FUNCTIONAL SAFETY ANALYSIS OF HIGH-SPEED MAGLEV TRAIN OPERATION CONTROL SYSTEM

DEMIN ZHANG, YADONG ZHANG, JIN GUO, TONG GAO

The School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China
Corresponding author's email: 1576365254@qq.com

Abstract: *The high-speed maglev train operation control system (OCS) performs control and protection of the maglev train by performing various functions. In order to ensure the correct execution of the system functions, functional safety analysis of the operation control system is required. In view of the characteristics of high-speed maglev railway, this paper uses FEMA combined with FTA to analyze the functional safety of the operation control system, and to identify the failure mode and its influence,and to find the cause of the failure. And the results of the analysis provide guidance for the design of the operational control system. Finally, The method is applied to the train operation control system of Shanghai Maglev Demonstration Line to verify the feasibility of the method.*

Keywords: *High-speed maglev train, Operation control system, Safety analysis, FEMA, FTA.*

I. INTRODUCTION

The high-speed maglev train operation control system (OCS) is the brain of the high-speed maglev transportation system which is connected to equipment or systems such as vehicles, traction lines and switches in the maglev system to complete the control, safety protection, automatic operation and dispatch management of the train. In order to ensure high-speed maglev train running at high speed and safely, and to adjust the operation plan according to the condition of the running train and line at any time, and to quickly deal with various emergencies during operation, the operation control system must correctly perform its functions. Therefore, it is necessary to perform functional safety analysis on the OCS to ensure the correct execution of the system functions.

According to the structure and function of high-speed maglev operation control system, this paper proposes a functional safety analysis method which uses FEMA combined with FTA. It uses FEMA to identify the functional failure mode of the operation control system and its influence on the system, and uses FTA to assist FEMA to find the cause of the failure. The final result is given in the form of a FEMA table.

This research was supported by National Natural Science Foundation of China (Grant No. 61703349), Key Research Projects of China Railway Corporation (Grant No. N2018G062, K2018G011), and Fundamental Research Funds for the Central Universities (Grant No. 2682017CX101)

II. ANALYSIS OF CHARACTERISTICS OF HIGH-SPEED MAGLEV TRAIN OPERATION CONTROL SYSTEM

The high-speed maglev train operation control system is a hierarchical and partitioned control system which functions need to be completed by each subsystem. FEMA (Failure Models and Effects Analysis) which can divide the system into subsystems and modules hierarchically and each component in the hierarchy can be analyzed by FEMA is a bottom-up systematic approach to assessing all possible failures in the system. Therefore, it has advantages to analyze the failure mode of the high-speed maglev train operation control system by FEMA.

The realization of the function of the high-speed maglev train operation control system is completed by software and hardware. The failure of the function must not only consider the hardware and software problems, but also the influence of environmental factors. The FEMA which focuses on finding system hardware failures that cause failures makes it difficult to detect the effects of software errors and environmental factors. However, the FTA (Fault Tree Analysis) can comprehensively analyze various factors that may cause system failures and then determine the cause of the failure such as hardware, software, environment, human factors, etc.

III. THE PROPOSED METHOD

The high-speed maglev train operation control system consists of subsystems and the functions of the system are represented by the functions of each subsystem. The method proposed in this paper completes the functional safety analysis of the OCS by performing functional safety analysis on each subsystem of the OCS. The analysis process is shown in the figure 1.

