Research on reliability models of HTR-PM reactor protection system

GUO Chao[1], ZHOU Shuqiao[1], and LI Duo[1]

1. *Institute of Nuclear and New Energy Technology, Collaborative Innovation Centre of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Tsinghua University, Beijing 100084, China (guochao@tsinghua.edu.cn)*

Abstract: Nuclear safety is a critical issue for a nuclear power plant (NPP), while the Reactor Protection System (RPS) plays a significant role for the safety operation of an NPP. Digital RPSs have been widely used in newly-built and upgraded NPPs because of the advantages over the analogue ones. The reliability analysis of digital RPS, which is a research hotspot in the I&C field of NPP, is required by regulation authorities, development organizations, and the final users. The RPS of High Temperature Gas-Cooled Reactor Pebble bed Module (HTR-PM) is the first self-developed digital RPS to be operated commercially in China. In this paper, this digital RPS system is modelled with both static and dynamic methods. Firstly, the failure modes and effects analysis and the fault tree analysis is performed and special attention is focused on the "2-out-of-4" and the bypassed logic. Furthermore, a dynamic modelling method, the Markov chain theory is adopted. All states and corresponding dynamic transition processes are analyzed especially the degradation process from 2-out-of-4 to 2-out-of-3. Moreover, the interval of surveillance test was optimized based on this Markov model.

Keywords: reliability model; reactor protection system; fault tree analysis; Markov model

1 Introduction

Reactor protection system (RPS) is the most important part of the instrument and control (I&C) system of an nuclear power plant (NPP) as it plays a significant role for the safe, reliable and stable operation of the NPP. Digital RPSs have been adopted widely in recent decades because of the advantages compared with analog ones such as improved sampling precision, better computation ability for complex algorithm, enhanced anti-interference ability, and so on[1]. While the application of digital technology also brings challenges to the design of RPS, such as more complicated system structure and potential risk of common cause failure caused by software [2]. How to evaluate the reliability of digital RPS is one of the hot topics in NPP I&C field. [3, 4]

In 2010, the Nuclear Regulatory Commission (NRC) of the United States put forward a Research Plan for Digital Instrumentation and Control, which includes researches on the reliability evaluation of the digital I&C system. [5] Many system reliability evaluation methods such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Markov theory have been applied to the reliability evaluation of I&C system. [6-10]

The development of High Temperature Gas-Cooled Reactor-Pebble bed Module (HTR-PM) NPP is one of the key projects in the National Science & Technology Major Project for the Eleventh and the Twelfth Five-Year Plan of China. [11, 12] The digital RPS is one of the key technologies of HTR-PM[13]. HTR-PM RPS is a special system developed for the protection function and performance requirement of HTR-PM. The activities of design, development and manufacture are all performed domestically in China. In this paper, the system reliability of HTR-PM RPS is studied with both the fault tree model and the Markov model. The fault tree model is based on both FMEA results of all RPS devices and the relationship between them. The fault tree model is a static model and cannot cover the changes between different RPS operating states, therefore it gives a conservative reliability evaluation. The Markov model considers all devices in one division of RPS as its analysis unit and takes into account multiple RPS operating states, including periodic test and equipment maintenance. The calculated reliability is improved since the periodic tests and prevention maintenance is reflected in the Markov model.

Received date: May 23, 2017
(Revised date: September 18, 2017)

The remaining sections of this paper are organized as follows. Section 2 introduces the architecture of HTR-PM RPS. Then the fault tree model and Markov model for RPS are proposed and discussed in Section 3 and Section 4, respectively. Section 5 gives some conclusions of this paper.

2 Architecture of HTR-PM RPS

HTR-PM RPS has four independent and interrelated logic divisions as shown in Fig. 1. Each logic division includes monitoring equipment, signal isolating devices, signal processing devices, coincidence logic devices, and trip breakers. To achieve diverse protection actions, the redundant protection variables of each postulated initiating event are divided into two groups, *i.e.* group x and group y, and separated signal processing devices and coincidence logic devices are implemented to deal with signals of groups x and y respectively.

The separated devices compose independent subsystems x and y. These two subsystems have the identical hardware devices but different software. They sample different protection variables, implement different algorithms, and execute reactor protection actions independently, which reduces the possibility of potential software common cause failure. For example, as a representative postulated initiating event, the earthquake arises the abnormal changes of both the nuclear power and the hot helium temperature, and these two protection parameters are dealt with groups x and y respectively to guarantee that this division works well even when devices of one group fail to send the trip signal out.

