ISBN: 978-981-18-5852-9
WCSE 2022 Spring Event: 2022 9th International Conference on Industrial Engineering and Applications
doi: 10.18178/wcse.2022.04.193

Dynamic Reliability Analysis of DCS in HTR-PM Considering Fault Self-Check Rate Based on Petri Net

Wen Guo [1], Chao Guo [1], Shuqiao Zhou [1], Fan Chen [1] and Xiaojin Huang [1]

[1] Institute of Nuclear and New Energy Technology of Tsinghua University, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Beijing 100084, China

Abstract. Digital distributed control system (DCS) is the most important monitoring and control platform in a nuclear power plant (NPP). The reliability and availability modeling and analysis of digital DCS are of great significance to ensure the stable and reliable operation of NPPs and to improve the economy of NPPs. With the continuous development of control system technology, the fault self-check rate of DCS equipment is getting higher and higher. It is necessary to consider the influence of this factor in the DCS reliability model and improve the model architecture. In this paper, a dynamic reliability model of DCS based on Petri Net is proposed by considering the factor of fault self-check rate. The DCS of High Temperature Gas-Cooled Reactor - Pebble bed Module (HTR-PM) was adopted for model verification, and the reliability of the DCS was calculated by Monte Carlo method. The calculation results show that the higher the fault self-check rate, the lower the unavailability of the DCS. When the fault self-check rate exceeds 40%, the unavailability of DCS will be reduced by an order of magnitude. This conclusion has important engineering practical significance.

Keywords: DCS reliability, Petri net, fault self-check rate, HTR-PM

1. Introduction

As the control centre of a nuclear power plant (NPP), the reliability of distributed control system (DCS) is related to the safe and reliable operation of the whole NPP, and is an important guarantee for the economy and safety of an NPP. The reliability analysis of DCS has important engineering significance. Compared with the analogue systems, the digital DCS is better in computing capacity, equipment scale, signal accuracy, human-machine interface friendliness, fault self-check ability, etc., but its dynamic characteristics also bring challenges to the analysis of NPP including probabilistic risk assessment (PRA). The traditional reliability analysis methods have some limitations in analyzing the digital system, which cannot fully reflect the characteristics of the digital systems. With the continuous development of digital Instrument and Control (I&C) systems, such as DCS, the ability of equipment online self-check is gradually improved, and the fault self-check rate of equipment has become a research factor that cannot be ignored. Therefore, in view of the characteristics of digital I&C system such as online self-check, research on modeling method is of great significance to the reliability evaluation of digital I&C systems.

DCS with the fourth generation of advanced NPP of High Temperature Gas-Cooled Reactor - Pebble bed Module (HTR-PM) NPP has a certain fault self-check function, which has improved its reliability, but how to evaluate the fault self-inspection function, especially the quantitative impact of fault self-inspection function on the reliability of DCS is not clear, it is urgent to study these two problems. This paper focuses on these two problems and carries out relevant research work.

In recent decades, with the rapid transformation of the I&C system of NPP from analog to comprehensive digital ones, a variety of methods have been used to analyze the reliability of digital systems [1]. NUREG/CR-6962 report analyzed the applicability of traditional PRA methods such as fault tree method and Markov method in digital I&C system [2]. In this report, FEMA analysis was firstly used. After considering the influence of human factors and software failures, models of feedwater control system and reactor protection system of an NPP were established respectively by using fault tree method and Markov method. The report also pointed out the limitations of FEMA analysis and fault tree analysis for reliability analysis of reactor protection systems. Shah J. A., based on the concept of fuzzy sets, proposed A basic event evaluation method of system fault tree based on fuzzy reliability. This method used fuzzy sets to quantitatively represent the occurrence probability of corresponding basic events in the fault tree and solved the problem of lack of failure rate or failure probability data of basic events [3].

Fault tree is the main method for reliability analysis of DCS system. Fault tree analysis method is a static method, which is difficult to accurately reflect the impact of online self-check and other detection and maintenance activities on the reliability of DCS system, nor can it describe the control loop and feedback loop logic, and each fault tree can only describe one top event, when the top event changes, it needs to be re-modeled [4-5]. Markov method [6-7] is a dynamic analysis method, which is generally only applicable to exponential distribution processes. But in fact, DCS failure and maintenance process do not fully obey the exponential distribution. In addition, with the increase of the number of components, the number of state space of Markov model increases exponentially, and the model becomes extremely large, leading to the difficulty of calculation [8].The NUREG/CR-6901 report compared analogue and digital I&C systems and described the problems that need to be solved by modelling the reliability of digital I&C systems and embedding the reliability of digital I&C systems into the existing PRA model in order to increase the contribution of digital I&C systems to power plant risk informed decision making [9].This report summarized the reliability modelling methods of digital systems, and the comparison results of various methods show that none of the reliability modelling methods can completely meet the reliability modeling requirements of digital systems [10-14]. Guo of Tsinghua University used a variety of methods to analyze the reliability of digital I&C systems in NPPs, including failure mode and effects analysis (FMEA), failure tree method (FT), dynamic flow graph mode (DFM) and Markov/CCMT (Cell-to-Cell Mapping Technique) to analyze the digital I&C systems.

