Nuclear Engineering and Technology 54 (2022) 3595–3603

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Optimization of preventive maintenance of nuclear safety-class DCS based on reliability modeling

Hao Peng*, Yuanbing Wang, Xu Zhang, Qingren Hu, Biao Xu

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu, 610213, China

ARTICLE INFO

Article history:
Received 11 January 2022
Received in revised form
11 May 2022
Accepted 13 May 2022
Available online 17 May 2022

Keywords:
Preventive maintenance
Maintenance period
Safety-class DCS

ABSTRACT

Nuclear safety-class DCS is used for nuclear reactor protection function, which is one of the key facilities to ensure nuclear power plant safety, the maintenance for DCS to keep system in a high reliability is significant. In this paper, Nuclear safety-class DCS system developed by the Nuclear Power Institute of China is investigated, the model of reliability estimation considering nuclear power plant emergency trip control process is carried out using Markov transfer process. According to the System-Subgroup-Module hierarchical iteration calculation, the evolution curve of failure probability is established, and the preventive maintenance optimization strategy is constructed combining reliability numerical calculation and periodic overhaul interval of nuclear power plant, which could provide a quantitative basis for the maintenance decision of DCS system.

1. Introduction

NASPIC- the nuclear safety level DCS system for nuclear power plants, which is developed by the Nuclear Power Institute of China, is the most important equipment for safety in nuclear power plants (NPPs). The main function for DCS is immediately shutdown the units while emergency event happening, thus, the complex logical judgement and a large number of components are contained.

Safety-class DCS in NPPs is responsible for emergency trip functions of reactor and engineered safety features actuation, reliability of whom related to implementation of the three safety barrier protection (fuel cladding, primary circuit boundary, containment) functions of the reactor, and directly affects nuclear safety. In engineering practice, DCS maintenance strategy includes two respects: preventive maintenance and corrective maintenance, also named after-the-fact maintenance. Preventive maintenance includes the measures such as regular tests and active maintenance (such as regular replacement of parts) to ensure that the system remains in normal state before the equipment failure. Corrective maintenance refers to the maintenance activities such as equipment repair when equipment failure already occurred.

Actually, corrective maintenance is characterized by suddenness, randomness and urgency, which may lead to unplanned and inadequate maintenance, resulting in secondary maintenance injuries. Therefore, preventive maintenance is a much economical and better choice, and widely applied in industrial fields [1–3]. However, determine an accurate preventive maintenance period, which means carrying out maintenance activities just before the system fail, is difficult. Therefore, planned preventive maintenance is often adopted, and it is carried out during the refueling cycle of NPPs, usually combine with the evaluation of the health status of equipment, maintenance resources and the evolution trend of system reliability in safety-class DCS, and finally determine the preventive maintenance period.

With the developing of preventive maintenance, many theoretical basis is come up with, and has been applied in many fields. Hierarchical Colored Petri Nets is used and simulation is accomplished for maintenance process evaluation and determination [4]. Tian investigated multi-component system, and proportional hazards model is proposed for preventive maintenance decision [5]. Machine learning algorithm such as Support vector machine and logistic regression algorithms are also used in perform the prediction, which support predictive maintenance of nuclear infrastructure [6]. Seo proposed a reliability evaluate method and maintenance suggestion using probabilistic safety assessment (PSA) method [7]. References [8,9] aim at the complex structure of wind turbines, establishes the optimal analytical model, seeks the optimal detection period and preventive maintenance threshold, and achieves the minimizing of long-term maintenance expense rate.

* Corresponding author.
E-mail address: tonghuaph@qq.com (H. Peng).

https://doi.org/10.1016/j.net.2022.05.011

Nomenclature

COM	communication module
DI	digital input module
EMU	electric multiple unit
E2	undetectable faults
IP	protection channel I
MCU	main control unit
MTTF	mean time to failure
PCB	printed circuit board
P_{GR}	state transition matrixes of subgroup
PIP_DI	digital input protection instrument pre-process system
P_{RPC}	state transition matrixes of protection group
P_{RTS}	failure probability of RTS
RTS	reactor trip system
$S_{GRIN}n$	subgroup input part in state n
$S_{RPC}N$	state n of the protection group
μ	maintenance rate
λ_{D_COM}	detectable abnormal failure rate of COM module
λ_{D_GR}	detectable subgroup abnormal failure rate
λ_{D_MCU}	detectable abnormal failure rate of MCU
λ_{D_PIPDI}	detectable abnormal failure rate of PIP-DI module
λ_{U_DO}	failure rate of undetectable DO anomalies
λ_{U_GRIN}	failure rate of undetectable input parts
λ_{U_PIPDI}	failure rate of undetectable PIP-DI anomalies
π_C	printed layer parameters
π_Q	quality parameters
DCS	digital control system
DO	digital output module
E1	detectable faults
Gr.n	Subgroup n
I&C	instrument and control
MTTR	mean time to repair
NPP	nuclear power plants
P_{D_RTS}	Probability of detectable failure of RTS
P_{GRIN}	state transition matrixes of input part
PIPS	protection instrument pre-process system
PSA	probabilistic safety assessment
P_{N_RTS}	Probability of undetectable failure of RTS
$S_{GR}n$	state of subgroup
$S_{MCUS}N$	state n of main control units
$S_{RTS}N$	state n of RTS
λ	failure rate
λ_{D_DO}	detectable abnormal failure rate of the DO module
λ_{D_GRIN}	detectable abnormal failure rate of the input part
λ_{D_RPC}	detectable abnormal failure rate of the protection group
λ_{U_COM}	failure rate of undetectable COM module anomalies
λ_{U_GR}	failure rate of undetectable subgroup anomalies
λ_{U_MCU}	failure rate of undetectable MCU anomalies
λ_{U_RPC}	failure rate of undetectable protection group anomalies
π_E	environmental parameters

The determination of preventive maintenance period is mainly to combine and optimized cost, life, reliability and other important factors. For nuclear safety-class DCS, because it is related to nuclear safety, the preventive maintenance period should mainly evaluate whether the system can perform safety functions during operation in the view of reliability, and the corresponding maintenance period can be formulated in actual engineering.

