOR actor.

The plant DiD risk monitor system can simulate the failures of the devices. In the software, there are two ways to set the malfunctions. First, the malfunction can be set during the simulation using the failure commands. Second, the malfunction can be edited and insert before the simulation. Fig. 17 shows all the malfunctions for AP1000 LOCA models. Then the malfunctions can be selected and insert to the simulation. In simulation, all valves (V002A, V012A, V002B and V012B) belongings to the ADS2 system are simulated as stuck closed by inserting the malfunctions as shown in Fig. 18. The value 1 means there are failure in the simulation and value 0 means there are no failure.

In the software, the malfunction can be set to recoverable or not. If the failure is recoverable, during the simulation the operator report the failures and the supervisor orders the operator to make operation, then the devices will be operated successfully. If the failure is not recoverable, even if the operator makes operation following the supervisor's order, the devices are still in failure state. After trying several times, the supervisor will give up and then continue to following functions.

The following gives the simulation results that the ADS2 system malfunction is inserted and they are recoverable. So after the operator making operation, the system is working successfully. The detailed results are at the bottom of Fig. 16.

a) The valves stuck closed at 12:50:28.
b) The operator confirmed it and reported to the supervisor at 12:50:30.
c) The operator tried to open the valves manually by the order of supervisor at 12:50:31.

The ADS2 is confirmed OK at 12:50:31.

