Research on simulation demonstration of urban rail transportation based on cloud platform architecture

Bin Chen[a,b*], Shusong Yang[a], Renxing Yao[a], Ruidong Luo[b]
[a] Ningbo Rail Transit Group Co., Ltd., Ningbo 315040, Zhejiang, China; [b] School of Civil and Transportation Engineering, Ningbo University of Technology, Ningbo 315211, Zhejiang, China

ABSTRACT

Based on the simulation demonstration of Urban Rail Transit under the framework of cloud platform, by collecting the front-end data of rail transit, the simulation test platform framework is built according to the five levels of trackside, vehicle, station and central test environment, and various operation scenarios of full auto drive system are simulated. The simulation system realizes the integration of the full automatic driving operation control simulation test system, and supports the test research of the full automatic driving operation control minimum system. The simulation of the cloud platform will play a positive role in the further development of the future rail transit operation mode in the direction of intelligence, network and collaboration.

Keywords: Auto drive system, urban rail transit, cloud platform architecture

1. INTRODUCTION

With the development of national economy, the process of urbanization in China is greatly accelerated, the urban population is expanding rapidly, and the urbanization such as traffic congestion and air pollution is becoming more and more serious. Because urban rail transit has the advantages of safety, punctuality, large passenger volume and no pollution, it has become the best way to solve traffic congestion and air pollution in big cities. With the deep integration of informatization and rail transit automation[1], rail transit automation and control network is also developing rapidly in the direction of distributed and intelligent. More and more communication protocols and interfaces based on TCP/IP are adopted, so as to realize the consistent identification, communication and control from the management information layer to the field equipment. However, while the rail transit system is becoming more and more open, it also weakens the isolation and security protection between its control system and the outside world. More and more viruses and Trojans continue to spread to the control network, and the potential safety problems of the rail transit control system are becoming more and more serious.

In recent years, intelligent urban rail integrated automation system characterized by driverless technology, cloud computing platform and big data application, digitization of vehicle and signal light equipment, integration of Transportation Command and dispatching system and information system has become the mainstream development trend of urban rail[2]. With the help of relevant contents of cloud computing and cloud storage, data related to dispatching can be managed cooperatively[3-8]. The application of these technologies puts forward higher requirements for the information security of urban rail integrated automation products[9-12].

In view of the problems encountered in the current rail transit field, this paper, based on the simulation demonstration of the cloud computing platform architecture, has greatly reduced the equipment capital investment and operation and maintenance cost by simulating the application in the rail transit integrated automation industrial control system. This research has improved the intelligent level of operation dispatching and equipment maintenance management, enhanced the information sharing and interconnection between rail transit industrial control subsystems, improved the handling capacity in case of disaster and abnormal emergency, and improved the quality of passenger service.

2. FRAMEWORK DESIGN SCHEME OF RAIL TRANSIT SYSTEM

The system function test platform adopts the cloud computing platform architecture to build a rail transit automation system

[*] chenbin.nb@163.com

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 1250661
© 2022 SPIE · 0277-786X · doi: 10.1117/12.2662718

that meets the requirements of full-automatic driverless, and forms a complete test environment through software simulation or real electromechanical and signal equipment. Figure 1 shows the minimum system architecture based on cloud computing platform.