The determination of preventive maintenance period is mainly to combine and optimized cost, life, reliability and other important factors. For nuclear safety-class DCS, because it is related to nuclear safety, the preventive maintenance period should mainly evaluate whether the system can reliably perform safety functions during operation, and the corresponding maintenance period can be formulated on the basis of system reliability.

The rest parts of this paper are arranged as follows: Section 2 Introduces the structural characteristics of nuclear safety-class DCS. And the basic principle of Markov model is introduced in Section 3. In Section 4, Markov model of RTS emergency trip function is constructed. Specifically, the model is constructed from the run-standby redundancy system, subgroup, protection group and emergency trip system, respectively. In Section 5, the iterating calculation is accomplished and the failure rates are discussed. In Section 6, the preventive maintenance strategy based on the revealed results is established. At last, some conclusions are proposed in Section 7.

2. Research object analysis

In order to achieve high reliability, nuclear safety-class DCS has the characteristics of more redundant than the traditional industrial system. According to the characteristics of nuclear safety-class DCS, preventive maintenance strategy should be formulated responding to the actual operation state and coordinating with the overhaul plan. According to this strategy, the components of nuclear safety-class DCS are maintained and replaced to achieve equipment operation.

The typical safety-class DCS composed of hot standby redundant system, protection group, subgroup, reactor emergency trip system (RTS) and special-purpose engineering safety equipment. A typical safety-class DCS is shown in Fig. 1. RTS consists of four protection groups (IP, IIP, IIIP and IVP), which send local action signals to each other. Each protection group includes two diversity redundant subgroups Gr.1 and Gr.2, which deal with different process parameters, respectively. When the exceed measured signal emerged, "local trip" signal for logical voting of the protection group would be generated. At the same time, the signal will be sent to other protection groups. The 2 out of 4 logic judgement is realized by hardware layout of trip circuit breakers, when the trip circuit breakers which corresponded to two protection groups are opened, the control rods would fall off to realize shutdown. Basically, the signal through the PIPS and DI module input the subgroup, and each subgroup includes two Main Control Unit (MCU), which are normally output by the master and the hot-standby slave synchronized. In case of suddenly failure of the master, hot standby switch occurs and the slave is upgraded to the host to execute functions.

3. Markov model

Markov model is a method to describe random process, which is widely used in modeling of system state transition, especially in industrial reliability estimation, the Markov model is widely applied. In the Markov model, the status of system are shown as Markov nodes, and the node could can be converted to each other [10,11].

The mathematical expression of Markov model is shown in the following formula.

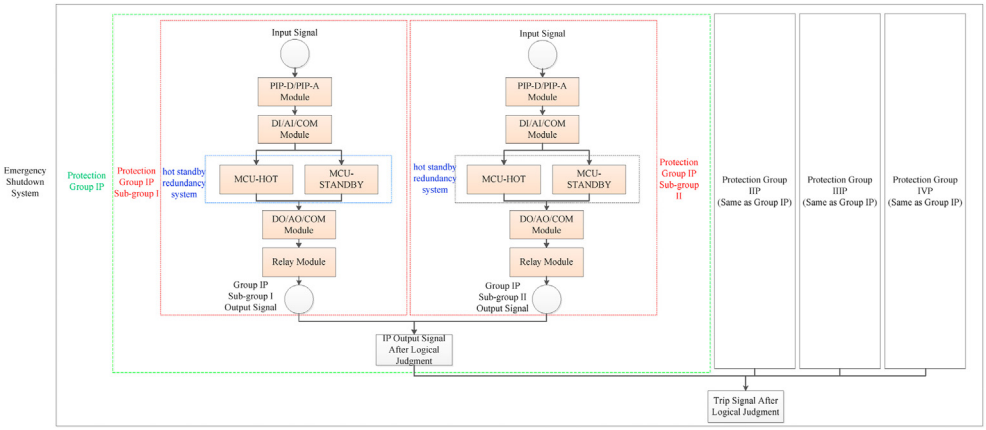

Fig. 1. Typical safety-class DCS structure diagram.

$$P(X_{t+1}|X_t,\ldots,X_1)=P(X_{t+1}|X_t) \tag{1}$$

Where P is the transition probability and X is the state set.

The probability of the system transitioning from state i at time a to state j through b steps is P¬$ij(a,a+b)$, which can be expressed as:

$$P_{ij}(a,a+b)=P\{X_{a+b}=j|X_a=i\} \tag{2}$$

Among them, $\forall a\geq 0, b\geq 1, i,j\in S$ (S is the state space). When b is greater than 1, that is, when there is more than one state transition, the state transition relationship can be expressed in matrix form.

The basic process of above could be expressed as Fig. 2. In engineering practice of DCS operation, because redundant design, minor damage would lead to system degradation, and failure accumulation will lead to system failure. The system states converting process could be indicated using failure rate and maintenance rate, and the process would be going on dynamically (see Fig. 3).

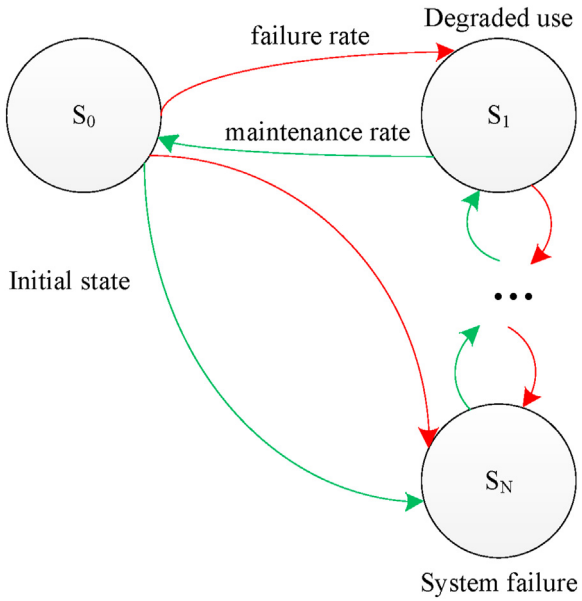

Fig. 2. Basic process of Markov model.

