Reliability analysis of Digital Pressurizer Water Level Control System in NPP based on Boolean logic Driven Markov Process

Yi-jing Mao[a], Xi-yu Chen[a, b], Shi-liang Zhou[a,b*], Tong-yu Xu[a], Irsa Rasheed[a]
[a]School of Nuclear Science and Engineering, North China Electric Power University, Beijing, China
[b]Beijing Key Laboratory of Passive Safety Technology for Nuclear Energy, Beijing, China

Abstract: Digital instrumentation and control systems have been widely used in nuclear power plants (NPPs). Being central nervous system of NPPs, its reliability is one of the critical factors for safe and reliable operation of NPP. Pressurizer is the key equipment for the primary circuit pressure control of NPP, its digital control system also plays a decisive role in the safe operation of NPP. Boolean logic Driven Markov Process (BDMP) is used to dynamic reliability analysis of Digital Pressurizer Water Level Control System (PWLCS). Based on the structure and control logic of PWLCS, the BDMP model has been constructed by KB3 software, and quantitatively analyze is accomplished using YAMS to calculate the cumulative failure probability. The mean time to failure of the equipment changes with the growth of the simulation times which can also be obtained.

Keywords: BDMP, Reliability analysis, Pressurizer, water level control, digital control system

1. INTRODUCTION

Recently, Digital Instrument and Control Systems (DICS) have been extensively used in NPP for control, monitoring and protection purposes. A significant transformation from the analog to digital-based systems has occurred because of the potential advantages of digital systems including better calibration, accuracy, higher data handling capability and computational capabilities. The implementation of DICS is improving methods and techniques to achieve the desired reliabilities.

However, DICS also have some limitations, and a malfunction can lead to severe issues. Therefore, for the reliability assessment of them, various methods have been proposed including software-based models and hardware-based models. These formal methods including deterministic models, event sequence diagrams, software metric-based methods, test-based methods and fault tree diagrams etc. have their advantages and disadvantages, demanding more research in the field of reliability analysis of digital I&C methods.

For the reliability and safety analysis of the digital system, the BDMP is a powerful modeling method [1]. BDMP seems very close to Fault Trees Analysis as their basic algorithm is the same, but connecting the Markov process at each node of the Fault Tree. Compared with Fault Tree Analysis, BDMP has a unique set of triggers, which can represent the time series relation between two nodes or two subsystems. Moreover, BDMP's efficient mathematical characteristics can reduce optimization problems and computational time for calculations. In comparison with traditional analysis method, BDMP has two main advantages: it can easily represent complex dynamic models; it has powerful and flexible mathematical characteristics [2].

Pressurizer of nuclear power plants controls pressure and provides overpressure protection. One of its significant roles is in providing a continuous water level monitoring system for the Nuclear Power Plant. The level control system of pressurizer is a decisive part of pressure controlling, which ensures the pressurizer can control the pressure of the primary loop and responds immediately in case of accidents.

BDMP is used for modeling the pressurizer of nuclear power plants and quantitative analysis is made via YAMS.

Shiliang-Zhou zhoushiliang@ncepu.edu.cn

2. THE DEFINITION AND CHARACTERS OF BDMP

BDMP is an advanced method for the reliability analysis, which associates Fault Tree Analysis with Markov process at every leaf of the fault tree. It improves the accuracy and precision of the reliability analysis system along with reducing the computational time for calculations. Compared with Fault Tree Analysis, BDMP has three advantages:

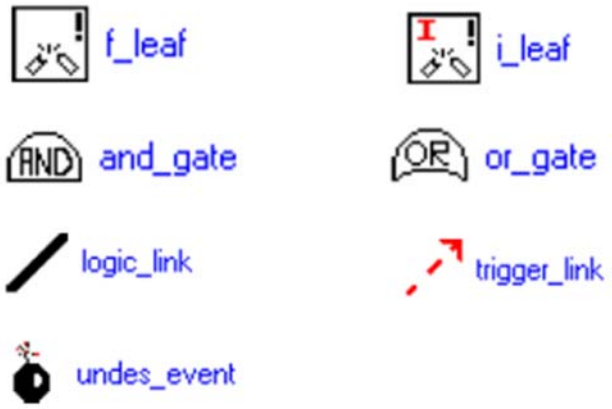
1) BDMP uses the Monte Carlo method to make quantitative analysis and simulate all the fault sequences. It can also remove the redundant sequences reducing combination optimism problems.