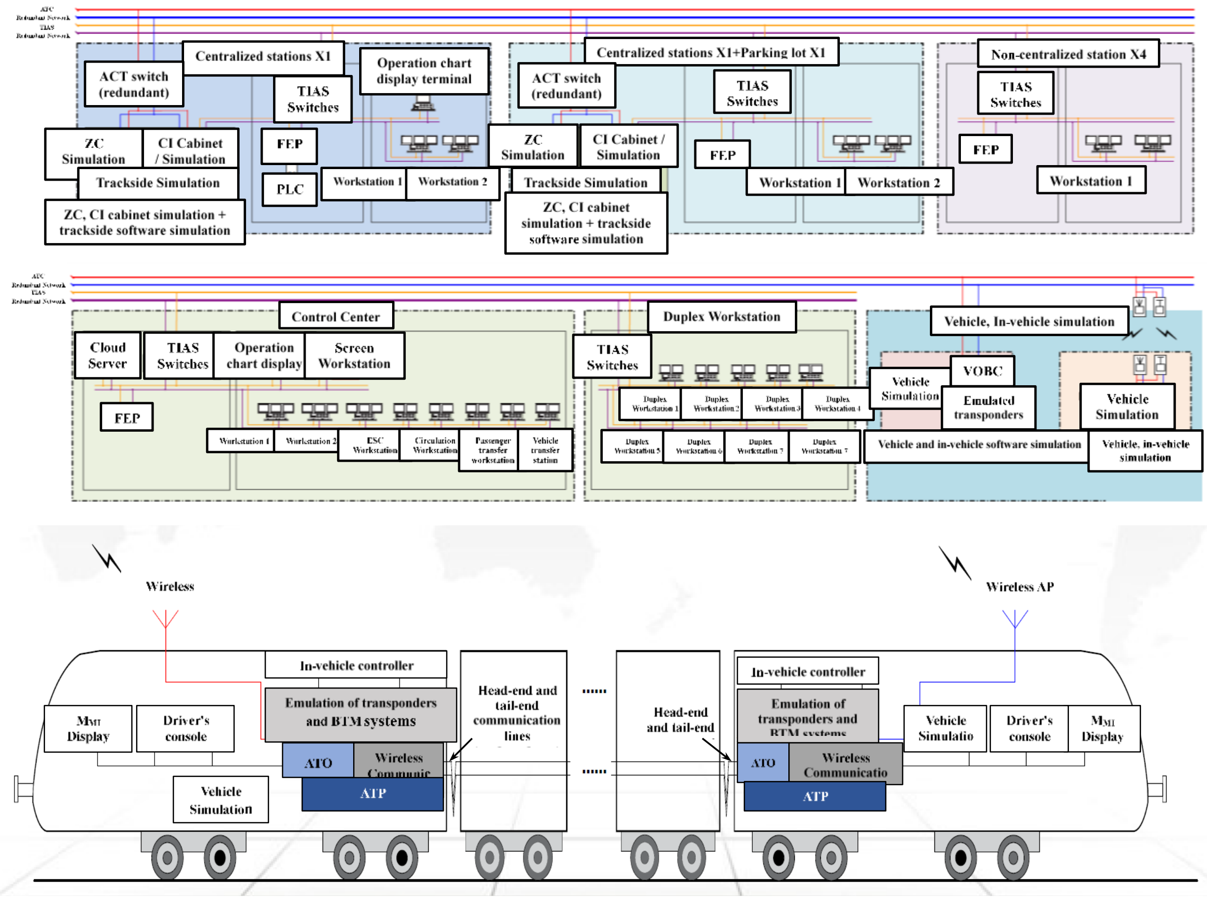

Figure 1. Minimum system architecture.

Information security function test tools include: algorithm and randomness tester, industrial security audit test tool (asics-am), industrial control simulation attack test tool, industrial security audit test tool (das-log), industrial control and other security 2.0 audit test toolbox, PLC simulation attack and security test toolbox The simulation attack and security monitoring tool set (including: industrial information security monitoring integrated machine, database detection tool and unauthorized access attack tool) is shown in Figure 2.

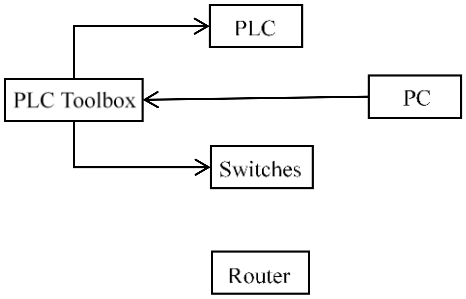

Figure 2. PLC simulation attack security detection toolbox.

The system function test platform adopts the cloud computing platform architecture to build a rail transit automation system that meets the requirements of full-automatic driverless, and forms a complete test environment through software simulation or real electromechanical and signal equipment; as shown in Figure 3.

