Living PSA modeling and updating for online risk monitoring

ZHANG Min[1], ZHANG Zhijian[2], CHEN Sijuan[3], and ZHANG Huazhi[4]

1. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (zhangmin@hrbeu.edu.cn)
2. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (zhangzhijian@hrbeu.edu.cn)
3. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (chensijuan@hotmail.com)
4. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (zhanghz05@163.com)

Abstract: An overview of the preliminary research is provided on the methodology for modeling and updating PSA models for online risk monitoring. In order to model the dynamic characteristics of nuclear power plant and to update the models automatically as soon as there are any changes of plant configuration or reliability data during the on-line risk monitoring of Nuclear Power Plants (NPPs). The demands of modeling and updating for three kinds of failure in PSA models which include independent failure, common cause failure and sequence-dependent failure are firstly clarified, and then a systematic method is suggested to implement the modeling and updating based on Living PSA methodology. Finally, a conceptual design is proposed of the program module division and data exchange of the Living PSA module of an On-Line Risk Monitor (OLRM). By using the modeling and updating methods proposed in this article, any detectable status changes of systems and components can be reflected automatically in an OLRM so that the reliability of time-dependent components can be considered. This means the influence of operation history on component reliability can be evaluated which is helpful for making the optimization of the maintenance plan.
Keyword: living PSA; modeling and updating; on-line risk monitoring

1 Introduction

As well known for large complex systems like Nuclear Power Plant (NPP), there will be many changes during their life cycle, including permanent changes like system structure change and operation procedure improvement, and temporary changes during plant operation like components unavailable, switching among redundant units, *etc*. There is a great need to update or modify the Probabilistic Risk/Safety Assessment (PRA/PSA) models when it becomes necessary to reflect those changes mentioned above, and it leads to the Living PSA concept which is first defined by IAEA as:

"Living PSA (LPSA) is a PSA of the plant, which is updated as necessary as possible to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information. The LPSA would be used by designers, utility and regulatory personnel for a variety of purposes according to their needs, such as design verification, assessment of potential changes to the plant design or operation, design of training programmes and assessment of changes to the plant licensing basis."[1]

Risk Monitor, as a popular application of Living PSA, is defined as *"a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the Risk Monitor reflects the current plant configuration in terms of the known status of the various systems and/or components – for example, whether there are any components out of service for maintenance or tests. The Risk Monitor model is based on, and is consistent with, the Living PSA."*[1]

Since the first Risk Monitor *"Essential Systems Status Monitor (ESSM, 1988)"*, it has kept playing an important role in support of operational decisions. However, because of the lack of plant on-line component monitoring and information acquisition technique, manual operation is necessary to run a

Received date: March 12, 2015
(Revised date: June 9, 2015)

Risk Monitor (RM), which usually induces a time delay for model updating and risk assessment. Thus, the RM is more often used off-line for optimization of plant future activity plan (maintenance plan, *etc.*). As the development of plant on-line component monitoring and information acquisition technique, it becomes possible to obtain component operation information and transfer it to a Risk Monitor on-line to activate PSA model and updating it automatically. When the RM is developed to real time on-line Risk Monitor, this can be called On-line Risk Monitor (OLRM) in this article in order to distinguish it from the current Risk Monitor. However, there may many problems come out for such Living PSA as the methodological basis of Risk Monitor, to realize such OLRM by the improvement of the current Living PSA method.

As mentioned above, the changes of a NPP may be permanent or temporary. The permanent changes of a NPP are usually implemented during refueling outages, and these kinds of PSA model updating have been involved in current Living PSA updating procedure. Thus the improvement included in this research will focus on the temporary changes which may occur at any time of a plant operation cycle.

Besides, the reliability data of each component may be different because it is relevant to the operating environments, procedure and history. So the reliability of systems and components should be assessed dynamically based on different conditions during the plant operation.

However, most of the currently used risk monitors[2] have been based on traditional PSA modeling methodology where the on-line dynamic characteristics (dependent property, *etc.*) of NPP systems are ignored, and the employed reliability data are taken as constant value based on a hypothetical prerequisite that components and systems always work under the predefined conditions. Moreover, the instantaneous risk during the operation duration is assessed by the assumption that the detected plant status will last for one year. This is also said to be idealized or can be said to be not true, and therefore it is difficult to judge whether the reliability value reduced by such way will be optimistic or pessimistic.