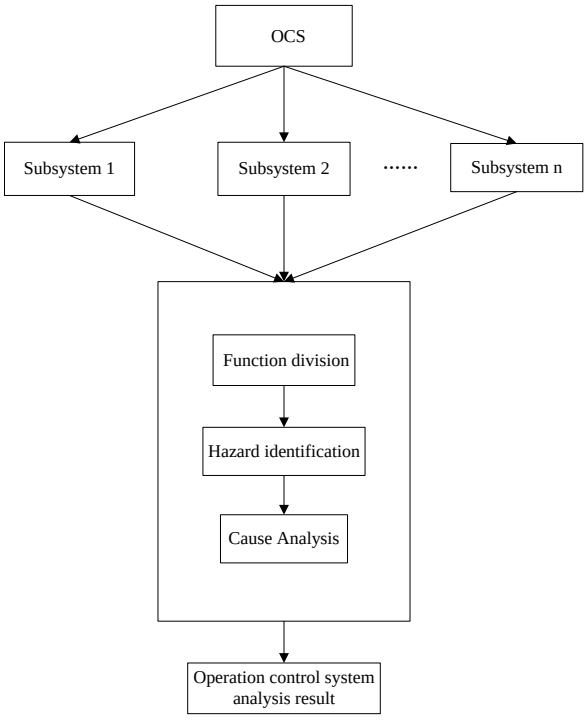

Figure 1. *Functional safety analysis process*

The method identifies the failure mode and its impact of each subsystem and finds the cause of the failure through three steps which include function division, hazard identification, cause analysis. The purpose of functional division is to obtain the main functions and sub-functions of the subsystem. The purpose of hazard identification is to obtain the failure mode of the main function of the subsystem by FEMA. The purpose of the cause analysis is to find out the cause of the failure of the subsystem function by FTA. The analysis results of each subsystem are presented in the form of FEMA tables which is used to represent the functional safety analysis results of the operational control system.

3.1. Function Division

a) According to the system technical specifications, requirements specifications, etc., to define the boundaries of the subsystems of the OCS, input and output information and the functions of the subsystem; b) A detailed description of the implementation process of the subsystem function; c) According to the description to determine the sub-functions of each subsystem.

3.2. Hazard Identification

The functional hazard identification of the high-speed maglev train operation control system is to identify the main functions of each subsystem. The hazard identification of the main functions of the subsystem is obtained through sub-function hazard identification and interface hazard identification. In the process of hazard identification, the FEMA is combined with expert experience to identify the failure mode of the function and its impact, and the results are corrected by expert inspection.

(1) Preparation stage for hazard identification

Before using the FEMA for analysis, you need to define a FEMA table, define the level of agreement, and define the numbering system for hazard identification, in preparation for subsequent sub-function hazard identification, interface hazard identification, and hazard identification of the main function. The specific process is as follows:

a) Determine the FEMA table format: Refer to the format specified in the Chinese military standard GJB1391-92 and combined with the characteristics of the high-speed maglev train operation control system to obtain a FEMA table suitable for OCS;

b) Define the agreement level: According to the functional relationship and composition characteristics of OCS, the system function hierarchy is divided and the main functions and sub-functions of the system are divided into different agreed levels;

c) Develop a numbering system for hazard identification: Including number of the OCS subsystem, functional failure mode and system interface failure mode, etc., to make the hazard identification process clearer and help to further analyze the cause of the hazard.

(2) Sub-function hazard identification

The hazard identification of the main functions of the subsystem starts from the sub-function hazard identification. The FEMA is used to analyze the sub-functions of each subsystem that identifies the sub-function failure mode and finds the local impact and final impact of the

functional failure. Then the results are corrected through expert inspection. The process is as follows:

a) Consider the high-speed maglev operation control system equipment and operating characteristics to determine the guiding words (such as not, errors, delays, etc.).

b) For each of the main functions of the subsystem, the sub-functions are analyzed by the guide words to obtain the failure modes of all possible sub-functions under the main function;

c) Determine the local and final effects of the sub-function failure mode and record the results of the hazard identification in the FEMA table of the main function.

d) Invite experts to discuss the results, modify and delete the incorrect failure mode, and improve the final result.

(3) Interface hazard identification

The system does not exist in isolation. Problems in the process of transmitting information between the system boundary and external devices will also affect the system function. It is also one of the reasons for the failure of the function. Therefore, it is necessary to identify the interface of the system. First, we must clarify the boundaries of subsystems and the information that interacts with other systems or devices and then use FEMA method analysis to obtain the interface FEMA table. The analysis process and sub-function hazard identification process are similar and will not be described again.

(4) Main function hazard identification

According to the definition of the functional agreement level, the local failure effect of the sub-function is the influence of the sub-function failure on its own agreed level and the final failure effect of a sub-function is the effect of sub-function failure on the agreed level at which the main function is located. According to the relationship between the agreed levels, the final effect of failure mode of the sub-function is the failure mode of the main function. The final effect of the sub-function failure mode is summarized, and the failure mode of the corresponding main function, that is, the failure mode of the subsystem function is obtained.