4. Reliability model of RTS

The reliability model of RTS includes three levels, which are, hot standby redundancy system layer, protection group layer and RTS layer, respectively. The failure rate parameters transfer from lower layer to upper layer, and the reliability is calculated in the process.

According to the actual operation situation of the RTS, the failures could be divided into detectable faults and unmonitored faults, which are named as *E1* and *E2* respectively. In case of the above faults, the 3 layers will be transferred from one state to another through above two conditions. The relationship between states of failure and repair is described by maintenance rate μ and failure rate λ.

4.1. Markov model of redundant system

The redundant hot standby system is run in dual operation mode, which is composed of MCU-hot and MCU-standby. When MCU-hot fails, MCU-standby automatically switches to the host. According to the functional characteristics of the redundant hot standby system, the state transformation analysis as follows:

The redundant system initial state is recorded as $S_{MCUS}0$; When *E1* occurs in the hot MCU or the standby MCU, the system transfers to stand-alone operation mode and is recorded as $S_{MCUS}1$; When *E2* occurs in the standby MCU, the system still maintains the dual-machine operation mode, but at this time, the system has lost redundant backup, which is recorded as $S_{MCUS}2$. When *E2* occurs in the hot MCU, the system cannot automatically switch to standby MCU because of undetectable faults, so the hot standby redundant system fails abnormally and is recorded as status $S_{MCUS}4$.

When the hot standby redundant system is in the state of $S_{MCUS}1$, only one MCU is running at this time. If *E1* occurs, the system is recorded as $S_{MCUS}3$. At this time, if *E2* occurs in MCU, abnormal failure occurs in hot standby redundant system, which is the same as $S_{MCUS}4$.

When the hot standby redundant system is in the state $S_{MCUS}2$, the system is still in the dual-operation mode, but actually only hot MCU is running. If *E1* or *E2* occurs at this time, the hot standby redundant system will fail abnormally, which is the same as $S_{MCUS}4$.

It should be pointed out that, as shown in the figure below, in case of detectable abnormality in the system, the original state can be restored by repair, and the repair rate is represented as μ_0. λ_{D_MCU} indicates the detectable abnormal failure rate of MCU, λ_{U_MCU} indicates the failure rate of undetectable MCU anomalies.

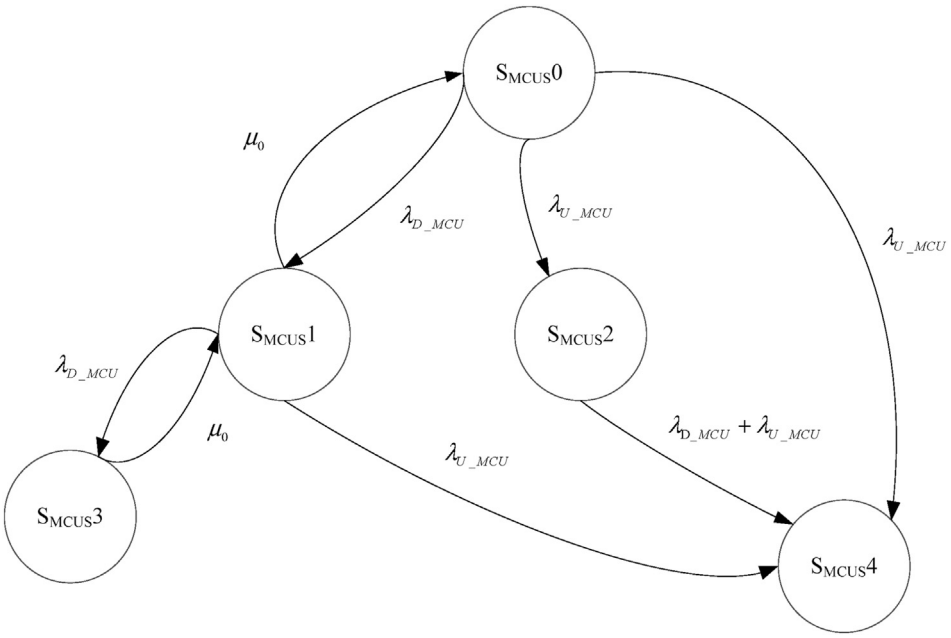

Fig. 3. Markov model of hot standby redundant system.

4.2. Protection group markov model

The structure of safety-class DCS is shown in Fig. 1, the protection group includes two subgroups, and each subgroup is divided into input part, DO part and output part, where input part includes PIP-DI, DI and COM modules, the DO part includes two parallel DO modules, and the output part includes MCU and relay modules. According to the composition of the protection group, the logic of the input part is complex, so it is analyzed separately, and then the subgroup part model is established, and the protection group model is established at last.

4.2.1. Input part

The input part in the subgroup consists of PIP_DI, DI and COM modules, and the voting function of 2 out of 4 (2oo4) logic is realized by software, and the voting logic can be automatically degraded according to the number of detectable faults in the subgroup, as shown in the following Fig. 4.

Part of the input initial state is defined as $S_{GRIN}0$; if *E1* occurs between PIP_DI and DI module, the subgroup input part degenerates into 2oo3 mode and is defined as state $S_{GRIN}1$; In case of *E2*, the input part still keeps 2oo4 mode, but in fact, only 3 channels are normal at this time, which is defined as state $S_{GRIN}2$.

When the subgroup input part is in state $S_{GRIN}1$, if *E1* occurs in COM module, the subgroup input part degenerates into 1oo2 mode, which is defined as state $S_{GRIN}3$. In case of *E2*, the input part of subgroup still keeps 2oo3 mode. In fact, only 2 channels are normal at this time, which is defined as state $S_{GRIN}4$.