For this study, the influencing factors considered in the modeling process of digital I&C system include:

1) The method can describe the dynamic transition process of system state.
2) The method can be widely used in various failure processes.
3) The method can embody the advantages of online self-check function of digital system.
4) The method can reflect the dynamic maintenance process.

As a description and analysis tool combining mathematics and graphics, Petri net method can better describe common phenomena such as synchronization, concurrency, distribution, conflict and resource sharing in complex systems. It can be used in distributed systems, information systems, discrete time systems and flexible manufacturing systems. It is an effective approach for modeling discrete event dynamic systems [15-19]. In recent years, Petri nets have been widely used in dynamic reliability modeling of complex systems [20]. The reliability model based on Petri net can describe random events subject to various distributions as well as certain events occurring at certain time [21]. In addition, the results obtained by using Petri net are instantaneous reliability of the system, which is convenient for finding and analyzing weak links [22]. In conclusion, Petri net method is more convenient to incorporate online self-inspection into the reliability modeling process of digital I&C systems.

In the second section, the basic architecture of DCS in NPP was introduced. On this basis, Petri net was employed for reliability modelling DCS in High Temperature Gas-Cooled Reactor - Pebble bed Module (HTR-PM), then self-check ratio was considered in the model. The impact of self-check ratio on the reliability analysis was discussed. In the end the conclusion was given.

2. Structure of DCS in HTR-PM

DCS has advanced architecture, complete functions, and comprehensive performance. It is the most widely used control platform in NPPs.

DCS has four basic components: process control station (PCS), operator station (OS), engineer station (ES), and system network (SN). PCS is the core equipment of DCS, and the major control functions of DCS are performed by it. The hardware of PCS includes: main controller unit, I/O unit, and internal bus. A PCS has enough capacity to perform the calculation and control functions of multiple control loops, and a DCS may include multiple PCSs. Operator stations are primarily used by operators as human-machine interface

(HMI) to monitor plant operating conditions and perform necessary manual operations. The engineer station is mainly used by DCS engineers as a tool for system configuration and maintenance. The equipment of operator station and engineer station consists of industrial computer loaded with corresponding software. The system network is used to connect the operator station, engineer station, and process control station. It includes network interface cards, switches and communication cables. In addition, large-scale DCS are usually configured with multiple system servers for centralized data storage and management. System server can be divided into real-time data server, history server, computing server, and so on.

In order to reduce the possibility of DCS function failure caused by a single fault and improve the reliability and continuous operation capability of DCS, DCS adopts redundancy configuration. Taking the DCS of HTR-PM as an example, it adopts multiple redundancy configurations: internal redundancy of PCS, communication network redundancy, power supply redundancy, network server redundancy, and operator station redundancy.

1) Internal redundancy of PCS: in order to reduce the possibility of PCS failure caused by a single fault, each PCS is equipped with redundant master controller; each I/O station is equipped with redundant communication interface modules; The redundant controller communicates with each I/O station using a redundant I/O bus.

2) Communication network redundancy: including network segment redundancy, loop network redundancy and subnet redundancy.

3) Server redundancy: computing servers, history servers, and I/O servers are all configured in redundancy mode.

4) Redundancy of operator stations: each operator station has the same display and operation capability and is mutually redundant.

In addition, the DCS of HTR-PM has on-line self-check function and good maintainability. The circuit module has on-line self-diagnosis ability and has status indication on the front panel. In the engineer station, fault diagnosis and status display can be centralized from the whole system to the module level. The circuit module can be electrically pluggable and supports plug and play (automatic recovery after insertion). The above measures further ensure the availability of the system.

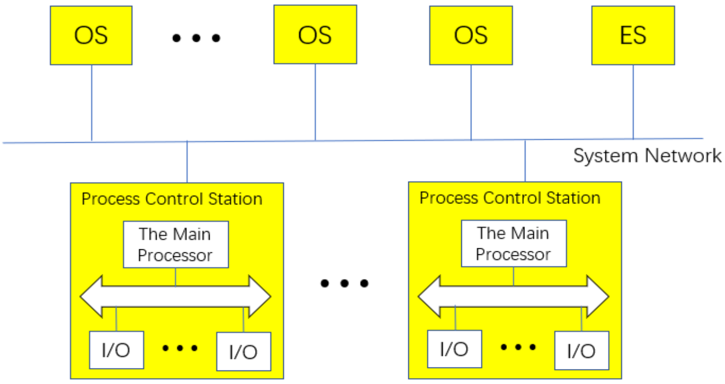

Fig. 1: Basic composition of DCS.