3.3. Cause Analysis

The functional failure modes of the subsystems which are obtained in Section 3.2 are analyzed and the FTA method is used to find the combination of cause events leading to functional failure. According to the relationship between the agreed levels, the failure mode of the sub-function and the interface are the failure reasons of the main function. The FTA method is used to establish the fault tree. The main function failure mode is used as the top event of the fault tree. The failure mode and the interface failure mode of all the sub-functions that constitute the main function are used as intermediate events to find the bottom event that causes the intermediate event to occur.

Referring to the relevant standards and combining the specific conditions of the equipment in the high-speed maglev train operation control system, the bottom events leading to the failure

of the sub-functions are found from four aspects: hardware failure, software failure, interface failure and environmental factors. a) hardware failure: the core control functions of each subsystem of the OCS are mainly completed by the main control unit, so the hardware failure is mainly the failure of the main control board; b) Software failure: mainly the failure of the main control program; c) interface failure: mainly the various problems that occur when sending and receiving information and the failure of the interface board; d) Environmental factors: Mainly consider electromagnetic interference, such as sudden changes in signals caused by electromagnetic radiation and electrical fast transient pulses, and the power supply failure of the power supply is also a cause of damage. Finally, the cause of the failure is recorded in the FEMA table of each of the main functions of the subsystems.

IV. CASE STUDY

4.1. Train Operation Control System of Shanghai Maglev Demonstration Line

As shown in the figure 2, the train operation control system of Shanghai Maglev Demonstration Line is composed of central control system (CCS), decentralized control system(DCS) and vehicle control system(VCS). The CCS is located in the control center to realize the development and execution of the train plan and to monitor and control the running status of the train. The DCS transmits train information and completes the protection of the train and the route, which is located in the traction substation or the switch room and corresponds to the traction section. The VCS is located on the maglev train to achieve train control and management.

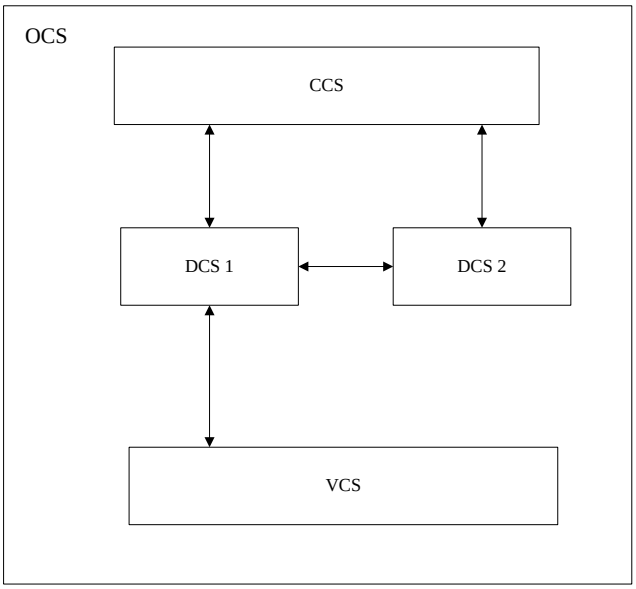

***Figure 2**. Train operation control system structure of Shanghai Maglev demonstration line*

The CCS automatically issues a route command to the DCS according to the timetable; The DCS completes functions such as route handling, switch protection and speed protection curve calculation, and transmits information such as line data and speed protection curve to the VCS.

4.2. Functional safety analysis

As shown in the figure 2, the OCS of Shanghai Maglev Demonstration Line is composed of three subsystems: CCS, DCS and VCS. Using the proposed method to perform functional safety analysis on the OCS requires functional safety analysis of the three subsystems. Due to the length limitations, only the functional safety analysis process of the DCS is given.

1. Function Division

The DCS is the core component of the OCS and completes six functions of driving sequence control, route protection, switch protection, train protection, train speed curve monitoring and traction cutting.

