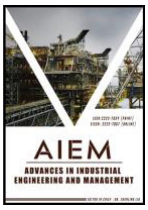
ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2222-7059 (Print)
EISSN: 2222-7067 (Online)

Advances in Industrial Engineering and Management (AIEM)

DOI: http://doi.org/10.7508/aiem.02.2024.170.176




CrossMark

REVIEW ARTICLE

# SAFETY ASSESSMENT OF DOUBLE TWO-OUT-OF-TWO REDUNDANT LCU SYSTEM

**Yanbiao Yang*, Yanwen Zhan**

*School of Electronics and Information Engineering, Tongji University, Shanghai 201804, China.*
**Corresponding Author E-mail: yangyanbiao1998@163.com*



## ARTICLE DETAILS

***Article History:***

Received 8 Jaunary 2024
Accepted 15 March 2024
Available online 20 March 2024

## ABSTRACT

In addressing the issues of multiple common-cause failures and data uncertainty in safety assessments of subway Logic Control Units (LCU), this study investigates the redundancy structure and safety assessment methods of LCU. The double two-out-of-two redundancy structure is implemented for the hardware redundancy design of the LCU, and the Markov method is applied for its safety evaluation. System states within the Markov model are defined based on the hardware structure and redundancy strategy. To address the deficiency of the $\beta$ factor model in common-cause failures, which does not account for multiple common-cause failures, structural factors are introduced for optimization. Separate Markov models for independent and common-cause failures are developed. To address parameter uncertainty within the Markov model, the Monte Carlo method is utilized for sampling these uncertain parameters, subsequently establishing LCU safety assessment model that accounts for common-cause failures under parameter uncertainty. Simulation results show that considering multiple common-cause failures results in a more conservative safety assessment for the LCU; both the fault coverage rate and the common-cause failure of undetectable faults significantly influence the LCU's safety; the safety assessment results of the LCU under parameter uncertainty, considering common-cause failures, is rated at SIL3. The findings of this research provide a theoretical basis for the development and safety assessment of high-performance LCU.

## KEYWORDS

Logic control unit, double 2-out-of-2 redundant, safety, common cause failures， data uncertainty.

## 1. INTRODUCTION

Traditional rail transit vehicle control systems use a large number of relays, but their wiring is complex, lacks redundancy mechanisms, and they frequently malfunction when operating in environments with vibration, high temperature, and humidity. According to statistics, over 60% of subway vehicle control failures are caused by relay faults (Li et al. 2020). The Subway Logic Control Unit (LCU), as a replacement for relays, adopts a contactless control method to directly control and drive external loads, effectively resolving the shortcomings of relay control circuits.

To enhance the safety of the LCU, Qin Jiaomei et al. adopted a dual-machine hot standby redundancy method in its system design (Qin et al. 2020). As subways develop towards a trend of fully automatic, unmanned operation, the safety of rail transit control systems needs further enhancement. The safety of the existing dual-machine hot standby LCU gradually fails to meet the operational requirements of the subway. Pang Xinran et al. analysed the safety of the two-out-of-three and double two-out-of-two redundancy structures (Pang et al. 2021), which showed better safety performance than the dual-machine hot standby structure, and thus have been widely applied in high-safety equipment.

Research both domestically and internationally reveals that studies on redundancy system structures and their safety in the field of rail transit are mainly focused on communication signals and computer interlocking control. However, research on the safety of the LCU is still in the exploratory stage, with relatively few results. Current research achievements in the safety of redundancy systems are mainly concentrated in safety assessment and common-cause failure analysis. In safety assessment, the Markov method is widely used because it can calculate the failure probabilities for systems with repair capabilities and multiple degraded states. Common-cause failure is an influential factor that cannot be ignored in the safety analysis of redundancy systems. Zhang Yongxian et al. introduced a factor model when evaluating the double two-out-of-two redundancy system, making the results more realistic (Zhang et al. 2019). However, the β factor model only considers independent failures and the simultaneous failure of all redundant components in the system, without addressing the issue of multiple common-cause failures involving two or more channels, leading to assessment results overestimated assessment results compared to

| Quick Response Code | Access this article online | |
|---|---|---|
| | Website: www.aiem.com.my | DOI: 10.7508/aiem.02.2024.170.176 |

Cite The Article: Yanbiao Yang, Yanwen Zhan (2024). Safety Assessment of Double Two-Out-of-Two Redundant Lcu System. *Advances In Industrial Engineering And Management*, 13(2): 170-176.

actual values.

Furthermore, in safety assessments, failure rates, fault coverage ratios, and other related parameters are often assumed to be fixed values, leading to the calculation of a single quantitative safety index. However, for newly designed systems, there are objective factors such as insufficient failure data and incomplete identification of related parameters, making it difficult to obtain accurate fault data. This results uncertainties in the input parameters of the safety assessment model. Fu Jianmin et al. proposed a method of safety integrity level assessment based on the Monte Carlo method in a phase-separation system with uncertain parameters (Fu et al. 2017). Zhang Hongyang et al. introduced a safety assessment method based on fuzzy theory to address the issue of unknown probability distributions of parameters in railway signal safety computers (Zhang et al. 2022).