The monitoring equipment is the sensors/transmitters, including signal processing circuits of nuclear instrumentation system and process parameters instrumentation system. The outputs of sensors/transmitters are isolated and sent to signal processing devices x and y independently. Signal processing devices sample protection signals, get protection variables, compare them with corresponding set points and output part-trip. Coincidence logic x and coincidence logic y receive part-trip warnings from four signal processing devices in the same sub system, carry out 2/4 logic processing for every protection variable warnings and generate a scram initiation. Any scram initiation would make coincidence logic device open relay contacts to output logic trip signals. The relay contacts of coincidence logic x and coincidence logic y are hardware wired as OR logic, which is the division trip outputs. Each division trip is used to control two trip breakers to disconnect their outputs, for example, division A controls the breakers A1 and A2. All outputs of eight trip breakers are hardware wired to implement the 2/4 logic processing, *i.e.* the final reactor trip, which is shown in Fig. 1.

3 Fault tree model

The mutual effects among devices of HTR-PM RPS are complex. Fault tree model is a common and effective method to analyze the overall RPS reliability, and Failure Modes and Effects Analysis (FMEA) are the basis to develop a fault tree model.

3.1 FMEA of HTR-PM RPS

The function of FMEA is considering the potential failure mode of each device and its corresponding effect on RPS. Preliminary FMEA is mainly focused on the analysis of reactor-trip function of RPS. Without loss of generality, the FMEA scope is limited to the devices of division A, together with trip breakers A1 and A2, which are shown in Fig. 1.

Since the output signals of each device directly reflect the device's status, this paper defines the failure modes of output signal as the failure mode of referred device. It should be emphasized that every device in division A may output more than one signal, and each signal may have two or more failure modes. For example, a coincidence logic x outputs two relay contact signals and each of them corresponds to two kinds of failure modes: Frozen signal output and Faulted signal output. Therefore a coincidence logic x has four kinds of failure mode in total.

Based on above information, failure modes of each device are identified and listed in detail, such as possible failure mechanisms, local effects, and designed provisions. An FMEA example of a coincidence logic x is shown in Table 1.

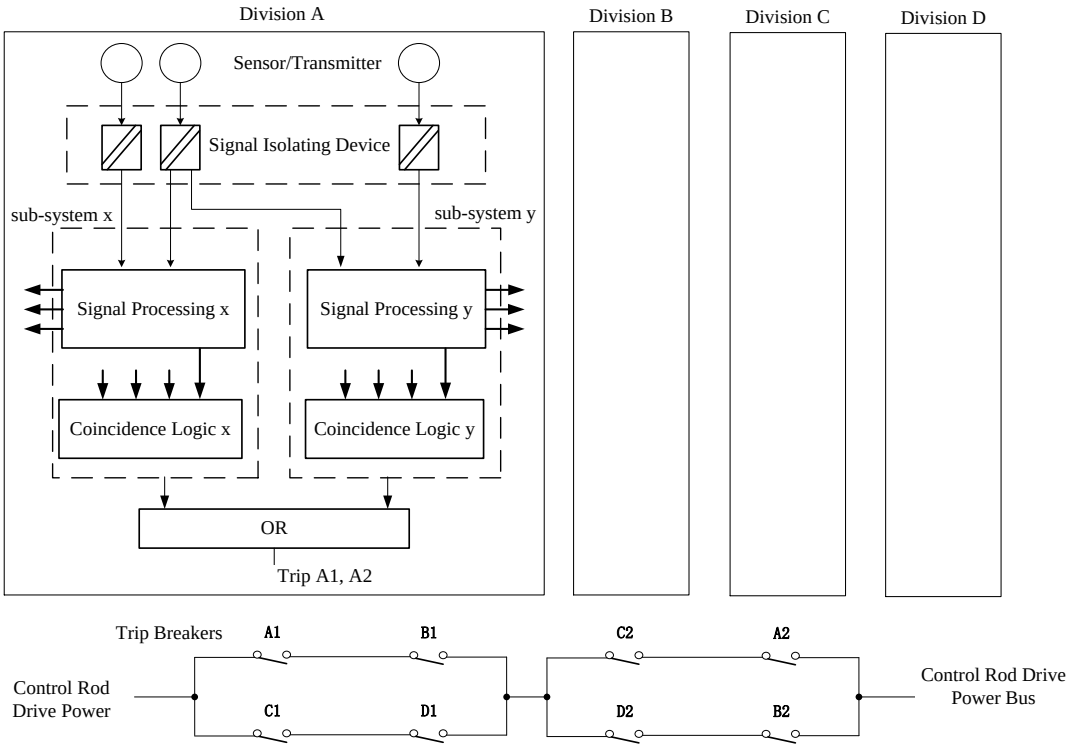

Fig.1 Architecture of HTR-PM RPS.