Therefore, it is necessary to establish a new modeling and updating method which can take into the problems mentioned above, in order to achieve more realistic and more accurate risk assessment of NPPs than by the present methods of risk monitor. The authors of this article will first give an overview on the researches on Living PSA method for on-line risk monitoring which covers the online PSA model updating for temporary changes during plant operation and the necessary improvements for Living PSA model construction, by considering the condition based reliability assessment of components. Major progress of the authors' research thus far conducted will be also described in this paper.

2 Demand analysis for living PSA updating

According to Kaplan and Garrick [3], risk is defined as the answer to three simple questions: What can go wrong, how likely is it, and what are the consequences? Moreover, we try to measure the likelihood of risk as the probability of failure.

For Level 1 PSA of NPPs the typical consequence of focus are whether or not the reactor core is damaged while for level 2 PSA it will be the failure of containment to bring large release of radioactive materials from the plant. So the aim of nuclear power risk assessments is to evaluate the likelihood of core damage (CD) as the core damage frequency (CDF) per year and the likelihood of large release (LR) as the large release frequency (LRF) per year. To evaluate the CDF or LRF by PSA methods, the critical factors are frequencies of various Initial Events (IEs), model structures of Event Trees (ETs) and Fault Trees (FTs), and the probabilities of Basic Events (BEs) of various machines and human elements.

Then for on-line risk assessment, the key problems which need to be considered include the ET/FT structure updating according to the current plant status and the re-evaluation of the frequencies of IEs and associated probabilities of failure of the BEs according to the plant operation conditions. The IEs

frequencies are normally taken as yearly average values and they may not need to be updated in such a timely manner. ETs, which delineate the accident sequences, are composed of the consecutive occurrence of loss of Functions which are described as Failure of Top Events (FEs). Since the occurrences of FEs are usually determined by FTs, so ET updating can be implemented by FT updating. Then, research can be focused on FT modeling and updating and the related evaluation of conditional probability of BEs.

Figure 1 shows the overall consideration of the demand analysis. For FT model structure, the updating should be implemented by changing the event parameters in the FT model, including intermediate events and basic events. By considering the dependent relationship of the components corresponding to FT events, the events can be divided into independent events and dependent events which can be further divided into CCF events and sequence dependent events. There are two ways to update the events status:(i) Change the logic to be true; and (ii)Change the probabilities as different conditions. For conditional probability evaluation of BEs, the influential factors are reliability models and model parameters. Large amount of reliability tests and long term industry data accumulation are necessary for model parameter evaluation. So there may be no need to update the model parameters on-line during a plant operation cycle. But the reliability models should be updated on-line as different component maintenance/testing strategies, current status and so on. Besides, the conditional probabilities of BEs also depend on different event categories.

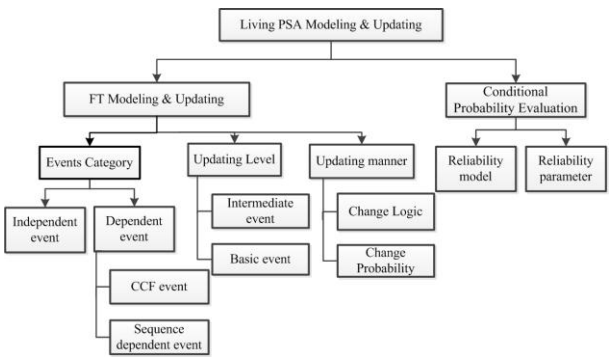

Fig.1 Research demand analysis.

Based on the analysis above, the key problems which need to be solved for Living PSA modeling and updating are: (i) Independent events modeling and updating, (ii)CCF events modeling and updating, and (iii)Sequence dependent events modeling and updating. The items to be modeled and updated involve model structure and condition based reliability model.

3 Living PSA modeling and updating

3.1 Independent events modeling and updating

For independent events, the updating is to reflect the events status and probabilities correctly in accordance with the equipment operating conditions. Thus, the key point is to assess the conditional failure probabilities (CFPs) of components by considering a series of conditions including environment, operating mode, current status, operating history, future demands, maintenance strategy and so on. Apparently, the CFPs are time-dependent.

Environmental effects such as pressure, temperature and vibration on a component are inherent characteristics of a component, which should be evaluated based on large number of reliability tests. These tests should cover all possible environmental conditions and be completed before installation and operation. That is to say, the relationship among component failure and environmental factors should have been completely analyzed before operation. This study focuses on the time duration of operation, assuming that the environment influenced component failure probabilities have been initially evaluated in a basic reliability database.