3. Petri Net Model of DCS in HTR-PM

3.1. Introduction to the Petri Net

Petri net is a directed graph composed of four elements: Place, Transition, Arc and Token [15-22].

As shown in Fig. 2, token is a small dot that can represent information, resources, and conditions. The circle used to represent the library, generally represents the channel or system state. Transition is represented by rectangles, generally representing the occurrence of events, states, resource transfers or information transmission. Directed arc refers to a clear arc that can only point to the transition from the library or from the transition to the library, generally indicating the direction of token's transition or the sequence of events.

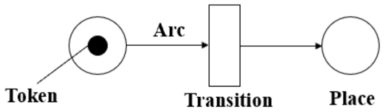

Fig. 2: Elements of Petri net.

The properties of Petri net are mainly related to transition, directed arc and Token. In order to better illustrate the modelling process, the transition and directed arc involved in this paper are first explained and specified. As shown in Fig. 3, transitions can be divided into three types according to their delay characteristics:

1) Transition with no time delay: the transition will be launched immediately after enabling.

2) Transition with deterministic time delay: the transition after enabling will delay a certain time before launching.

3) Transition with stochastic time delay: after enabling, the transition will randomly generate delay time according to the set distribution, and launch after the delay time arrives.

Directed arcs are used to connect places and transitions, and are generally divided into normal arcs and inhibitory arcs:

1) Normal arc: when the token quantity in the input place connected to the normal arc is not less than its weight, it means that the enabling condition is met.

2) Inhibitory arc: if the token number in the input place connected to the suppression arc is less than the weight, the transition downstream of the suppression arc can be enabled. Otherwise, the transition downstream of the suppression arc will not be enabled.

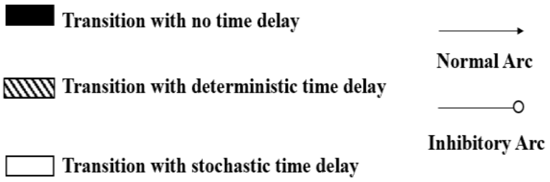
Transition with no time delay
Transition with deterministic time delay
Transition with stochastic time delay
Normal Arc
Inhibitory Arc

Fig. 3: Transition and directed arc type description.

3.2. DCS Modelling by Petri Net

The reliability block diagram of DCS in HTR-PM is shown in Fig. 4. Some necessary simplifications are made when building reliability structure block diagrams:

1) Simplify the operator station into HMI subsystem of 1 out of 4. Each operator station has the same display and operation capability as other 3 ones. For the convenience of modeling, the operator station is simplified as a redundant subsystem of 1 out of 4.

2) Simplify the Level 1 and Level 2 double looped network into two 1 out of 2 redundant subsystems, and simplify the redundant computing servers, I/O servers, and history servers into 1 out of 2 subsystems.

3) The 90 process control stations uniformly adopt the following simplified structure, that is, 1 power supply module for 1 out of 2, 1 CPU module for 1 out of 2, 10 I/O board cards without redundancy and 1 communication module for 1 out of 2.

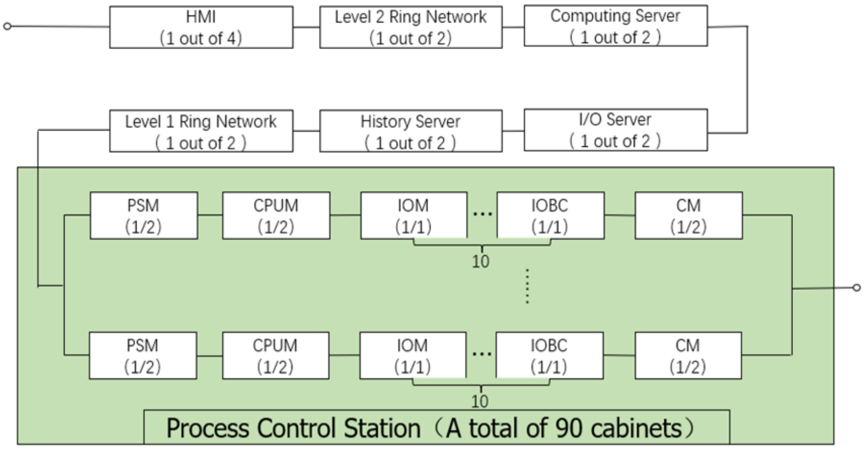

Fig. 4: Reliability structure block diagram of DCS in HTR-PM.