The driving sequence control function receives commands and driving parameters from the CCS, and checks and disassembles them. If the received command can pass the check, the decomposed parameters are assigned to the corresponding subordinate function modules. It can be seen that the driving sequence control function is to check, analyze and distribute the information sent by the CCS. SO driving sequence control function can be further divided into three sub-functions: checking the function of the message sent by the CCS, parsing the function of the message sent by the CCS and assigning the parsed message function. By analogy, the six main functions of the partition control system can be divided into 22 sub-functions as shown in table 1.

Table 1. *Sub-functions of the DCS*

Number	Function	Subfunction
1	Driving sequence control function	Check the message sent by the central control system
		Parsing the message sent by the central control system
		Assign the parsed message
2	Route protection function	Obtain track section status
		Route reservation
		Lock track section
		Check switch move request
		Cancel route reservation
3	Switch protection function	Unlock switch
		Identify switch position
		Lock switch
4	Train protection function	Check train integrity
		Train registration
		Manage train operation mode
		Manage train status
		Train safety suspension
		Activate train safety brake
5	Train speed curve monitoring function	Manage parking spots
		Monitor driving directions
6	Traction cutting function	Electronic cutoff
		Electric cut off
		Read back read current decision signal

2. Hazard identification

Considering the characteristics of the OCS, the format of the FEMA table is determined, as shown in table 2.

Table 2. *Header used in this article*

Number	Identifier	Failure mode	Reason for failure	Local impact	Final impact

In the table 2, column 1 indicates the number of the system function; Column 2 shows the number of functional failure mode; Column 3 represents the fault manifestation of the function; Column 4 indicates the cause of the failure; Column 5 indicates the effect of functional failure on the level of the function itself; Column 6 indicates the impact of the functional failure on the highest level.

The main function and sub-function of the DCS are defined as the initial agreement level and the minimum agreement level respectively to complete the agreed hierarchy of defining DCS functions. For example, the driving sequence control function that is one of the main functions is defined as the initial agreement level and the three sub-functions are defined as the minimum agreement level.

The hazard identification number system of the DCS is defined. First, we perform the main function and sub-function number of the DCS. Table 3 shows the part function numbers of the DCS.

Table 3. *Function Number of DCS*

Number	Function	Number of Subfunction	Subfunction
1	Driving sequence control function	1-1	Check the message sent by the CCS
		1-2	Parsing the message sent by the CCS
		1-3	Assign the parsed message
2	Route protection function	2-1	Obtaining track section status
		2-2	Route reservation
		2-3	Lock track section
		2-4	Check switch move request
		2-5	Cancel route reservation

Secondly, the functional failure mode is labeled, and the DCS is represented by 1 with the main function failure modes numbered 1-1, 1-2, 1-3 and so on. The number of failure modes of each sub-function is 1-1-1, 1-1-2, 1-1-3 and so on. The interface numbers are in order of I-1, I-2, I-3, and so on. The interface failure mode numbers are I-1-1, I-1-2, I-1-3, and so on.

After completing the preparation phase, we continue to identify sub-function hazards. According to the function realization process of the DCS and the characteristics of the signals transmitted between the functions determine that guiding words of the sub-functions are incapable of execution, error execution, delayed execution/timeout and always execution. The guide words are used to analyze all the sub-functions of each main function of the DCS, and all the failure modes of the sub-functions are listed. The local and final impact of the sub-function failure mode are analyzed and the effects of each sub-function on the six main functions of DCS are summarized as failure, error, delay/timeout and always the same. The results which are improved and organized multiple times are recorded in the FEMA table of the corresponding main function. The DCS has a total of 6 FEMA tables, which are the driving sequence control function FEMA table, the route protection function FMEA table, the switch protection function FMEA table, the

train protection function FMEA table, the train speed curve monitoring function FMEA table and the traction cut-off function FMEA table. Due to the length limitations, only part of the FEMA table of the driving sequence control function is shown, as shown in table 4.