Therefore, to enhance the safety of the LCU, the double two-out-of-two redundancy structure, which has higher safety performance is adopted in this paper. Structural factors are introduced to distinguish various common-cause failures, and the influence of parameter uncertainty on the LCU's safety assessment is taken into consideration. In this paper, the safety assessment of the hardware structure of the double two-out-of-two redundant LCU system is conducted by combining the Markov process with the Monte Carlo method.

## 2. THE DOUBLE 2-OUT-OF-2 REDUNDANT LCU SYSTEM

The double 2-out-of-2 redundant LCU system employs a dual redundant structure. The hardware architecture of both systems is identical. In each system, the redundant functional modules only output signals when they are consistent 2-out-of-2 voting. A master-slave switchover function is triggered when the primary system fails or the 2-out-of-2 voting is inconsistent, enabling a seamless transition to the backup system. Traditional double 2-out-of-2 redundant LCU systems use a system-level redundancy mechanism. In these systems, the input collection, logical operations, and output of System A and System B operate independently before executing a master-slave switchover. When a local failure occurs in either System A or B, that system is completely isolated and no longer participates in the system operation. The system then degrades to 2-out-of-2 redundant mechanism and continues to operate.

In this paper, a modular redundancy approach is adopted to design the double 2-out-of-2 redundant LCU system. Its core functional units consist of three parts: the input signal collection module, the master control module, and the output module, as shown in Figure 1. The input modules of System A and B, after 2-out-of-2 voting, transmit the input signals to both master control modules of the two systems. Logical operations are then performed simultaneously, and the results of these operations are cross-output to the output modules of both systems. Finally, the master-slave switch selects the primary system for output. When a failure occurs in the input, master control, or output module of any system, only the faulty module needs to be isolated, without the need for complete isolation of the entire system. This significantly improves the utilization of system resources and maximizes system availability.

## 3. SAFETY ASSESSMENT METHOD FOR DOUBLE 2-OUT-OF-2 REDUNDANT LCU SYSTEM

### 3.1 Failure Rate Calculation Method

#### *3.1.1 Calculation under the Traditional $\beta$ Factor Model*

Common-cause failure refers to the simultaneous failure of two or more functional units in a system due to the same reason. Since redundant systems use similar structures in hot backups, common-cause failure is an indispensable factor in the failure analysis of redundant systems. From this perspective, the failure rate can be divided into common-cause failure rate $\lambda_C$ and independent failure rate $\lambda_N$ :

$$\begin{aligned} \lambda_C &= \beta\lambda \\ \lambda_N &= (1-\beta)\lambda \end{aligned} \tag{1}$$

After incorporating the $\beta$ factor model, the above-mentioned failures can be further categorized into the following eight patterns. SDN: Detected Safe Independent Failure; SUN: Undetected Safe Independent Failure; SDC: Detectable Dangerous Common-Cause Failure; SUC: Undetected Safe Common-Cause Failure; DDN: Detected Dangerous Independent Failure; DUN: Undetected Dangerous Independent Failure; DDC: Detected Dangerous Common-Cause Failure; DUC: Undetected Dangerous Common-Cause Failure.

#### *3.1.2 Calculation Considering Multiple Common-Cause Failures*

Given that the double 2-out-of-2 redundant LCU system comprises four sets of channels with identical structures, the previously mentioned factor model can only analyze the occurrence of independent failures in a single channel or simultaneous failures in two channels. However, it does not address the issue of multi-order failures, such as the simultaneous failures of three or four channels. Therefore, this paper employs a multi-factor model to resolve the issue of multi-order common-cause failures.

Structural factors and are introduced. They respectively represent the probability of a third channel experiencing a common-cause failure simultaneously when two channels have a common-cause failure, and the probability of a fourth channel experiencing a common-cause failure simultaneously when three channels have a common-cause failure. The rates of quadruple common-cause failure, triple common-cause failure, double common-cause failure, and independent failure are defined as follows:

$$\begin{aligned} \lambda_4 &= \beta_3\beta_2\beta\lambda \\ \lambda_3 &= (1-\beta_3)\beta_2\beta\lambda \\ \lambda_2 &= (1-2\beta_2+\beta_3\beta_2)\beta\lambda \\ \lambda_N &= (1-3\beta+3\beta_3\beta_2-\beta_3\beta_2\beta)\lambda \end{aligned} \tag{2}$$