When the subgroup input part is in state $S_{GRIN}2$, if *E1* occurs in COM module, the subgroup input part degenerates to 2oo3 mode. In fact, only two of the four channels have normal signals at this time, and the state is the same as $S_{GRIN}4$. In case of *E2*, the input part of subgroup keeps 2oo4 mode. In fact, only 2 channels out of 4 channels are normal at this time, and the defined state is $S_{GRIN}5$.

While the subgroup input part is in state $S_{GRIN}3$, if *E1* occurs in COM module, the subgroup input part has detectable failure, which is defined as state $S_{GRIN}6$; if *E2* occurs, the subgroup input part has abnormal failure, which is defined as state $S_{GRIN}7$.

When the subgroup is in $S_{GRIN}4$ and $S_{GRIN}5$, the input part of the subgroup will fail abnormally regardless of *E1* and *E2* in the COM module, which is defined as the state $S_{GRIN}7$.

In Fig. 5, λ_{D_PIPDI} indicates the detectable abnormal failure rate of PIP-DI module,λ_{U_PIPDI} indicates the failure rate of undetectable PIP-DI anomalies. λ_{D_COM} indicates the detectable abnormal failure rate of COM module, λ_{U_COM} indicates the failure rate of undetectable COM module anomalies.

4.2.2. Subgroup

In the previous section, the input part of the subgroup has been analyzed, and the model of total subgroup is proposed below. In addition to the input part, the subgroup owns DO part composed of two parallel DO modules, and output part composed of a hot standby redundant system (composed of MCU modules) and a relay module.

The initial state of subgroup is defined as $S_{GR}0$. If *E1* occurs in the input part or output part, detectable failure occurs in subgroup, and the defined state is $S_{GR}3$. In case *E2* occurs in the input part, master DO module and output part, abnormal failure occurs in the subgroup, which is defined as state $S_{GR}4$. In case *E1* occurs in the subgroup DO card, because the DO card is designed as main and standby redundancy, the subgroup operates as a single DO module, and the defined status is $S_{GR}1$; If *E2* occurs in the sub-group DO

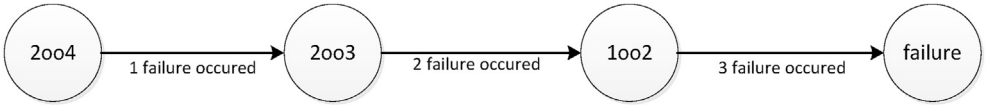

Fig. 4. Degradation function of 2oo4 voting logic.

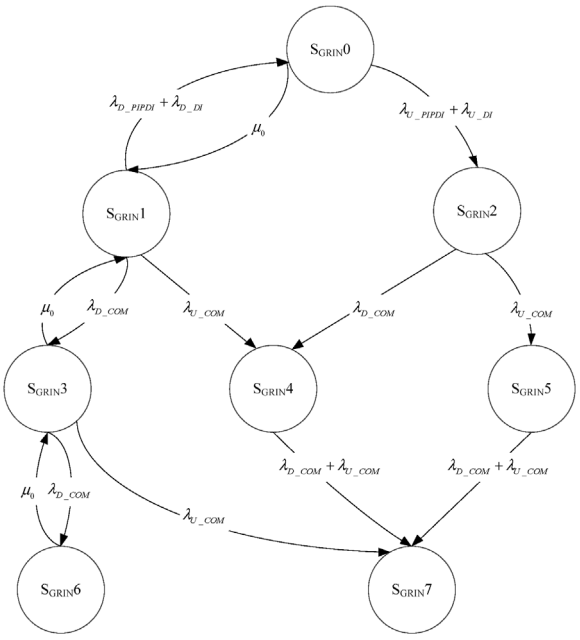

Fig. 5. Markov model of subgroup input part.

card, the system keeps the double DO operation mode, but actually has lost the backup, and the defined status is $S_{GR}2$.

When the subgroup is in $S_{GR}1$, if *E1* occurs in the input part, output part or DO card of the subgroup, the system will have detectable failure, and the status is the same as $S_{GR}3$; In case of *E2*, the system fails abnormally, and it is in the same state as $S_{GR}4$.

When the subgroup is in $S_{GR}2$, if *E1* occurs in the input part, output part or DO card of the subgroup, the system will have detectable failure, and the status is the same as $S_{GR}3$; In case of *E2*, the system fails abnormally, and it is in the same state as $S_{GR}4$.

In Fig. 6, λ_{D_DO} indicates the detectable abnormal failure rate of the DO module, λ_{U_DO} indicates the failure rate of undetectable DO anomalies, λ_{D_GRIN} indicates the detectable abnormal failure rate of the input part, λ_{U_GRIN} indicates the failure rate of undetectable input parts. In the subgroup composition, MCU and relay are connected in series to form the output part, so the failure rate of the output part is the sum of both, so the following relationship is shown in the following figure:

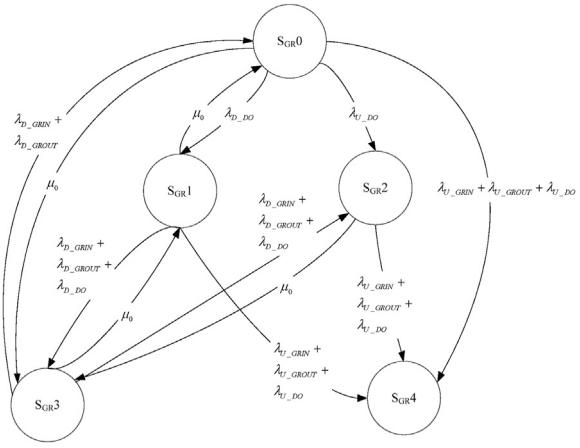

Fig. 6. Subgroup Markov model.

$$\begin{aligned}\lambda_{D\_GROUT} &= \lambda_{MCU\_D} + \lambda_{RELAY\_D}\\ \lambda_{U\_GROUT} &= \lambda_{MCU\_U} + \lambda_{RELAY\_U}\end{aligned} \tag{3}$$

4.2.3. Protection group

A protection group consists of two subgroups, which are backed up from each other. The initial state of the protection group is defined as $S_{RPC}0$. When *E1* occurs in one of the subgroups, the protection group degenerates into a single group mode, and the defined state is $S_{RPC}1$; When *E2* occurs in one of the subgroups, the protection group still keeps the double-group backup mode. In fact, only one subgroup can work normally, and the defined status is $S_{RPC}2$.