2) BDMP associates Fault Tree Analysis with Markov process, ensuring that it has the dynamic characteristics and calculation ability which is lacked in Fault Tree Analysis.

3)BDMP uses trigger key which can activate the model immediately. This means when the top model is triggered, the target node will be activated, and the subsystem connected will also be enabled.

BDMP is usually formed by the components below: Fault Tree (F) ， main top event (r), a group of 'trigger' (T), basic event (Pi) which are also known as "Triggered Markov Processes". Usually, there are two categories of states of Pi, which are 'true' and 'false' [3]. All the kinds and functions of the triggers used in standard BDMP models are shown in Fig. 1.

Fig. 1 The kinds and functions of the triggers used in normal BDMP models



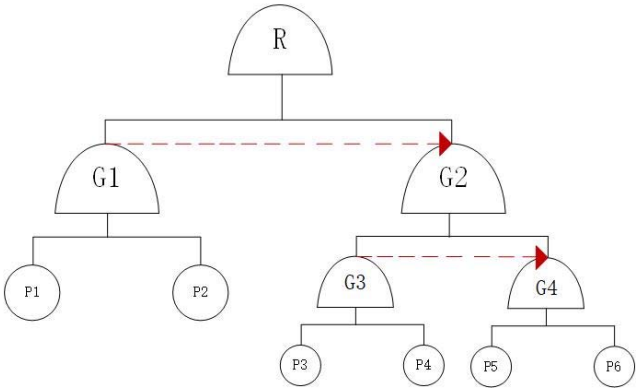
- f_left：It expresses that the model loses its efficacy in reacting. And it loses its efficacy only under 'recommend' pattern. This kind of efficacy lose can be repaired.
- i_left ：It expresses the request to calculate the model loses efficacy. It makes components changes from 'uncommand' to 'command'.
- and_gate：It expresses 'and' gate, compromises logic sum algorithm.
- or_gate：It expresses 'or' gate, compromises logic or algorithm.
- undes_event：Represents the failure state of the model system. It is similar to the top event of the fault tree model.
- logic_link：It expresses logic link.
- trigger_link：It expresses trigger link. It has trigger function, which only exists in BDMP.

As it is shown in Fig. 2, the main top event R is an'and'gate, while G1, G2, G3, G4 are 'or'gates. P1,

P2, P3, P4, P5, P6 are basic events. There are two trigger links (red arrow) in the model. When P1, P2 are in normal condition, the subsystems of G2 will not be considered as the cause for the top event to happen. But when one of P1 and P2 is false, the subsystems of G2 and its lower nodes will be considered. These dynamic characteristics will be shown directly by trigger links. Similarly, when P3, P4 are in normal conditions, G4 and its subsystems will not be considered as the cause that leads to the change of G2. When one of P3 and P4 is false, the subsystems of G4 will be considered. When the subsystems of G4 false, G2 will false, and finally leads to the happening of a top event. BDMP uses the Monte Carlo method for calculations, and by a plethora of experiments gets the unavailability of each node. As the speed of analysis increases, the changing trend of the unavailability of nodes decides the unavailability of equipment at each node. By this way, we can get the changing trend of MTTF (mean time to fail) that changes with the increasing of paces. This trend can be simulated by YAMS software.

YAMS implements the Monte Carlo method for the simulation purposes which broadens the safety research in automation application of KB3 software. YAMS models are based on FIGARO0 languages, estimating the standard value provided by users.