The multiple $\beta$ factor model reconstructs the common-cause failure,

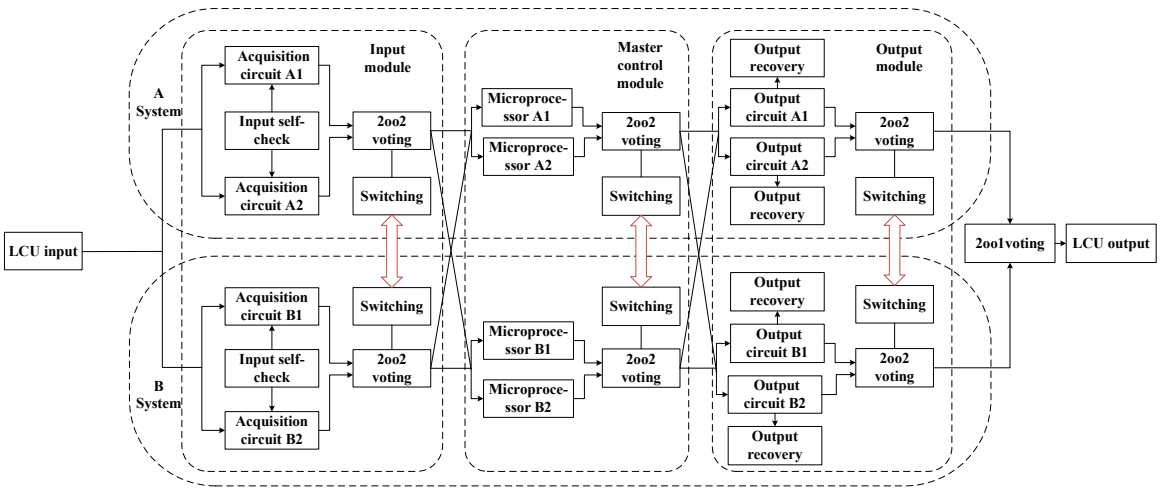



**Figure 1:** The overall architecture diagram of double 2-out-of-2 redundant LCU

| **Table 1:** The state division of LCU | |
|---|---|
| Symbol | State Description |
| State 0 | All modules are functioning normally |
| State 1 | Single system, single channel measurable fault |
| State 2 | Backup system, single channel SUN |
| State 3 | Main system, single channel SUN |
| State 4 | Single system, single channel DUN |
| State 5 | Main system normal, backup system safety unmeasurable |
| State 6 | Single system, one fault measurable, the other system, one safety unmeasurable fault |
| State 7 | Each system has one safety unmeasurable fault |
| State 8 | Single system with two faults, at least one measurable |
| State 9 | Backup system hazard unmeasurable, main system normal |
| State 10 | Three safety unmeasurable faults |
| State 11 | Backup system, two faults measurable, main system one safety unmeasurable |
| State 12 | Backup system hazard unmeasurable, main system one safety unmeasurable |
| State 13 | Fault - Safety Output |
| State 14 | Fault - Hazard Output |

further dividing it into quadruple common-cause failure, triple common-cause failure, and double common-cause failure.

Taking Safe Detectable Failures as an example, with $\beta_3$ and $\beta_2$ having typical values of 0.3 and 0.5 respectively, the probability of a quadruple SDC is: $\lambda_{4SDC} = C_4\lambda_{SD} = 0.15\beta\lambda_{SD}$, the probability of a triple SDC is: $\lambda_{3SDC} = C_3\lambda_{SD} = 0.15\beta\lambda_{SD}$, the probability of any SDC occurrence is: $\lambda_{2SDC} = C_2\lambda_{SD} = 0.75\beta\lambda_{SD}$, and the probability of only SDN occurring is: $\lambda_{SDN} = C_N\lambda_{SD} = (1.45 - 3.15\beta)\lambda_{SD}$. In a similar manner, the failure rates for common-cause failures and independent failures of other types, after reclassification, can also be determined.

### 3.2 Safety Assessment Method for LCU System based on Markov

#### *3.2.1 Division of Markov States*

Based on the system structure framework and redundancy strategy shown in Figure 1, the working states of the double 2-out-of-2 redundant LCU system can be divided as shown in Table 1.

#### *3.2.2 Establishment of the Markov State Transition Model*

In the analysis of the state transition process, the above states are divided into modules such as the no-fault operation module (state 0), single-channel fault-tolerant operation module (states 1, 2, 3, 4), dual-channel fault-tolerant operation module (states 5, 6, 7, 8, 9), triple-channel fault-tolerant operation module (states 10, 11, 12), and failure output module (states 13, 14). States 1, 6, 8, 11, and 13 are repairable, the probability of them being repaired is equal to the repair rate.

Markov state transition model of LCU independent failures and common-cause failures are established based on the state transition process and module division, as shown in Figure 2 and Figure 3, respectively.