When the subgroup is in state $S_{RPC}1$ and *E1* occurs in the running subgroup, the protection group fails and is defined as state $S_{RPC}3$; In case of *E2*, the protection group has abnormal failure, which is defined as state $S_{RPC}4$.

When the subgroup is in the state $S_{RPC}2$, only a single subgroup is actually running. At this time, no matter whether *E1* or *E2* occurs, the protection group will have abnormal failure, that is, the state $S_{RPC}4$.

In Fig. 7, λ_{D_GR} indicates the detectable subgroup abnormal failure rate, λ_{U_GR} indicates the failure rate of undetectable subgroup anomalies.

4.3. Markov model of RTS

The function of the RTS is characterized as, at least two or more protection groups output trip signals, the trip circuit breaker is triggered to act to realize the emergency trip function.

The RTS is defined as $S_{RTS}0$ in the initial state. When an event *E1* occurs in a certain protection group, the emergency trip is triggered when at least one of the other three protection groups of RTS outputs a trip signal, and the state is recorded as $S_{RTS}1$. In case of event *E2* in one protection group, emergency trip will be triggered only when at least one of the other three protection groups of RTS outputs trip signal, and the status will be recorded as $S_{RTS}2$.

When RTS is in the state $S_{RTS}1$, if an event *E1* occurs in a certain protection group, RTS has a system failure, and the state is recorded

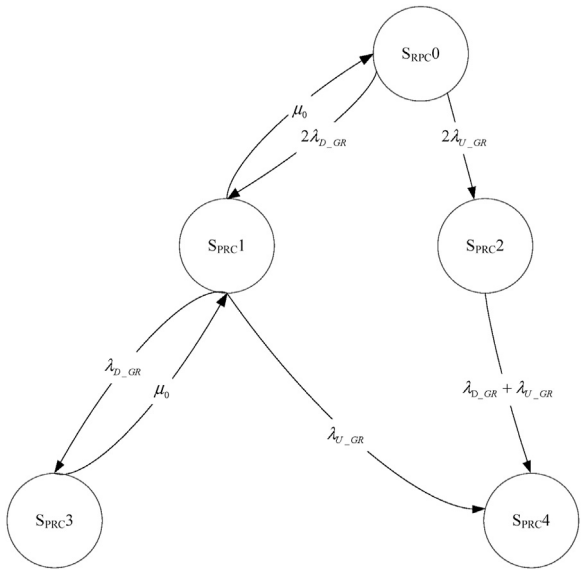

Fig. 7. Markov model of protection group.

as $S_{RTS}3$; In case of event *E2* in a certain protection group, RTS will have abnormal system failure, and the status will be recorded as $S_{RTS}4$.

While RTS is in the state $S_{RTS}2$, if an event *E1* occurs in a certain protection group, RTS will have a system failure and the state will be recorded as $S_{RTS}3$; In case of event *E2* in a certain protection group, RTS will have abnormal system failure, and the status will be recorded as $S_{RTS}4$.

In Fig. 8, λ_{D_RPC} indicates the detectable abnormal failure rate of the protection group, λ_{U_RPC} Indicates the failure rate of undetectable protection group anomalies.

5. Calculation of model failure rate

According to the module failure rate data obtained from the investigated NPP as shown in Table 1, the detectable failure rate of module is obtained according to the general electrical equipment reliability prediction standard (for example SIMENS NORM SN-29500).The failure rate of Printed Circuit Board(PCB) could be calculated by $\lambda = (\lambda_{b1}N+\lambda_{b2})\pi_E\pi_Q\pi_C$, λ_{b1} and λ_{b2} is basic failure rate, which could be obtained in the main-text of standard, and π_E is environmental parameters, π_Q is quality parameters, π_C is printed layer parameters, N is number of metallized holes, which could be obtained by production process documents for each kind of module. On the other hand, the undetectable failure rate is obtained by statistic. The results are shown in Table 1. The failure probabilities of the hot standby redundant system, the subgroup, the protection group and the RTS are calculated.

According to the regulations of Nuclear Power Institute of China, the DCS maintenance including DCS depart auto-operation mode and the unit switch to manual mode, power-on confirmation of replacement modular, replacement operation, tracking manual control and switch to auto-operation mode, the total time consuming not longer than 2 h. Considering the time consumption of replacement modular inventory confirm, delivery from storehouse to filed and other factor, combining with previous operating statistics, the total time consumption is about 4 h, which means the system failure recovery time (MTTR) is 4 h, conducting the maintenance rate $\mu = 0.25$.

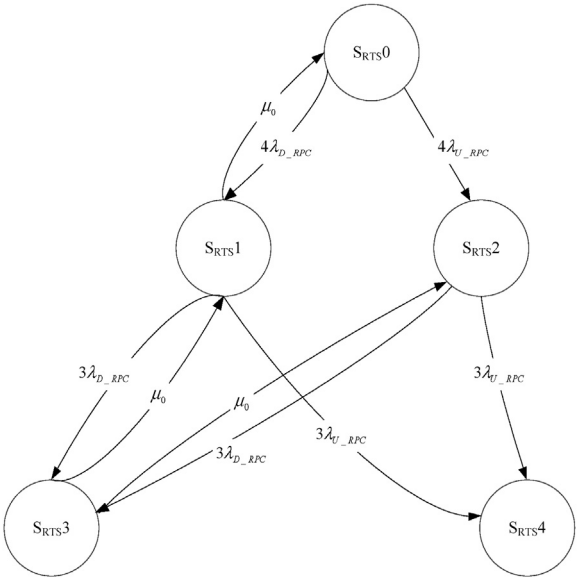

Fig. 8. Markov model of RTS.

