Train Control Uncertainty Treatment and Safety Assurance: Shifting from Manual Driving to Fully Automation

Fei Yan, Associate Professor Ph.D., School of Electronic and Information Engineering, Beijing Jiaotong Univ.
Chunhai Gao, Professor of Beijing Jiaotong Univ, Chairman and President of Traffic Control Technology Co., Ltd.
Ru Niu, Associate Professor Ph.D., School of Electronic and Information Engineering, Beijing Jiaotong Univ.
Tao Tang, professor, School of Electronic and Information Engineering, Beijing Jiaotong Univ.

SUMMARY

Large cities depend heavily on their metro systems to alleviate traffic jams, while disruptive incidents have become more common, causing threats to passenger safety and transport service plans. Adopting a Fully Automatic Operation (FAO) system with advanced technology, stable performance and, efficiency has become the urgent need of global rail transit construction. The objective of this paper is to show how to deal with train control uncertainty in driverless metro and give a possible solution to realize a resilient metro system. This paper uses an FAO system scenario to perform a causal scenario search method based on Systems-Theoretic Process Analysis (STPA) for safety analysis to, increase the identification of causal scenarios and related safety requirements. At the same time, it discusses the safety process of testing, verification and validation. The safety assurance scheme of the FAO system in the design and development process is proposed.

1 INTRODUCTION

FAO systems are a new generation of urban rail transit systems aimed at enhancing operational services via modern information and automation technology that improve functionality and performance of system equipment. Although rail traffic is becoming more and more automated, the demand for safety has never changed. The traditional methods of safety analysis are mainly Failure Mode and Effect Analysis (FMEA) [1] and Fault Tree Analysis (FTA) [2]. However, both FMEA and FTA are based on the event chain model. These models are suitable for accidents caused by failures of physical components and for simple systems, but suffer from serious deficiencies when they are applied to software-intensive, complex engineering systems [3]. In 2004, Leveson proposed a new model called System-Theoretic Accident Models and Process (STAMP) to explain accidents in a unique way. This model is based on control theory and a proposed method called Systems-Theoretic Process Analysis (STPA) [4]. It provides a good idea for solving problems experienced with traditional analytical theory, and has been widely used in the fields of aviation, nuclear power and energy exploitation. For complex safety-critical system such as FAO, the STPA method is undoubtedly the first choice for its safety analysis.

2 SCENARIO AND ARCHITECTURE OF FAO SYSTEM

2.1 System Description and Architecture

FAO is a fully automatic, highly centralized train operation and control system. It is a new generation of urban rail transit system based on modern technologies of computer, communication, control, and system integration to achieve the automated train operation.

The architecture of a General FAO system is shown in fig.1.The VOBC subsystem Calculates the Movement Authority (MA) and generates the correct signal for the rear train, based on the position of the front train, the status of the line obstacles, the interlock condition, and the speed limit of the train. The on-board equipment compares the running speed of the train with the information received in real-time. If the speed of the train exceeds the speed limit, the on-board equipment will automatically implement the common brake or emergency brake to ensure the train stops at a position of the safety. The train-ground information transmission system could adopt wireless communication, cross-ground induction loop, waveguide, or track circuit. To ensure safety, the train must accurately determine its position and direction, where the on-board computer, the speed meter/speed sensor/ accelerometer (for measuring distance, velocity and acceleration), and the trackside balise can be operated collaboratively to obtain the accurate position.

