

# RELIABILITY AND SAFETY ANALYSIS ON RAILWAY SIGNAL REGIONAL COMPUTER INTERLOCKING SYSTEM

H. SU & J. WEN

School of Automation and Electrical Engineering, Lanzhou Jiaotong University, China.

## ABSTRACT

Regional computer interlocking system (RCIS) is a signal control system, which performs all of the interlocking logic operations and implements the centralized control on multiple stations using one set of interlocking equipment alone. There are two diverse RCIS solutions in China, namely, the centralized interlocking scheme and the distributed interlocking scheme. The main deficiency of the former lies in that the entire system would be paralyzed once the central interlocking equipment fails. The latter overcomes the flaw of the former and can disperse the danger. However, it is not suitable for some small stations due to higher upfront investment. Hence, a better selection is that the two schemes are combined together to play their respective advantages and overcome each other's shortcomings. As a safety-critical system, the RCIS is broadly applied but the investigations on it are rarely reported in reliability and safety. Based on it, this paper establishes the Markov model of the RCIS and investigates its reliability and safety. During modeling some significant factors, such as common-cause failure, coverage rate of diagnostic systems, online maintainability, and periodic inspection maintenance, and as well as diverse failure modes, are fully considered. The relevant researches show that the combination of the two RCIS schemes possesses better safety and reliability, and is an ideal realization mode, not only for the stations but also for the open lines between the stations.

*Keywords: Interlocking scheme, Markov model, railway signal, regional computer interlocking system (RCIS), reliability, safety.*

## 1 INTRODUCTION

Different from traditional computer interlocking systems, the regional computer interlocking system (RCIS) completes interlocking logic operations and implements centralized control on multiple stations only using one set of interlocking equipment in a range of whole control area. Generally, the RCIS possesses some significant characteristics such as centralized control, and centralized dispatch, and requires less maintenance.

The RCIS applications are more developed abroad, such as 471-mile long Madrid Seville high-speed railway using nine interlocking centers to manage 29 stations, and as well as 270-mile long railway using seven interlocking centers to be in charge of 35 stations in Finland [1]. Practical applications show that the RCIS owns greater benefits compared with traditional interlocking systems. In the 1990s, the government organized a research and development department to investigate and demonstrate RCIS in China, and now it has already reached the practical application stage. In China, the RCIS has already been applied in some larger hub stations, and urban transportations, and Lhasa section in Qinghai-Tibet railway where the weather is bad. For instance, in Tongliao south marshalling station, a set of computer interlocking system is used to realize regional signal control of all the four yards [2]. In Lake East marshalling station, the first and the second yard adopt dispatching supervision adding the centralized interlocking scheme to allow the RCIS control. Interlocking machine passes information and control commands to each remote station through the interlocking bus to complete the measurements and control in range of the whole area [3]. Harbin hub adopts distributed interlocking scheme adding centralized dispatch to

realize the RCIS, where each substation is independently arranged a set of computer interlocking system, and the commands of dispatching center are transmitted by optical fiber cable to each substation to implement the control of each station's signaling devices independently [4]. RCIS is also used in the urban transportation, such as extension line of Dalian express rail line 3 using a set of DS6-K5B RCIS to complete control on seven stations [5]. In addition, RCIS is also suitable for Qinghai–Tibet railway, where environment is harsh and maintenance is inconvenient. The railway from west Lhasa to Liuwu is a good case that realizes regional control of two stations using one set of computer interlocking system [6]. In January 6, 2004, China's first RCIS was used from Jining to Benhong, there are five stations in this scope of control [7]. The cases above show that RCIS possesses very good application potential in China. Presently, many researchers have already begun conducting reliability and safety analysis of key redundant equipment for traditional station interlocking such as the dual hot spare module, double 2-vote-2, 3-vote-2 voting, etc. [8–10]. However, the investigations on RCIS in reliability and safety are quite few. Based on it, this paper investigates the reliability and safety of the RCIS, and implements comparison with centralized computer interlocking systems. The relevant research results possess certain guidance significance for RCIS application.

## 2 SYSTEM DESCRIPTION

### 2.1 RCIS schemes

(1) *Centralized interlocking scheme, i.e. dispatching supervision*: Its main feature is in which the interlocking machine is set up only in the master station, while I/O data collection and drive equipment is just arranged in controlled stations. The advantage of this scheme lies in that equipment maintenance is convenient, but whose deficiency is that the entire region will be paralyzed once the center interlocking machine fails. Lake East marshaling station, and north Linyi station, and the first RCIS opened from Jining to Benhong belongs to this interlocking type.

(2) *Distributed interlocking scheme, i.e. dispatching centralization*: In this scheme, both the central station and the controlled stations all configure the interlocking equipments. Thus, the impact scope of single station devices fault only is only within itself rather than the whole system. The potential risk is also decreased largely as any one of interlocking machines gets failure. In addition, each station interlocking cell can operate independently so that the operation modes of the whole system become more flexible. However, the scheme results in a higher upfront investment, and is not suitable for some small stations. Harbin railway hub and Lake East station take this mode.

### 2.2 RCIS principle in hub station

To reduce the construction investment and avoid the potential risk, we combine the two schemes above together after comprehensive consideration on the advantages and disadvantages of the two, and define it as the combination scheme. The principle of the scheme is that the whole station interlocking is divided into several subregions, and each subregion adopts the centralized interlocking while the relationships among them are the distributed one, such as two-region RCIS and three-region RCIS.