Fig. 2 The structure of a BDMP model



3. WATER LEVEL CONTROL SYSTEM OF PRESSURIZER

3.1 Summarize of digital water level control system of pressurizer

When the pressure of the RCP system (Reactor Coolant Primary System) is higher than the threshold of the pressurizer safety valve, the control system will adjust the pressure of the primary loop. The principle of adjustment is: the pressurizer is filled with saturated steam in the upper part and saturated water in the lower part. The temperature of the steam and water is equal to the saturated state temperature. When the system pressure is relatively low, the electric heater will heat the water to increase the pressure; when the system pressure is relatively high, the pressurizer will spray water to decrease the pressure [4].

The water level control system of pressurizer is one of the significant components of DICS. In normal operation, when the operation efficiency of the nuclear power plant changes, the temperature of the primary circuit water changes [5], which changes the volume of the primary circuit water, leading to the rise or fall of the water level in the pressurizer. Therefore, the concept of monitoring of the water level is put forth, the temperature of each circuit corresponds to a suitable water level of the regulator. The average temperature is indicated by the average water level, and it changes according to the average temperature determined by the load of the second loop. The water level monitoring channel collects and

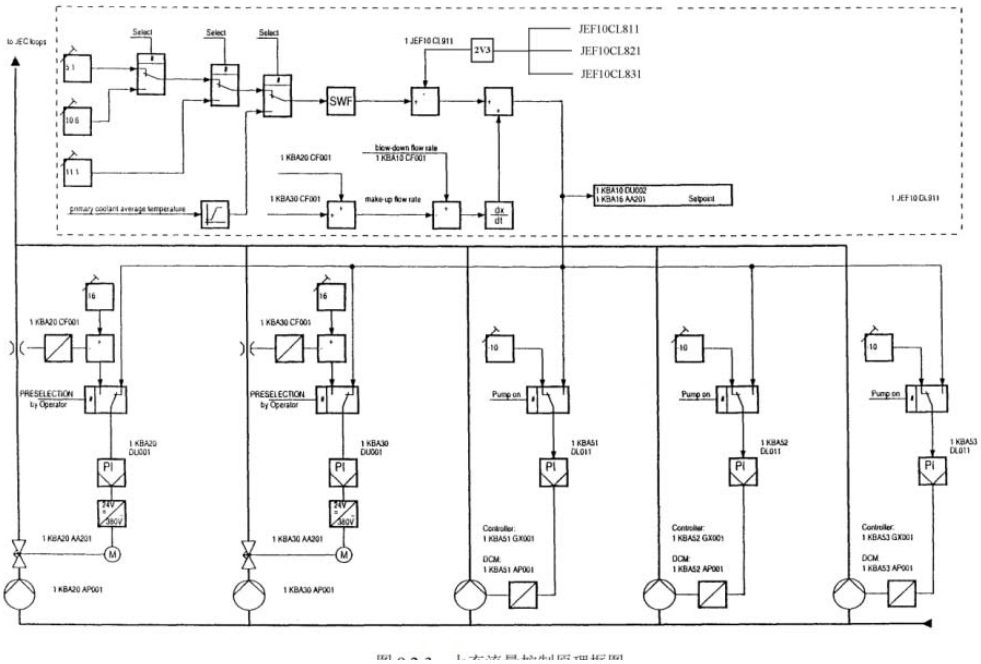
integrates the level measurement data, filling up the discharge in real time. Then it releases the discharge and averages the temperature. The reference temperature and the level measurement data are fed as input to the controller, which calculates the deviation of the water level measurement value from the set value. The set value of the supercharged flow rate is calculated according to the discharge, which is used as the benchmark by the flow controller PI. By controlling the opening of the charging valve, the supercharge flow of the chemical and capacity control system is regulated, and the water level of the regulator is finally controlled.

Under abnormal conditions, when the water level in the regulator is too low, the heater will be cut off automatically, and the discharge line will be closed. When the water level is too high, reactor shutdown happens to protect it under extreme conditions.