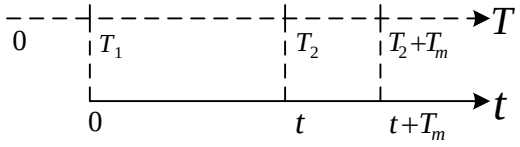

Fig.2 The time points considered during analyzing.

Figure 2 illustrates two time domains employed by the authors of this article, where the dotted axis is the time line of a component operation while the solid axis, the time line for online risk monitoring. There are three key time points for online risk monitoring as shown in solid axis. They are: (I)The start point of risk calculation, which is the current time($t=0$) when a plant configuration change is detected; (ii) Any time t after the current time when an accident may happen and PRA related components will be asked to fulfill

their mission to mitigate the accident; and (iii) the time point $t+T_m$ when PRA related components will be allowed to be out of service after the accident, where T_m is the mission time of the component for certain demanding circumstance. All these time points can be found in the component operation axis (the dotted line), where T_1 is the time to indicate the current time point, because the component may be started before the current time point. Then T_1 refers to the operation history of components, and the values should be different for different components in the same PRA model. If the plant configuration change is is assumed to be a certain component is started, then T_1 for the component is 0. In this case the two time axis for the component coincide with each other but not for other components.

Then the modeling for independent events during online risk monitoring is to determine what is the probability a component may fail from the current time ($t=0$) to any concerned future time $t+T_m$ under the condition of the current status, which is here called as $CFP(t)$.

Take $X(t)$ as the component status at time t. Assume that $X(t)$ only has two values of either 0 or 1, where 0 means the component is available while 1 means the component is failed. According to the analysis above, the $CFP(t)$ of a component can be expressed as

$$CFP(t)=P[X(t+T_m)=1|X(0)] \quad (1)$$

Then the mathematical expression of $CFP(t)$ for a certain event should be determined according to the characteristics of the relative component, like failure mode and operation and maintenance strategy.

For failure mode, it is usually divided into time-dependent failure and demand-based failure from the reliability theory. And for the latter category, the parameter for quantitative assessment is usually a fix probability which is not time dependent. So the research on $CFP(t)$ evaluation is focused on time-dependent failure.

The PSA related components are usually operated by the following three modes:

(i) Long term operation. In this mode, an equipment will start as reactor starts and keep running during plant operation, with a failure rate $\lambda(t)$.

(ii) Cold standby. Equipment stays in dormant state and start in certain condition like after accident, with failure rate $\lambda(t)=0$ in dormant state and $\lambda(t)$ in operation.

(iii)Warm standby. Equipment will not keep functioning during plant operation but will be linked to systems preparing to service when needed, with failure rates $\lambda'(t)$ in preparing state and $\lambda(t)$ in operation.

According to maintenance strategies, the components are divided into on-line repairable components and non-repairable components. In the former case, the failed component can be repaired without reactor shutdown or power decrease, but not so in the latter. Here a new parameter of maintenance rate $\mu(t)$ is introduced for the quantitative reliability assessment of repairable component, wherein two assumptions are adopted for repairable components reliability assessment:

(i) Exponential distribution assumption for repairable components, which means that the failure rate and maintenance rate are constant;

(ii) Maintenance cannot be implemented during accident processing, which means it is not needed to consider the maintenance rate during the mission time period in reliability models.

From the above, the failure probability of basic events considering a series of factors can be acquired by mathematical derivation, and the items need to be updated during on-line risk monitoring can be obtained too. The main results are summarized in Table 1 and Table 2. The detailed process of the authors was published in Ref. [4].

Then the online updating of independent events of PSA models can be implemented by change the event logic values or related reliability models during the online risk monitoring, in accordance with the conditions of component category, detected component status and recorded component operating time T_1, also as shown in Table 1 and Table 2. For instance, if a non-repairable component which has

kept in service for 1 month is available at the current time when recalculation of plant risk, then the risk monitor should change the value of T_1 in the reliability model of $CFP_L^{NR,s}(t)$ in Table 1 to be set as 1 month. And if a repairable component which has been in service is detected to be failed, then the risk monitor should update the PSA model by changing the reliability model of the component as $CFP_L^{R,f}(t)$.