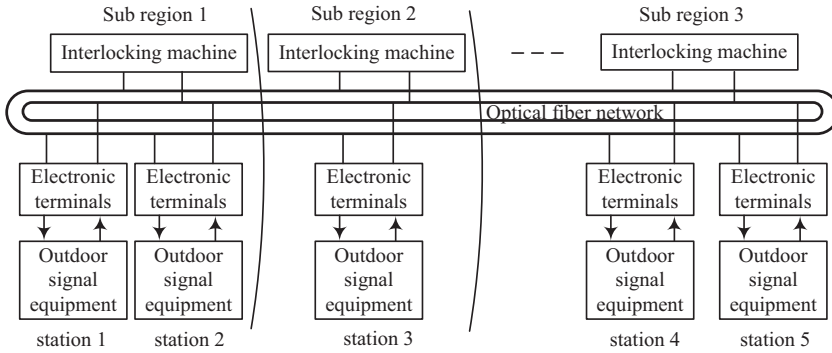


Figure 1: RCIS structure in hub station.

Figure 1 shows a three-region RCIS structure in hub station, where the whole area is divided into three subregions, and each subregion is provided with one set of interlocking cell. According to the number of signal equipments, each subregion may have different numbers of stations but possess roughly same number of signaling equipments. As shown in subregion 1 in Fig. 1, the multiple stations belonging to same subregion share one set of interlocking equipment that can effectively reduce the investment. In addition, if any one interlocking cell generates a detected failure, it will then be taken over by another one working normally coming from other subregions. To do this, there will be an increase working load of the interlocking machine taking over, but it ensures normal operation of the whole area. It also wins a repairing time for the failure cell and improves the work efficiency of the full area.

### 3 RELEVANT CONCEPTS

#### 3.1 Basic concepts

For high reliability and high safety systems, diagnostic coverage rate is a significant factor and is defined as the probability that it can be detected out as one failure occurs. Computer interlocking system is a safety-critical system, and so its diagnostic coverage rate is higher.

Common cause failure (CCF) is referring to one that multiple modules failure occurs at the same time arising by single cause. Clearly, CCF offsets the advantage of a fault-tolerant system. And so, CCF is a factor not to be able to be ignored in the analysis on high safety and high reliability systems. In this paper, we select the most commonly used beta factor model to simulate CCF during modeling.

Let the failure rate of the cell be  $\lambda$ , and the parameter of the beta factor model be  $\beta$ , and thus  $\lambda$  is divided into the two parts, that is  $\lambda^C$  and  $\lambda^N$ , wherein  $\lambda^C$  is aroused by CCF, and  $\lambda^N$  is aroused by normal failure independent from CCF. And then,  $\lambda^C$  and  $\lambda^N$  can be represented by

$$\lambda^C = \beta\lambda \tag{1}$$

$$\lambda^N = (1-\beta)\lambda \tag{2}$$

Probability of failing safely (PFS) is defined as the probability that the system locates in a safe side when one failure happens, and conversely, probability of failing on demand (PFD) is referring to one that the system locates in danger side when one failure happens.

Let reliability function of the cell be  $R(t)$ , and the probability density function of failure time be  $f(t)$ , the mean time to failure (MTTF) can be then expressed by

$$\text{MTTF} = E(T) = \int_0^{+\infty} tf(t) dt = - \int_0^{+\infty} t d[R(t)] = \int_0^{+\infty} R(t) dt \quad (3)$$

### 3.2 Failure mode analysis

For convenience analysis, we conduct some basic assumptions below.

1. System comparators, and voting cells, and interface circuits, and as well as communication lines used to constitute interlocking cells are considered completely reliable.
2. The interlocking machine in different subregions possesses same failure rate, and both the repairing time and the failure time follow the exponential distribution.
3. The failure rate of interlocking cells will increase when it takes over the task of other failure cells. Let normal failure rate of one cell be  $\lambda$ , and then the failure rate of which becomes  $\lambda_1$  after taking over one failing cell, and  $\lambda_2$  for taking over two, clearly,  $\lambda_2 > \lambda_1 > \lambda$ .
4. Inspection and maintenance are perfect, that is, the cell can restore to its original state after it is repaired.

After considering the diagnostic ability of the diagnostic system and CCF, the failure rate of the cell can be divided into eight types such as  $\lambda^{\text{SDN}}$ ,  $\lambda^{\text{SDC}}$ ,  $\lambda^{\text{SUN}}$ ,  $\lambda^{\text{SUC}}$ ,  $\lambda^{\text{DDN}}$ ,  $\lambda^{\text{DDC}}$ ,  $\lambda^{\text{DUN}}$ , and as well as  $\lambda^{\text{DUC}}$ . Here,  $\lambda^{\text{SDN}}$  expresses the safe detected normal failure rate,  $\lambda^{\text{SDC}}$  means the safe detected CCF rate,  $\lambda^{\text{SUN}}$  denotes the safe undetected normal failure rate,  $\lambda^{\text{DDN}}$  expresses the dangerous detected normal failure rate,  $\lambda^{\text{SUC}}$  is the safe undetected CCF rate,  $\lambda^{\text{DDC}}$  means the dangerous detected CCF rate,  $\lambda^{\text{DUN}}$  is the dangerous undetected normal failure, and  $\lambda^{\text{DUC}}$  means dangerous undetected CCF rate. Let the gross failure rate of the cell be  $\lambda$ , the safety-side failure rate be  $\lambda^{\text{S}}$ , the danger-side failure rate be  $\lambda^{\text{D}}$ , and then we obtain

$$\lambda = \lambda^{\text{S}} + \lambda^{\text{D}} \quad (4)$$

According to Zhao *et al.* [11], the danger ratio  $\sigma$  can be written as  $\sigma = \lambda^{\text{D}}/(\lambda^{\text{S}} + \lambda^{\text{D}})$ , and then

$$\begin{aligned} \lambda^{\text{S}} &= (1 - \sigma)\lambda \\ \lambda^{\text{D}} &= \sigma\lambda \end{aligned} \quad (5)$$