Table 1 FMEA results of a coincidence logic x

No.	Output Signal	Failure Mode	Failure Mechanism	Local Effect	Method of Failure Detection	Provision	Effect on System
1	Logic trip signal 1	Frozen signal output	Failure of input module Failure of relay contact Failure of data-processing software	Sub-system x cannot trigger Breaker A1.	Periodic test Software check by system surveillance station	Triggering signals of both sub-system x and sub-system y in one division are sent to Trip-Breaker Actuation Device after "OR" calculation	No effect
2		Faulted signal output	Failure of input module Failure of relay contact Failure of data-processing software	Trip Breaker A1 is incorrectly triggered.	Software check by system surveillance station	2-out-of-4 redundant structure of trip breakers	No effect
3	Logic trip signal 2	Frozen signal output	Failure of input module Failure of relay contact Failure of data-processing software	Sub-system x cannot trigger Breaker A2.	Periodic test Software check by system surveillance station	Triggering signals of both sub-system x and sub-system y in one division are sent to Trip-Breaker Actuation Device after "OR" calculation	No effect
4		Faulted signal output	Failure of input module Failure of relay contact Failure of data-processing software	Trip Breaker A2 is incorrectly triggered.	Software check by system surveillance station	2-out-of-4 redundant structure of trip breakers	No effect

3.2 Development of fault tree model

According to the reliability analysis of HTR-PM RPS, there are two kinds of failure mode for reactor trips, *i.e*. failure to trip and spurious trip, and failure to trip is chose as the top event to develop a fault tree in this paper as this failure mode is related to the safety operation of the power plant.

HTR-PM project sets several protection parameters to actuate reactor trips, and any one would actuate

reactor trips when its value went over the set point. Therefore the RPS failure to trip is caused by events such as high hot end temperature failure to trip, high nuclear power failure to trip, high humidity failure to trip, and so on. The top events is the OR results of all these events, which is shown in Fig. 2. Any event that causes the top event should be analyzed and several similar sub-trees would be developed. One sub-tree developed from the event of high nuclear power failure to trip is shown as follows.

The direct cause of high nuclear power failure to trip is trip breakers failures. HTR-PM has eight trip breakers and their outputs are hard-wired connected to perform 2-out-of-4 logic voting. When any two trip breakers belonging to two different divisions receive actuating command, the breakers outputs will be opened, thus the power supply of control rods will be cut down, and an emergency trip will be actuated. As shown in Fig. 2, the event of high nuclear power failure to trip is decomposed continually to such events as trip breaker A1 failure to open and trip breaker B1 failure to open. The AND or OR logic voting events of trip breakers are developed according to their hard-wired connection shown in Fig. 1. Failure to open of a trip breaker is caused by two events: breaker failure to receive actuation command and breaker outputs frozen. The former cause should be analyzed continually to develop a sub-tree, while the latter cause becomes a leaf in the fault tree, and the analyzing is ended with the reliability of trip breaker itself.

Further analysis of the breaker failure to receive actuation command can continually build the next layer of the fault tree branch, and step-by-step analysis of the trip breaker drive device failure, the coincidence logic device failure.

The coincidence logic device is the focus and difficulty of fault tree development. To construct tree branches under a coincidence logic device, the potential causes include four aspects:

(1) The coincidence logic device itself fails: the device rejects to output trip signals;
(2) This division is bypassed by mistake: the output trip signals are latched by the spurious bypass signal;
(3) Input signal errors: if at least three divisions have no scram signals, the coincidence logic device fails to output trip signal;
(4) Other divisions are bypassed by mistake: if this coincidence logic device matches the bypass signal of the other divisions, the coincidence logic processing will be degraded from 2/4 to 2/3 and the coincidence logic device fails to output trip signal;

Continually with the above aspect 3, the reason why a signal processing device does not output a "nuclear power high" scram signal may include: the internal error of data packet sent from the signal processing device to the coincidence logic device, the accuracy variation of the nuclear power signal output by the isolation device, and the accuracy variation of the nuclear power sensor. All of them perform as the leaf nodes of the fault tree.

Continually with the above aspect 4, if division B sent by passed signals by mistake, coincidence logic devices in division A, C and D would degrade their coincidence logic from 2/4 to 2/3 and fail to output trip signals. On the other hand, if the coincidence logic device in division A received a spurious bypassed signal, the signal would be sent from division B, C or D. This part of the fault tree branch of the expansion is shown in Fig. 3.

The fault tree of HTR-PM RPS is built based on the above analysis in this section and related qualitative analysis like the minimal cut set analysis can be further performed to investigate the vulnerabilities of the system. It should be noted that the trip breakers, sensors/transmitters, signal isolation devices, and bypass logic devices are the weak parts of the system according to minimal cut set analysis. Special attention should be paid to the bypass logic device of these four devices. The bypass logic device is only used during maintenance and periodic test of certain division. If this device fails and the bypass signal is incorrectly issued, the corresponding division will fail to output the trip signals, thus increasing the probability of failure to trip, and this conclusion is consistent with the previous analysis of this section.