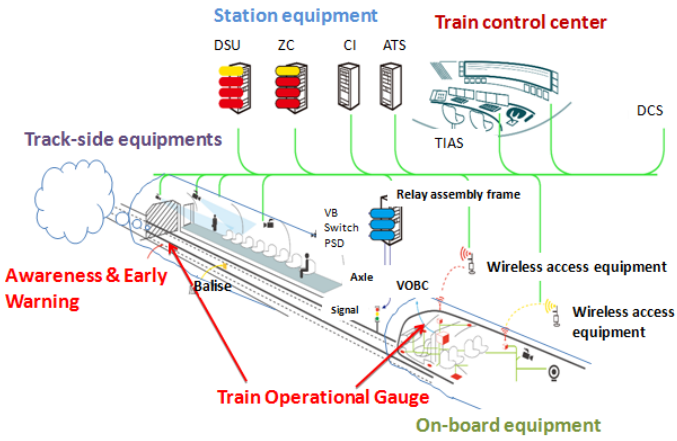

Figure 1 ：General FAO system architecture

2.2 Operational Scenario

There are 41 scenarios in a FAO system, including 18 normal scenarios and 23 abnormal scenarios as shown in fig.2. Based on the timetable, the system operates the train automatically into main line operation, and completing a series of functions such as:

Travelling between stations, accurate parking at stop, automatic door opening and closing, automatic departure from the station, automatic back into depot, automatic dormancy, and automatic car wash. The whole process of train operation is automatic, freeing the driver from a single repetitive operation and, further reducing the intensity of operational staff as well as reducing the impact of human factors on the operation. Thus, reducing accidents caused by human misoperation, improving system safety, operational capabilities, automation level and operation and maintenance functions.

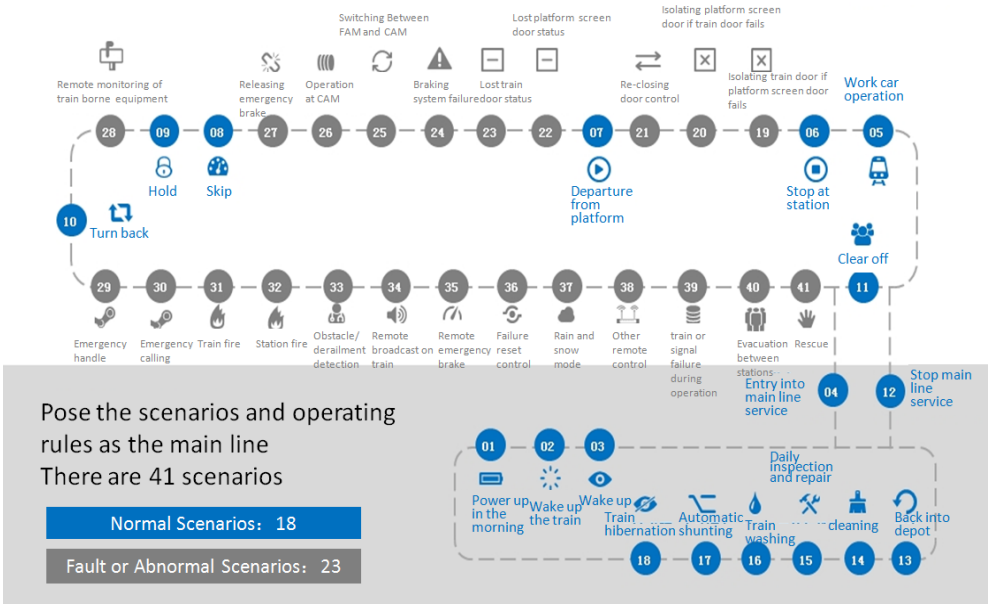

Figure 2 ：Schematic diagram of FAO scenarios

3 SAFETY ASSURANCE

3.1 STPA Analysis

The system may enter a dangerous state due to incorrect behaviour when interacting with other elements outside the system. Passengers are the main audiences of the FAO system, and when passengers are waiting, or arriving at a platform, they are at the interface of the station and the train subsystem. There is a lot of interaction between the train and the platform equipment at this time, so the possibility of exposure to a dangerous state is greatly increased. Fig. 3 shows the framework of safety analysis based STPA to FAO system.