After considering the diagnostic coverage capability, the safety-side failure rate is then partitioned into two parts. The one is detected safety failure rate  $\lambda^{\text{SD}}$  and the other is undetected safety failure rate  $\lambda^{\text{SU}}$ . Similarly, the danger-side failure rate is also divided into two parts, i.e. detected dangerous failure  $\lambda^{\text{DD}}$  and undetected dangerous failure rate  $\lambda^{\text{DU}}$ . Thus, we obtain

$$\lambda^{\text{S}} = \lambda^{\text{SD}} + \lambda^{\text{SU}} \quad (6)$$

$$\lambda^{\text{D}} = \lambda^{\text{DU}} + \lambda^{\text{DD}} \quad (7)$$

Further, any one of the four failure rates at right side in (6) and (7) can be divided into two parts again according to normal failure and CCF; thus, we obtain eight types of the failure rates. Let the diagnosis coverage rate be  $c$  and CCF factor be  $\beta$ , and then  $\lambda^{\text{SDC}}$  can be calculated by

$$\lambda^{\text{SDC}} = \beta\lambda^{\text{SD}} = \beta c\lambda^{\text{S}}$$

Similarly, we can work out the other failure rates.

## 4 TWO-REGION RCIS MODEL

### 4.1 Structure of two-region RCIS

Figure 2 shows a structure of two-region RCIS, where the whole control area is divided into two subregions and each subregion is provided with a set of interlocking equipment. If any one of interlocking cells generates a detected failure, it will be then taken over by another subregion cell which works properly.

### 4.2 Two-region RCIS model

There are two kinds of working modes for two-region RCIS. The one is degradation not allowed, and the other is degradation allowed. The former refers to the one that the total system is thought to be invalid as long as any one subregion malfunctions due to an undetected failure. And conversely, the latter is understood as that the rest of system still can work normally after one subregion becomes invalid since it suffers an undetected safety failure. Certainly, if all of the subregions malfunction, then the total system is thought invalid. Clearly, the former is more conservative and has higher safety.

#### 4.2.1 Two-region RCIS model with degradation not allowed

Assume that the system consists of two identical cells, and then the Markov state transition diagram can be described as shown in Fig. 3. In Fig. 3, the state 0 expresses that the two cells are perfect and the system works normally, the state 1 expresses that one cell ceases work and is being repaired due to a safety failure being detected out and another cell takes over its task and works under heavy loads, the state 2 represents that one cell ceases work and is being repaired due to a dangerous failure being detected out and another cell takes over it and works under heavy loads, the state 3 expresses the system safety failure, the state 4 represents the

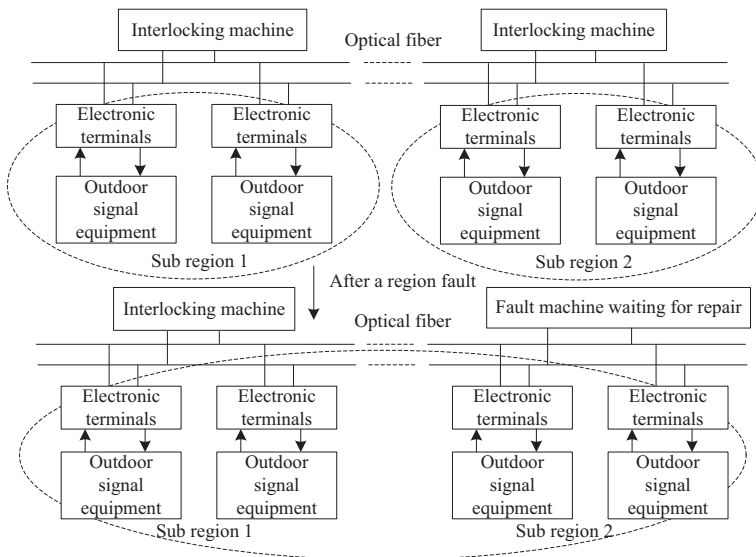


Figure 2: Structure of two-region RCIS.

system dangerous failure but this failure can be detected out, and the state 5 represents the system dangerous failure but it cannot be detected out. From the state 0 to the state 2, the system works normally. The parameter  $\mu_0$  is online maintenance rate, and  $\mu_{SD}$  is a reciprocal of the system restart time after a safety failure occurs.