3.2 Working of PWLCS

Pressurizer water level regulation is achieved via maintaining a constant discharge flow and altering the charging flow. The monitoring of charging water level is implemented through 3 small capacity filling pumps(KBA51，52，53 AP001) and 2 with big capacity filling pumps（KBA20，30 AP001）, which adjust the capacity and boron concentration, as demonstrated in Fig 3. During normal operation, one of the three small capacity pump runs, second as a backup and the last helps during examining and repairing. The regulation valves KBA14,15,16 AA201 participate in discharging flow regulation, and KBA16 AA201 can participate in the control of the PZR water level [6].

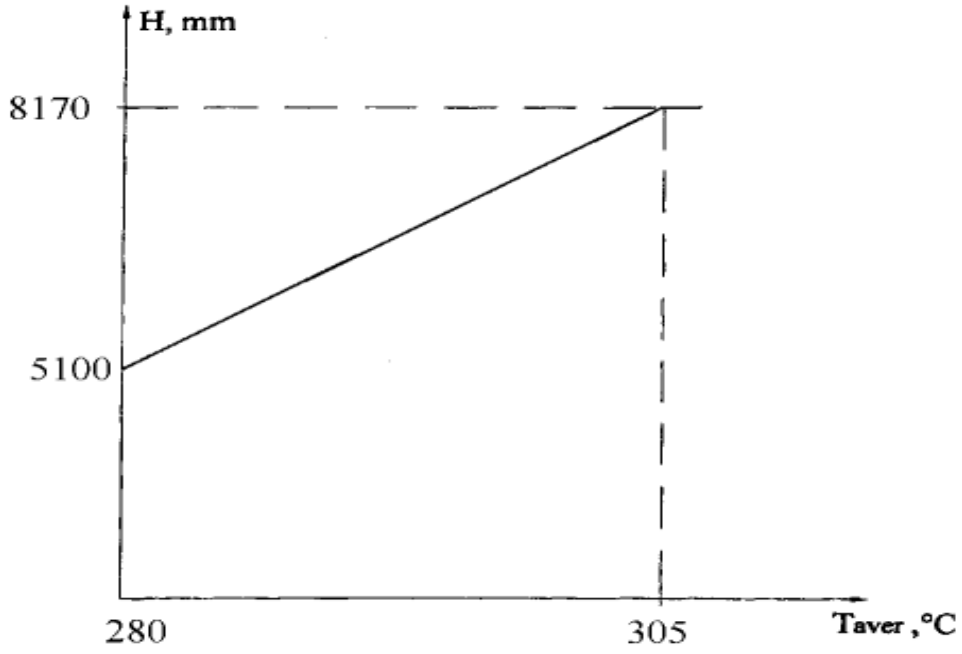
Fig. 3Flow control principle diagram



The PZR is based on two controllers, boot-shutdown level controller and standard level controller. The boot-shutdown level controller monitors the opening of regulating valve KBA20 AA201 and KBA 30 AA201, located in the outside the KBA20 AP001 and KBA30 AP001.These regulating valves control the charging flow. During normal operation, the standard level controller regulates the three pumps KBA51，52，53 AP001.In the level regulation circuit, according to the curve of Fig. 4, the regulator water level is set by primary circuit average temperature T_{av}, and the reference value of the first circuit average temperature T_{ref} is introduced to correct it. This is because the change of the secondary loop load will affect the pressurizer water level to form a set value, which is compared with the level measurement signal to acquire the level deviation value. The imbalance between charging and

discharging flow also has an impact on the level, making this factor to be considered. The water level measurement signal is sent to the water cooling regulation circuit by three hot water level measured signals from 007MN,008MN,011MN according to three out of two logic. Finally, the control of the flow rate is realized by changing the speed of the controller via frequency transformer（KBA51，52，53 GX001.Its speed is changed according to the output signal of the controller through the operation of the regulating logic circuit. The controller used is a non-static error proportional integrated (PI) controller.