13	12:49:06 .192	SBLOCA Start	On Entry[Primary Event Handler]/SBLOCA_...	PLANT
15	12:49:06 .756	ALARM:Reactor trip@PLANT	Action/On Entry[Primary Event Handler]/R...	PLANT
19	12:49:06 .916	ALARM:Safeguard signal@PLANT S	Action/On Entry[Primary Event Handler]/S...	PLANT
23	12:49:07 .127	ALARM:SG feedwater stop@PLANT	Action/On Entry[Primary Event Handler]/S...	PLANT
44	12:49:07 .341	Confirm OK SGFeedwater target:STOP	On Entry[Primary Event Handler]/state co...	OPERATOR
47	12:49:07 .464	ALARM:Main steam isolation@PLANT	Action/On Entry[Primary Event Handler]/...	PLANT
51	12:49:07 .630	Confirm OK MainsteamIsolation target:isolation	On Entry[Primary Event Handler]/state co...	OPERATOR
52	12:49:07 .630	ALARM:RCS pump trip@PLANT	Action/On Entry[Primary Event Handler]/R...	PLANT
57	12:49:07 .797	Confirm OK RCSPumpTrip target:TRIP	On Entry[Primary Event Handler]/state co...	OPERATOR
64	12:49:07 .931	Confirm OK CMTInjection target:START	On Entry[Primary Event Handler]/state co...	OPERATOR
67	12:49:07 .941	Confirm OK PRHRSystem target:START	On Entry[Primary Event Handler]/state co...	OPERATOR
71	12:49:14 .947	ALARM:Accumulator Start@PLANT	Action/On Entry[Primary Event Handler]/A...	PLANT
86	12:49:15 .101	Confirm OK CMTInjection target:STOP	On Entry[Primary Event Handler]/state co...	OPERATOR
89	12:49:15 .110	Confirm OK ACCInjection target:START	On Entry[Primary Event Handler]/state co...	OPERATOR
93	12:49:48 .290	ALARM:Accumulator Empty@PLANT	Action/On Entry[Primary Event Handler]/A...	PLANT
115	12:49:48 .480	Confirm OK CMTInjection target:START	On Entry[Primary Event Handler]/state co...	OPERATOR
119	12:50:21 .554	ALARM:ADS Stage1@PLANT	Action/On Entry[Primary Event Handler]/A...	PLANT
133	12:50:21 .592	ADS1OK received	ADS1OK [Internal Event Handler]/ADS Sta...	PLANT
136	12:50:21 .598	ADS1OK received	ADS1OK [Internal Event Handler]/ADS Sta...	PLANT
137	12:50:21 .744	Confirm OK ADS1 target:OK	On Entry[Primary Event Handler]/state co...	OPERATOR
140	12:50:28 .603	ALARM:ADS Stage2@PLANT	Action/On Entry[Primary Event Handler]/A...	PLANT
143	12:50:28 .616	FAIL V002A stuck closed	On Entry[Primary Event Handler]/ValveCh...	PLANT
144	12:50:28 .617	ALARM:V002A stuck closed@PLANT	Action/On Entry[Primary Event Handler]/V...	PLANT
147	12:50:28 .628	FAIL V012A stuck closed	On Entry[Primary Event Handler]/ValveCh...	PLANT
148	12:50:28 .629	ALARM:V012A stuck closed@PLANT	Action/On Entry[Primary Event Handler]/V...	PLANT
151	12:50:28 .636	FAIL V012B stuck closed	On Entry[Primary Event Handler]/ValveCh...	PLANT
152	12:50:28 .637	ALARM:V012B stuck closed@PLANT	Action/On Entry[Primary Event Handler]/V...	PLANT
155	12:50:28 .643	FAIL V002B stuck closed	On Entry[Primary Event Handler]/ValveCh...	PLANT
156	12:50:28 .643	ALARM:V002B stuck closed@PLANT	Action/On Entry[Primary Event Handler]/V...	PLANT
160	12:50:28 .811	Confirm FAILED ADS2 target:OK current:NONE	On Entry[Primary Event Handler]/state co...	OPERATOR
163	12:50:29 .330	Confirm FAILED ADS2 target:OK current:NONE	On Entry[Primary Event Handler]/state co...	OPERATOR
166	12:50:29 .906	Confirm FAILED ADS2 target:OK current:NONE	On Entry[Primary Event Handler]/state co...	OPERATOR
169	12:50:30 .425	Confirm FAILED ADS2 target:OK current:NONE	On Entry[Primary Event Handler]/state co...	OPERATOR
171	12:50:30 .438	REPORT:State confirmation failed@SUPERVISOR OK@ADS2	Action/On Entry[Primary Event Handler]/r...	OPERATOR
174	12:50:31 .047	ORDER:Order to make operation@OPERATOR OK@ADS2	Action/On Entry[Primary Event Handler]/o...	SUPERVISOR
176	12:50:31 .093	OPERATION:make operation@PLANT OPEN@V012A	Action/On Entry[Primary Event Handler]/w...	OPERATOR
177	12:50:31 .093	OPERATION:make operation@PLANT OPEN@V002A	Action/On Entry[Primary Event Handler]/w...	OPERATOR
178	12:50:31 .093	OPERATION:make operation@PLANT OPEN@V012B	Action/On Entry[Primary Event Handler]/w...	OPERATOR
179	12:50:31 .094	OPERATION:make operation@PLANT OPEN@V002B	Action/On Entry[Primary Event Handler]/w...	OPERATOR
181	12:50:31 .145	OPEN@V012A now operation	make operation@PLANT [External Event ...	PLANT
183	12:50:31 .200	OPEN@V002A now operation	make operation@PLANT [External Event ...	PLANT
187	12:50:31 .265	OPEN@V012B now operation	make operation@PLANT [External Event ...	PLANT
189	12:50:31 .319	OPEN@V002B now operation	make operation@PLANT [External Event ...	PLANT
193	12:50:31 .649	Confirm OK ADS2 target:OK	On Entry[Primary Event Handler]/state co...	OPERATOR
197	12:50:40 .641	ALARM:ADS Stage3@PLANT	Action/On Entry[Primary Event Handler]/A...	PLANT
213	12:50:40 .824	Confirm OK ADS3 target:OK	On Entry[Primary Event Handler]/state co...	OPERATOR
217	12:51:35 .758	ALARM:ADS Stage4a@PLANT	Action/On Entry[Primary Event Handler]/A...	PLANT
218	12:51:35 .759	ADS3OK pressure down	On Entry[Primary Event Handler]/ADS Sta...	PLANT
226	12:51:35 .920	Confirm OK ADS4a target:OK	On Entry[Primary Event Handler]/state co...	OPERATOR
230	12:51:41 .795	ALARM:ADS Stage4b@PLANT	Action/On Entry[Primary Event Handler]/A...	PLANT
239	12:51:41 .991	Confirm OK ADS4b target:OK	On Entry[Primary Event Handler]/state co...	OPERATOR