Table 4. *Driving sequence control function FMEA table*

Number	Subfunction	Identifier	Failure mode	Local impact	Final impact
1-1	Check the message sent by the CCS	1-1-1	Cannot check messages sent by the CCS	Cannot check messages sent by the CCS	Cannot perform driving sequence control
		1-1-2	Error checking messages sent by the CCS	Error checking messages sent by the CCS	Wrong execution of driving sequence control
1-2	Check the message sent by the CCS	1-2-1	Cannot parse messages sent by the CCS	Cannot parse messages sent by the CCS	Cannot perform driving sequence control
		1-2-2	Error parsing messages sent by the CCS	Error parsing messages sent by the CCS	Wrong execution of driving sequence control
		1-2-3	Timeout parsing the message sent by the CCS	Timeout parsing the message sent by the CCS	Delayed execution of driving sequence control

Then we perform the interface hazard identification of the DCS. The interface between the DCS and external devices is shown in Figure 3. There are mainly CCS, VCS, adjacent DCS, ground devices, and traction control systems. The hazard identification of the DCS interface in this section is only for the interface related to its six main function information transmission, that is, the interface with the CCS, the VCS, the adjacent DCS, the ground equipment and the traction control system. The hazards of all relevant interfaces are considered when looking for the cause of the hazard.

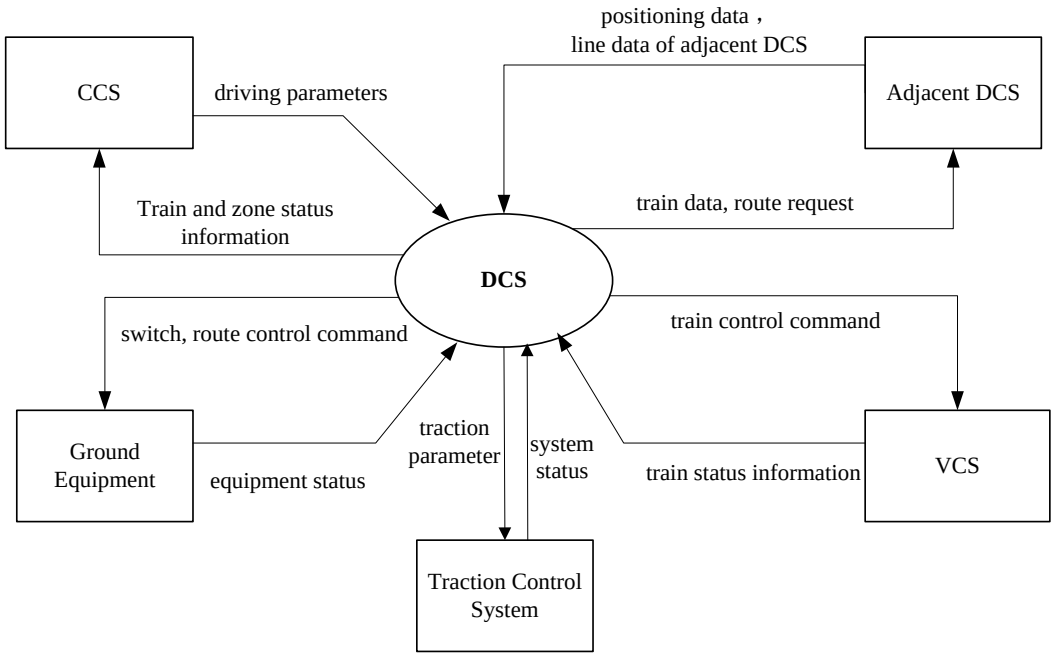

Figure 3*. DCS Interface*

The interface between the DCS and the external device is mainly to complete the receiving and sending of information. According to the failure mode that may occur in the signal, the failure mode of the interface can be identified as follows: cannot receive external device information, receive external device information incorrectly, cannot send information to external devices, send information to external devices incorrectly, cannot send information to the system, send information to the system incorrectly, cannot receive system information, receive system information incorrectly, communication with external devices is always the same and communication delay with external devices. The local and final effects are the same as the hazard identification of the sub-function. After several times of improvement and finishing, the FEMA table of the DCS interface was obtained. Table 5 shows the partial contents of the FEMA table of the DCS interface.