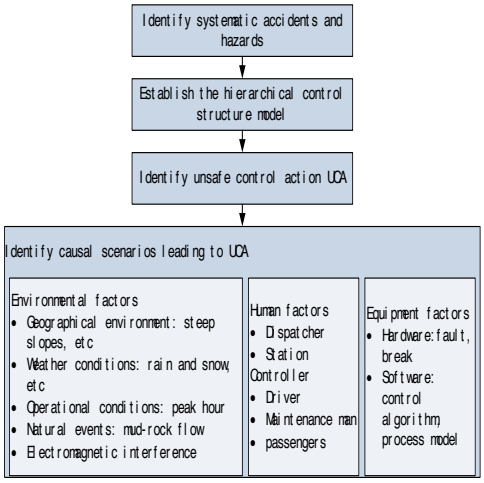

Figure 3 ：Safety analysis framework based on STPA

3.2 Optimized Causal Scenario Search Method

Unsafe control behavior (UCA) can be obtained based on the STPA method. In the search for the cause of the unsafe control behavior, it is obvious that the STPA method does not provide enough guidance. It relies on manual judgment and analysis, resulting in the arbitrariness of the generated cause scenario. It cannot guarantee the comprehensiveness and precision, hence the subsequent safety requirements are insufficient, which weakens the guiding significance of safety analysis. It still takes a lot of time and manpower, but it cannot get satisfactory analysis results.

In response to this defect, the generation part of the causal scenarios in the STPA method must be improved and optimized, relying on the powerful storage, calculation and processing capabilities of the computer. Embedding the advanced safety analysis method as the core algorithm, making the safety analysis process efficient, intelligent, more comprehensive and accurate. It is convenient to carry out the whole process safety management, improve the efficiency of safety analysis, reduce the manual workload, quickly generate the causal scenarios and safety requirements, and obtain the restricted conditions to prevent the occurrence of dangerous accidents.

The basic steps of the causal scenario search method based on the FAO system are described below:

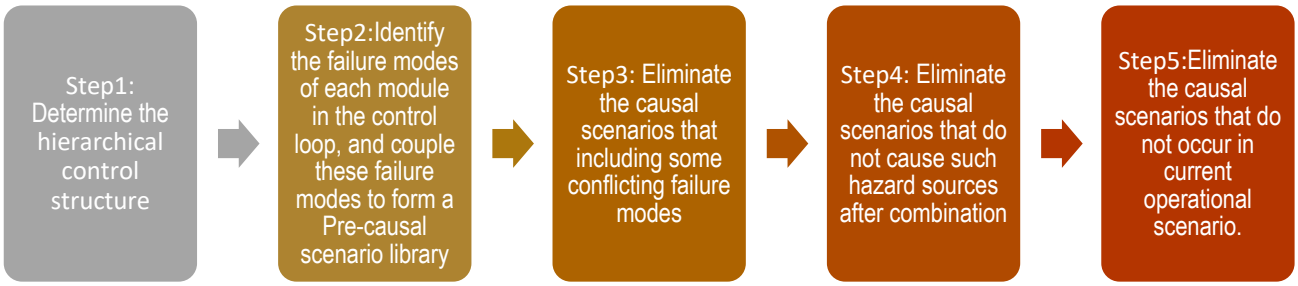

Figure 4 ：The basic steps of the causal scenario search method

Taking gated protection of the FAO system as an example, the causal scenario search method is used to generate the following causal scenarios.

Step1: Determine the hierarchical control structure

System hierarchical control structure is the basis of the STPA safety analysis. The hierarchical control structure of the gated protection is shown in Fig.5.