Fig. 16. A part of interaction simulation result.

```
1 AP1000/ADS4a.scm,V004a stuck closed,0
2 AP1000/ADS4a.scm,V014a stuck closed,0
3 AP1000/ADS4b.scm,V004b stuck closed,0
4 AP1000/ADS4b.scm,V014b stuck closed,0
5 AP1000/ADS3.scm,V003A stuck closed,0
6 AP1000/ADS3.scm,V013A stuck closed,0
7 AP1000/ADS3.scm,V013B stuck closed,0
8 AP1000/ADS3.scm,V003B stuck closed,0
9 AP1000/ACC.scm,V027A stuck closed,0
10 AP1000/ACC.scm,V028A stuck closed,0
11 AP1000/ACC.scm,V029A stuck closed,0
12 AP1000/ACC.scm,V027A stuck opened,0
13 AP1000/ACC.scm,V028A stuck opened,0
14 AP1000/CMT.scm,V016A stuck closed,0
15 AP1000/CMT.scm,V017A stuck closed,0
16 AP1000/CMT.scm,V015A stuck closed,0
17 AP1000/CMT.scm,V014A stuck closed,0
18 AP1000/CMT.scm,V015A stuck opened,0
19 AP1000/ADS2.scm,V002A stuck closed,1
20 AP1000/ADS2.scm,V012A stuck closed,1
21 AP1000/ADS2.scm,V012B stuck closed,1
22 AP1000/ADS2.scm,V002B stuck closed,1
23 AP1000/PRHR.scm,V108A stuck closed,0
24 AP1000/PRHR.scm,V108B stuck closed,0
25 AP1000/PRHR.scm,V101 stuck closed,0
26 AP1000/ADS1.scm,V001A stuck closed,0
27 AP1000/ADS1.scm,V011A stuck closed,0
28 AP1000/ADS1.scm,V011B stuck closed,0
29 AP1000/ADS1.scm,V001B stuck closed,0
```

Fig. 17. Failures for the AP1000 PXS models.

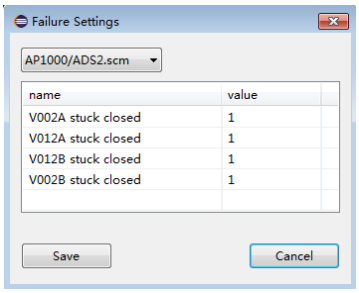

Fig. 18. Failure insertion for the devices.

5 Conclusions and future work

Based on the proposed risk monitor system, the plant DiD risk monitor system was designed and developed. The requirement of the plant DiD risk monitor software was summarized as how to model the system by the object oriented software based on functional modeling approach. And the software was developed using the UML to model the

knowledge-based information in the form of "State Chart Diagram". First the basic task can be modeled by "State Chart Diagram" in the lower level. Then the complicated tasks can be modeled effectively and easily by combining the basic task as the part in the upper level.

The passive safety AP1000 plant was studied and modeled using the software considering the SBLOCA as the design basis accident. It is shown that all knowledge-base information essential to simulate human-machine interactions can be modeled in the form of the "State Chart Diagrams". Once the users model the basic task in the "State Chart Diagrams", more complicated tasks can be modeled by "State Chart Diagram" effectively and easily by combining them as the parts. So the large knowledge-base for the NPP may be made with small effort by the technique. It is demonstrated that the modeling of human-machine interaction by applying "State Chart Diagram" is graphically made, and it is easy to understand by the user intuitively. And the interaction among the actors can be simulated and simulation results are shown as the time sequence log. It is further demonstrated that the software can model the system in a hierarchical manner and the malfunction can be set for the simulation, in the plant DiD risk monitor software. The developed software demonstrated that it is feasible and convenient to model the nuclear power plant knowledge base using the software modeling technique.