Some necessary simplifications and assumptions are made in the establishment of Level 1 Double Looped Network Petri net model:

1) A single set of Level 1 loop network is regarded as a whole, namely A set and B set, which is conducive to analyzing the influence of the state of each set on the overall reliability of Level 1 Double Looped Network.

2) Set A and Set B of Level 1 Double Looped Network are mutually standby and constitute redundancy, with similar performance and no significant difference in reliability parameters. A Level 1 Double Looped Network is considered available as long as either loop is in normal operation.

3) When the Level 1 Double Looped Network fails, it has sufficient maintenance resources and the maintenance method is replacement spare parts. The fault is completely repaired after delayed average maintenance time.

In Fig. 5, a single set of 1st layer loop network is viewed as a whole and has two states: "normal" (State 1) and "failed" (State 2), represented by two Places "L1LN1_P1ANorm" and "L1LN1_P2AFail" respectively. When a single set of 1st layer loop network is in State 1, there are two triggering conditions for the transition from state 1 to state 2: one is the end of delay of the random delayed transition "L1LN1_T2ALife" which follows exponential life distribution, and the other is the activation of instantaneous transition "L1LN1_T1AOperatingToFail" which indicates the failure of a single set of 1st layer loop network in operation. It can go from state 1 to state 2 if either of these conditions are satisfied. When a single set of 1st layer loop network is in State 2, the triggering condition for the change from State 2 to State 1 is that the fixed delay change representing the average maintenance time "L1LN1_T3AMT" delay ends.

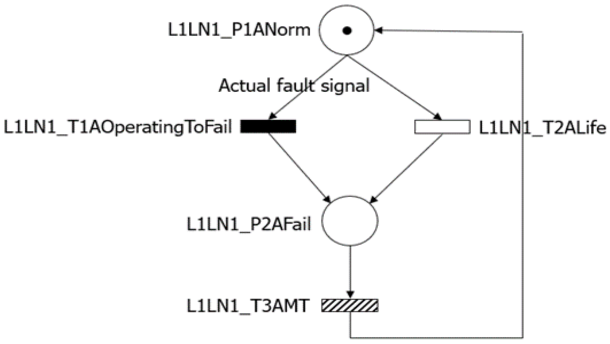

Fig. 5: Level 1 Single Looped Network Petri net model.

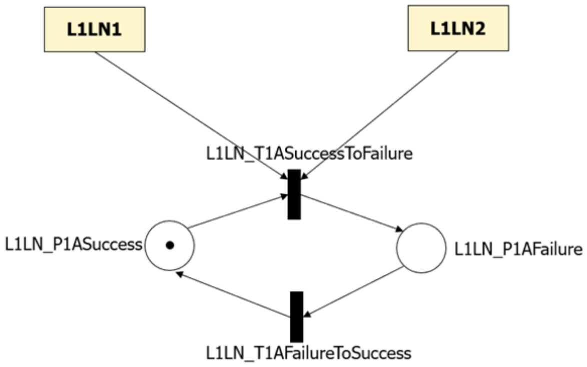

Fig. 6: Level 1 Double Looped Network Petri net model.

Fig. 6 shows the logical voting diagram of Level 1 Double Looped Network. The Place "L1LN_P1ASuccess" indicates that the Level 1 Double Looped Network subsystem is available. In this state, at least one of the two loop networks are in normal state. The Place "L1LN_P1AFailure" indicates that the Level 1 Double Looped Network subsystem is unavailable. In this state, neither of the two loop networks is working properly.

As the modelling process above, we can build the Petri net models for HMI subsystem, Level 2 Double Looped Network subsystem, computing server subsystem, the I/O server subsystem, history server subsystem, and each PCS subsystem. The Petri net model of DCS of HTR-PM can then be correspondingly obtained by combining these models according to the reliability block diagram shown in Fig. 4.

3.3. Analysis of Fault Consequence of Typical DCS

Monte Carlo method was used to solve the Petri net model of DCS in HTR-PM. In this study, we use the Monte Carlo method on the Petri nets model above 1 million times, 2000 hours of simulation experiment. After the experiment, the statistics of the DCS in various parameters and operating conditions to keep the total number of normal state and failure state are used to approximately calculate instantaneous availability and unavailability of DCS system in 2000 hours.

The model parameters of each device are shown in Table 1, and the simulation results are shown in Fig. 7 and Fig. 8, respectively.

Table 1: Petri net model parameters of DCS in HTR-PM.