Table 5. *DCS Interface FMEA Table*

Number	Subfunction	Identifier	Failure mode	Reason for failure	Local impact	Final impact
I-1	CCS interface module	I-1-1	Cannot receive CCS information	1. Communication line break 2. No power supply 3. Interface board failure 4. Interface module software failure 5. Long communication lines and signal attenuation	Cannot receive CCS information	There is no CCS information. Cannot perform driving sequence control, route protection, etc.
		I-1-2	Error receiving CCS information	1. The content of the message is incorrect. 2. Electromagnetic radiation 3. Electrical fast transient pulses lead to signal mutations 4. Interface module software failure 5. Interface board failure	Error receiving CCS information	Causes the DCS to perform the correspondi-ng function error

Finally, we perform hazard identification of the main function of the DCS. According to the relationship between the defined agreed levels, the final effect of the identified sub-function failure mode is the failure mode of the main function. The final effects of the failure mode obtained in the sub-function hazard identification of the DCS are summarized, and a total of 26 failure modes of the main functions of the DCS are obtained. Partial failure modes are shown in table 6. We will analyze 26 failure modes in the next step, find the cause of the failure, and improve the FEMA table.

Table 6. *Main function failure mode of the DCS*

DCS number 1		
Serial number	Number	Main function failure mode
1	1-1	Cannot perform driving sequence control
2	1-2	Error execution of driving sequence control
3	1-3	Delayed execution of driving sequence control
4	1-4	Cannot protect the route
5	1-5	Error execution of protecting route
6	1-6	Delayed execution of protecting route
7	1-7	Cannot perform route reservation
8	1-8	Error execution of performing route reservation
9	1-9	Delayed execution of performing route reservation

3. Cause analysis

The FTA method is used to analyze the main function failure modes of 26 types of DCS to find the cause of the failure mode, and fill in the FEMA table. The 26 main function failure modes are respectively used as the top event of the fault tree, and the corresponding sub-function failure mode and interface failure mode are taken as intermediate events which are analyzed to find the bottom event that caused the intermediate event. Due to space limitations, the fault tree analysis process of the failure mode that cannot protect route in table 6 is given as an example.

First, the failure mode that cannot protect route is taken as the top event of the fault tree. Then, the sub-function failure mode that caused it to fail is found according to the contents in the final impact column of the route protection function hazard identification FMEA table. There are total of 3 sub-function failure modes, such as cannot lock the track section, cannot acquire the track section status, and cannot check the switch movement request. The three sub-function failure modes are used as the intermediate events of the fault tree, and the causes of the sub-function failure modes are analyzed one by one.

It is known from Section 3.3 that the cause of sub-function failure mainly considers the main controller software failure, main control board failure, electromagnetic radiation, electrical fast transient pulse, and also consider whether the information obtained from the external device when the main control unit completes the function will cause the failure mode to occur. The intermediate event that cannot acquire the track section status in this example is analyzed and it is found that the communication interface failure with the ground device will also cause the system to fail to protect the route. For further analyze the reasons for the failure of the interface transmission information, we refer to the content of the failure reason column in the DCS interface hazard identification FEMA table. The failure mode causes of other sub-functions are analyzed as above and will not be described again. The fault tree that cannot protect the route is shown in figure 4.