5.1. Failure rate of hot standby redundant system

According to the Markov model of hot standby redundant system, the state transition matrix of hot standby redundant system is as follows:

$$T_{MCU} = \begin{bmatrix} 1-\sum & \lambda_{D\_MCU} & \lambda_{U\_MCU} & 0 & \lambda_{U\_MCU} \\ \mu_0 & 1-\sum & 0 & \lambda_{D\_MCU} & \lambda_{U\_MCU} \\ 0 & 0 & 1-\sum & 0 & \lambda_{U\_MCU}+\lambda_{D\_MCU} \\ 0 & \mu_0 & 0 & 1-\sum & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (4)$$

Where Σ represents the sum of the values of other columns. λ_{D_MCU} indicates the detectable abnormal failure rate of MCU, λ_{U_MCU} indicates the failure rate of undetectable MCU anomalies. It is necessary to calculate the probability of hot standby redundancy system in detectable failure state $S_{MCUS}3$ and abnormal failure state $S_{MCUS}4$ through T_{MCU}.

For example, the probability of $S_{MCUS}3$ as an example, a truncated array Q_{MCU} without state $S_{MCUS}3$ information is established (which means the information do not include another failure state S_{MCUS4}), as shown in formula (5).

$$Q_{MCU} = \begin{bmatrix} 1-\sum & \lambda_{D\_MCU} & \lambda_{U\_MCU} \\ \mu_0+\lambda_{U\_MCU} & 1-\sum & 0 \\ \lambda_{U\_MCU}+\lambda_{D\_MCU} & 0 & 1-\sum \end{bmatrix} \quad (5)$$

I is an identity matrix of dimension 3x3 and the superscript −1 indicates the inverse matrix. The $[1-Q_{MCU}]^{-1}$ is solved, the first row of the matrix indicates the total time increment when the system starts from the state $S_{MCUS}0$, and the cumulative sum indicates $MTTF_{D\_MCUS}$ that the system starts from the state $S_{MCUS}0$ to the state $S_{MCUS}3$. Because the safety-class DCS system is electronic equipment, and the exponential distribution can be used to described the reliability model. Therefore, the formula below can be concluded.

$$\lambda = 1/\mathrm{MTTF} \quad (6)$$

The failure rate $\lambda_{D_MCU} = 0.007$Fit can be obtained when the system is in state $S_{MCUS}1$, and $\lambda_{U_MCU} = 31.8$Fit can be also obtained.

5.2. Failure rate of protection group system

According to the Markov model of hot standby redundant system, the state transition matrix of hot standby redundant system is as follows:

According to the Markov models established in 4.2.1, 4.2.2 and

Table 1
Failure rate data of related functional modules.

Functional module	PIP-DI(fit)	DI(fit)	COM(fit)	MCU(fit)	DO(fit)	RELAY(fit)
λ_D	690.7	3723.3	816.8	1209.3	1849.1	0
λ_U	7.3	46.2	8.3	17.1	26.8	40

4.2.3, the state transition matrixes of input part, subgroup and protection group can be obtained as formula (7)-formula (9), respectively.

$$P_{GRIN}=\begin{bmatrix} 1-\Sigma & \lambda_{D\_PIPDI}+\lambda_{P\_DI} & 0 & 0 & 0 & 0 & 0 & 0 \\ \mu_0 & 1-\Sigma & 0 & \lambda_{D\_COM} & \lambda_{U\_COM} & 0 & 0 & 0 \\ 0 & 0 & 1-\Sigma & 0 & \lambda_{D\_COM} & \lambda_{U\_COM} & 0 & 0 \\ 0 & \mu_0 & 0 & 1-\Sigma & 0 & 0 & \lambda_{D\_COM} & \lambda_{U\_COM} \\ 0 & 0 & 0 & 0 & 1-\Sigma & 0 & \lambda_{D\_COM}+\lambda_{D\_COM} & \\ 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & \\ 0 & 0 & \mu_0 & 0 & 0 & \lambda_{U\_COM} & 1-\Sigma & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{D\_COM} & 1 \end{bmatrix} \tag{7}$$

$$P_{GR}=\begin{bmatrix} 1-\sum & \lambda_{D\_DO} & \lambda_{U\_DO} & \lambda_{D\_GRIN}+\lambda_{D\_GROUT} & \lambda_{U\_GRIN}+\lambda_{U\_GROUT}+\lambda_{U\_DO} \\ \mu_0 & 1-\sum & 0 & \lambda_{D\_GRIN}+\lambda_{D\_GROUT}+\lambda_{D\_DO} & \lambda_{U\_GRIN}+\lambda_{U\_GROUT}+\lambda_{U\_DO} \\ 0 & 0 & 1-\sum & \lambda_{D\_GRIN}+\lambda_{D\_GROUT}+\lambda_{D\_DO} & \lambda_{U\_GRIN}+\lambda_{U\_GROUT}+\lambda_{U\_DO} \\ 0 & \mu_0 & \mu_0 & 1-\sum & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{8}$$

$$P_{RPC}=\begin{bmatrix} 1-\sum & 2\lambda_{D\_GR} & 2\lambda_{U\_GR} & 0 & 0 \\ \mu_0 & 1-\sum & 0 & \lambda_{D\_GR} & \lambda_{U\_GR} \\ 0 & 0 & 1-\sum & 0 & \lambda_{D\_GR}+\lambda_{U\_GR} \\ 0 & \mu_0 & 0 & 1-\sum & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{9}$$

Referring to the method described in the hot standby redundancy system, the failure rates of the input part of the subgroup, the subgroup and the protection group in detectable failure and abnormal failure are calculated. The results are: λ_{D_GRIN}=*0.51Fit*、λ_{U_GRIN} = 5.9*Fit*、λ_{D_GR}=*1775.3Fit*、λ_{U_GR} = 96.1*Fit*、λ_{D_RPC}=*3750.7Fit*、λ_{U_RPC} = 272.6*Fit*.