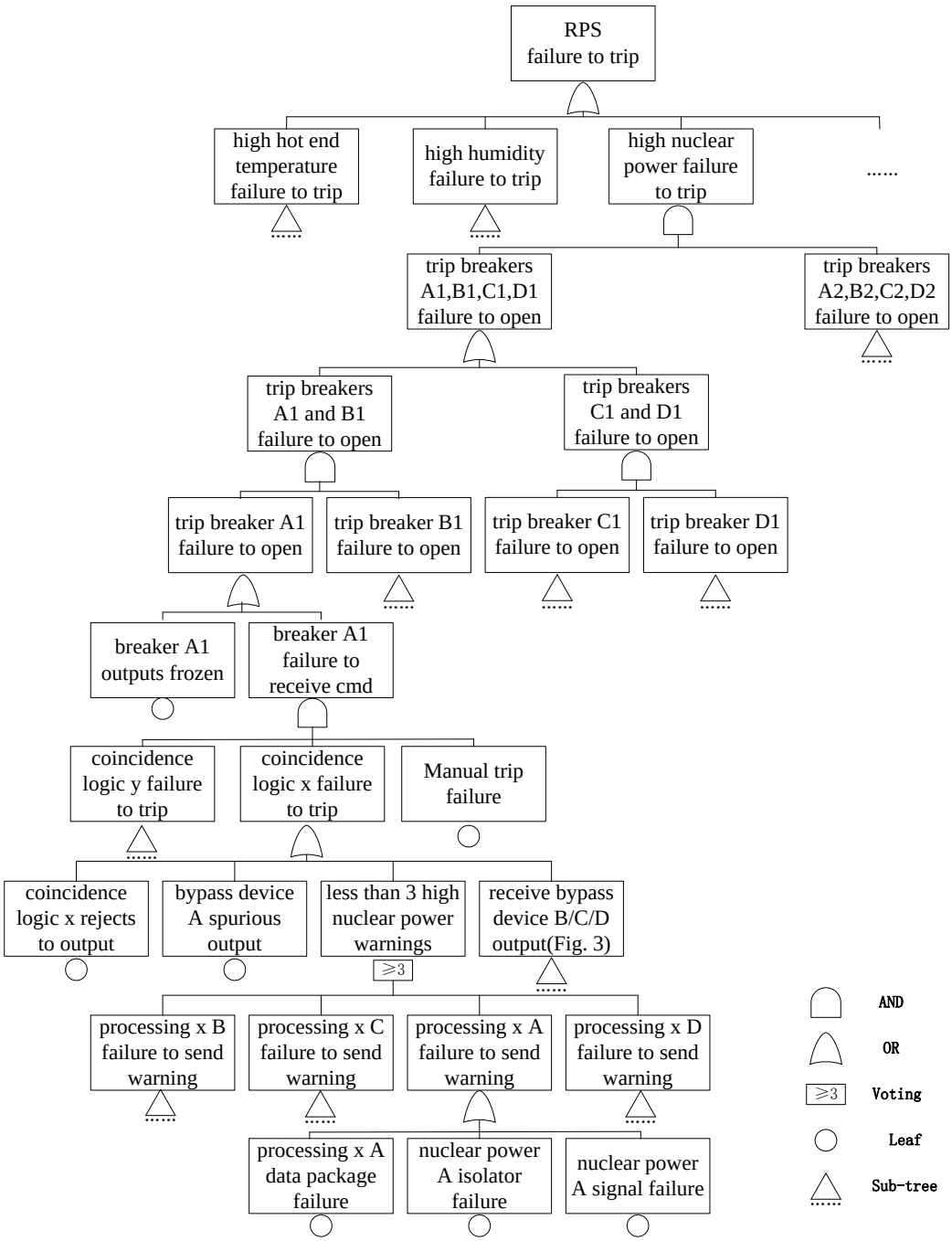

Fig.2 Frame of RPS fault tree.