According to Fig. 3, the state transition matrix  $P$  can be easily written as follows:

$$P = \begin{matrix} & \begin{matrix} \text{"0"} & \text{"1"} & \text{"2"} & \text{"3"} & \text{"4"} & \text{"5"} \end{matrix} \\ \begin{matrix} \text{"0"} \\ \text{"1"} \\ \text{"2"} \\ \text{"3"} \\ \text{"4"} \\ \text{"5"} \end{matrix} & \left[ \begin{array}{cccccc} 1-\Sigma & 2\lambda^{SDN} & 2\lambda^{DDN} & \lambda^{SDC} + \lambda^{SUC} + 2\lambda^{SUN} & \lambda^{DDC} & \lambda^{DUC} + 2\lambda^{DUN} \\ \mu_0 & 1-\Sigma & 0 & \lambda_1^S & \lambda_1^{DD} & \lambda_1^{DU} \\ \mu_0 & 0 & 1-\Sigma & \lambda_1^S & \lambda_1^{DD} & 0 \\ \mu_{SD} & 0 & 0 & 1-\Sigma & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right] \end{matrix}$$

4.2.2 Two-region RCIS model with degradation allowed

Markov model of two-region RCIS with degradation allowed is shown in Fig. 4. The relevant state descriptions are basically consistent with ones in Fig. 3 except that the state 2 that expresses the degradation state of system, the state is understood as that there is only one

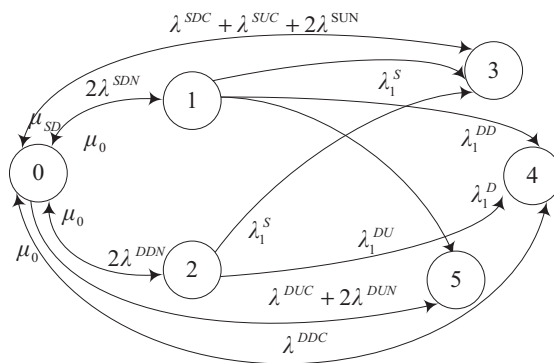


Figure 3: Two-region RCIS model with degradation not allowed.

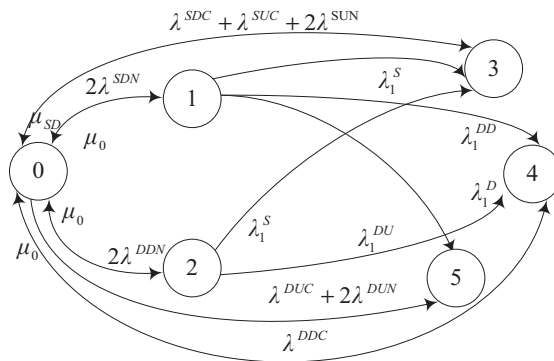


Figure 4: Two-region RCIS model with degradation allowed.

subregion operating in system due to an undetected safety failure. From the state 0 to 3, the system works normally.

According to Fig. 4, the state transition matrix  $P$  can be written as follows:

$$\begin{matrix}
 & \text{"0"} & \text{"1"} & \text{"2"} & \text{"3"} & \text{"4"} & \text{"5"} & \text{"6"} \\
 \mathbf{P} = \begin{matrix} \text{"0"} \\ \text{"1"} \\ \text{"2"} \\ \text{"3"} \\ \text{"4"} \\ \text{"5"} \\ \text{"6"} \end{matrix} & \begin{bmatrix}
 1 - \Sigma & 2\lambda^{\text{SDN}} & 2\lambda^{\text{SUN}} & 2\lambda^{\text{DDN}} & \lambda^{\text{SDC}} + \lambda^{\text{SUC}} & \lambda^{\text{DDC}} & \lambda^{\text{DUC}} + 2\lambda^{\text{DUN}} \\
 \mu_0 & 1 - \Sigma & 0 & 0 & \lambda_1^{\text{S}} & \lambda_1^{\text{DD}} & \lambda_1^{\text{DU}} \\
 0 & 0 & 1 - \Sigma & 0 & \lambda^{\text{S}} & \lambda^{\text{DD}} & \lambda^{\text{DU}} \\
 \mu_0 & 0 & 0 & 1 - \Sigma & \lambda_1^{\text{S}} & \lambda_1^{\text{DD}} & 0 \\
 \mu_{\text{SD}} & 0 & 0 & 0 & 1 - \Sigma & 0 & 0 \\
 \mu_0 & 0 & 0 & 0 & 0 & 1 - \mu_0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1
 \end{bmatrix}
 \end{matrix}$$

### 5 THREE-REGION RCIS MODEL

#### 5.1 Structure of three-region RCIS

The structure of three-region RCIS is shown in Fig. 5, where the whole control area is divided into three subregions and each subregion is provided with a set of interlocking equipment.

#### 5.2 Three-region RCIS model

Three-region RCIS possesses three kinds of different working modes, respectively, corresponding to the three models, that is, the secondary degradation allowed model (SDAM), primary degradation allowed model (PDAM), and primary degradation not allowed model (PDNAM). Conservative thinking, PDNAM means that the total system will be seen as failure as long as there is one subregion failure due to an undetected failure occurring. Different from PDNAM, PDAM expresses that the total system will be a failure as long as there is one subregion failure due to an undetected dangerous failure occurring, namely the rest of the system still work normally when one subregion ceases to work due to an undetected safety failure. On the basis of PDAM, if another subregion then fails, at the moment, only the sole one subregion works normally, which is defined as SDAM in three-region RCIS. Clearly, only if all subregions fail, the whole system is seen as failure.