For the future work, i) the interaction analyzer that is designed to evaluate the procedure of the plant will be developed to complete the whole software of the plant DiD risk monitor system. ii) As the following step, the procedure or guideline based model will be further researched to more realistically model the operation of the plant and the response. iii) Furthermore, based on the research results of the procedure or guideline based model, we will examine the use of symptom based state characteristics within the plant DiD risk monitoring system. iv) Then the failure probability of the safety systems will be modeled using the plant DiD risk monitor system. v) Last the communication functions with the human operators will be designed and integrated.

References

[1] YOSHIKAWA, H., LIND, M., YANG, M., HASHIM, M., and ZHANG, Z.: Configuration of risk monitor system by plant defense-in-depth risk monitor and reliability monitor, Nuclear Safety and Simulation, Vol. 3, Number 2, June 2012, 140-152.

[2] YOSHIKAWA, H., YANG, M., HASHIM, M., LIND, M. and ZHANG, Z.: Design of risk monitor for nuclear reactor plants, Nuclear. Safety and Simulation, 2011, 3(2): 266-274.

[3] Nuclear Energy Agency. Risk Monitors, The state of the art in their development and use at nuclear power plants. NEA/CSNI/R, 2004.

[4] IAEA-TECDOC-1106, Living Probabilistic Safety Assessment (LPSA), IAEA, 1999.

[5] YOSHIKAWA, H., LIND, M., MATSUOKA, T., HASHIM, M., YANG, M., and ZHANG, Z.: A new functional modeling framework of risk monitor system, Nuclear Safety and Simulation, Vol. 4, Number 3, September 2013,192-202.

[6] MATSUOKA, T., and KOBAYASHI, M.: The GO FLOW reliability analysis methodology-analysis of common cause failures with uncertainty, Nuclear Engineering and Design, 1997, 175: 205-214.

[7] HASHIM, M., YOSHIKAWA, H., and YANG, M.: Addressing the fundamental issues in reliability evaluation of passive safety of AP1000 for a comparison with active safety of PWR, Nuclear Safety and Simulation, Vol. 4, Number 2, June 2013, 147-159.

[8] HASHIM, M., MATSUOKA, T., and YANG, M.: Development of a reliability monitor for the safety related subsystem of a PWR considering the redundancy and maintenance of components by fault tree and GO-FLOW methodologies, Nuclear Safety and Simulation, Vol. 3, Number 2, June 2012, 164-175.

[9] YOSHIKAWA, H., YANG, M., LIND, M., and MATSUOKA, T.: Integrated functional modeling method for configuring NPP plant did risk monitor and its application for AP1000, Proceedings of the 22nd International Conference on Nuclear Engineering, July 7-11, 2014, Prague, Czech Republic.

[10] Object Management Group: UML Version 2.4 Specification, http://www.omg.org/spec/UML/2.4, November 2011.

[11] Eclipse foundation: Eclipse IDE for Java Developer Version: Luna (4.4.1), http://www.eclipse.org, September 2014.

[12] Eclipse foundation: GEF(Graphical Editing Framework) Release 3.9.101,https://eclipse.org/gef, September 2014.

[13] Westinghouse Electric Company. AP1000 design control document. Accident analysis. Westinghouse Electric Company; 2009.

[14] YANG, J., WANG, W., QIU, S., TIAN, W., SU, G., and WU, Y.: Simulation and analysis on 10-in. cold leg small break LOCA for AP1000, Annals of Nuclear Energy, 2012, 81-89.