In Figure 2, the condition for transitioning from state 0 to state 1 is the occurrence of a dangerously undetectable independent failure in any channel, with a probability of $P_{01} = 4\lambda_{SDN} + 4\lambda_{DDN}$. Similarly, the transition probabilities between the various states in the diagram can be determined as follows: $P_{0-2,3} = P_{16} = P_{27} = P_{37} = P_{46} = P_{510} = P_{811} = P_{912} = 2\lambda_{SUN}$, $P_{04} = 4\lambda_{DUN}$, $P_{35} = P_{213} = P_{710} = P_{713} = P_{1213} = \lambda_{SUN}$, $P_{18} = P_{48} = P_{611} = P_{1013} = P_{1113} = \lambda_{DN} + \lambda_{SN}$, $P_{2,3-6} = P_{1,4,8-13} = P_{914} = 2\lambda_{SDN} + 2\lambda_{DDN} + 2\lambda_{DUN}$, $P_{2,3-8} = P_{711} = P_{613} = P_{1214} = \lambda_{SDN} + \lambda_{DDN} + \lambda_{DUN}$, $P_{49} = \lambda_{DUN}$.

In Figure 3, similarly, the transition probabilities for common-cause failures between the various states in the diagram can be determined as follows: $P_{05} = P_{210} = P_{2,5,6,8,9-13} = \lambda_{SUC}$, $P_{08} = 2\lambda_{SDC} + 2\lambda_{DDC}$, $P_{09} = P_{212} = P_{5,8-14} = \lambda_{DUC}$, $P_{010} = 2\lambda_{3SUC}$, $P_{07} = 4\lambda_{SUC}$, $P_{214} = \lambda_{3DUC}$, $P_{1,3,4-13} = \lambda_{SUC} + \lambda_{3SUC}$, $P_{014} = \lambda_{DUC} + 2\lambda_{3DUC} + \lambda_{4DUC}$, $P_{1,4-11} = P_{310} = 2\lambda_{SUC}$,

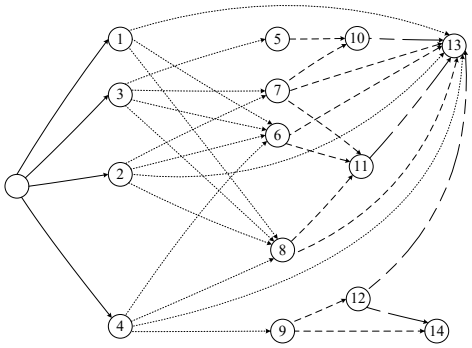



**Figure 2:** Markov state transition diagram of LCU independent failures

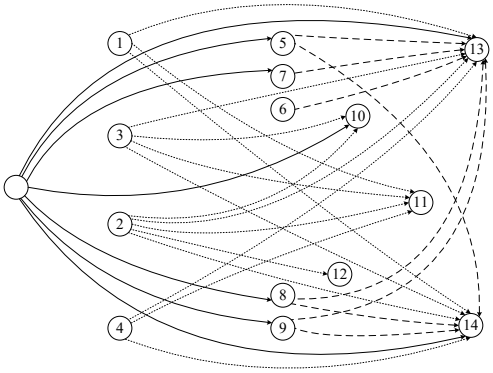



**Figure 3:** Markov state transition diagram of LCU common- cause failures

$P_{013} = \lambda_{SUC} + 2\lambda_{3SUC} + \lambda_{4SUC}$, $P_{1,3,4-14} = \lambda_{DUC} + \lambda_{3DUC}$, $P_{211} = P_{311} = \lambda_{SDC} + \lambda_{DDC}$, $P_{713} = P_{914} = \lambda_{SDC} + \lambda_{DDC} + \lambda_{DUC}$.

#### *3.2.3 Steps for Safety Assessment of the LCU System*

The main steps for assessing the safety of the LCU system based on the Markov process are as follows:

a) Divide the Markov states based on the hardware redundancy structure of LCU.

b) Establish separate Markov state transition models for independent failures and common-cause failures, and calculate the state transition

probability matrices $p_N$ and $p_C$.

c) Combine the independent and common-cause failures. From $A=(p_N+p_C)-E$, the Markov state transition rate matrix A can be determined as:

$$!=\begin{bmatrix} 1-\sum & 4*\lambda_{SDN} & 4*\lambda_{SUN} & 4*\lambda_{DUN} & \cdots & 4*\lambda_{DUC}+4*\lambda 3_{DUC}+\lambda 4_{DUC} \\ u0 & 1-\sum & 0 & 0 & \cdots & 2*\lambda_{DUC}+\lambda 3_{DUC} \\ 0 & 0 & 1-\sum & 0 & \cdots & 2*\lambda_{DUC}+\lambda 3_{DUC} \\ u0 & 0 & 0 & 1-\sum & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1-\sum \end{bmatrix}$$

d) Let the initial condition be $P(0)=[1,0,0,\cdots 0,0]$. Based on $\frac{d}{dt}p(t)=p(t)A$, the probability of the system being in each state at any time can be calculated as $P(t)=[p_0(t),p_1(t),p_2(t),\cdots p_{13}(t),p_{14}(t)]$, and the safety of the system, denoted as $S(t)=1-p_{14}(t)$, can also be determined.