It is noticed that the reliability models of cold standby non-repairable components and repairable components have nothing to do with time T_1, and it seems conflicting with the authors' claim mentioned above but in fact it is not so. Generally speaking, there are two aspects on whether the operational history will affect the component reliability in future: (i) The initiating status of assessment, which can be detected online, and (ii) In what stage of life cycle the component will be during the concerned time interval, which determines the failure rate and maintenance rate used for calculating and related to T_1. For cold standby component which is non-repairable and available when conducting on risk reassessment, there will not be any new failure before demanded after accident, so the initiating status should be always available, and the failure rate should be the values from 0 to component mission time. So the reliability model is not a function of T_1. And for repairable component, exponential distribution assumption is adopted in this study, which is consistent with the status by engineering judgment. So the operated time T_1 will not affect future reliability of the components because of the memoryless property of exponential distribution. So the only influence factor of repairable component reliability is the detected initiating status, which is clarified in the reliability models which are indicated by superscripts in the both Tables 1 and 2.

Table 1 Advice on reliability models and updating for Non-repairable components

Operating mode	Long term operating	Cold standby	Warm standby
Reliability model	$CFP_L^{NR,f}(t)=1$ $CFP_L^{NR,s}(t)=1-e^{-\int_0^{t+T_m}\lambda(u+T_1)du}$	$CFP_C^{NR,f}(t)=1$ $CFP_C^{NR,s}(t)=1-e^{-\int_0^{T_m}\lambda(u)du}$	$CFP_W^{NR,f}(t)=1$ $CFP_W^{NR,s}(t)=1-e^{-\int_0^{t}\lambda'(u+T_1)du-\int_0^{T_m}\lambda(u)du}$
Inputs	$\lambda(t), T_1, T_m$	$\lambda(t), T_m$	$\lambda(t), \lambda'(t), T_1, T_m$
updating	Logic=1 when failed; Update T_1 every recalculation during operating		

The meanings of superscripts:
'NR' =non-repairable; 'f'= unavailable at current moment; 's' =available at current moment.

Table 2 Advice on reliability models and updating for Repairable components

Operating mode	Long term operating	Cold standby	Warm standby
Reliability model	$CFP_L^{R,f}(t)=1-\frac{e^{-\lambda T_m}}{\lambda+\mu}(\mu-\mu e^{-(\lambda+\mu)t}))$ $CFP_L^{R,s}(t)=1-\frac{e^{-\lambda T_m}}{\lambda+\mu}(\mu+\lambda e^{-(\lambda+\mu)t}))$	$CFP_C^{R,f}(t)=1-e^{-\lambda T_m}(1-e^{-\mu t})$ $CFP_C^{R,s}(t)=1-e^{-\lambda T_m}$	$CFP_W^{R,f}(t)=1-\frac{e^{-\lambda T_m}}{\lambda'+\mu}(\mu-\mu e^{-(\lambda'+\mu)t})$ $CFP_W^{R,s}(t)=1-\frac{e^{-\lambda T_m}}{\lambda'+\mu}(\mu+\lambda' e^{-(\lambda'+\mu)t})$
Inputs	λ, μ, T_m	λ, μ, T_m	$\lambda, \lambda', \mu, T_m$
updating	Change the reliability models according to current status at every recalculation.		

The meanings of superscripts:
'R' =repairable; 'f'= unavailable at current moment; 's' =available at current moment.

3.2 Common cause failure modeling and updating

Common cause failure (CCF) is defined as two or more components failing at the same time or within a short time interval, as a result of commonly shared cause among the several different components[5]. In large complex Industrial systems like NPPs, redundancy has been always played an important role in system reliability design. However, CCF may exist among the redundant devices because similar design, operating conditions, and so on make CCF critical factor for redundant system failure. Therefore, it is important to make an accurate assessment on CCF during system risk analysis.

There are basically two ways to model CCFs: implicit and explicit approaches. The explicit approach is

applied when the cause of CCF is quite evident and can be incorporated within the FT model as a separate basic event. The implicit approach is used when the cause of CCF is too complex to describe by explicitly or in such situations when the explicit modeling may result in overwhelmingly complicated models.

In case of implicit approach for CCF in PSA models, common cause parameter models[6] like the Multiple Greek Letter (MGL) model are used to model CCFs, in which the parameters vary as different CCF trains. If the component status changes happen in a redundant subsystem during on-line risk monitoring, the train of the corresponding CCF group in PSA model will decrease, and the CCF parameters may be different from the original values. However, most modern risk monitors proposed currently ignores this problem except for only few ones like in EOOS (Equipment Out Of Service), where parameters of a CCF group in different trains are initialized according to the general statistical data based on industry experiences and pre-stored as different files which can be invoked respectively during software operation. However, there still remain some problems such as:

(i) There may be lack of experiences for high train CCFs in the general statistic database, and

(ii) The plant specific data may have been acquired for certain train CCF, but they are inconsistent with the general statistic data.