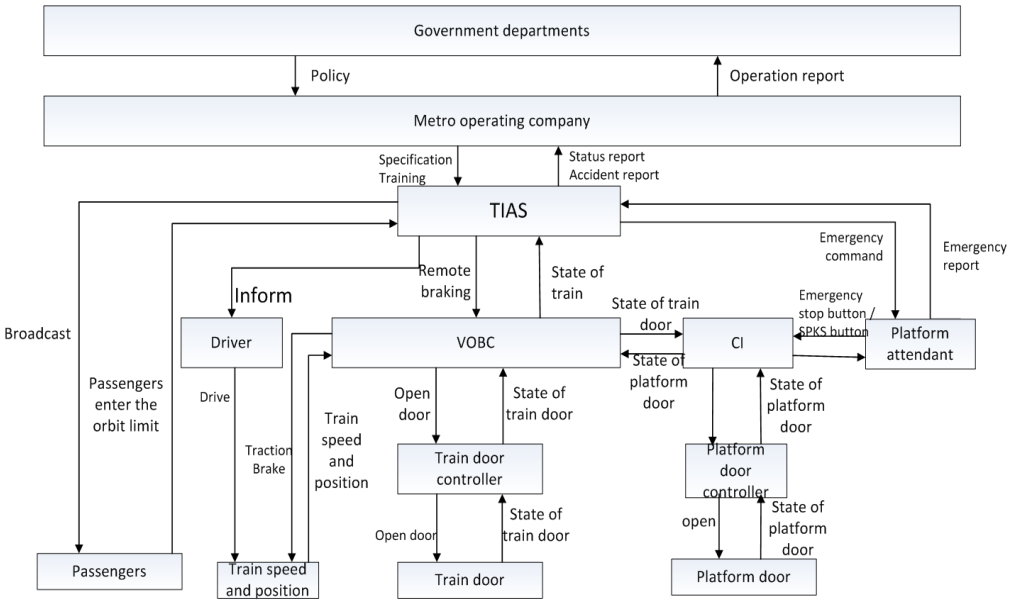

Figure 5：Hierarchical control structure of the gated protection

Step2: Identify the failure modes of each module in the control loop, and couple these failure modes to form a Pre-causal scenario library

Gated protection includes a speed measuring module, positioning module, VOBC computing fusion speed module, VOBC computing safety position module, VOBC issuing open door software implementation module, VOBC issuing departure command software implementation module, door state detection module, TCMS processing door closing Command module, TCMS transmission information module, etc. 22 kinds of fault modes can be found, and 4,194,304 kinds of pre-causal scenarios can be obtained by using simple combination algorithm according to equation (1). The value of n here is 22.

$$C_n^1 + C_n^2 + \cdots + C_n^{n-1} + C_n^n = 2^n - 1 \qquad (1)$$

Step3: Eliminate the causal scenarios that including some conflicting failure modes.

A software module can be used to reduce the pre-causal scenarios by eliminating scenario combinations, by checking that a condition is incorrect and that a condition cannot occur simultaneously. Algorithm 1 describes the screening process.

ALGORITHM 1: Conflict screening algorithm

Input: PCSL：A large number of precaution scenario libraries generated by simple combinatorial algorithm

Data： PCSs = Pre-causal scenarios, F1CS = Causal scenarios filtered through the first algorithm, SubMs = Safety related submodules during the process of control, RELAs = Correspondence between submodules and their failure modes， FM = failure mode of submodule.

Output: F1CSL: A causal scenario library generated by eliminating incapable fault patterns.

Description:

1. **Parse** PCSL into SubMs, RELAs, FMs, PCSs
2. **Extract all data:** PCSs, SubMs, RELAs, FMs ←PCSL
3. **For each** SubM **do**
4. **If** the sum of RELAs > =2,
5. **If** one FM of the RELA include “check”, others include “not check”

Delete the corresponding PCS that include all of them.
6. end for
7. Add F1CSL←PCSs
8. Return F1CSL

After the screening of algorithm 1, the above-mentioned causal scenarios containing both failure modes F5 and F6 are eliminated, and the remaining causal scenarios include 3,145,728 causal scenarios.

Step4: Eliminate the causal scenarios that do not cause hazard after combination.

It can be divided into two sub-steps:

1) Find the minimum coupling factor. Some modules have a single failure mode that can be dangerous, so all cause scenarios that are coupled to it can be eliminated. Similarly, the occurrence of two or more failure modes can be dangerous, eliminating all cause scenarios for higher level coupling.