### 3.3 Safety Assessment Method for LCU System under Parameter Uncertainty

During the safety assessment of the LCU system, due to the lack of feedback data from new systems, failure parameters are often difficult to obtain. This results in uncertainty in the assessment parameters. Therefore, it is necessary to handle the uncertainty of input parameters in the Markov model, making the assessment results more reliable.

The Monte Carlo method (MC) is a numerical computation method based on probability theory and statistics, often used to handle complex problems involving parameter uncertainty. Compared to deterministic methods, MC can provide a distribution range for output results, which is more comprehensive and accurate than describing outputs with a single value.

#### *3.3.1 Fitting of Distribution Functions*

Before conducting a safety assessment using the MC method, it is necessary to determine the probability distribution of each parameter. Failure data typically conform to common probability distribution types such as triangular distribution, uniform distribution, normal distribution, and log-normal distribution. Among these, the log-normal distribution, due to its non-negativity and long-tailed characteristics, is the most widely applied distribution type in safety assessments.

When the maximum value M, minimum value m, and recommended value T of a parameter are known, let $F=\frac{M}{T}$ or $F=\frac{T}{m}$, which allows the parameter to be fitted to a log-normal distribution:

$$\mu=\ln T \qquad \sigma=\frac{\ln(F)}{\sqrt{2}inverf(P)} \tag{3}$$

The Gaussian error function $erf(x)$ is defined as:

$$erf(x)=\frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt \tag{4}$$

$P$ represents the probability of being between the maximum value M and the minimum value m:

$$P=P=\int_m^M \frac{1}{\sqrt{2\pi}\sigma x}e^{-\frac{1}{2\sigma^2}\left[\ln\left(\frac{x}{T}\right)\right]^2}dx=erf\left(\frac{1}{\sqrt{2\sigma}}\ln(F)\right) \tag{5}$$

If only the maximum value M and the minimum value m are known, then T and F can be set as follows: $T=\sqrt{mM}$, $F=\sqrt{M/m}$.

#### *3.3.2 Combining Monte Carlo and Markov for Safety Assessment*

According to the distribution types of various parameters, random sampling is conducted to obtain a large number of random samples for assessment parameters. These samples are then inputted into the Markov model for solving, thereby acquiring random samples for safety degree. Subsequently, statistical methods can be applied to obtain the confidence interval for the safety degree. The main steps of combining Monte Carlo with safety assessment under parameter uncertainty as follows:

a) Determine the probability distribution of each parameter in accordance with the IEC61508 standard;

b) Sample each uncertain parameter according to its probability distribution to generate a set of input parameters;

c) Substitute a set of input parameter values into the Markov model to calculate the Safety $S(i)$ and the Average Probability of Dangerous Failure on Demand $PFD_{\text{avg}}(i)$;

d) Repeat steps 2 and 3 until the set number of sampling times N is reached, obtaining output values for $S(N)$ and $PFD_{\text{avg}}(N)$;

e) Plot histograms and cumulative distribution functions, calculate mean values, and determine the 95% confidence interval;

f) Assess the safety integrity level using the output range of PFDavg.

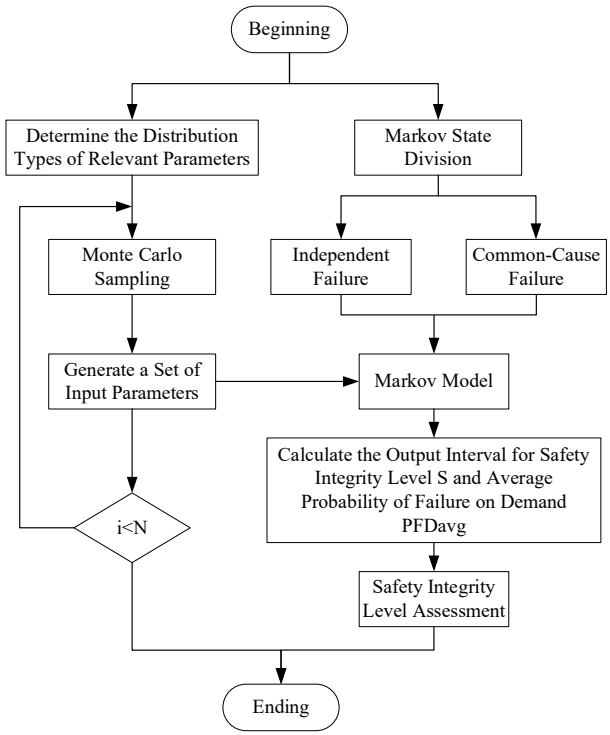



**Figure 4:** The process of safety assessment under parameter uncertainty

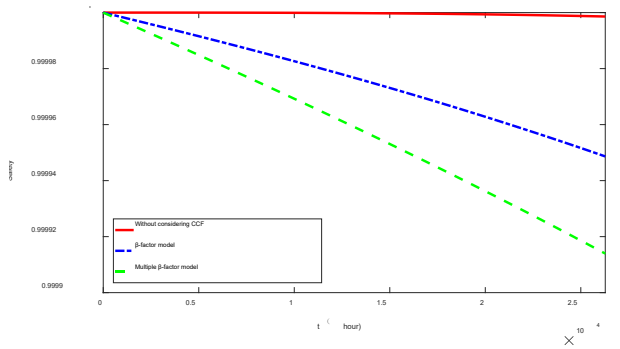



**Figure 5:** The system safety considering common-cause failure

When the number of effective samples n in the Monte Carlo simulation approaches infinity, the arithmetic mean of the sought random variable approximates its mathematical expectation.