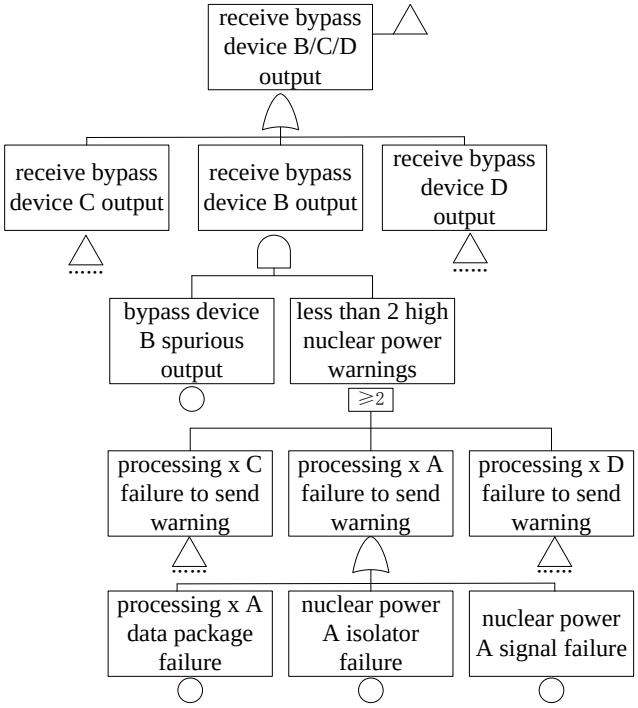

Fig.3 Degraded coincidence logic device in the fault tree model.

4 Markov model

Fault tree analysis can clearly demonstrate the relationships between all devices of the RPS in HTR-PM. The reliability of the whole RPS can be calculated based on the reliability data of all the devices, such as MTBF of leaf nodes in the fault tree. However, the relationships between RPS devices will be changed between different operating states. In order to maintain the high reliability, RPS periodic tests are required during system operation. In the test states, all equipment in one division of the RPS are changed to be off-line by setting maintenance bypass, and all equipment are thoroughly tested using a dedicated test instrument. If some faults are found, further reparations or replacements of the faulty parts are required. Fault tree model is a static model, which is difficult to describe the dynamics of the changing states. In this section, a reliability model of HTR-PM RPS is studied and developed based on Markov chain theory. The Markov model takes into account multiple RPS operating states, including periodic test and equipment maintenance.

4.1 Reliability calculation based on static model

Based on fault tree model, the reliability of each division of RPS can be determined and their failure rates can be obtained. We assume that the failure rates of four divisions are constant and their values are λ_1, λ_2, λ_3, and λ_4. Also, it is assumed that the failures of each division of RPS occur independently and with an exponential distribution.

If there are two divisions fail, the RPS will trigger the reactor trip signal to shut down the reactor. In other words, the RPS can function normally if and only if there are no less than three divisions are in normal condition. Suppose the reliabilities of four divisions at time t can be denoted as $R_1(t)$, $R_2(t)$, $R_3(t)$, and $R_4(t)$. Based on the relationship between the failure rate and reliability, we have:

$$R_i(t) = e^{-\lambda_i t}, i \in \{1,2,3,4\}. \tag{1}$$

Then the reliability of the entire RPS can be calculated as Eq. (2). The previous four parts in Eq. (2) denotes the probability that three of four divisions work normally. The last part in Eq. (2) denotes the probability that all four divisions work normally.

$$\begin{aligned} R_{sys}(t) = {} & R_1(t)R_2(t)R_3(t)\left(1-R_4(t)\right) \\ & + R_1(t)R_2(t)R_4(t)\left(1-R_3(t)\right) \\ & + R_1(t)R_3(t)R_4(t)\left(1-R_2(t)\right) \\ & + R_2(t)R_3(t)R_4(t)\left(1-R_1(t)\right) \\ & + R_1(t)R_2(t)R_3(t)R_4(t) \end{aligned} \tag{2}$$

By substituting Eq. (1) to Eq. (2) we can obtain the system's reliability as Eq. (3).

$$R_{sys}(t) = e^{-(\lambda_1+\lambda_2+\lambda_3)t} + e^{-(\lambda_1+\lambda_2+\lambda_4)t} + e^{-(\lambda_1+\lambda_3+\lambda_4)t} + e^{-(\lambda_2+\lambda_3+\lambda_4)t} - 3e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} \tag{3}$$

Moreover, based on the algebraic relationship between failure rate and reliability, the failure rate of the entire system can be calculated as Eq. (4). In Eq. (4), the item d$R_{sys}(t)$/dt is still a function of time t.

$$\lambda_{sys1}(t) = -\frac{1}{R_{sys}(t)} \cdot \frac{dR_{sys}(t)}{dt} \tag{4}$$

4.2 Development of Markov model

Based on the periodic tests additional maintenances can be done to RPS system and then its reliability will be improved. The maintenance rates of the four divisions are denoted as μ_1, μ_2, μ_3 and μ_4. It is also assumed that the maintenance rate μ_i is determined by the periodic tests interval (the time duration between two tests) T_i and the repairing time T_{ri} (the time duration for reparation or replacement):

$$\mu_i = \frac{1}{T_i + T_{ri}}, i \in Z, i \in [1,4]. \tag{5}$$

With a periodic test interval of T_i h, the average time from failure to the time that the failure is detected is about T_i/2 h. Thus it is important to note that the maintenance rate μ_i calculated by Eq. (5) is prone to be more conservative than that of the actual situation.

