Reliability analysis of logic control system of automatic ground control neutral section passing

Yuwei Song*, Baodi Xiao
School of Automation & Electrical Engineering Lanzhou Jiaotong University Lanzhou, China

*0618419@stu.lzjtu.edu.cn

Abstract. Neutral section passing technology in railway power supply had always been a technical problem in current domestic traction power supply industry. In recent years, there are many technical schemes for passing neutral section. There are two main schemes of automatic neutral section passing at present: the vehicle control neutral section passing and automatic ground control neutral section passing, the automatic ground control neutral section passing is a relatively popular technical route in both schemes. Now incorporating fail-safe principle of signal specialty in automatic ground control neutral section passing and proposing the logic control system of automatic ground control neutral section passing based on the idea of “fail safe” in the interlocking system, and the risk identification and safety analysis are carried out based on the dynamic fault tree and HAZOP method. The fault tree is constructed based on the results of HAZOP analysis. Finally, the system reliability is quantitatively calculated through the fault tree.

Keywords: Automatic ground control neutral section passing, logic control system, dynamic fault tree, HAZOP, reliability.

1. Introduction

In order to balance the three-phase load of the power system as much as possible, the catenary of electrified railway uses section commutation power supply, and two phases are separated by air or insulation, which is called electric phase separation or neutral section. Therefore, there is a power supply dead zone of approximate 30 meters in the catenary every 20-25 kilometers. When the electric locomotive arrives here, the driver has to cut off the power through a series of operations[1]. This not only affects the driving speed, consumes the driver's energy, but also is extremely unfavorable to the operation safety. If there is any negligence and improper operation, it will pull the arc to burn the split phase insulator. For quasi high-speed and high-speed lines, it is difficult to operate by the driver because the train will pass more than ten electric phase separations per hour. For high slope and heavy load section, excessive power failure will decelerate the speed of trains greatly, and the passing time of throat section will be greatly prolonged due to the difficulty of starting speed in high slope section. Neutral section passing technology aims to reduce the labor intensity of drivers and reduce the faults of locomotive and power supply equipment. It can not only solve the difficulty of operation at high speed, but also improve the transport capacity of throat section. At present, there are three kinds of main automatic neutral section passing...
technology: pole-mounted switches automatic neutral section passing, vehicle control automatic neutral section passing and ground control automatic neutral section passing. In China, vehicle control automatic neutral section passing and ground control automatic neutral section passing are mainly used[2].

Reference [3-4] mainly introduces the application of ground control automatic neutral section passing technology and the definition of professional terms in the industry. Reference [5] introduces the overall structure of the ground control automatic neutral section passing device and the control scheme of train passing, and analyzes the dead time and switching voltage during neutral zone switching. In reference [6], the potential danger of ground control automatic neutral section passing is analyzed, the risk level is proposed, and the corresponding protection scheme is discussed. However, there is no correlation analysis on the reliability of logic control system of ground control automatic neutral section passing in the above literature.

This paper will introduce the structure of logic control system of ground control automatic neutral section passing and two working modes. The reliability of logic control system is analyzed by HAZOP and dynamic fault tree.

2. Ground control automatic neutral section passing technology

Compared with vehicle control automatic neutral section passing, ground control automatic neutral section passing overcomes the traction and running speed loss which is caused by power interruption and coasting, and it overcomes the transportation impact which is caused by extended operation time[3]. The ground control automatic neutral section passing can alternately supply power to neutral zone without operating the main circuit breaker of locomotive. The time of locomotive power loss is short and the speed loss is small. It can meet the needs of China's railways in high-speed, high slope, heavy haul, passenger dedicated line, passenger and freight lines, and can significantly improve the efficiency of railway comprehensive transportation[4]. For ground control automatic neutral section passing technology, logic control system is the core system of the whole technology, and its reliability is the key to the development and application of the system.

If the train straight enters the neutral area with electrification, the arc will be drawn between the catenary and the pantograph, which will burn the catenary and endanger the traffic safety; When the neutral zone has any random phase power, and the train passes through the catenary insulation, it will cause two feeders to short circuit and cause substation trip, but it will not burn down the catenary, which is safe for train. Refer to "fail safe" of interlocking system. Specifically, the system devices and equipment should have the function of reducing or even avoiding losses in case of obstacles, errors and failures, so as to ensure the safety of working. It is defined as the dangerous side when the train enters the neutral zone with electrification, when designing logic control system, it is necessary to guide the fault side to the safe side.