2) Set multiple variables for each UCA and failure mode. For example, UCA3: When the train moves, the door opens. Train status: moving or zero speed stop; door status: open or closed or lost status. Emergency: Yes or No, etc. This step is to establish a correspondence between the UCA and the causal scenario.

Algorithm 2 describes the screening process for the causal scenario of UCA.

ALGORITHM 2: Hazard screening algorithm

Input: F1CSL：After a deleted cause scenario Library; UCA

Data：U Variables = Multiple variables for each UCA and fault mode set, **F**Variables = Multiple variables for each fault mode set, F1CS = Causal scenarios filtered through the first algorithm, F2CS = Causal scenarios filtered through the algorithm 2 ;FM = failure mode of submodule.

Output: F2CSL: After rejection, no duplication will lead to the cause scenario of a dangerous source.

Description:

1. **Parse** F1CSL into FMs, F1CS; UCA into Uvariables
2. **Extract all data:** FMs, F1CS ←F1CSL; Fvariables ←FMs ； Uvariables ←UCA
3. **For each** F1CS **do**
4. **If** all of the Uvariables of F1CS can be found in Fvariables
Add F2CSL←F1CS
5. end for
6. **For each** F2CS **do**
If the sum of FM=i
Delete the corresponding F2CS that sum of FM > i
7. end for
8. Return F2CSL

After screening through this step, 128 causal scenarios can be obtained for the gated protection.

Step5: Eliminate the causal scenarios that do not occur in current operational scenario.

First, safety protections should be extracted in the operational scenario. For example, in the “stop in the station” scenario, there is gate protection, and the “sleep” scenario does not require gate protection. However, even if there are door protection in different scenarios, the corresponding causal scenarios are different, such as emergency evacuation scenarios and normal inbound parking. The protection of the door during the outbound process and the protection of the doors at the platform need to be targeted to specific operations. Algorithm 3 describes the screening process.

ALGORITHM 3: Operation scenario screening algorithm

Input: F2CSL：The causal scenario library after two elimination; OS

Data： OS= operation scenarios, OCP= the control protection of operation scenarios, OVariable= the Characteristic variable of operation scenarios, FCP=the control protection of F2CS, FVariable= the

Characteristic variable of F2CS, F3CS = Causal scenarios filtered through the third algorithm
Output: F3CSL: The causal scenario library after three elimination
Description:
1. **Parse** F2CSL intoF2CS; OS into OCPs
2. **Extract all data:** F2CS←F2CSL; OCPs←OS; FCP←F2CS
3. **For each** F2CS **do**
4. **If** the FCP of F2CS can be found in OCPs
Add F3CSL←F2CS
5. end for
6. **For each** F3CS **do**
7. If the FVariablecan not be found in OVariable,
Delete the corresponding F3CS that include the FVariable
8. end for
9. Return F3CSL

For the operation scenarios corresponding to the train door protection, there are mainly inbound parking, platform departure, emergency evacuation, etc. There are 128 causal scenarios corresponding to the operational scenario-stop at station. Part of the remaining causal scenarios after screening based on the algorithm is shown in Fig.6.