The most popular CCF parameter models include Beta Factor Model, Alpha Factor Model and Multiple Greek Letter (MGL) Model. Wherein the latter two models are usually more accurate for high-train CCF groups and the parameters of CCF models can be transferred from one model to the other one in the both models. This procedure is here called as" mapping down process", and it is adopted in the authors' research to reevaluate the CCF parameters for the Alpha Factor model, based on the original values and the current status. Two basic assumptions used in the authors' research are:

(i) The failures of redundant components have the same distribution, and

(ii) The common causes are external events which are independent with the number of components.

And then the third assumption is adopted in the authors' current research, which claims that the failures except all components have failed in a CCF group are independent failures.

Table 3 Four train system mapping down process

Failure Type	BEs in Original Group		BEs in Target System	
	4-Train System	Frequency	3-Train System	2-Train System
Independent Failure	A	$Q_1^{(4)}$	A	A
	B		B	B
	C		C	None
	D		None	None
Two Failure	AB	$Q_2^{(4)}$	AB	AB
	AC		AC	A
	AD		A	A
	BC		BC	B
	BD		B	B
	CD		C	None
Three Failure	ABC	$Q_3^{(4)}$	ABC	AB
	ABD		AB	AB
	ACD		AC	A
	BCD		BC	B
All Failure	ABCD	$Q_4^{(4)}$	ABC	AB

$Q_k^{(4)}$ is the frequency of k components fail in the 4 train system, k=1,2,3,4.

The mapping down process[7] of a case system is as shown in Table 3. The transformation law of the probabilities of BEs from 4-train system to 3-train system and 2-train system can be obtained from Table 3, and then the similar laws from n-train system to (n-i)-train system can be deduced by the following way:

$$\begin{aligned} Q_t^{(n-i)} &= Q_t^{(n)} && i=1,2,...,n-1; \\ Q_k^{(n-i)} &= \sum_{m=0}^{i} C_i^m Q_{k+m}^{(n)} && k=1,2,...,n-i \end{aligned} \tag{2}$$

where,

$Q_k^{(n)}$ is the frequency of k(k=1,2,...,n) components fail in a n-train system;

$Q_t^{(n)} = \sum_{k=1}^{n} C_{n-1}^{k-1} Q_k^{(n)}$ is the total failure frequency of each component.

Then the CCF model parameters of (n-i)-train system, which are the new parameters demanded by updated PSA model for on-line risk monitoring, can be deduced from the CCF parameters of the original n-train system (see Table 4 for the results for Alpha Factor Model).

Table 4 Parameters updating for Alpha Factor Model

Model	Non-staggered testing situation	Staggered testing situation
Parameter definition	$\alpha_k^{(n)} = \frac{C_n^k Q_k^{(n)}}{\sum_{k=1}^{n} C_n^k Q_k^{(n)}}$	$\alpha_k^{(n)} = \frac{C_{n-1}^{k-1} Q_k^{(n)}}{Q_t^{(n)}}$
Updated factors	$\alpha_k^{(n-i)} = \frac{C_{n-i}^k \left(\sum_{m=0}^{i} \frac{C_i^m}{C_{k+m}^m} \alpha_{k+m}^{(n)} \right)}{1 - \sum_{m=1}^{i} \frac{C_i^m}{C_n^m} \alpha_m^{(n)}}$	$\alpha_k^{(n-i)} = \sum_{m=0}^{i} \frac{C_{n-i-1}^{k-1} C_i^m}{C_{n-1}^{k+m-1}} \alpha_{k+m}^{(n)}$

$\alpha_k^{(n)}$ is the fraction of the total frequency of failure events that occur in the n-train system, involving the failure of k components.

Table 5 CCF updating example for Alpha Factor Model

Sys-tem	Group members	Parameters
The original system	Pump B fails to start Pump C fails to start Pump D fails to start	$\alpha_{11}^3, \alpha_{12}^3, \alpha_{13}^3$
	Pump A fails on operation Pump B fails on operation Pump C fails on operation Pump D fails on operation	$\alpha_{21}^4, \alpha_{22}^4, \alpha_{23}^4, \alpha_{24}^4$
System with A failed	Pump C fails to start Pump D fails to start	$\alpha_{1k}^2 = \frac{(3-k)\alpha_{1k}^3 + (k+1)\alpha_{1(k+1)}^3}{3 - \alpha_{11}^3}$
	Pump B fails on operation Pump C fails on operation Pump D fails on operation	$\alpha_{2k}^3 = \frac{(4-k)\alpha_{2k}^4 + (k+1)\alpha_{2(k+1)}^4}{4 - \alpha_{21}^4}$

Note:
1.The parameters of CCF model is from non-staggered testing situation.
2. α_{lk}^m is the k^{th} alpha factor of a m-train CCF group referring to the l^{th} failure mode of the group components.