## 4. SIMULATION VERIFICATION

### 4.1 Safety of LCU Considering Common-Cause Failures

Simulations are conducted in MATLAB using the ode4 solver. The system failure rate is set to (1/hour), the safety failure factor at 0.5, the fault coverage rate c at 0.90, and the Mean Time to Repair (MTTR) at 8 hours. The repair rate is taken as the reciprocal of MTTR. The common-cause failure factors and are set to 0.02 and 0.01, respectively. The simulation covers a time range from 0 to 26,280 hours.

Simulations are conducted to evaluate the system safety under three scenarios: without considering common-cause failures, using the factor model, and using the multiple factor model. The simulation results are depicted in Figure 5.

From Figure 5, it is evident that if common-cause failures are not considered during the safety assessment of the double 2-out-of-2 redundant LCU system, the assessment results of the safety are significantly overstated, meaning the safety performance of the LCU system at this time is overestimated. When the $\beta$ factor model is used to consider the impact of common-cause failures, the assessment results are more conservative. However, since the factor model does not take into account multiple common-cause failures, its assessment results are still slightly high. When the multiple $\beta$ factor model is used to optimize the issue of multiple common-cause failures, the assessment results are more in line with actual conditions compared to the $\beta$ factor model.

### 4.2 Analysis of The Impact of Input Parameters on Safety

With other parameters remaining constant, the impact of the repair rate $\mu$, fault coverage rate c, and common-cause failure factors $\beta$ and $\beta_D$ on safety assessment are analysed. The simulation results are shown in Figures 6.

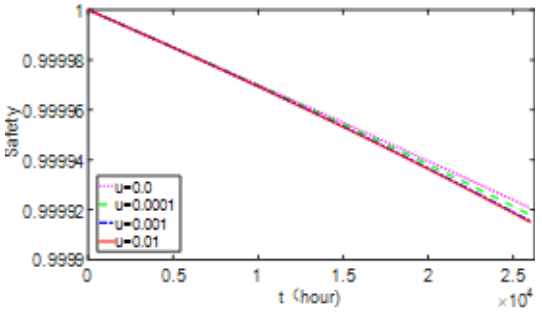
From Figure 6(a), it is observed that before 15,000 hours, the repair rate has almost no impact on the assessment of system safety. After 15,000 hours, as the repair rate increases, the probability of detectable faults being repaired increases, leading to a higher probability of undetectable faults occurring while the system is in normal operation. Therefore, the system's safety slightly decreases with an increase in the repair rate $\mu$.

As seen in Figure 6(b), with an increase in fault coverage rate, the proportion of detectable faults increases and that of undetectable faults decreases, hence increasing the safety. When the fault coverage rate is 1, all faults in the system are detectable, and there are no undetectable faults, making the system completely safe.

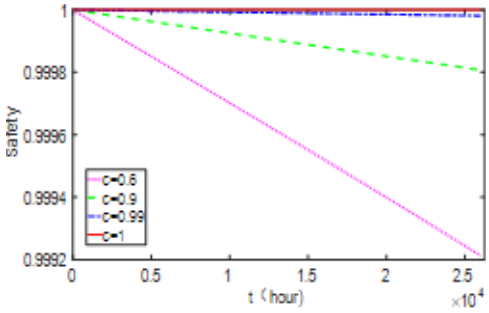
Figure 6(c) and figure 6(d) show that when the common-cause failure factor for undetectable faults $\beta$ is set to 0 or a very small value, the system either does not consider common-cause failures or has a very low probability of their occurrence, leading to a significantly overestimated safety. As the value of $\beta$ increases, the probability of common-cause failures increases, and the safety decreases. The common-cause failure factor for detectable faults $\beta_D$ has almost no impact on the safety assessment. Thus, it can be concluded that the main factor affecting the safety assessment in common-cause failures is the undetectable faults' common-cause failure.