No.	致因场景编号	致因场景序列描述 The remaining causal scenarios after screening
	CS1	场景6-进站停车→MA由站台撤回→输入到ATP的MA有误→ATP发送了错误的 EBI→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS2	场景6-进站停车→MA由站台撤回→ATP的EBI计算控制算法未对MA实施有效控制→ATP发送了错误的 EBI→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS3	场景6-进站停车→MA由站台撤回→ATP发送了正确的 EBI→ATO到牵引制动模块的传输有误→EBI被错误执行→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS4	场景6-进站停车→MA由站台撤回→ATP发送了正确的 EBI→ATO的自动驾驶执行算法缺陷→EBI被错误执行→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS5	场景6-进站停车→MA由站台撤回→ATP发送了正确的 EBI→ATO硬件故障→EBI被错误执行→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS6	场景6-进站停车→MA由站台撤回→ATP发送了正确的 EBI→ATP到ATO的传输有误→EBI被错误执行→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS7	场景6-进站停车→MA由站台撤回→ATP发送了正确的 EBI→牵引制动模块硬件故障→EBI被错误执行→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS8	场景6-进站停车→MA由站台撤回→ATP发送了正确的 EBI→司机对车辆发出了与ATP冲突的控制→事故1-列车与前车相撞,事故11-列车与轨面障碍物相撞脱轨.
	CS9	场景6-进站停车→反馈的列车位置偏离实际值过大→BTM到ATP的列车位置1反馈传输有误→输入到ATP的列车位置有误→ATP错误发送EBI命令→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS10	场景6-进站停车→反馈的列车位置偏离实际值过大→BTM的 位置报文反馈算法缺陷，对列车位置的反馈有误→输入到ATP的列车位置有误→ATP错误发送EBI命令→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS11	场景6-进站停车→反馈的列车位置偏离实际值过大→BTM硬件故障，对列车位置的反馈有误→输入到ATP的列车位置有误→ATP错误发送 EBI→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS12	场景6-进站停车→反馈的列车位置偏离实际值过大→ATP的EBI计算控制算法未对列车位置实施有效控制→ATP发送了错误的 EBI→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS13	场景6-进站停车→反馈的列车位置偏离实际值过大→ATP发送了正确的 EBI→ATO到牵引制动模块的传输有误→EBI被错误执行→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS14	场景6-进站停车→反馈的列车位置偏离实际值过大→ATP发送了正确的 EBI→ATO的自动驾驶执行算法缺陷→EBI被错误执行→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS15	场景6-进站停车→反馈的列车位置偏离实际值过大→ATP发送了正确的 EBI→ATO硬件故障→EBI被错误执行→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS16	场景6-进站停车→反馈的列车位置偏离实际值过大→ATP发送了正确的 EBI→ATP到ATO的传输有误→EBI被错误执行→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS17	场景6-进站停车→反馈的列车位置偏离实际值过大→ATP发送了正确的 EBI→牵引制动模块硬件故障→EBI被错误执行→事故1-列车与前车相撞,事故3-列车超速脱轨.
	CS18	场景6-进站停车→反馈的列车位置偏离实际值过大→ATP发送了正确的 EBI→司机对车辆发出了与ATP冲突的控制→事故1-列车与前车相撞,事故3-列车超速脱轨.