Subsystem/component	λ/h^{-1}	**Fixed maintenance time**	τ/h^{-1}
The Human Machine Interface	5×10^{-5}	0.5	1
Double Looped Network of Level 1	2×10^{-5}	1	1
Double Looped Network of Level 2	2×10^{-5}	1	1
Computing Server	2×10^{-5}	4	1
History Server	2×10^{-5}	4	1
I/O Server	2×10^{-5}	4	1
Power Supply Module	1×10^{-5}	0.5	1
CPU Module	1×10^{-5}	0.5	1
The I/O Board Card	2×10^{-5}	0.5	1
Communication Module	1×10^{-5}	2	1

As can be seen from Fig. 7, the availability of DCS is very high during normal operation, and the availability remains stable at 0.9999 when t is around 1000h. When DCS components or subsystems fail, the availability of DCS is significantly reduced. When the fault is fixed, the availability of DCS is restored to normal level. Different types of failures have completely different effects on the availability of DCS.

As can be seen from Fig. 8, the unavailability of DCS is very low during normal operation, and the unavailability remains stable at the level of 10-4 when t is around 1000h. When DCS components or subsystems fail, the unavailability of DCS increases significantly. When the fault was repaired, the unavailability of the DCS system returned to normal levels. The impact of different types of faults on the unavailability of DCS is completely different.

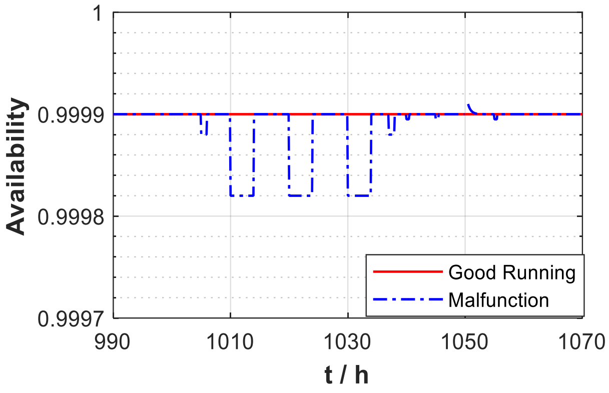

Fig. 7: Impact of component failures of DCS on system availability.

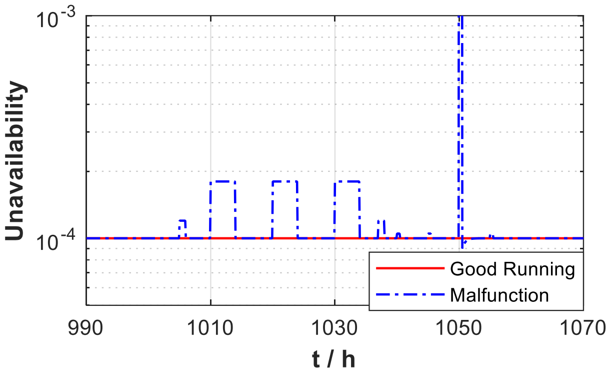

Fig. 8: Impact of component failure of DCS on system unavailability.

The fault sequence of the hypothetical DCS components is shown in Table 2.

Table 2: Fault sequence of DCS components.

The fault name	**A set of HMI is not available**	**A segment of the Double Looped Network of Level 2 is unavailable**	**Computing server A is faulty**
Fault occurrence time /h	1000	1005	1010
Fault repair time /h	1000.5	1006	1014
History server A is faulty	**I/O server A is faulty**	**The fault name**	**A segment of the Double Looped Network of Level 1 is unavailable**
1020	1030	Fault occurrence time /h	1037
1024	1034	Fault repair time /h	1038
Power supply module A of the power control cabinet is faulty	**CPU module A of the power control cabinet is faulty**	**one I/O board card in the power control cabinet is faulty**	**Communication module A of the power control cabinet is faulty**
1040	1045	1050	1055
1040.5	1045.5	1050.5	1055.5

When t = 1000h, an HMI is supposed to be unavailable and DCS availability decreased slightly. Half an hour later, the HMI fault was repaired and DCS availability returned to normal level. This is because the HMI is in 1 out of 4 redundancy, even if one HMI fails, there are still three available, so a failure of HMI on the overall availability of DCS is negligible.

When t = 1005h and t = 1037h, a segment failure occurred in the Double Looped Network of Level 2 and Level 1 respectively, resulting in the availability of DCS decreased to a certain extent. One hour later, the faults of Double Looped Network of Level 2 and Level 1 were repaired respectively, and the availability of DCS returned to the normal operation level. As the redundant structure, the failure of Looped Network also has limited effect on the availability of DCS.

When t is 1010h, 1020h, and 1030h, respectively, the computing server, history server, and I/O server suffered a server failure, resulting in a significant decrease in the availability of the DCS. Four hours later, each server was correspondingly repaired, and the availability of the DCS was restored to the normal level. Unlike loop network failures, server failures lead to a significant decrease in DCS availability. This is due to the different reliability of the loop network and the server. Compared with loop network, the servers have lower reliability. Therefore, it has lower availability of single set, longer maintenance time. Thus the failure of servers has greater impact to the DCS availability.