### 4.2 Analysis of the Impact of Input Parameters on Safety

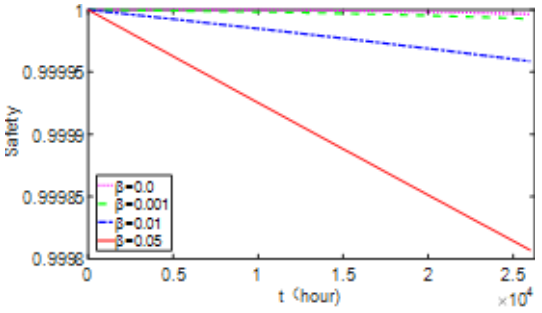
According to the reference values for various parameters given in the IEC61508 standard, the range of values for the failure rate $\lambda$ is: $1\times10^{-7} \sim 5\times10^{-5}$, with the mode taking a typical value: $1\times10^{-6}$; the common-cause failure factor β for undetectable failures ranges between: $0.02 \sim 0.2$, and the common-cause failure factor for detectable failures ranges between: $0.01 \sim 0.1$. The above three parameters are all fitted to a log-normal distribution, with the probability P of being between the maximum and minimum values set to 0.9. For the fault coverage ratio c, the reference values given in IEC61508 are 0.6, 0.9, and 0.99, but considering that the LCU system designed in this paper is a high-safety device, it is therefore fitted to a uniform distribution on the interval [0.6, 0.99]. The Mean Time to Repair (MTTR) is taken as a fixed value of 8 hours, and the repair rate $\mu$ is the reciprocal of MTTR. The distributions of the fitted parameters are as follows: $\lambda \sim \log N(-12.6586, 2.1032)$; $\beta \sim \log N(-2.760, 0.6999)$; $\beta_D \sim \log N(-3.453, 0.6999)$; $C \sim U(0.9, 0.99)$; $MTTR = 8$.



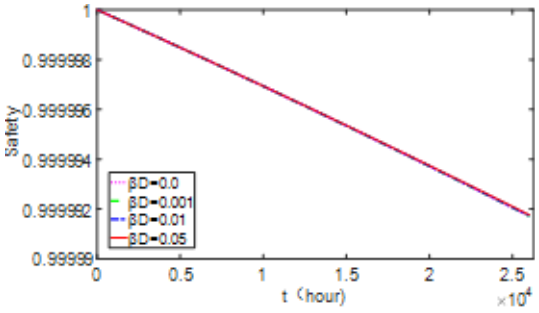

(a) The impact of $\mu$ on safety




(b) The impact of *c* on safety.

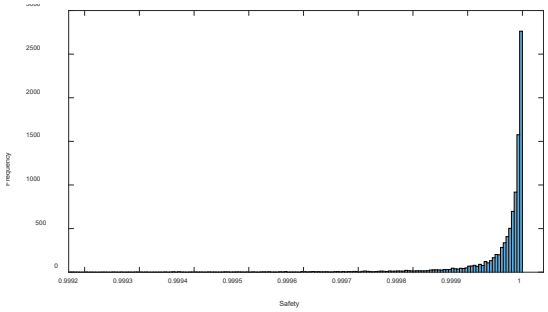



(c) The impact of $\beta$ on safety

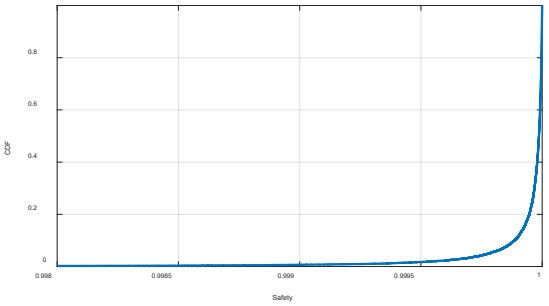



(d) The impact of $\beta_D$ on safety.

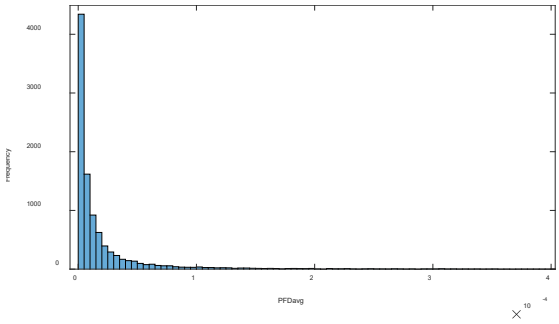
**Figure 6:** The impact of common-cause failure on safety



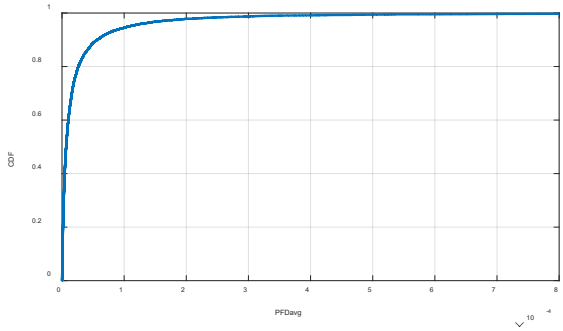

(a) Histograms of S




(b) cumulative distribution functions of S




(c) Histograms of $PFD_{avg}$




(d) cumulative distribution functions of $PFD_{avg}$

Figure 7: Histograms, cumulative distribution functions of S and $PFD_{avg}$

Sample the parameters according to the distributions mentioned above to generate a set of valid input samples. Then, input these samples into the Markov model to solve for the safety. Repeat this process until the Monte Carlo method's set number of sampling iterations, 5000, is reached. The detection time is set at 8760 hours. The histograms and cumulative distribution functions obtained for Safety and $PFD_{avg}$ are shown in Figure 7.