Figure 6 ：Analysis of the results of the new method

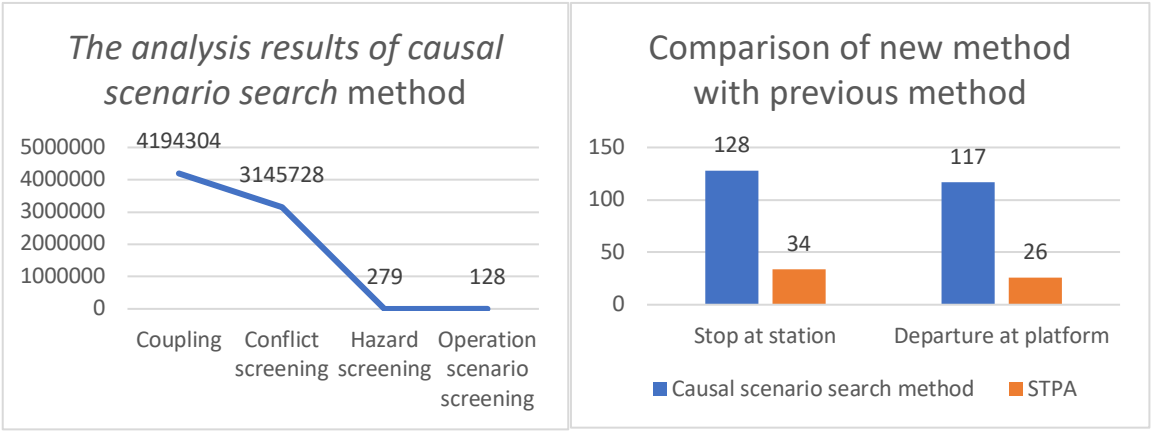

Figure 7 ：Analysis of the results of the new method

The results of the analysis based on the new method are shown in Fig.7. Obviously, using the causal scenario search method compared with the previous STPA method can obtain more comprehensive and specific analysis results, which is helpful to propose targeted design suggestions to improve the safety of the FAO system. We will continue to improve the algorithm in the future.

3.3 Multi-level, Full Coverage of Testing, Verification and Validation System

Based on the filtered causal scenarios and safety requirements of the previous section of safety analysis, the subsequent tests are arranged. All subsystems of a FAO system must undergo rigorous hardware and software integration testing and system-level testing, integrate the various subsystems into a FAO system and ensure that the entire fully automatic system complies with all safety requirements set by the system through further testing, verification and validation of the overall system.

1)Features of FAO system

The FAO system is a giant, complex, high-safety (SIL4 and SIL2) system that takes driving as the core and integrates the sub-system of signals, vehicles, integrated monitoring and communication. The FAO system has systematic, networked and informational characteristics. The FAO system operates in a complex environment and is powerful, the difficulty of testing and verification is much greater than the general FAO application, and the complexity is much larger than the general safety-critical system.

2)Testing, verification and validation system

Based on the standards of EN50126 [5], EN50128 [6] and EN50129 [7], the access, exact conditions and the qualifications for each stage should be strictly defined to build a multi-level and comprehensive testing system.

Considering the characteristics of the FAO system, to ensure the completeness and effectiveness of the testing process industry-standard test and verification systems will be used.

3)Multi-level testing

To ensure the availability, reliability and safety of a fully automatic operating system, extensive testing, verification and validation activities are required

Modular testing is mainly for software / hardware specification implementation verification. Considering that an FAO system is a safety-critical product, a series of modular testing is required to find and solve the defects in the implementation process in software and hardware.

Before the FAO products are applied on certain rail transit lines, it is necessary to carry out multi-level and repetitive field tests in combination with other system features such as the characteristics of line layout, vehicle characteristics and communication system. This will ensure that all the risks are controlled to a level of the owner through the multiple verification testing process including the indoor test, on-site commissioning, on-site commissioning of moving cars, on-site multi-car debugging, on-site running test according to the timetable and so on. Fig. 8 describes the requirements of the life cycle test process.