Fig. 4 'T' pattern of PWL setting diagram



4. BDMP MODELING

4.1 Modeling Hypothesis

Considering the complexity of pressurizer digital water level control system and the limitations of the KB3 software modeling, the following assumptions were made before establishing the model:

1) Ignoring the failure of the system caused by human factors, such as improper operation and manual adjustment error etc.
2) Assume that the Mean Time To Repair (MTTRs) for all components is 24 h [7].
3) Out of three small capacity pump (KBA51，52，53 AP001),one unit is in operation, second is in reserve, and the other is in hot standby. When the KBA51 is in normal operation, KBA52,53AP001 are on hot standby. When the KBA51 fails, the signal of KBA52 is output by triggering the link. Thus, KBA52 implements the system function.
4) This model assumes that the power plant is operating under normal operating conditions, and only considers the influence of the average temperature of the primary circuit on the system, the influence of the pressure change is not included.

4.2 BDMP Modeling and Analysis

4.2.1 Model of Water level Control system of　PWLCS

The BDMP model of the Pressurizer level control system mainly includes the charging and discharging flow regulation system. Due to the limitation of KB3 modeling, this model emphasizes the charging flow regulation system only. It consists of three small capacity supercharge pumps, one (KBA51, KBA52,KBA53), and two full capacity pumps which are only considered when KBA51 fails. Failure principles of KBA52, KBA53AP001D, are the same as the KBA51. Therefore, we take the KBA51 as an example.

As described above, the water level control system of the regulator is mainly controlled by the charging and the discharging flow regulation system. The charging and the discharging flow regulation system are two independent systems, and only the former one is discussed here. The three small capacity pumps form a triple redundancy, KBA52 will start up via a trigger link when KBA51 fails, playing a role in preventing emergencies and accidents. The BDMP model is demonstrated in the Fig. 5， The failure probability of the related module is shown in Table 1.

Table 1:The failure probability of the related module [8-10]

Module	Failure rate [FIT]
Thermometer	**1925**
Content gage	**1250**
Flowmeter	**900**
Up flow pump	**4200**
Reference temperature	**451**

4.2.2Analysis of computing result

YAMS analysis shows that the failure distribution probability (CFP) of repairable and non-repairable systems changes with the simulation time. As shown in Fig. 6, CFP of the non-repairable system increases significantly with time in the range of 0 - 6.29×10^{6}h and then stabilizes gradually approaching to 1 indefinitely after 6.29×10^{6} h. When CDP is 0.499, the mean time to failure (MTTF) of the reciprocal system of the corresponding simulation step is 3.655×10^{-6} / h <Fpwlcs< 4.0×10^{-6} / h.
As for the repairable system, in the simulation step of the former 453600, the CFP gradually increased to 2.83×10^{-5}, and then gradually approached 3×10^{-5} indefinitely. Since the failure rate was 1/24h=0.04/h, the repair rate was much greater than the failure rate. Therefore Fig. 6 meets the results of many repeated samplings.

5. SUMMARY AND PROSPECT

As one of the important equipments for NPPs, pressurizer is of great significance in safe operation of the NPPs. There are few researches on the reliability analysis of PWLCS, and its reliability of the DICS are critical for the safety of NPP. Traditional reliability analysis methods, such as FT or RBD can not desicrible the repaire and other dynamic interaction of control system. Therefore, BDMP is uded for PWLCS reliability analysis. The BDMP model of PWLCS is established by KB3 software, and the Monte Carlo simulation of the model is carried out by YAMS.

The MTTF (average pre-failure time) of the repairable and non-repairable system was changed with the increase of the number of test steps[7]. The cumulative failure probability (CFP) of the unrepairable system becomes infinitely close to 1 after 6.29×10^{6} h, that is, the system gradually completely fails. The

CDP of the repairable system is less than 0.05, which means that the probability of system failure in the BDMP model of PWLCS is extremely low during the normal operating life of the reactor. The CFP of the repairable system increases from 0 and stabilizes to 0.298 used 7×10^{6}h .The failure rate is 1/24h=0.04/h, and the repair rate is much larger than the failure rate. In other words, the repairable system can be repaired in time even if it fails.