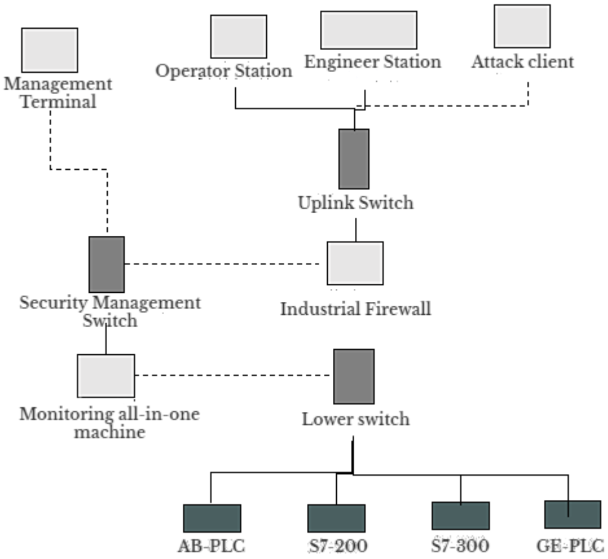

Figure 3. Interface diagram of industrial information security detection integrated machine.

3. DESIGN OF SIMULATION DEMONSTRATION PLATFORM BASED ON CLOUD COMPUTING

The simulation demonstration platform is built according to the standard of rail transit automation industrial control system based on cloud computing platform architecture and supporting full-automatic driverless. The semi physical method is adopted to simulate the working process of urban rail transit communication, signal, integrated monitoring, vehicle and other disciplines in the fully automatic driverless mode. It is capable of testing the cooperative working process of various systems under the full automatic driving mode, including normal scenarios such as morning power on, train wake-up, sleep, inbound parking, platform departure, turn back and end change, passenger clearance, as well as abnormal scenarios such as platform fire, door failure and interval evacuation. The simulation demonstration platform environment is shown in Figure 4.

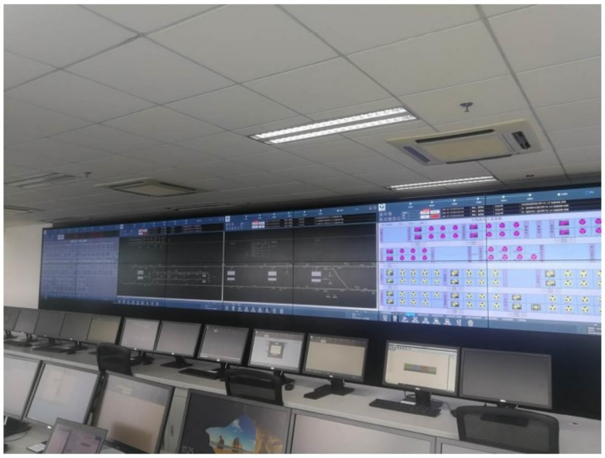

Figure 4. Rail transit fully automatic operation network system.

4. INFORMATION SECURITY RISK ASSESSMENT OF INDUSTRIAL CONTROL SYSTEM

There are three main types of information security risk assessment methods for industrial control system, namely empirical analysis method, qualitative analysis method and quantitative analysis method[8]. The empirical analysis method is applicable to the evaluators with insufficient evaluation experience, and the experienced experts formulate the safety baseline for the evaluators to use for reference; Quantitative analysis method is to assign value to risk elements when measuring risk, and then quantify the evaluation results; The qualitative analysis method is to classify the risk elements, which can be generally divided into three levels: “high, medium and low”, and finally express the evaluation results by level. Based on analytic hierarchy process, this paper combines quantitative analysis and qualitative analysis to evaluate the information security risk of industrial control system.

4.1 Information security risk assessment model

Referring to the implementation guide for risk assessment of information security technology industrial control system and the application guide for security control of information security technology industrial control system, the information security risk assessment of industrial control system is carried out from the four aspects of assets, vulnerability, threats and security measures. The evaluation model is shown in Figure 5, with the target layer, criterion layer and factor layer from top to bottom[13].