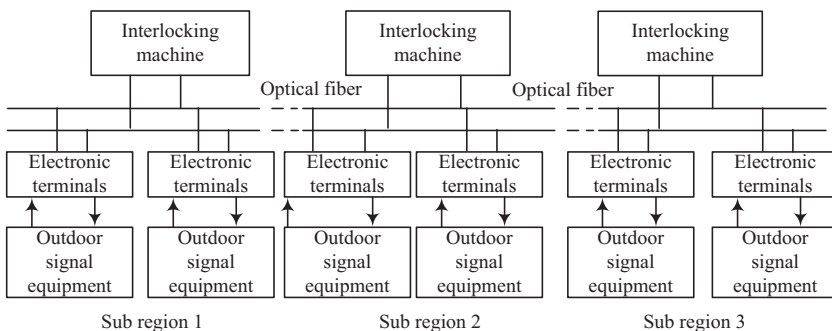


Figure 5: Structure of a three-region RCIS.

5.2.1 PDNAM in three-region RCIS

The system state transition diagram of the PDNAM can be seen in Fig. 6. The state 0 expresses that the three cells are perfect and the system works normally, and the state 1 means that one cell fails and is being repaired due to a detected safety failure; at this time, there is one cell overloading and the remaining one is at normal state. At the state 2, one cell generates a detected dangerous failure and is being repaired, and one cell overloads and the remaining one is at normal state. The descriptions on other states are the same with the ones of degradation not allowed model of 2-region RCIS.

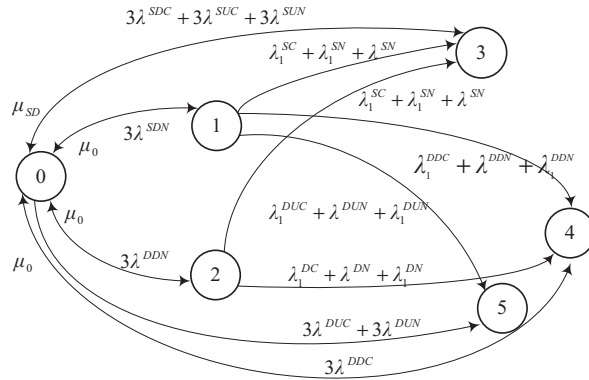


Figure 6: State transition diagram of PDNAM in three-region RCIS.

According to Fig. 6, the state transition matrix  $P$  can be written as follows:

$$P = \begin{bmatrix} 1 - \Sigma & 3\lambda^{SDN} & 3\lambda^{DDN} & 3\lambda^{SDC} + 3\lambda^{SUC} + 3\lambda^{SUN} & 3\lambda^{DDC} & 3\lambda^{DUC} + 3\lambda^{DUN} \\ \mu_0 & 1 - \Sigma & 0 & \lambda_1^{SC} + \lambda_1^{SN} + \lambda^{SN} & \lambda_1^{DDC} + \lambda^{DDN} + \lambda_1^{DDN} & \lambda_1^{DUC} + \lambda^{DUN} + \lambda_1^{DUN} \\ \mu_0 & 0 & 1 - \Sigma & \lambda_1^{SC} + \lambda_1^{SN} + \lambda^{SN} & \lambda_1^{DC} + \lambda^{DN} + \lambda_1^{DN} & 0 \\ \mu_{SD} & 0 & 0 & 1 - \Sigma & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 1 - \mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

5.2.2 PDAM in three-region RCIS

The state transition diagram on PDAM in three-region RCIS is shown in Fig. 7. The relevant state descriptions are basically consistent with the ones in Fig. 6 except that the state 2 expresses the system degradation state; at this state, one cell generates an undetected safety failure, whereas the other two cells are perfect.

The state transition matrix  $P$  can be as follows:

$$P = \begin{bmatrix} 1 - \Sigma & 3\lambda^{SDN} & 3\lambda^{SUN} & 3\lambda^{DDN} & 3\lambda^{SDC} + 3\lambda^{SUC} & 3\lambda^{DDC} & 3\lambda^{DUC} + 3\lambda^{DUN} \\ \mu_0 & 1 - \Sigma & 0 & 0 & \lambda_1^{SC} + \lambda_1^{SN} + \lambda^{SN} & \lambda_1^{DDC} + \lambda^{DDN} + \lambda_1^{DDN} & \lambda_1^{DUC} + \lambda^{DUN} + \lambda_1^{DUN} \\ 0 & 0 & 1 - \Sigma & 0 & \lambda^{SC} + 2\lambda^{SN} & \lambda^{DDC} + 2\lambda^{DDN} & \lambda^{DUC} + 2\lambda^{DUN} \\ \mu_0 & 0 & 0 & 1 - \Sigma & \lambda_1^{SC} + \lambda_1^{SN} + \lambda^{SN} & \lambda_1^{DC} + \lambda^{DN} + \lambda_1^{DN} & 0 \\ \mu_{SD} & 0 & 0 & 0 & 1 - \Sigma & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 0 & 1 - \mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$



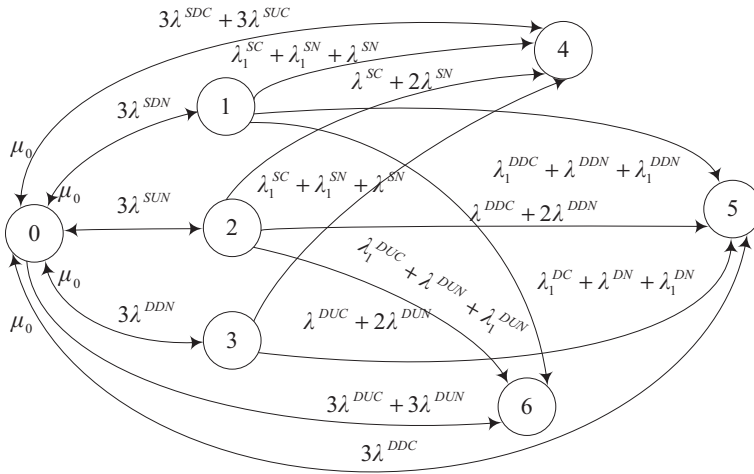


Figure 7: State transition diagram of PDAM in three-region RCIS.