Thus, the CCF updating for on-line risk monitoring should be implemented by the following two steps:

(i) To refresh the CCF group members. The failure modes of the failed component should be removed out of the CCF groups, and the new groups should be rebuilt up according to the operation manner of the new system, and

(ii) To update the CCF parameters using the formulas in Table 4 for new CCF groups.

For instance, there is a 4 redundancy pump system. Normally, pump A is on operation and the others (pump B, C and D) are in standby. Then pump A is detected to be failed and B has been started during plant operation. Table 5 shows the updated CCF groups and parameters for on-line risk monitoring, based on the original CCF model and parameters.

3.3 Sequence dependent failure modeling and updating

Sequence dependent failure is defined as the phenomenon that the output event will not happen unless its inputs happen in a specific order. Figure 3 is a two-train redundant system. Normally, signal/flow can be transferred by A to D. If A fails, B will be excited by switch S, then the signal/flow can be transferred by B to D. As the switching to B is an instantaneous function, B will keep functioning once excited even if following by failure of S. But if S has failed when A fails, B will not be excited. Then D will have no inputs, leading to failure of the redundant system. It is the sequence dependent failure that the failures of A and S will lead to different results as different failure order[8].

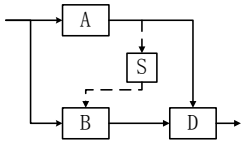

Fig.3 Example of sequence dependent failure.

To model sequence dependent failure, "PAND" (Priority-AND) gates are adopted in the authors' research, where output event happens only when all its inputs happen and the left ones happen no later than the right ones. Then the fault tree of the system in Fig.3 with the top event ' D has no output' is constructed as in Fig.4. The 'PAND' gate 'G5' is used to describe the failure relationship that both S and G6 happen and S happens no later than G6, whose structure function can be taken as 'S>G6'. Boolean Algebra is still applicable for this fault tree. And we can get the structure function of this fault tree as follows:

$$\begin{aligned} T = G1 &= G2 + G3 = D + D_s + G4 + G5 \\ &= D + D_s + (A + A_s)(B + B_s) + S > G6 \\ &= D + D_s + (A + A_s)(B + B_s) + S > (A + A_s) \\ &= D + D_s + AB + AB_s + A_s B + S > A + S > A_s \end{aligned} \quad (3)$$

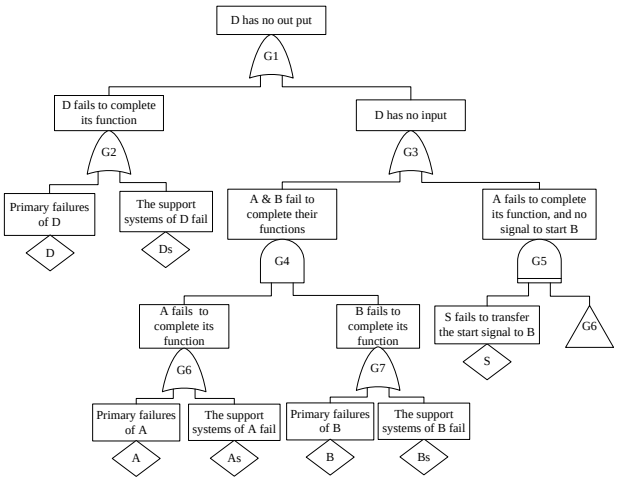

Fig.4 Fault tree of the sample system in Fig.3.

For quantitative calculation of S>A, assuming that A happens at time τ（$0 \le \tau \le T_m$）, the probability that S has failed when A fails should be

$$F_S(\tau) = \int_0^{\tau} f_S(t_S)dt_S \tag{4}$$

Then, the probability of S>A (Both A and S fail at time t and S fails before A) is

$$F(S > A, t) = \int_0^t f_A(\tau)\int_0^{\tau} f_S(t_S)dt_S d\tau \tag{5}$$

And then the probability of the top event can be calculated by using the probability formula for compatible events. The term $f(t)$ is the probability density function of the corresponding event, depending on the failure distribution.