5.3. RTS failure rate

According to the Markov model of RTS established in 4.3, the state transition matrix of RTS can be obtained as shown in formula (10), which will lead to the failure probability of RTS and used in preventive maintenance period decision.

$$P_{RTS}=\begin{bmatrix} 1-\sum & 4\lambda_{D\_RPC} & 4\lambda_{U\_RPC} & 0 & 0 \\ \mu_0 & 1-\sum & 0 & 3\lambda_{D\_RPC} & 3\lambda_{U\_RPC} \\ 0 & 0 & 1-\sum & 3\lambda_{D\_RPC} & 3\lambda_{U\_RPC} \\ 0 & \mu_0 & \mu_0 & 1-\sum & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{10}$$

6. Decision strategy of preventive maintenance period

The data management of I&C emulation system is closely related to its logic operation and simulation features. Based on the analysis of system architecture and simulation function for a specific emulation system, this paper introduces a new data management method, and its effectiveness has been verified in various experiments by combining the simulation function.

According to the properties of Markov process, the probabilities of RTS being in $S_{RTS}3$ and $S_{RTS}4$ respectively after n hours (n transitions) can be calculated according to formula (10). They are denoted as P_{D_RTS} and P_{N_RTS}, respectively.

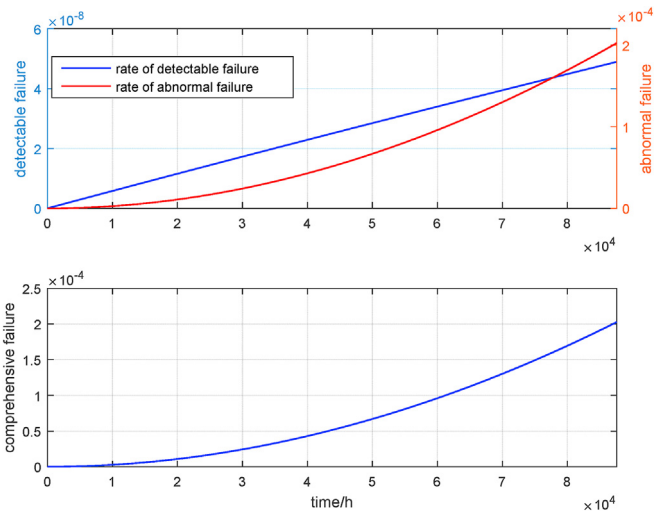

Fig. 9. RTS failure probability evolution curve.

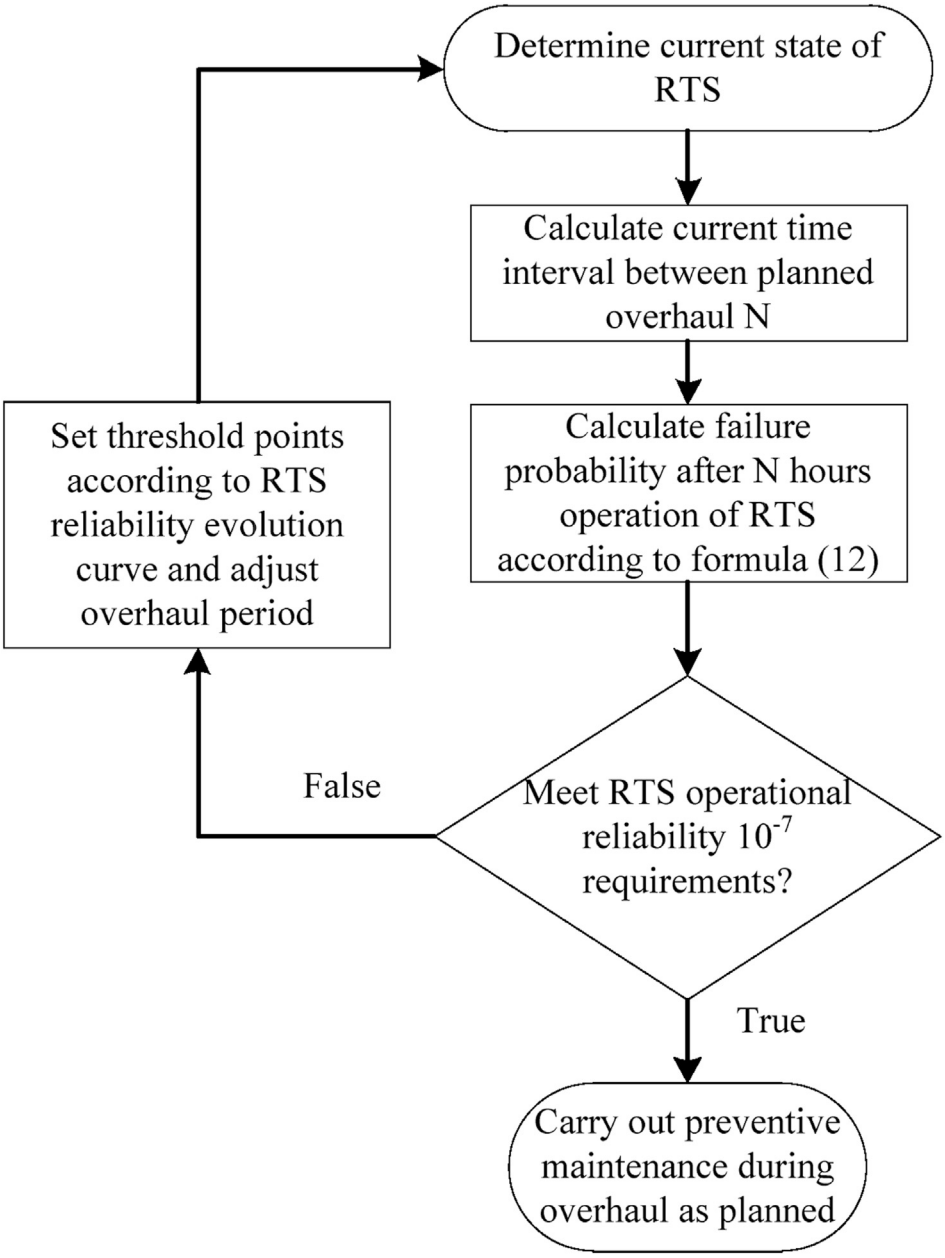

Fig. 10. Preventive maintenance period determination strategy.