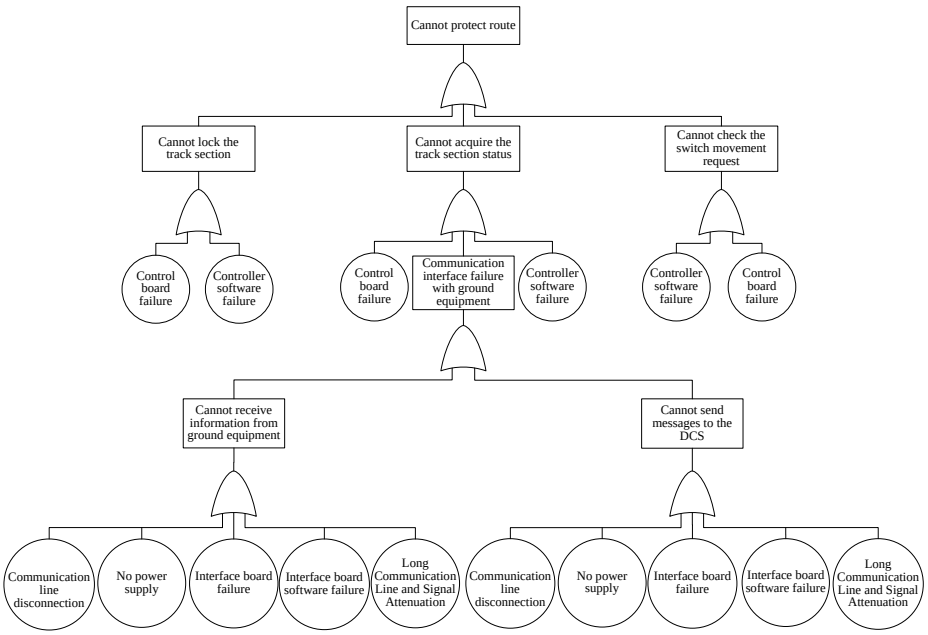

Figure 4. *Fault tree that cannot protect the route*

After the cause analysis, we found the cause of the failure of the main function of the DCS, and recorded the reason in the failure reason column of the corresponding main function FEMA table. As shown in table 7.

Table 7. *Driving sequence control function FMEA table*

Number	Subfunction	Identifier	Failure mode	Reason for failure	Local impact	Final impact
1-1	Check the message sent by the CCS	1-1-1	Cannot check messages sent by the CCS	1. Controller software failure 2. Control board failure 3. Communication interface with the CCS cannot transmit information	Cannot check messages sent by the CCS	Cannot perform driving sequence control
		1-1-2	Error checking messages sent by the CCS	1. Controller software failure 2. Control board failure 3. Communication information error with the CCS interface 4. Electromagnetic radiation 5. Electrical fast transient pulses make the signal abrupt	Error checking messages sent by the CCS	Wrong execution of driving sequence control
1-2	Check the message sent by the CCS	1-2-1	Cannot parse messages sent by the CCS	1. Controller software failure 2. Control board failure 3. No command to receive the CCS	Cannot parse messages sent by the CCS	Cannot perform driving sequence control
		1-2-2	Error parsing messages sent by the CCS	1. Controller software failure 2. Control board failure 3. Receive incorrect CCS commands 4. Electromagnetic radiation 5. Electrical fast transient pulses make the signal abrupt	Error parsing messages sent by the CCS	Wrong execution of driving sequence control
		1-2-3	Timeout parsing the message sent by the CCS	1. Controller software failure 2. Control board failure 3. CPU frequency is too low 4. Delay in communicating information with the CCS	Timeout parsing the message sent by the CCS	Delayed execution of driving sequence control

We used the proposed method to analyze the DCS, and finally got six main function FEMA tables and one interface FEMA table and use the contents of the table to represent the results of the security analysis. For OCS, we use the primary functional FEMA table and interface FEMA table of each subsystem to represent the safety analysis results.

V. CONCLUSIONS

This paper proposes a method for functional safety analysis of high-speed maglev train operation control system and applies it to the functional safety analysis of train operation control system of Shanghai Maglev demonstration line. Through analysis, we obtained the functional failure mode of the OCS and gave the reason for each failure mode. On the one hand, the method allows the analyst to understand the operating principle of the system through the analysis process, and has a comprehensive understanding and grasp of the system function failure. On the other hand, the designer can deeply consider the causes of the functional failure and provide guidance for the design. However, this method focuses on the qualitative analysis of the system, lack of quantitative analysis of the system. In the following research, we will introduce qualitative analysis technology to qualitatively analyze the high-speed maglev train operation control system.

References

[1]. *Wei Qing-chao*, Maglev Railway System and Technology[M]. China Science and Technology Press, Beijing, 2010.

[2]. *Wu Xiang-ming*, Maglev Train [M]. Shanghai Science and Technology Press, Shanghai, 2003.

[3]. GJB1391-92: Failure Mode, Impact and Hazard Analysis Program[S]. National Defense Science and Technology Commission, Beijing, 1992.

[4]. *Clifton A. Ericson H*. Hazard Analysis Techniques for System WILEY-INTERSCIENCE,2005:95-114,261-292,365-382.

[5]. *M. H .Faber*. Risk assessment for civil engineering facilities :critical overview and discussion [J]. Reliability Engineering and System Safety, 2003，80 (2).