Similarly, the formula for n sequence dependent events can be deduced, among which the i^{th} event should happens before the $(i-1)^{th}$ event. The probability of the output event of the PAND gate with n inputs should be given by

$$\begin{aligned} &F(E_n > E_{n-1} > \cdots > E_2 > E_1, t) \\ &= \int_0^t f_1(t_1)\int_0^{t_1} f_2(t_2)\cdots\int_0^{t_n} f_n(t_n)dt_n \cdots dt_2 dt_1 \end{aligned} \tag{6}$$

Therefore, by using the "PAND" (Priority-AND) gates and the corresponding mathematical model, the sequence dependent feature among redundant components can be modeled. For on-line updating when there is a component failure or change for operation arrangement, the most difficult problem is to determine the new sequential relation automatically by software. So the PSA experts may be asked to enumerate possible sequential relations and model them as sub-trees with house events at the beginning of PSA model construction. So the model updating can be implemented by automatically setting the house events values to be true or false accordingly.

3.4 Procedure of Living PSA updating module

According to the analysis above, the procedure of Living PSA updating module for on-line risk monitoring is proposed as shown in Fig.5.

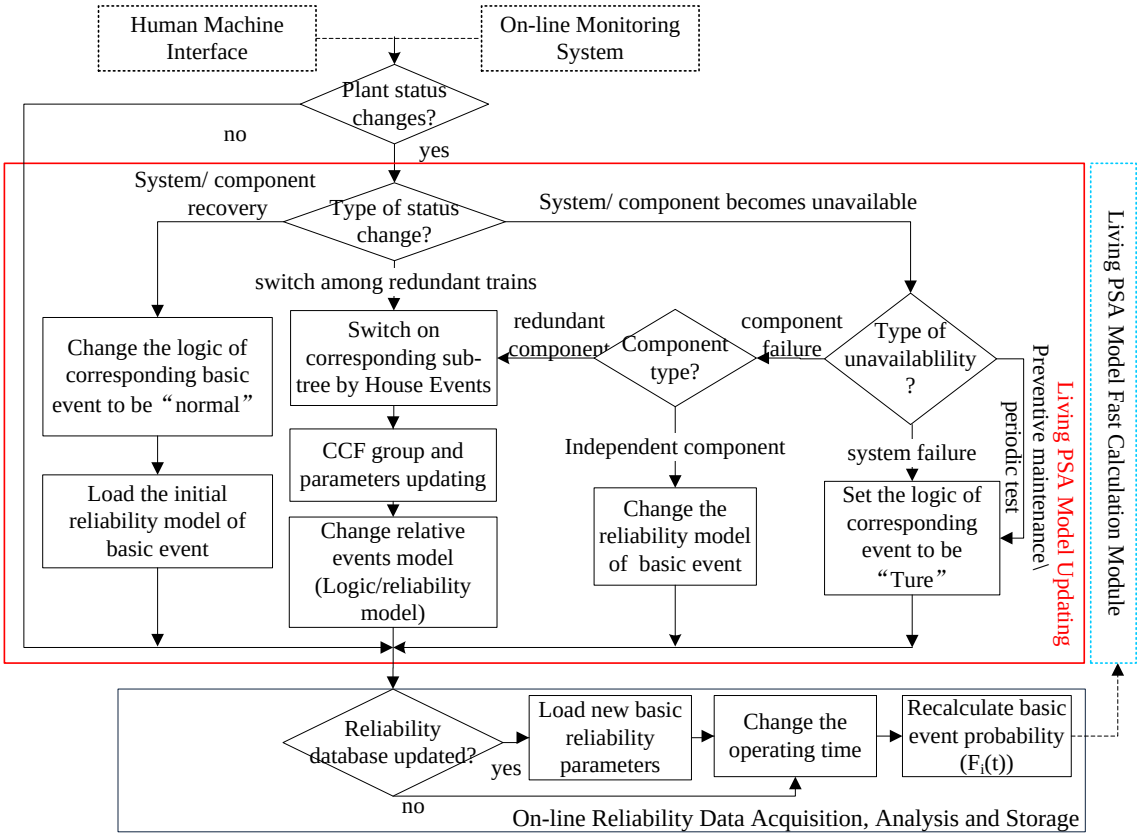

Fig.5 Procedure of Living PSA updating module.

The information for plant status changes comes from the on-line monitoring system or the human-machine interface of the on-line risk monitor. The on-line risk monitor reassesses the plant risk mainly in two situations. One is when there is a status change, and it is necessary to update both the PSA models and parameters correspondingly, by referring to the 'yes' branch of 'Plant status changes?' in Fig. 5. The other is periodic reassessment, such as one recalculation per hour, when only the parameters should be updated but not PSA models, by referring to the 'no' branch of 'Plant status changes?'. The Living PSA updating module covers mainly the former situation.