When t = 1050h, an I/O board of power control cabinet failed and the DCS availability dropped to 0. After half an hour the faulty board was replaced, the availability of DCS first rose to a higher level, and then quickly fell. The reason why the availability drops to 0 is that the I/O board has no redundancy and is in series with other components in the reliability structure. When the I/O board fails, the DCS power control cabinet completely loses its function, so the DCS availability drops to 0. When the faulty board is repaired, the availability of DCS first rises to a higher level than normal because the board is repaired by replacement maintenance, that is, repair as new hypothesis. And then as time goes on, it goes down quickly.

As can be seen in Fig. 8, the failure of redundant components has little impact on the system unavailability, but the failure of non-redundant parts has a great impact on the DCS reliability.

3.4. Analysis of Influence of Fault Self-check Rate on DCS Reliability

The DCS of HTR-PM has the function of fault self-check. Some faults can be automatically detected and quickly located. All maintenance methods are considered as replacement maintenance, so that the fault point is considered as new after being repaired. Some faults cannot be discovered by the fault self-check function. Manual inspection is required to discover this kind of fault and start maintenance work periodically. This process requires an average detection time (τ).

In order to study the influence of fault self-check function on DCS reliability, the concept of fault self-check rate is adopted in this paper. Fault self-check rate (rs) is defined as the ratio of faults that can be detected by the fault self-check function to all possible faults in the DCS. The higher the fault self-check rate is, the easier the system fault is to be accurately detected and located.

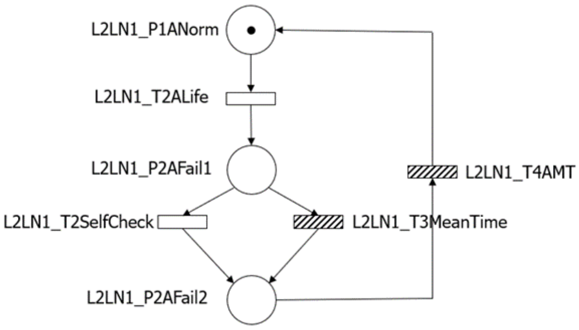

Fig. 9: Level 2 Single Looped Network Petri net model.

Fig. 9 and Fig. 10 show the Petri net model established for Level 2 Single and Double Looped Network subsystem. Fig. 9 shows a set of Level 2 Double Looped Network as a whole, with three states, "Normal" (State 1), "Failure detected" (State 2) and "Failure detected" (state 3), represented by three places "L2LN1_P1ANorm", "L2LN1_P2AFail1" and "L2LN1_P2AFail2" respectively. The trigger condition from state 1 to state 2 is the end of the random delay "L2LN1_T2ALife" which obeys exponential lifetime distribution. There are two triggering conditions for the transition from state 2 to state 3. One is triggered by "L2LN1_T2SelfCheck", which indicates the random change of fault self-check rate; the other is the definite delay change of the average time "L2LN1_T3MeanTime" when the fault is artificially detected. The trigger condition for the transition from State 3 to State 1 is the change of the defined delay representing the average maintenance time. "L2LN1_T4AMT" delay ends.

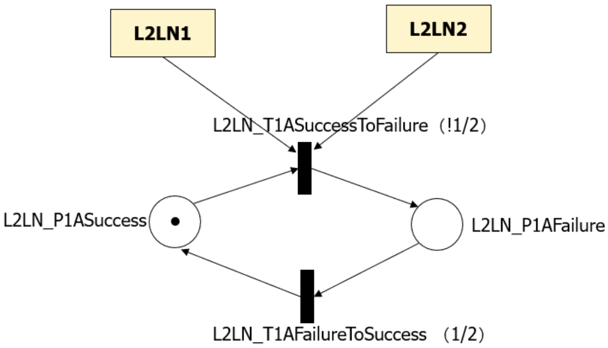
L2LN1
L2LN2
L2LN_T1ASuccessToFailure （!1/2）
L2LN_P1ASuccess
L2LN_P1AFailure
L2LN_T1AFailureToSuccess （1/2）

Fig. 10: Level 2 Double Looped Network Petri net model.

Fig. 10 shows the logical voting diagram of Level 2 Double Looped Network. “L2LN_P1ASuccess” indicates that the Level2 network subsystem is available. In this state, at least one of the two Level2 networks is in the normal state. “L2LN_P1AFailure” indicates that the Level2 network system is unavailable. In this state, both Level2 ring networks are abnormal.