2.1. Logic control system

The system composition diagram is shown in Figure 1, and the logic control system adopts a hierarchical architecture. The core of the control system is the logic operation host with logic operation unit, communication unit and driving acquisition unit as the core. The logic operation host is composed of two systems. Each system adopts a two out of two redundancy structure, and the whole structure is a double two out of two structure. Two systems are hot standby for each other, and the fault of standby system does not affect the operation of the whole system. After the master system fails, the standby system automatically switches to the master system. After the fault is removed, the fault system goes online again, synchronizes with the master host, and becomes the standby machine. At the same time, it enters the hot standby state.

The logic operation unit first collects the data from the train position detection system through the communication unit and the established program of the logic operation unit. After a series of logical operations, the logic operation unit sends communication commands to the communication unit, and the communication unit sends the corresponding commands to the equipment below to control the relevant equipment to perform correct actions.
2.2. Normal train passing mode

The main wiring diagram of the system is shown in Figure 2. Under normal operation of the system (take the direction shown in the figure as an example), series connection backup switches QF1C and QF2C are all closed. When it is detected that the locomotive enters the first detection section which is composed of J1 and J2, QF1 is closed, at this time, the neutral area is connected with the power input from the A-phase feeder, and the neutral area is provided with A-phase power supply. When the locomotive enters the neutral zone (equivalent to entering the second detection section combined by J2 and J3), QF1 is open, QF2 is closed, after a brief power loss, at this time, the neutral area is connected with the power input from the B-phase feeder, and the neutral area is provided with B-phase power supply. After that, the locomotive continues to travel. When it drives out of the second detection section, QF2 is open and the neutral zone is powered off, it returns to no power state again until the next train enters the first detection section [5]. The normal train passing mode process is shown in Figure 3.

The scheme realizes the automatic switching of different phase power supply in neutral area. The locomotive can automatically pass through the neutral zone without any operation. When the main switch get breakdown, the standby logic control will be started and operate the corresponding standby load switch to complete the opening and closing operation, thus ensure the correct and safe switching process of the neutral zone.
Whether the first detection section is occupied

QF1 closed, the neutral zone is connected with feeder A.

Whether the second detection section is occupied

QF1 open and OF2 closed, the neutral zone is connected with feeder B.

QF2 open, the neutral zone power down and return to dead state.

Fig.3 Normal train passing mode

2.3. Fault standby mode

Take QF1 as an example, when QF1 fails to close, make its parallel standby switch QF1B close. If QF1B also fails to close at the same time, the train will break through the neutral zone with electricity, which belongs to the dangerous side. At this time, make QF2B switch closed to make the neutral zone carry B-phase power supply. When the train passes through the catenary insulation, the two phases will be short circuited, the substation protection trips, and the system guides to the safe side. QF1 fault standby logic is shown in Figure 4.

Fig.4 QF1 fault standby logic
3. Method overview

3.1. HAZOP analysis

HAZOP (hazard and operability analysis method) is a structured and systematic analysis method used to identify design defects, process hazards and operational problems[6]. HAZOP is based on guiding words and parameters, and divides the risk identification scope into reasonable nodes (or process units), after that, analyzing each node and using "parameter + guide word" to generate all potential deviations. Identifying the deviation with practical significance, then according to these deviations a further comprehensive analysis will be made. The analysis process is shown in Figure 5.

![HAZOP analysis process diagram](image)

Fig. 5 HAZOP analysis process

3.2. Dynamic fault tree analysis

1. Overview of dynamic fault tree.

Modern systems are becoming more and more complex in nature. This kind of system usually has the ability to respond to failures through partial self-healing. With the increase of system complexity and scale, the uncertainty of these behaviors becomes more and more common, dynamic behavior can be observed in almost any large industrial system. The dynamic behavior of the system leads to different dynamic fault characteristics, such as the priority of function related events and fault events, the classical fault tree cannot simulate such a dynamic scene[7].