There are three kinds of plant status changes during plant operation: (i) Subsystem/component which has failed returns to work; (ii) Subsystem/component becomes unavailable; and (iii) Switch among redundant trains. The related updating objects for each kind of status change are illustrated in Fig.5.

There are several key points which are needed to explain in Fig.5 are summarized as below:

(i) For the reliability models for events, including not only the events for independent component failures but also the ones referring to the primary failures of dependent components, it should be determined in accordance with Table 1 and Table 2;

(ii) For redundant components, both CCF parameters and sequential relations should be updated once a component fails or component should be rearranged, and

3) The CCF parameters updating should abide by the formulas in Table 4, and the updating process should be as described in 3.2.

The updated PSA models and reliability models will be transferred to the On-line Reliability Data Acquisition, Analysis and Storage module to update the reliability parameters used in the models, and then the models with parameters will be finally transferred to the fast calculation module for qualitative and quantitative assessment.

4 Conclusion

In order to develop an on-line risk monitor system, the methodological research on Living PSA modeling and updating was conducted as will be implemented in the authors' on-line risk monitor system. The first step of this research is the demands analysis, referring to the updating objects, updating level and updating manner. Accordingly, research has been carried out on three types of PSA modeling and updating, which are (i) Independent failure modeling and updating, (ii) CCF modeling and updating, and (iii) Sequence-dependent failure modeling and updating. Also, the procedure for Living PSA updating is proposed.

By employing Living PSA modeling and updating methodology as proposed in this research for developing an on-line risk monitor, any risk related plant status changes can be reflected in the PSA models automatically, and also the time dependent reliability of components can be considered. Thus, by the On-line Risk Monitor, not only the instantaneous risk at the current moment can be assessed, but also the future risk at any time concerned can be predicted.

There remains further subjects in the authors' research which will face many challenges, and they are:

(i) The failures of components in preventive maintenance and periodic testing are taken as true events in this research. It will lead to conservative results of risk. Further research should be carried out according to the real engineering situation.

(ii) The component failures in a CCF group may be independent failures or caused by common cause. This research at current stage only considered about the CCF updating when independent failures occurred. It is necessary to pay more effort to the updating in condition that components in CCF group fail due to common causes.

(iii) Enumerating modeling for sequence dependent failures could be very exhausting work for PSA experts and may lead to mistakes in PSA models. So more effort should be paid to establish a universal method to model and update this kind of failure automatically.

(iv)Verification and validation of the proposed method by applying for appropriate sample systems is necessary.

Acknowledgement

This study is supported by the National Science and Technology Major Project of China *'Research on Living PSA and On-line Risk Monitor and Management of Nuclear Power Plant'* (2014ZX06004-003).

References

[1] IAEA. IAEA-TECDOC-1106.: Living probabilistic safety assessment (LPSA), Vienna: International Atomic Energy Agency, 1999.

[2] Nuclear Energy Agency, Committee on the Safety of Nuclear Installations: RISK MONITORS: The State of Art in their Development and Use at Nuclear Power Plants: NEA/CSNI/R(2004)20, Nuclear Energy Agency, Committee on the Safety of Nuclear Installations, 2004.

[3] KAPLAN, S., and GARRICK, B.J.: On the quantitative definition of risk. Risk Analysis, Vol. 1, No. 1, 1981.

[4] ZHANG Min, ZHANG Zhijian, and MA Yingfei: Conditional Failure Probability Evaluating for NPPs Risk Monitoring. Proceedings of 2014 ANS Winter Meeting and Nuclear Technology Expo, California, American Nuclear Society, 2014.

[5] JIN Xing, HONG Yanji, and DU Hongmei: Reliability analysis methodology for Common Cause Failure System, Beijing: National Defense Industry Press, 2008: 1-38, 98-111.

[6] NRC.NUREG/CR-6268.: Guidelines on Modeling Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, Washington: U.S. Nuclear Regulatory Commission, 2007.

[7] CHEN Sijuan: Common Cause Failure Analysis for Cooling Water System of AP1000, Harbin Engineering University, 2013.

[8] WALKER, M., and PAPADOPOULOS, Y.: Qualitative Temporal Analysis: Towards a Full Implementation of the Fault Tree Handbook. Control Engineering Practice (2008), doi:10.1016/j.conengprac.2008.10.003