Suppose "1" represents the state that a division works normally and "0" represents the state that a division fails. The working states of RPS and their relationships can be described as Fig. 4. As the divisions are independent of each other and the assumptions that the failing and the repairing processes are with the exponential distributions, the states in Fig. 4 can be further analyzed based on Markov chain theory.

For each state in Fig. 4, the variation of its probability can be described by deducting the outputting probability from the inputting probability. Suppose the probability of the i-th ($i \in Z, i \in [0,10]$) state at time t is denoted as $P_i(t)$, the relationships between the probabilities and the failure/maintenance rates are obtained as Eq. (7). Each equation in Eq. (7) represents the variation of the reliability of a state in Fig. 4.

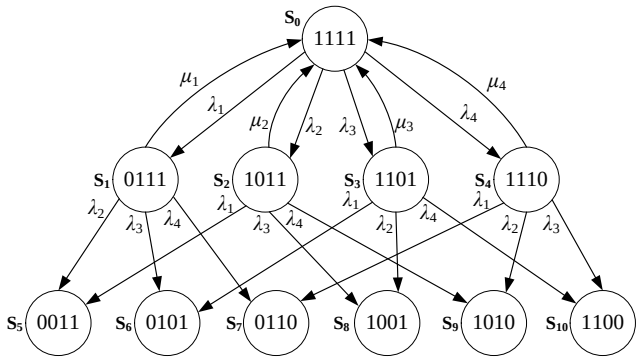

Fig.4 Markov chain model for the HTR-PM RPS.

$$\mathbf{M} = \begin{bmatrix}
-(\lambda_1+\lambda_2+\lambda_3+\lambda_4) & \mu_1 & \mu_2 & \mu_3 & \mu_4 & 0 & 0 & 0 & 0 & 0 & 0 \\
\lambda_1 & -(\lambda_2+\lambda_3+\lambda_4+\mu_1) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\lambda_2 & 0 & -(\lambda_1+\lambda_3+\lambda_4+\mu_2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\lambda_3 & 0 & 0 & -(\lambda_1+\lambda_2+\lambda_4+\mu_3) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\lambda_4 & 0 & 0 & 0 & -(\lambda_1+\lambda_2+\lambda_3+\mu_4) & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \lambda_2 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \lambda_3 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \lambda_4 & 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \lambda_3 & \lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \lambda_4 & 0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \lambda_4 & \lambda_3 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \tag{6}$$

$$\begin{cases}
\frac{dP_0(t)}{dt} = -(\lambda_1+\lambda_2+\lambda_3+\lambda_4)P_0(t) + \mu_1 P_1(t) + \mu_2 P_2(t) + \mu_3 P_3(t) + \mu_4 P_4(t) \\
\frac{dP_1(t)}{dt} = -(\lambda_2+\lambda_3+\lambda_4+\mu_1)P_1(t) + \lambda_1 P_0(t) \\
\frac{dP_2(t)}{dt} = -(\lambda_1+\lambda_3+\lambda_4+\mu_2)P_2(t) + \lambda_2 P_0(t) \\
\frac{dP_3(t)}{dt} = -(\lambda_1+\lambda_2+\lambda_4+\mu_3)P_3(t) + \lambda_3 P_0(t) \\
\frac{dP_4(t)}{dt} = -(\lambda_1+\lambda_2+\lambda_3+\mu_4)P_4(t) + \lambda_4 P_0(t) \\
\frac{dP_5(t)}{dt} = \lambda_2 P_1(t) + \lambda_1 P_2(t) \\
\frac{dP_6(t)}{dt} = \lambda_3 P_1(t) + \lambda_1 P_3(t) \\
\frac{dP_7(t)}{dt} = \lambda_4 P_1(t) + \lambda_1 P_4(t) \\
\frac{dP_8(t)}{dt} = \lambda_3 P_2(t) + \lambda_2 P_3(t) \\
\frac{dP_9(t)}{dt} = \lambda_4 P_2(t) + \lambda_2 P_4(t) \\
\frac{dP_{10}(t)}{dt} = \lambda_4 P_3(t) + \lambda_3 P_4(t)
\end{cases} \tag{7}$$

The coefficient matrix of the equations in Eq. (7) can be represented as Eq. (6) and then Eq. (7) can be denoted as Eq. (8), where

$$\mathbf{P}(t)=\begin{bmatrix}P_1(t) & P_2(t) & \cdots & P_{10}(t)\end{bmatrix}^T.$$
$$\frac{d\mathbf{P}(t)}{dt}=\mathbf{M}\mathbf{P}(t). \quad (8)$$

Supposing that the initial state is **P**(0), the solution of Eq. (8) can be obtained as follows:

$$\mathbf{P}(t)=e^{\mathbf{M}t}\mathbf{P}(0). \quad (9)$$

In our RPS, $\mathbf{P}(0)=\begin{bmatrix}1&0&0&0&0&0&0&0&0&0\end{bmatrix}^T$ is satisfied.