Dynamic fault tree analysis (DFTA) combines the advantages of both fault tree analysis and Markov process. By introducing a new type of logic gate to represent the dynamic characteristics, the corresponding dynamic fault tree is established for analysis[8]. Compared with the traditional fault tree analysis method, a dynamic logic gate is added to describe fault-tolerant, redundant and repairable systems. It is more appropriate to describe the dynamic random fault of the system and the correlated faults with sequence. Due to the establishment and solution of Markov model is very complex, this paper uses the idea of modularization to modularize the dynamic fault tree and get the corresponding independent subtree. Markov process is used to analyze the subtree to improve the efficiency of analysis.

Compared with the common fault tree, DFTA introduces dynamic logic gate, such as prior-and gate, sequential correlation gate, hot standby gate, etc. Figure 6 shows the hot standby gate etc. Event X1 and Event X2 are both normal, then event X does not occur; If either event X1 or event X2 fails, event X does not occur; Event X1 and Event X2 are both failed, then event X occur.
2. Markov analysis method

Markov process mainly describes the state of the future, which is only related to the present, not to the past. For \( \forall s \geq s_1 \geq s_2 \geq L \geq s, \forall t \geq 0, \forall i, j, i, K, i \in I \), Formula (1) is held.

\[
P(X(s+\Delta t) = j|X(s)=i, X(s_i)=i, \ldots, X(s_k)=i_k) = P(X(s+\Delta t) = j|X(s)=i)
\]

When the life and post failure replacement time of all components of the system obey exponential distribution, the system can be described by Markov process[9]. Now supposing system X is composed of two components: \( x_1, x_2 \), and supposing the failure rate of the two components are \( \lambda_1, \lambda_2 \) respectively, the repair rate of the two components are \( \mu_1, \mu_2 \) respectively; Supposing \( N(t) \) is the number of failed times of a component, then \( N(t) \) obeys Poisson distribution with parameter \( \lambda \). When component X fails, then the probability of \( N(t) = 1 \) is

\[
P(N(t) = 1) = e^{-\lambda t} = P(N(\Delta t) = 1) = \lambda \Delta t + o(\Delta t),
\]

The situation is similar for component \( x_2 \) failure and two components replacement. According to the working condition of X:

There are four states for X: \( S_1, S_2, S_3, S_4 \). State \( S_1 \) means that \( x_1, x_2 \) are in normal state, X works normally; State \( S_2 \) means that \( x_1 \) is in normal state and \( x_2 \) is in fault state, X works normally; State \( S_3 \) means that \( x_2 \) is in normal state and \( x_1 \) is in fault state, X works normally; State \( S_4 \) means that \( x_1, x_2 \) are in fault state, X is in fault state; In this situation, the state transition diagram is as follows:

As can be seen from the above figure:

\[
\begin{align*}
p_1(\Delta t) &= p_1(0)p_{3,4}(\Delta t) + p_1(0)p_{3,4}(\Delta t) + p_2(0)p_{3,4}(\Delta t) + p_1(0)p_{3,4}(\Delta t) \\
p_2(\Delta t) &= p_2(0)p_{3,4}(\Delta t) + p_1(0)p_{3,4}(\Delta t) + p_2(0)p_{3,4}(\Delta t) + p_1(0)p_{3,4}(\Delta t) \\
p_3(\Delta t) &= p_3(0)p_{3,4}(\Delta t) + p_2(0)p_{3,4}(\Delta t) + p_3(0)p_{3,4}(\Delta t) + p_2(0)p_{3,4}(\Delta t) \\
p_4(\Delta t) &= p_4(0)p_{3,4}(\Delta t) + p_3(0)p_{3,4}(\Delta t) + p_4(0)p_{3,4}(\Delta t) + p_3(0)p_{3,4}(\Delta t)
\end{align*}
\]

Take a derivation at \( t = 0 \) of the above formula \( p_\delta(t) \):