### 5.2.3 SDAM in three-region RCIS

As shown in Fig. 8, the descriptions on the states 0, 1, and 2 are the same as that of PDNAM in three-region RCIS. In these states, the system works normally. The state 3 expresses that one cell generates a safety undetected failure and the other two cells are perfect. The state 6 expresses that one cell generates a safety undetected failure one cell generates a safety detected failure, and the remaining cell overloading. The state 7 expresses that one cell generates a safety undetected failure, one cell generates a dangerous detected failure, and the remaining cell overloading. The state 4 expresses that two cells generate undetected safety failure and the remaining cell is perfect. When system works at states 3, 6, and 7, there are two subregions working properly. When system works at state 4, there is only one subregion working properly. The state 10 represents the system safety failure. The state 11 presents the system dangerous failure but can be detected. The state 12 expresses the system dangerous failure but cannot be detected. The states 10, 11, and 12 present the system failure states. The state 5 expresses that one cell generates a safety detected failure and another cell generates a dangerous detected failure. The state 8 expresses that two cells generate dangerous detected failure. The state 9 expresses that two cells generate safety detected failure. When system works at states 5, 8, and 9, the system generates two detected failures and the remaining cell is perfect. In these states, the system has only one cell working properly that completes the interlocking logical operation of the entire area. In this case, the working principle of the system is equivalent to the centralized interlocking scheme.

The state transition matrix  $P$  can be easily written as follows:

## 6 RELIABILITY COMPUTATION

Let the initial state probability vector of the system be  $S_0$ , the state transfer probability matrix be  $P$ , and then according to Markov chain principle [12], the transient probability after  $n$ -step transfer can be calculated by

$$S_n = S_0 P^n \tag{8}$$

The system PFS equals the probability sum of all safety states, and the PFD equals the probability sum of all dangerous states. Let time increment be 1 h, each state probability of the



system can then be calculated out after 10,000 h. To resolve the MTTF, we must first eliminate the arcs from the failure states to work states in Markov model, and then a section-matrix  $Q$  is obtained. Secondly,  $Q$  is then subtracted using unit matrix  $I$ , and then is inverted, and thus we will obtain  $N=(I-Q)^{-1}$ . Finally, according to  $N$  matrix and time increment, we may work out MTTF, which can be expressed by

$$MTTF = S_0 N e_w \tag{9}$$

where  $e_w$  expresses a column vector with its dimension equaling to the column number of  $N$ , and all elements equal 1.

### 7 CASE STUDIES

To depict the advantages and disadvantages of the two kinds of interlocking schemes, from the view of system redundancy, we implement some comparisons on them. In the centralized interlocking schemes, the models of dual hot spare and double 2-vote-2 refer to [10], and the model of 3-vote-2 voting refer to [13]. In terms of the RCIS proposed, the diverse redundancies such as dual hot spare, 3-vote-2 voting, double 2-vote-2 voting as well as single machine are considered. The calculation method of system failure rates for diverse redundancies refers to [14].

Based on the current industrial level of control computers, the failure rate of single interlocking cell is expressed by  $\lambda = 1.0 \times 10^{-5} \text{ h}^{-1}$ , and the failure rate of interlocking machine after taking over one region cell task increases to  $\lambda_1 = 1.11 \times 10^{-5} \text{ h}^{-1}$ , and the failure rate of interlocking machine after taking over the task of the two cells soars to  $\lambda_2 = 1.22 \times 10^{-5} \text{ h}^{-1}$ . The diagnostic coverage rate  $c$  equals 0.999, the CCF factor  $\beta_1$  of the two cells is 0.075, and the CCF factor  $\beta_2$  of the three cells is 0.025. The average repairing time is considered as 8 h, and so the repairing rate is expressed by  $\mu_0 = 0.125 \text{ h}^{-1}$ . Assuming that the system will shut down when it detects out a safety failure and could restart within 24 h so that we obtain  $\mu_{SD} = 1/24 \text{ h}^{-1}$ . During modeling, the periodic maintenance is not considered since we assume that the periodic maintenance can find any problems and perform the repairing to make the system return to the original state. Hence, the considered indexes are limited on the scope of time interval between the two periodic maintenances. And thus, based on the former analysis, each failure rate can be calculated as shown in Table 1.

From the above analysis, the safety and reliability indexes are calculated and compared between diverse RCIS modes and centralized interlocking one as shown in Table 2.

From Table 2, the reliability and safety indexes of the combination scheme are much better than that of centralized interlocking scheme after redundancy. And there are some interesting results found for two-region RCIS models under the same kind of redundancy. The PFD of

Table 1: Computation results of diverse failure rates.