Similar with the modeling process in Fig. 9 and Fig. 10, we can build the Petri net models of HMI subsystem, Level 1 double looped network subsystem, computing server subsystem, I/O server subsystem, history server subsystem and each process control station subsystem.

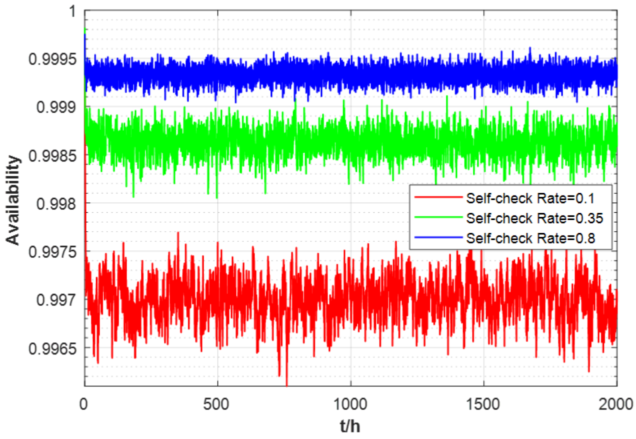

Fig. 11: Availability curve of DCS in HTR-PM.

The above subsystem models were combined into the Petri net model of DCS in HTR-PM according to the reliability block diagram in Fig. 4. Monte Carlo method was used to solve the Petri net. The model parameters and simulation results are shown in TABLE I and Fig. 11, respectively. The selection of model parameters is mainly based on expert opinions. The simulation time was 2000 hours and the simulation times were one million.

As can be seen from Fig. 11, when the fault self-check rate rs = 0.8, the availability of DCS soon drops to 0.9995 from 1 after t = 0, and then fluctuates up and down in 2000 hours, with the average availability between 0.9991 and 0.9995. The average period of fluctuation of availability is related to the average maintenance time of DCS. The shorter the average maintenance time is, the shorter the fluctuation period of availability is, which is the inevitable result for the fixed delay for maintenance. From the overall view of the availability curve, although the DCS structure is relatively complex, due to reasonable redundant structure and high reliability of key components, DCS can maintain high availability for a long time.

When the fault self-check rate rs = 0.1 (or rs = 0.35), compared to rs = 0.8, the availability of the DCS in a short period of time after t = 0 decreases more rapidly, and the availability within 2000 hours also appears to be significantly reduced, with fluctuations also getting bigger. This is mainly because when the fault self-check rate is low, the average time required for system faults to be detected and repaired is longer, so the availability of DCS is significantly reduced. The fluctuation of availability is directly related to the fault self-check rate.

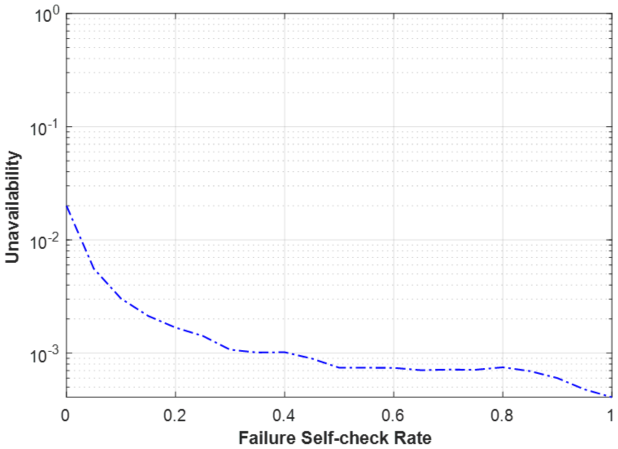

Fig. 12: Relationship between DCS unavailability and fault self-check rate.

Fig. 12 shows the relationship between DCS unavailability and fault self-check rate. It can be seen from the figure that the higher the fault self-check rate, the lower the unavailability of DCS, which is consistent with the expected conclusion. However, higher fault self-check rate means higher fault diagnosis costs. It can also be seen from the figure that maintaining a fault self-check rate of more than 40% can reduce the unavailability of DCS by an order of magnitude, which has important engineering significance.

4. Conclusion

DCS is the most important monitoring and control platform in an NPP. The reliability and availability modeling and analysis of digital DCS are of great significance to ensure the stable and reliable operation of NPPs. Petri net is a conventional modeling tool combining graphics and mathematics, which can visually describe the system model and is widely used in dynamic reliability modeling.

In this paper, the DCS of HTR-PM was modeled by Petri net, and the dynamic reliability of the DCS was calculated by Monte Carlo method. The results show that the failure of non-redundant subsystem components has a greater impact on The availability of DCS than that of redundant subsystem components. Particularly, the influence of fault self-check rate on the availability of the DCS was analyzed. The calculation results show that the higher the fault self-check rate, the lower the unavailability of the DCS. When the fault self-check rate is above 40%, the unavailability of DCS will be reduced by an order of magnitude. This conclusion has important engineering practical significance.