The probability of dangerous failure of RTS system in the *n th* hour is:

$$P_n = P_{D\_RTS} + P_{U\_RTS} \tag{11}$$

It is assumed that the RTS is in normal operation state $S_{RTS}0$ when it starts operation, i.e., $P_0 = [1\ 0\ 0\ 0\ 0]$, and the probability of each state after running for *n* hours can be expressed as:

$$P_n = P_0 \times P_{RTS}^n = [p_0\ p_1\quad p_2\quad p_3\quad p_4\,] \tag{12}$$

The elements of the matrix P_n are the probabilities that the RTS is in $S_{RTS}0$~ $S_{RTS}4$ in turn. For detailed analysis, the changing trend of p_3 and p_4 in the matrix P_n (i.e. the probabilities that RTS is in detectable failure and abnormal failure) with time is analyzed, as shown in the following Fig. 9.

It can be revealed that the probability of detectable failure of RTS increases linearly with time, which reflects the controllable failure of the system, and its occurrence probability is much lower than the abnormal failure probability. With the increase of system running time, the change rate of abnormal failure probability increases, which reflects that the uncertainty of fault increases with the increase of running time. According to the above analysis, it is necessary to match the quantitative calculation result of RTS failure with the overhaul period of the system, and help operators to formulate a preventive maintenance plan. According to the DCS operation and maintenance requirements of a NPPs (lower than 10^{-7}), the preventive maintenance strategy is formulated as shown in the following Fig. 10. The summary steps are as follows:

(1) Comparing with Markov model of RTS, confirming RTS status regularly;

(2) Obtaining the interval between current time to the planned overhaul time (N hours) ;
(3) According to formula (12), calculate the probability sum of SRTS3 and SRTS4 for RTS after running for N hours;
(4) If the result meets the RTS reliability requirement, preventive maintenance can be carried out according to calculation;
(5) If the requirement could not be met, determining the corresponding time when the system reaches the lower limit of reliability according to the RTS reliability evolution curve obtained by formula (12), and properly is carried out overhaul in advance.

7. Conclusions

In this paper, the structural characteristics of nuclear safety-class DCS is investigated, and the reliability modeling is accomplished using Markov process, and the proposed model characterized layer-iteration process, which described the redundant characters of DCS innovatively. Based on the established model, the quantitative RTS failure rate is obtained, and the detectable failure and abnormal failure are considered, respectively, the simulation results reveal the reliability trends of system. Combining with the reliability estimation result, the preventive maintenance determination strategy is carried out, which provided an effective measure to formulate overhaul plan in actual NPPs operation.

Funding

The project was funded by Sichuan Provincial Science and Technology Fund for Distinguished Young Scholars (2020JDJQ0068).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] O.C. Görür, X. Yu, F. Sivrikaya, Integrating predictive maintenance in adaptive process scheduling for a safe and efficient industrial process, Appl. Sci. 11 (11) (2021) 5042, https://doi.org/10.3390/app11115042.
[2] F. Calabrese, A. Regattieri, M. Bortolini, et al., Predictive maintenance: a novel framework for a data-driven, semi-supervised, and partially online prognostic health management application in industries, Appl. Sci. 11 (8) (2021) 3380, https://doi.org/10.3390/app11083380.
[3] A. Jardine, D. Lin, D. Banjevic, A review on machinery diagnostics and prognostics implementing condition-based maintenance, Mech. Syst. Signal Process. 20 (7) (2006) 1483–1510.
[4] S.P. Orlov, S.V. Susarev, R.A. Uchaikin, Application of hierarchical colored Petri Nets for technological facilities' maintenance process evaluation, Appl. Sci. 11 (11) (2021) 5100, https://doi.org/10.3390/app11115100.
[5] Z. Tian, H. Liao, Condition based maintenance optimization for multi-component systems using proportional hazards model, Reliab. Eng. Syst. Saf. 96 (5) (2011) 581–589.
[6] H.A. Gohel, H. Upadhyay, L. Lagos, et al., Predictive maintenance architecture development for nuclear infrastructure using machine learning, Nucl. Eng. Technol. 52 (7) (2020) 1436–1442.
[7] J. Seo, H.G. Kang, E.C. Lee, et al., Experimental approach to evaluate software reliability in hardware-software integrated environment, Nucl. Eng. Technol. 52 (7) (2020) 1462–1470.
[8] B.R. Sarker, T. Ibn Faiz, Minimizing maintenance cost for offshore wind turbines following multi-level opportunistic preventive strategy, Renew. Energy 85 (2016) 104–113.
[9] C. Zhang, W. Gao, S. Guo, et al., Opportunistic maintenance for wind turbines considering imperfect, reliability-based maintenance, Renew. Energy 103 (2016) 606–612.
[10] P. Kumar, L.K. Singh, C. Kumar, Performance evaluation of safety-critical systems of nuclear power plant systems, Nucl. Eng. Technol. 52 (3) (2019) 560–567.
[11] E.C. Lee, S.K. Shin, P.H. Seong, Evaluation of availability of nuclear power plant dynamic systems using extended dynamic reliability graph with general gates (DRGGG), Nucl. Eng. Technol. 51 (2) (2018) 444–452.