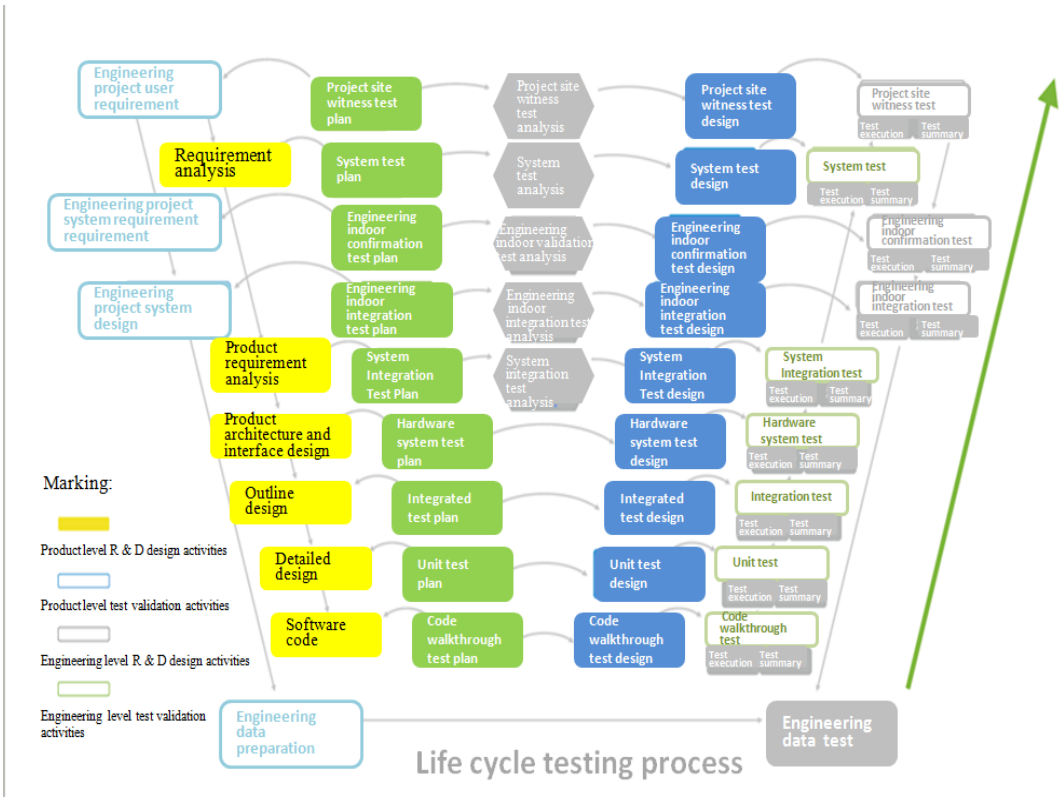

Figure 8 ： Requirements of the life cycle test process

4 CONCLUSION

In the process of shifting from manual driving to full automation, the degree of automation of the train control system is increased, and more unknown risks are introduced. This paper shows the treatment strategy and safety assurance measures for the uncertainty of a FAO system, so as to improve safety of the rail transit system.

An optimized causal scenarios search method based on the STPA method was used to analyze the safety of a scenario of an FAO system. The analysis results proved the feasibility and superiority of the optimized method in the fully automatic system to give more guidance to analysts and reduce manual work pressure. For each operational scenario, it can identify its specific causal scenario and propose more targeted measures. In addition, the safety assurance process also includes comprehensive testing, verification, and validation. These activities are aimed at ensuring that FAO systems provide safer and more secure services than existing CBTC systems.

As the first FAO line with complete independent intellectual property rights, Yanfang Line has been operating stably and efficiently for more than 441 days since its opening. The data shows that the average commitment rate of Yanfang Line is 99.998%, and the average punctuality rate is 99.995%. Through the assessment of the Municipal Transportation Commission, the results of Yanfang Line are all "excellent", which fully reflects the safe, efficient, stable and reliable automatic operation system of Yanfang Line. We believe that through the rigorous safety analysis, comprehensive safety management and multi-phase verification proposed in this paper, the FAO system can provide safer, more efficient and more energy-efficient solutions for urban rail transit systems worldwide.

ACKNOWLEDGEMENTS

The research presented in this paper has been supported by Beijing Natural Science Foundation (L181006), Beijing Laboratory of Urban Rail Transit and Beijing Higher Institution Engineering Research Center of Urban Rail Transit CBTC System.

5 REFERENCES

[1] IEC 60812, Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA), 2nd ed., 2001

[2] Camdzic, S., & Products, A. (2006). Fault Tree Analysis (FTA). Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis. John Wiley & Sons, Inc.

[3] Min, O., Liu, H., Yu, M. H., & Qi, F. (2010). Stamp-based analysis on the railway accident and accident spreading: taking the china-jiaoji railway accident for example. Safety Science, 48(5), 544-555.

[4] Leveson, N. (2012). STPA: A New Hazard Analysis Technique. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.

[5] CENLEC. EN50126:Railway Applications-the Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)[S]. 2002.

[6] CENLEC. EN-50128-2001,Railway applications-Communications. signalling and processing systems-Software for railway control and protection systems[S]. 2001.

[7] CENLEC. EN-50129—1999. Railway Applications：safety related electronic systems for signalling [S]. 1999