From this, we can obtain the output values for the safety: $y_{max}$ = 0.99999996, $y_{min}$ = 0.972280, and $y_{mean}$ = 0.99994; subsequently, we can calculate the 95% confidence interval to be: [0.999939, 0.999941], which means there is a 95% probability that this interval contains the true mean value of the safety.

The output value for the PFDavg is: $y_{max}$ = 0.013; $y_{min} = 1.933 \times 10^{-8}$, and $y_{mean} = 2.906 \times 10^{-5}$;and the 95% confidence interval can be calculated as: $[2.861 \times 10^{-5}, 2.952 \times 10^{-5}]$. This means that there is a 95% probability that this interval contains the true mean value of PFDavg. When evaluating the safety using the output mean value, the system's safety performance is SIL4. From Figure 7(d), we can deduce that there is a 94.51% probability that the system meets the requirements for SIL4, and a 99.82% probability that it meets the requirements for SIL3. In this case, the system's safety performance is SIL3.

## 5. CONCLUSION

In this paper, by considering common-cause failures, repair rates, and fault coverage rates, the Markov model for the double 2-out-of-2 redundant LCU system was established, and optimizations were made to the safety assessment model to account for multiple common-cause failures and parameter uncertainties. The simulations led to the following conclusions:

1)Not considering common-cause failures significantly overestimates the safety performance of the LCU system. The optimized assessment, which accounts for multiple common-cause failures, is more conservative.

2)The repair rate has a minimal impact on safety; higher fault coverage rates lead to a safer system; and the main factor affecting system safety in common-cause failures is the common-cause failure of undetectable faults.

3)The safety assessment results of the LCU under parameter uncertainty are distributed across different safety integrity levels according to different probability values. Compared to assessment results with a single value, these results are more referential. The safety performance of the double two-out-of-two LCU system designed in this paper is SIL3, with a 94.51% probability of achieving SIL4.

Based on the above conclusions, the following recommendations are proposed for the design process of redundant systems: During the design phase, consideration should be given to the impact of multiple common-cause failures on the system, and measures such as designing diverse redundant channels or isolation should be employed to reduce the impact of common cause failures. Each module should be designed with fault diagnosis units to improve fault coverage.

## REFERENCES

Fu, J., Li, C., Dong, J. 2017. Study on method of SIL verification of safety instrumented systems under data uncertainty. Journal of China University of Petroleum (Edition of Natural Science), 41(3): Pp. 129-135. https://doi.org/10.3969/j.issn.1673-5005.2017.03.016

Jiao, Z., Yu, L. 2021. Research on reliability of catenary system based on dynamic Bayesian network. Journal of Railway Science and Engineering, 18(11): Pp. 3040-3047. https://doi.org/10.19713/j.cnki.43-1423/u.T20201146.

Li, X., Wu, J., Li, S. 2020. Optimization design of subway vehicle logic control unit. Urban Mass Transit, 23(02): Pp. 112-115. https://doi.org/10.16037/j.1007-869x.2020.02.027

Mathebula, V. C, Saha, A. K. 2022. Reliability of IEC61850 based substation communication network architecture considering quality of repairs and common cause failures. Protection and Control of Modern Power Systems, 7(1). https://doi.org/10.1186/s41601-022-00234-1

Pang, X., Lai, Y., Dong, Q. 2021. Safety and availability assessment of triple—channel and double-triple-channel systems. Industrial Control Computer, 34(12): Pp. 42-45. https://doi.org/10.3969/j.issn.1001-182X.2021.12.016

Qin, J., Li, Z., Gai, M. 2020. Research and development of contactless logic control unit based on redundant design. Rolling Stock, 23(02): Pp. 112-115+120.

Torres, E. S., Sriramula, S., Celeita, D. 2020. Reliability model and sensitivity analysis for electrical/electronic/programmable electronic safety-related systems. IEEE Transactions on Industry Applications, 56(4): Pp. 3422-3430. https://doi.org/10.1109/TIA.2020.2990583

Zhang, H., Liang, Z., Wang, L. 2022. SIL verification of railway signal safety computer hardware considering uncertainty. Journal of the China Railway Society, 44(6): Pp. 66-74. https://doi.org/10.3969/j.issn.1001-8360.2022.06.008

Zhang, Y., Liao, Z., Wang, Y. 2019. Common cause failure analysis method for double two out system. Computer Engineering and Design, 40(01): Pp. 285-289. https://doi.org/10.16208/j.issn.1000-7024.2019.01.048