We further define $P_{\text{fail}}(t)$ as the probability that the entire RPS is in failure state at time *t*. Then, according to the definition of the failure rate, the rate of the total failure rate of the RPS can be calculated as follows:

$$\lambda_{sys2}(t)=\frac{\left(dP_{fail}(t)/dt\right)^+}{1-P_{fail}}, \quad (10)$$

where, $\left(dP_{fail}(t)/dt\right)^+$ denotes the rate that the system is going to enter into the fail states at time *t*. According to Fig. 4, we have:

$$\begin{aligned}\left(dP_{fail}(t)/dt\right)^+ &= (\lambda_2+\lambda_3+\lambda_4)P_1(t)\\ &+(\lambda_1+\lambda_3+\lambda_4)P_2(t)\\ &+(\lambda_1+\lambda_2+\lambda_4)P_3(t)\\ &+(\lambda_1+\lambda_2+\lambda_3)P_4(t).\end{aligned} \quad (11)$$

Also, the value $P_{\text{fail}}(t)$ can be calculated as:

$$\begin{aligned}P_{fail}(t) &= P_5(t)+P_6(t)+P_7(t)\\ &+P_8(t)+P_9(t)+P_{10}(t)\end{aligned} \quad (12)$$

By substituting Eq. (9) in Eq. (11) and Eq. (12), then the rate of the total failure of RPS can be obtained by Eq. (10). Compared to $\lambda_{sys1}(t)$ in Eq. (4), the effects of the periodic test and reparation are reflected in Eq. (10).

4.3 Comparison between static model and Markov model

To compare the static model and Markov model, the parameters in Table 2 are used in the calculation. The λ_1~λ_4 in Table 2 are the failure rates of division 1~4 per an hour. The calculation results are shown in Fig. 5.

Base on the results in Fig. 5, the conclusions can be drawn as follows:

(1) The two models (*i.e*. the static model and Markov model) can match each other perfectly when the effects of reparation are not considered. In Fig. 5, the curve of 'λ_{sys1}' is the RPS's failure rate calculated by the static model. The curve 'λ_{sys2} with μ_i=0' represents the failure of the whole RPS calculated by Markov model when the RPS is running without any periodic tests and related maintenance. Thus, the related test intervals are mathematically infinite and then μ_1, μ_2, μ_3 and μ_4 are all 0. It is revealed by the two perfectly matched curves that Markov model based on the Markov chain theory can also describe the special case when the RPS is without any prevention maintenance.

(2) Compared to the static model, the improving performance of the periodic test and related prevention maintenance can be reflected in Markov model. In Fig. 5, 'μ_i=1/1440' represents that each division is tested with an interval of 1440 hours (*i.e*. 2 months). By comparing the two curves marked by 'λ_{sys1}' and 'λ_{sys2} with μ_i=1/1440', the effects of periodic tests and the related reparation are shown apparently. When the interval of the periodic test is chosen to be 2 months, the system failure rate is much lower and keeps in a stable level.

(3) The further analysis is focused on the relationship between the failure rate and the periodic tests intervals. In Fig. 6, three curves with 'μ_i=1/720, 1/1440, 1/2160' (*i.e*. 1, 2, 3 months) are shown together. The conclusion is that the shorter the periodic tests interval is adopted, the lower system failure rate can be achieved.

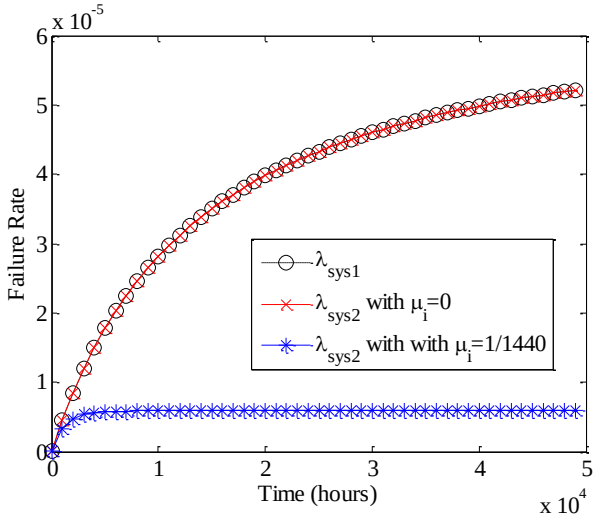

Fig.5 Calculation results by the static model and Markov model.