Failure rate type	Numerical value ( $\text{h}^{-1}$ )	Failure rate type	Numerical value ( $\text{h}^{-1}$ )
$\lambda^{\text{SDC}}$	$6.743250 \times 10^{-7}$	$\lambda^{\text{SDN}}$	$8.316675 \times 10^{-6}$
$\lambda^{\text{SUC}}$	$7.492500 \times 10^{-8}$	$\lambda^{\text{SUN}}$	$9.240750 \times 10^{-7}$
$\lambda^{\text{DDC}}$	$6.750000 \times 10^{-10}$	$\lambda^{\text{DDN}}$	$8.325000 \times 10^{-9}$
$\lambda^{\text{DUC}}$	$7.500000 \times 10^{-11}$	$\lambda^{\text{DUN}}$	$9.250000 \times 10^{-10}$

Table 2: Comparison of reliability and safety indexes between two-region RCIS and centralized computer interlocking.

System structure of RCIS		PDF	PFS	MTTF
Two-region RCIS with degradation disallowed	Single module	$1.984905 \times 10^{-7}$	$1.846183 \times 10^{-5}$	$1.298654 \times 10^6$
	Dual hot spare	$3.1751419570 \times 10^{-11}$	$2.947383 \times 10^{-9}$	$8.134677 \times 10^9$
	3-vote-2 voting	$9.5239023585 \times 10^{-11}$	$8.840739 \times 10^{-9}$	$2.711990 \times 10^9$
	Double 2-vote-2	$6.3502838961 \times 10^{-11}$	$5.894767 \times 10^{-9}$	$4.067337 \times 10^9$
Two-region RCIS with degradation allowed	Single module	$1.984953 \times 10^{-7}$	$1.805725 \times 10^{-5}$	$1.301054 \times 10^6$
	Dual hot spare	$3.1751419703 \times 10^{-11}$	$2.876432 \times 10^{-9}$	$8.149711 \times 10^9$
	3-vote-2 voting	$9.5239024781 \times 10^{-11}$	$8.627927 \times 10^{-9}$	$2.717002 \times 10^9$
	Double 2-vote-2	$6.3502839492 \times 10^{-11}$	$5.752867 \times 10^{-9}$	$4.074854 \times 10^9$
Centralized interlocking System	Dual hot spare	$8.449358 \times 10^{-6}$	$2.026980 \times 10^{-5}$	$1.171061 \times 10^6$
	3-vote-2 voting	$2.502280 \times 10^{-8}$	$6.017287 \times 10^{-5}$	$3.947916 \times 10^5$
	Double 2-vote-2	$2.873122 \times 10^{-7}$	$6.908398 \times 10^{-7}$	$2.621586 \times 10^5$

degradation allowed model is higher than that of degradation not allowed model, but its PFS is lower than that of degradation not allowed. The reason lies in that an undetected safety failure directly changes into the safety failure in the degradation not allowed model, and so its PFD becomes smaller whereas PFS is larger. At the same time, the MTTF of degradation allowed is larger than that of degraded not allowed. This is because the system can continue working a period of time under degradation allowed mode, whereas this is impossible under degradation not allowed mode.

Similarly, we also can work out the reliability and safety indexes of three-region RCIS models as shown in Table 3.

From Table 3, the indexes of the reliability and safety of the combination scheme are better than that of centralized interlocking scheme. In terms of the safety, the PFD of PDAM is higher than the one of PDNAM, whereas its PFS is lower than the one of the latter. The reason is that an undetected safety failure is directly converted into safety failure under PDNAM, and thus its PFD gets small. The PFS and PFD of SDAM are lower than the ones of another two models, the reason lies in that the SDAM increases six states from state 4 to state 9, which are acting as normal working states of the system, and all of these states in PDAM and PDNAM are directly transferred into system failure states. In addition, the transfer probabilities from failure state to normal work states under PDNAM and PDAM are far greater than the ones of SDAM, the reason is that the transfer probabilities of the former two contain two-cell CCF as well as three-cell CCF while the latter only has the two-cell CCF. Furthermore, we still find from Fig. 8 that the state 8 after repaired transfers to normal working state, which further reduces the danger-side failure probability, and the state 9 after repaired transfers to normal state further reduces the safety-side failure probability. Through careful comprehension on three-region RCIS operation behaviors, it is thought to be reasonable that the PFS and PFD of SDAM are both less than the ones of another two models. Under PDNAM, there are

Table 3: Comparison of reliability and safety indexes between three-region RCIS and centralized computer interlocking.