Because KB3 software has limitations on the number of model elements, reliability is analyzed under certain assumptions, the BDMP of PWLCS is far from a comprehensive one. Since YAMS is used for quantitative analysis of BDMP, and it is neither a popular nor well verified Monte Carlo simulation tool, the widly accepted Markov chain tool or Monte Carlo simulation software is needed to verify the calculation results later.

Fig. 5 The BDMP model of digital Pressurizer Water Level Control System

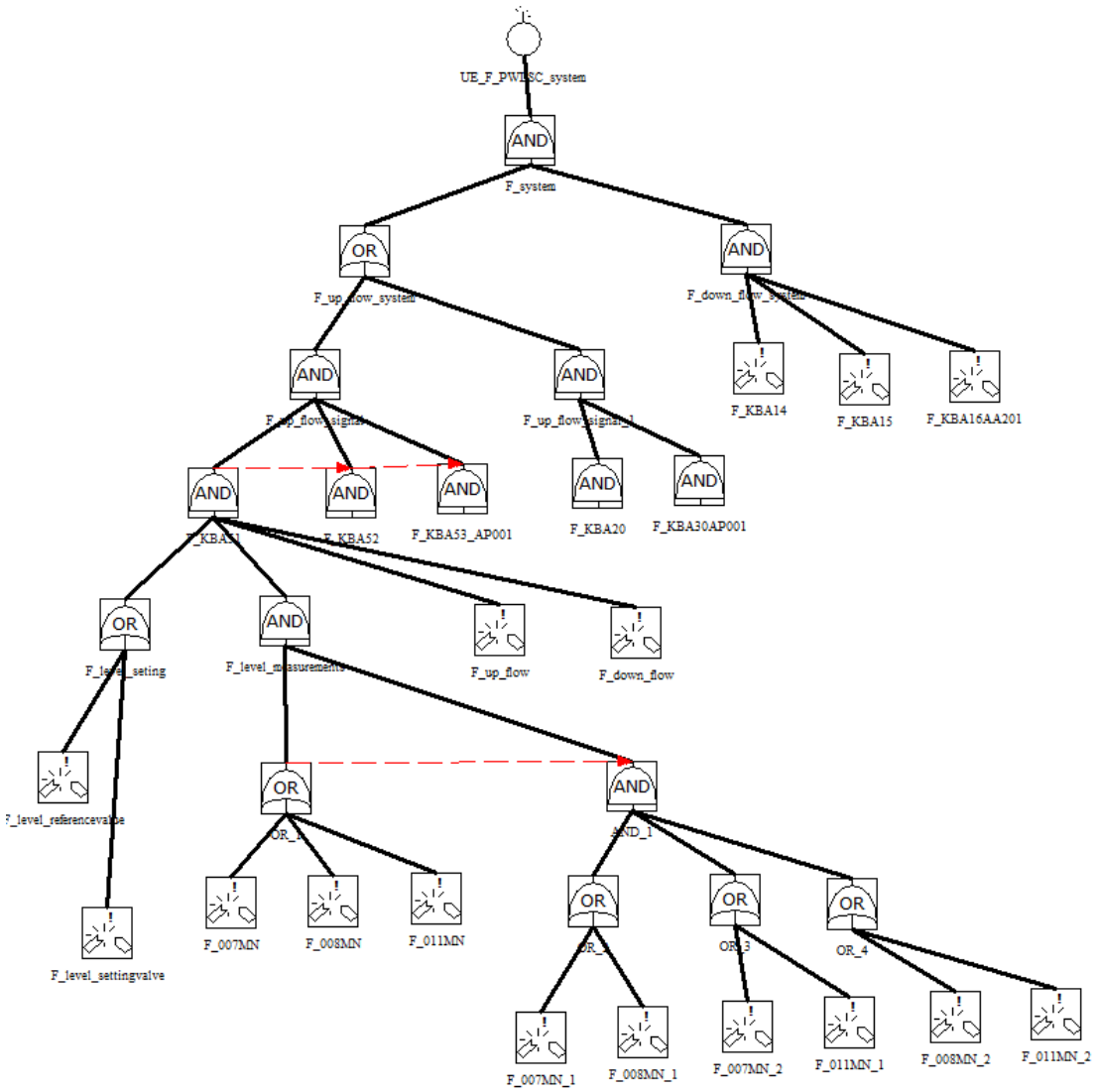


Fig. 6 The cumulative failure probability with simulation time

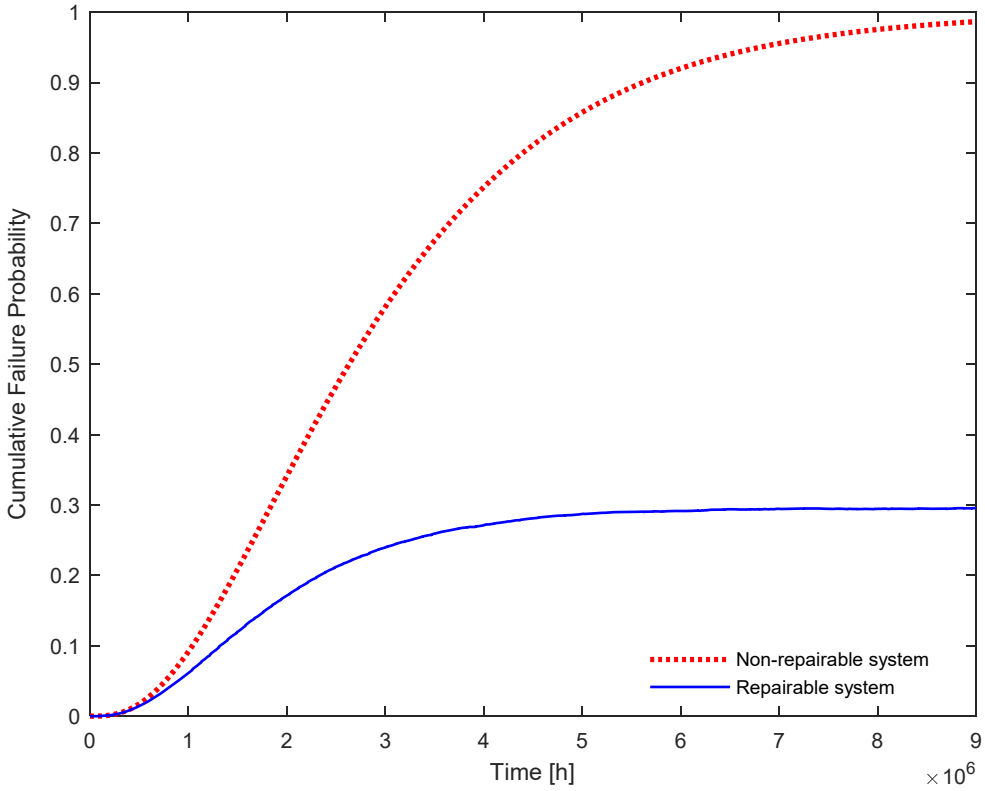
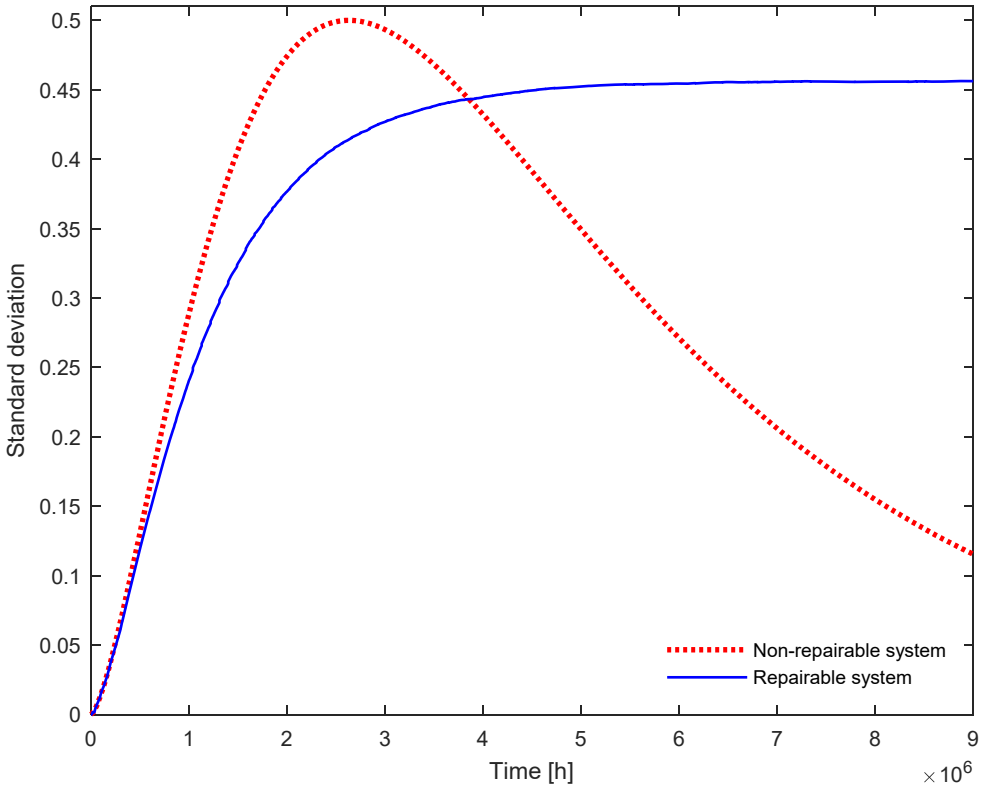