Fig. 6 Hot standby gate

Fig. 7 System X state transition diagram
\[ \frac{dp_x}{dt}(\Delta t) = p_{x_1}(0)q_{s_1,s_5} + p_{x_2}(0)q_{s_2,s_5} + p_{x_3}(0)q_{s_3,s_5} + p_{x_4}(0)q_{s_4,s_5} \]
\[ \frac{dp_y}{dt}(\Delta t) = p_{y_1}(0)q_{s_1,s_5} + p_{y_2}(0)q_{s_2,s_5} + p_{y_3}(0)q_{s_3,s_5} + p_{y_4}(0)q_{s_4,s_5} \]
\[ \frac{dp_z}{dt}(\Delta t) = p_{z_1}(0)q_{s_1,s_5} + p_{z_2}(0)q_{s_2,s_5} + p_{z_3}(0)q_{s_3,s_5} + p_{z_4}(0)q_{s_4,s_5} \]
\[ \frac{dp_w}{dt}(\Delta t) = p_{w_1}(0)q_{s_1,s_5} + p_{w_2}(0)q_{s_2,s_5} + p_{w_3}(0)q_{s_3,s_5} + p_{w_4}(0)q_{s_4,s_5} \]

Namely:

\[ \begin{pmatrix} p_x(t) \\ p_y(t) \\ p_z(t) \\ p_w(t) \end{pmatrix} = \begin{pmatrix} p_{x_1}(t) \\ p_{y_1}(t) \\ p_{z_1}(t) \\ p_{w_1}(t) \end{pmatrix}Q \]

Transfer intensity matrix Q:

\[ Q = \begin{pmatrix} q_{s_1,s_1} & q_{s_1,s_2} & q_{s_1,s_3} & q_{s_1,s_4} \\ q_{s_2,s_1} & q_{s_2,s_2} & q_{s_2,s_3} & q_{s_2,s_4} \\ q_{s_3,s_1} & q_{s_3,s_2} & q_{s_3,s_3} & q_{s_3,s_4} \\ q_{s_4,s_1} & q_{s_4,s_2} & q_{s_4,s_3} & q_{s_4,s_4} \end{pmatrix} \]

\[ = \begin{pmatrix} -\lambda_1 - \lambda_2 & \lambda_2 & \lambda_1 & 0 \\ \mu_2 & -\lambda_1 - \mu_2 & 0 & \lambda_1 \\ \mu_1 & 0 & -\mu_1 - \lambda_2 & \lambda_2 \\ 0 & \mu_2 & \mu_1 & -\mu_1 - \mu_2 \end{pmatrix} \]

4. Reliability index

For system components, there are only two discrete states that they can be: normal state or fault state. Now supposing that the system consists of \( n \) independent components, when a component fail, replace it immediately, the life and replacement time of all components obey exponential distribution. The life of the \( i \)-th component can be regarded as a random variable which obeys the exponential distribution of parameter \( \lambda_i \), and the replacement time of the \( i \)-th component can be regarded as a random variable which obeys the exponential distribution of parameter \( \mu_i \); At this time, each component is a switching system: the components start to work and enter the ON state; after a period of time interval, they should be replaced and enter the OFF state; then enter the ON state again. The average duration of the \( i \)-th component in the ON state is \( 1/\lambda_i \), and that of the \( i \)-th component in the OFF state is \( 1/\mu_i \), If the normal operation of the component is 0 and the fault is 1, then the state of the \( i \)-th component at time \( t \) is \( X_i(t) \), then \( \{X_i(t)\} \) is a continuous time Markov chain, and the state space is \( E = \{0,1\} \). The state transition diagram of the \( i \)-th component is as follows:

![Fig.8 Transition diagram of component state](image)

According to formula (4), it can be concluded that:

\[ (p_0(t)) \begin{pmatrix} p_1(t) \\ p_2(t) \\ p_3(t) \end{pmatrix} = \begin{pmatrix} -\lambda & \lambda \\ \mu_1 & -\mu_1 \end{pmatrix} \]

By substituting the formula (4) and the initial conditions \( (p_0(0), p_1(0)) = (0, 1) \), the differential equation can be concluded that:
\[ p_0(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \]

\[ p_1(t) = \frac{\lambda}{\lambda + \mu} \left[ 1 - e^{-(\lambda + \mu)t} \right] \]

Availability \( A(t) \) refers to the probability that the component can work normally at time \( t \) under the condition of normal operation at initial time. In particular, when the failure and repair of the components follow the exponential distribution, \( A(\infty) \) will converge to a constant independent of \( t \), that is, the steady-state availability \( A[10] \).