System structure of RCIS	PFD	PFS	MTTF	
Three-region RCIS PDNAM	Single module	$3.206226 \times 10^{-7}$	$6.069636 \times 10^{-5}$	$3.950264 \times 10^5$
	Dual hot spare	$5.1288810445 \times 10^{-11}$	$9.694529 \times 10^{-9}$	$2.473374 \times 10^9$
	3-vote-2 voting	$1.538418211 \times 10^{-10}$	$2.907895 \times 10^{-8}$	$8.245893 \times 10^8$
	Double 2-vote-2	$1.0257762041 \times 10^{-10}$	$1.938906 \times 10^{-8}$	$1.236686 \times 10^9$
Three-region RCIS PDAM	Single module	$3.206427 \times 10^{-7}$	$6.013224 \times 10^{-5}$	$3.955951 \times 10^5$
	Dual hot spare	$5.1288811023 \times 10^{-11}$	$9.588104 \times 10^{-9}$	$2.476936 \times 10^9$
	3-vote-2 voting	$1.538248263 \times 10^{-10}$	$2.875974 \times 10^{-8}$	$8.257768 \times 10^8$
	Double 2-vote-2	$1.0257762272 \times 10^{-10}$	$1.917622 \times 10^{-8}$	$1.238467 \times 10^9$
Three-region RCIS SDAM	Single module	$3.044512 \times 10^{-7}$	$1.205101 \times 10^{-5}$	$4.694086 \times 10^5$
	Dual hot spare	$4.870799 \times 10^{-11}$	$9.588098 \times 10^{-9}$	$2.485086 \times 10^9$
	3-vote-2 voting	$1.452139 \times 10^{-10}$	$2.875969 \times 10^{-8}$	$8.284945 \times 10^8$
	Double 2-vote-2	$9.682475 \times 10^{-11}$	$1.917620 \times 10^{-8}$	$1.242543 \times 10^9$
Centralized interlocking	Dual hot spare	$9.289021 \times 10^{-6}$	$2.228529 \times 10^{-5}$	$1.065266 \times 10^6$
	3-vote-2 voting	$2.751377 \times 10^{-8}$	$6.615977 \times 10^{-5}$	$3.590953 \times 10^5$
	Double 2-vote-2	$3.237938 \times 10^{-7}$	$7.786893 \times 10^{-7}$	$7.073477 \times 10^5$

three subregions being at working condition before the system becomes failure, whereas under the PDAM there are two subregions being at working condition before the system fails, and under SDAM there is only one subregion being at working condition before the system gets failure. Known from the analysis above, both the PFS and PFD of SDAM decline slightly compared with the other modes, it keeps in the same order of magnitude. Obviously, since there are two subregions not working under the mode of SDAM, which can affect the traffic efficiency, the utilization of system reaches the minimum. In terms of reliability, the MTTF increases apparently as the system degradation operation is considered. The reason lies in that the degradation allowed increases in the working time of the system. In a word, the combination of two computer interlocking schemes has more advantages than centralized interlocking scheme alone.

### 8 CONCLUSION

The paper analyzes the reliability and safety indexes in terms of two kinds of computer interlocking schemes under diverse kinds of operation modes. The results show that their combination scheme can effectively prevent the potential risks, which may possibly result in the whole region paralysis due to the center interlocking machine failure, which is the main drawback of this type interlocking scheme. The investigations still show that redundancy measures can effectively improve the reliability and safety properties of the system. With the

continuing development of the railway signaling intelligence, networking and informatization, the RCIS will be a main development trend for computer interlocking.

#### ACKNOWLEDGEMENTS

This project is supported by Railways Ministry Science and Technology Research and Development Program (2012X003-B) and Gansu Province Natural Science Foundation (Grant No. 1212RJZA071).

#### REFERENCES

- [1] Huang, W., The realization and implementation of regional computer interlocking system. *Railway Signaling and Communication*, **41(9)**, pp. 6–10, 2005.
- [2] Liu, S., Research and application of regional computer interlocking technology in marshalling station. *Railway Standard Design*, **11**, pp. 112–115, 2011.
- [3] Zhang, P., Zhao, Y. & Hu, Y., Lake East marshalling station computer interlocking control system. *Railway Standard Design*, **1**, pp. 35–37, 1999.
- [4] Zhang, P., Zhao, Y. & He, M., The research on railway regional computer interlocking system. *Journal of Scientific Instrument*, **24(4)**, pp. 356–359, 2003.
- [5] Sun, C., Regional computer interlocking system in Dalian Express Rail Line 3 extension line. *Urban Railway*, **1**, pp. 52–53, 2011.
- [6] Li, H., Study on regional computer interlocking scheme of west Lhasa and Liuwu line. *Railway Signaling and Communication*, **48(4)**, pp. 33–34, 2012.
- [7] Chen, H., Technology and maintenance on regional computer interlocking system of DS6-K5B. *Railway Engineering*, **2(6)**, pp. 33–35, 2005.
- [8] Shen, J. & Dan, D., Reliability and safety analysis of TMR computer-based interlocking system. *Journal of Northern Jiaotong University*, **22(5)**, pp. 111–114, 1998.
- [9] Qin, Y. & Xu, Z., Study of security of the double 2-vote-2 computer interlocking control system. *Proceedings of the 5th World Congress on Intelligent Control and Automation*, Hangzhou, China, pp. 5292–5296, 2004.
- [10] Liu, F. & Wang, H., A comparison between double 2-vote-2 and dual hot spare interlocking system with computer-based. *Railway Signaling and Communication*, **44(2)**, pp. 26–29, 2008.
- [11] Zhao, Z., *Computer Interlocking System Technology*, China Railway Publishing House: Beijing, pp. 236–239, 2010.
- [12] Goble, W.M., *Control Systems Safety Evaluation and Reliability*, China Electric Power Publishing House: Beijing, pp. 143–145, 2010.
- [13] Su, H., Reliability and security analysis on 3-vote-2 voting system. *Telkommnika*, **7(4)**, pp. 335–336, 2013.
- [14] Yang, J., Study on subway main control system reliability evaluation method based on FTA. Master thesis, Southwest Jiao Tong University, pp. 43–50, 2009.