5. Acknowledgements

This research was supported by National Natural Science Foundation of China (Grant No. 71801141), LingChuang Research Project of China National Nuclear Corporation, and National Science and Technology Major Project of China (Grant No. ZX069).

6. References

[1] S. Kabir and Y. Papadopoulos. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review, 2019, **115**: 154-175.

[2] T. L. Chu, G. Martinez-Guridi, M. Yue, J. Lehner and P. Samanta. Traditional Probabilistic Risk Assessment Methods for Digital Systems(NUREG/CR-6962), U.S.NRC, 2008.

[3] J. A. Shah, D. Sukheja, P. Bhatnagar and A. Jain. A decision-making problem using dissimilarity measure in picture fuzzy sets, Materials Today: Proceedings, 2010, **101**: 1111-1115.

[4] M. Walker and Y. Papadopoulos. Qualitative temporal analysis: Towards a full implementation of the Fault Tree Handbook, Control Engineering Practice, 2009, **17**: 1115-1125.

[5] S. Junga, J. Yoo and Y.-J. Leeb. A Software Fault Tree Analysis Technique for Formal Requirement Specifications of Nuclear Reactor Protection Systems, Reliability Engineering and System Safety, 2020, **203**: 107064.

[6] H. Y. Cheng and H. L. Sheng. Reliability analysis of digital instrument and control system in nuclear power plant based on Markov model, Automation Applications, 2015, **02**: 20-21.

[7] Y. Jun, Z. Bowen and Y. Ming. Bidirectional implementation of Markov/CCMT for dynamic reliability analysis with application to digital I&C systems, Reliability Engineering and System Safety, 2019, **185**: 278-290.

[8] A. Deser and J. Kuhne. Unipolar and bipolar aerosol charging as time continuous Markov processes, Journal of Aerosol Science, 2021: 105819.

[9] T. Aldernir, D. W. Miller, M. P. Stovsky, J. Kirschenbaurr, P. Bucci, A. W. Fentiman and L. T. Mangan. Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, 2006.

[10] S. J. Lee, W. Jung and J.-E. Yang. PSA model with consideration of the effect of fault-tolerant techniques in digital I&C systems, Annals of Nuclear Energy, 2016, **87**: 375-384.

[11] J. H. Purba, D. T. S. Tjahyani, S. Widodo and A. S. Ekariansyah. Fuzzy probability based event tree analysis for calculating core damage frequency in nuclear power plant probabilistic safety assessment, Progress in Nuclear Energy, 2020, **125**: 103376.

[12] T. Aldemir. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants, Annals of Nuclear Energy, 2013, **52**: 113-114.

[13] Y. X. Jian. Research on key Technologies of complex System reliability based on GO Method, Beijing Institute of Technology, 2016.

[14] G. X. Ming. Research on Reliability Analysis Methods of Digital I&C System for Nuclear Power Plant, Tsinghua University, 2011.

[15] M. Zeinalnezhad, A. G. Chofreh, F. A. Goni, L. S. Hashemi and J. r. J. Kleme. A hybrid risk analysis model for wind farms using Coloured Petri Nets and interpretive structural modelling, Energy, 2011, **229**: 120696.

[16] L. H. Fierroa, R. E. Canoa and J. I. Garcíaa. Modelling of a multi-agent supply chain management system using Colored Petri Nets, ScienceDirect Procedia Manufacturing International Conference on Industry 4.0 and Smart Manufacturing (ISM 2019), vol. 42, pp. 288-295, 2020.

[17] J. Zhou and G. Reniers. Modeling and application of risk assessment considering veto factors using fuzzy Petri nets, Journal of Loss Prevention in the Process Industries, 2020, **67**: 104-216.

[18] N. Chahrour, M. Nasr. J.-M. Tacnet and C. Bérenguer, Deterioration modeling and maintenance assessment using physics-informed stochastic Petri nets: Application to torrent protection structures, Reliability Engineering and System Safety, 2021, **210**: 107524.

[19] C. Lindemann. Performance Modeling with Deterministic and Stochastic Petri Nets, Science of Computer Programming, 2000, **38**: 143-146.

[20] Z. Rochdia, B. Drissb and T. Mohamedc. Industrial systems maintenance modelling using Petri nets, Reliability Engineering and System Safety, 1999, **65**: 119-124.

[21] C. Lindemann. Performance Modelling with Deterministic and Stochastic Petri Nets, Computer Communications, 1999: 980-981.

[22] W. Hongzhou. A survey of maintenance policies of deteriorating systems, European Journal of Operational Research, 2002, **139**: 469-489.