Then \( p_0(t) \) is the instantaneous availability \( A(t) \) of the component, and the steady-state availability can be obtained by calculating the limit of \( p_0(t) \):

\[ A = \lim_{t \to \infty} p_0(t) = \frac{\mu}{\lambda + \mu} \quad (6) \]

For the state transition diagram of \( X \), Markov chain \( \{X(t)\} \) is aperiodic irreducible chain, and its stationary distribution is the limit distribution. Then the steady-state efficiency expression of the whole \( x \) is as follows:

\[ A = p_{s_1} + p_{s_2} + p_{s_3} = \lim_{t \to \infty} p_{s_1}(t) + \lim_{t \to \infty} p_{s_2}(t) + \lim_{t \to \infty} p_{s_3}(t) \]

\[ = \frac{\mu_1 \mu_2 + \mu_1 \lambda_2 + \mu_2 \lambda_1}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)} \quad (7) \]

5. Case analysis

The automatic ground control neutral section passing was first put into use in Guanyinshan neutral section on November 18, 1998, which marks the second country in the world to master the technology of automatic ground control (Live) neutral section passing system after Japan[3]. With the development of automatic neutral section passing technology in recent years, it is outstanding in many freight and heavy haul railways, which can effectively shorten the train neutral section passing time and improve the transportation efficiency; but at the same time, in the process of operation, there are some hidden dangers, such as the control core failure, which has a greater impact on transportation. This paper takes the automatic ground control neutral section passing system under test in Xi’an South Railway Station of Xikang passenger and freight on the same line as the research object, and analyzes the safety and weak links of the logic control system in the automatic ground control neutral section passing system by using HAZOP and dynamic fault tree.

The causes of risk events are usually summarized as: design reasons, manufacturing reasons, construction reasons, operation reasons and external factors[11]. With the combination of logic control system and guide words, all deviations are traversed, and the deviations related to the system structure are screened to generate the list of hazard sources, as shown in Table 1.

| Parameter                  | Guide Words         | Deviation                                      | Possible Reasons                                                                 | The worst possible outcome of the system                        |
|----------------------------|---------------------|------------------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Logic Control System       | None                | Offline and no response                        | Power module failure, network transmission channel                               | System offline                                                  |
|                            | Accompany           | Interference and noise                        | Electromagnetic interference generated by thunderstorm weather and high pressure environment on site | Switch mistake moving                                          |
|                            | Part                | Only some functions can be realized           | Communication unit, logic host, drive acquisition and other parts of the fault   | Unable to complete normal logic operation and distribution       |
|                            | Abnormal            | Abnormal arrival of train in Section Detection | Occupancy detection section of other engineering vehicles                        | Detection has been occupied by the vehicle, the switch is closed, and the neutral zone is always charged |
According to the list of hazard sources, the comprehensive lightning protection system can be added for interference and noise at the beginning of design, and the power lightning protection box shall be set at the power lead-in end[12]. The outdoor equipment shall be introduced through the lightning protection distribution cabinet, and then connected to the control system. For a section that takes too long, it can be solved by setting the first axis not to collect but not in a continuous way. The remaining deviations can be modeled as intermediate events according to their possible causes. Taking "system failure, endangering driving safety" as the top event, the possible cause of each deviation as the intermediate event, the fault tree is constructed as follows. The fault tree is shown in the following figure, and the basic events in the figure are shown in Table 2.

Fig.9 Fault tree of logic control system

| No. | Basic Events                      | No. | Basic Events                      |
|-----|-----------------------------------|-----|-----------------------------------|
| 1   | Machine mainboard fault           | 11  | Power supply module 2 fault       |
| 2   | Logic operation module 1 fault    | 12  | Detection point 1 axle counter 1 fault |
| 3   | Logic operation module 2 fault    | 13  | Detection point 1 axle counter 2 fault |
| 4   | Communication module 1 fault      | 14  | Detection point 2 axle counter 1 fault |
| 5   | Communication module 2 fault      | 15  | Detection point 2 axle counter 2 fault |
| 6   | Driven collect unit 1 fault       | 16  | Detection point 3 axle counter 1 fault |
| 7   | Driven collect unit 2 fault       | 17  | Detection point 3 axle counter 2 fault |
| 8   | Communication bus 1 fault         | 18  | Cable channel 1 fault             |
| 9   | Communication bus 2 fault         | 19  | Cable channel 2 fault             |
| 10  | Power module 1 fault              |     |                                   |