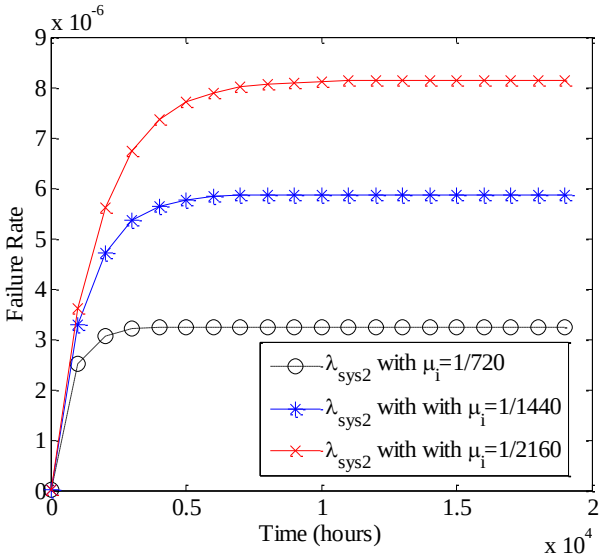

Fig.6 Reliability versus different test periods.

Table 2 Key parameters for reliability calculation

Parameter	Value	Parameter	Value
λ_1	1/50000	λ_4	1/50000
λ_2	1/50000	$T_{ri}(i=1,2,3,4)$	24 hours
λ_3	1/50000	–	–

5 Conclusion

This paper outlines the research of HTR-PM RPS system reliability. The fault tree model and Markov model are studied and discussed. The fault tree model can clarify the detail relationship inside RPS and give a conservative reliability evaluation. The vulnerabilities of the RPS system can be qualitatively analyzed using this static method. In particular, the trip breakers, sensors/transmitters, signal isolation devices, and the bypass logic devices are regarded as the weak points of the HTR-PM RPS according to minimal cut analysis. The Markov model takes into account multiple PRS operating states and improves the reliability calculation. The interval of surveillance test of the HTR-PM RPS are optimized based on the Markov model in this paper.

Acknowledgement

This work has been supported by the National Science and Technology Major Project (Grant No. ZX06901) and Tsinghua University Initiative

Scientific Research Program (Grant Nos. 20151080380, 20151080382).

References

[1] LI, D., XIONG, H., and GUO, C.: "Design and Development of HTR-PM Reactor Protection System," 2013 21st International Conference on Nuclear Engineering, 2013, Chengdu, China.

[2] U.S. Nuclear Regulatory Commission, "Review of New Digital Instrumentation and Control Probabilistic Risk Assessments," 2008.

[3] CHEOL, K.I.M.M.: "Reliability analysis of digital I&C systems at KAERI," Nuclear Safety and Simulation, 2012, 3(4): 276-280.

[4] GUO, C., LI, D., and XIONG, H.: "Preliminary Study on Reliability Analysis of Safety I&C System in NPP," 2011 2nd International Congress on Computer Applications and Computational Science, Bali, Indonesia, 2012.

[5] U.S. Nuclear Regulatory Commission, "NRC Digital System Research Plan FY 2010-FY 2014," 2010.

[6] MUTA, H., and MURAMATSU, K.: "Quantitative modeling of digital reactor protection system using Markov state-transition model," Journal of Nuclear Science and Technology, 2014, 51(9): 1073-1086.

[7] ALDMIR, T., STOVSKY, M. P., and KIRSCHENBAUM, J., *et al*.: "Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments," 2009 6th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, Knoxville, U.S.A., 2007.

[8] U.S. Nuclear Regulatory Commission, "NUREG/CR-6997 Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods," 2009.

[9] GUO, C., LI, D., and XIONG, H.: "Development and Analysis of Fault Tree Model of HTR-PM Reactor Protection System," Atomic Energy Science and Technology, 2013, 47(11): 2069-2077.

[10] U.S. Nuclear Regulatory Commission, "NUREG/CR-5500 Reliability Study: Babcock & Wilcox Reactor Protection System, 1984-1998," 2001.

[11] ZHANG, Z., WU, Z., and WANG, D., *et al*.: "Current status and technical description of Chinese 2×250 MWth HTR-PM demonstration plant," Nuclear Engineering and Design Journal, 2009, 239(7): 1212-1219.

[12] ZHANG, Z., DONG, Y., and LI, F., *et al*.: "The Shandong Shidao Bay 200 MWe High-Temperature Gas-Cooled Reactor Pebble-Bed Module (HTR-PM) Demonstration Power Plant: An Engineering and Technological Innovation," Engineering, 2016, 2(1): 112-118.

[13] LI, D., GUO, C., and XIONG, H.: "Development and Reliability Analysis of HTR-PM RPS," 2014 7th International Topical Meeting on High Temperature Reactor Technology, Weihai, China, 2014.