Fig. 7 The standard deviation with simulation time



Acknowledgements

The authors are grateful to the anonymous reviewers for their valuable suggestions and comments to improve the quality of the paper. This research is supported by the National Nature Science Foundation of China (71301049).

References

[1] Piètre-Cambacédès L, Bouissou M. *Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP)*. European: IEEE, Dependable Computing Conference (EDCC), 2010: 199-208.

[2] Hao Y. A *GREY ASSESSMENT MODEL OF REGIONAL ECO-ENVIRONMENT QUALITY AND ITS APPLICATION*. China: Environmental Engineering, 2002, 20(4):66-68.

[3] Bouissou M. *A generalization of dynamic fault trees through Boolean logic driven Markov processes(BDMP)*. EU: Proceedings of the 16th European Safety and Reliability Conference (ESREL'07), 2007

[4] Jiangsu Nuclear Power Co. LTD. *Full Digital Instrument and Control System of Tianwan Nuclear Power Plant*. China: Jiangsu Nuclear Power Co. LTD, 2002:269-275

[5] Yang Xue, Jing Lin, Yuan Li, Jianbiao Feng. *Research on Pressurizer Water Level Control in Nuclear Reactor*. China: Applied Mechanics & Materials, 2013, 336-338(1): 608-613

[6] Haipeng Lu. *The summary of the water level control system of pressurizer in AP1000*. China: Shandong Nuclear Power Co. LTD, 1007-0745（2013）02-0070-02: 70-71

[7] Hao Wang, Jiawei Yu, Shiliang Zhou, Yijing Mao, Tongyu Xu. *Reliability Assessment for Steam Generator Water Level Control System in NPP Based on BDMP* . China: Atomic Energy Science and Technology, 2017: 1, 3

[8] *R Handbook. Safety Equipment Reliability Handbook*, 1nd ed. Selleraville, PA: Exida, 2007;1-231.[1.1]Page 45;[1.2]Page 145;[1.3]Page 92

[9] *R Handbook. Safety Equipment Reliability Handbook* , 1nd ed. Selleraville, PA: Exida, 2015

[10] *R Handbook. Safety Equipment Reliability Handbook* , 1nd ed. Selleraville, PA: Exida, 2007; 347

[11] Billinton R, Allan R N. *Reliability evaluation of engineering systems*. New York: Plenum press, 1992.