The relevant reliability data of the equipment are shown in Table 3.
Table 3. Equipment reliability data

| Equipment name          | Failure rate (10^-6) |
|-------------------------|----------------------|
| Logic operation module  | 0.3306               |
| Communication module    | 0.3733               |
| Driven collect unit     | 9.629                |
| Machine mainboard       | 0.0257               |
| Communication bus       | 1.3875               |
| Power supply module     | 0.2317               |
| Axle counter module     | 2.4436               |
| Cable channel           | 0.1568               |

According to all the data in Table 3, the failure rate \( \mu = 1/MTR = 2h^{-1} \) of logic control system is \( 1.3014 \times 10^{-5} \) and the steady state availability is 99.9993%.

6. Conclusion

This paper introduces the logic control system of ground control automatic neutral section passing technology, train normal passing mode and fault standby mode, and introduces the definition of "fault—safety" of ground control automatic passing through neutral section. It is one of the most important links in the system design to avoid burning the catenary. When the fault leading to the hazardous side occurs, the system will be directed to the safe side through the fault standby logic, with the worst result of the substation protection trip. After that, the reliability of automatic ground control neutral section passing logic control system is analyzed and the following conclusions are obtained:

Through the use of HAZOP method, the worst possible results and causes of the system are analyzed to generate a list of hazard sources. At the same time, the dynamic fault tree is constructed according to the deviation and possible causes, so as to avoid the problems of multiple fault trees in fault tree construction.

The steady state availability of the logic operation system with the structure of Double2-vote-2 is up to 99.9993%, which indicates that the logic control system has high availability in the structural design, but lacks the actual operation data of field equipment. With the development of automatic ground control neutral section passing in China's railways, the actual data can be used for further reliable analysis in the future. Meanwhile, artificial and weather factors are considered in the analysis to make the whole result more accurate.

References

[1] Shen Mansheng and Zhou Fangyuan. Development status and trend of railway traction power supply technology at domestic and foreign [J]. Electric Railway, 2019, 30 (01): 1-7+12
[2] Hu Jiaxi and Zhou Fangyuan. Status and development of neutral section passing technology for electrified railway trains [J]. Electric Drive for Locomotives, 2019 (03): 1-5.
[3] Luo Wenji and Xie Bing. Study and application of the technology of ground auto-phase-break-system for electrified railway [J]. Railway Locomotive and Car, 2008,28 (S1): 27-33.
[4] Luo Xing, Luo Wenji, Zhu Jiankai and Pu Jiangang. Study on the application of engineering design of automatic ground control neutral-section passing on electrified railway line of high speed, great gradient and heavy haul [J]. Railway Standard Design, 2013 (07): 101-105.
[5] LV shunkai. Ground automatic phase separation device of electrified railway section post [J]. Technology Innovation and Application, 2019 (05): 7-10.
[6] Zhao Wenfang, Jiang Chunming, Jiang Weiwei and Zhang Weihua. The core technology of hazop analysis [J]. Safety Health and Environment, 2005 (03): 1-3
[7] Sohag Kabir. An overview of fault tree analysis and its application in model based dependability analysis[J]. Expert Systems With Applications,2017,77.
[8] Li Junli and Zhang Youpeng. Research on safety and performance analysis of computer based interlocking system based on dynamic fault tree analysis [J]. Journal of Railway Science and Engineering, 2019,16 (06): 1543-1552
[9] Ji Huiyuan. Research on dynamic fault tree analysis method [D]. National University of Defense Technology, 2002.

[10] Yan Qi. Reliability evaluation of relay protection system based on Markov process [D]. North China Electric Power University, 2012.

[11] Wang Fang. Research and safety analysis of high voltage thyristor valve ground phase separation scheme [J]. Electric Railway, 2018,29 (03): 11-13+18.

[12] Mo Zhigang, Luo Hanbin. Safety evaluation of urban rail transit signal system based on hazop and alarp principles [J]. Electric Drive for Locomotives, 2018 (03): 85-89+95.