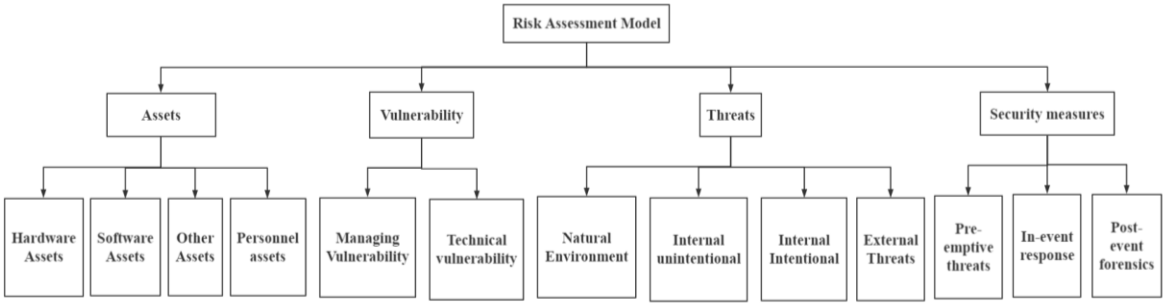

Figure 5. Rail transit fully automatic operation network system.

From top to bottom, there are target layer, criterion layer and factor layer[14]. The target layer is the main body of the industrial control system. The criterion layer includes assets, vulnerability, threats and security measures. The factor layer includes hardware assets, software assets, personnel assets, other assets, management vulnerability, technical vulnerability, natural environment, internal unintentional risk, internal intentional risk, external threats, pre defense, in-process response and post evidence[15].

The hardware assets include: IED, PLC, DCS and other industrial field control layer equipment; Router, gateway, switch and other network equipment; Industrial firewall, intrusion detection system, network gate and other security equipment; Server, workstation, HMI and other computer equipment; Disk array, mobile hard disk and other storage devices.

Software assets include: database system, operating system and other system software; Remote control software, OPC software, application software, etc.; Industrial control code, field equipment firmware and other source programs; Industrial production data, industrial control real-time data, operation management data.

Management vulnerability includes industrial production environment vulnerability and production equipment vulnerability. Technical vulnerability includes: industrial control network boundary vulnerability, industrial control system network equipment vulnerability, industrial control system network communication vulnerability, industrial wireless network vulnerability, industrial control system hardware vulnerability, software vulnerability and configuration vulnerability.

Natural environment includes static electricity, dust, humidity, electromagnetic interference, accidents and other environmental hazards or natural disasters. Internal unintentional risks include: internal employees do not follow rules and regulations and operating procedures, resulting in industrial control system failure or attack. Internal intentional risks include: internal employees destroy the industrial control system or steal system information. External threats include: external personnel attack the industrial control system.

4.2 System platform test

The prototype system of urban rail transit full-automatic driverless integrated automation industrial control system based on cloud computing platform meets all the specific functions and performance indicators to be realized, and has passed the test of China Software Evaluation Center, an independent third-party testing organization with CNAS qualification. All the evaluation indicators have successfully passed the test of China software evaluation center, test report is shown below:

Relying on the project "improvement of core technical capability of industrial control system in rail transit industry", the information security research center of China Institute of electronic technology standardization has launched the information security research center from August 10, 2020 to September 18, 2020. According to the safety function indicators in the project implementation plan of "improvement of core technical capability of industrial control system in rail transit industry", the safety function test was conducted on the core products of Hollysys industrial control system in the project of "improvement of core technical capability of industrial control system in rail transit industry".

The test basis includes the implementation scheme of "improvement of core technical capability of industrial control system in rail transit industry" and some safety function requirements in the national standard "information security technology programmable logic controller safety technical requirements and test evaluation method" (Draft for approval).

The test results show that the system basically meets the safety function index requirements involved in the implementation scheme of "improvement of core technical capability of industrial control system in rail transit industry" and the national standard "information security technology programmable logic controller safety technical requirements and test evaluation methods" (Draft for approval).

5. CONCLUSION

Based on the simulation of cloud platform, this study simulates and evaluates the possible risks in the operation of rail transit through the information security risk assessment model, and puts forward preventive measures for the more likely risks. Bring potential social benefits to passengers and operating companies, improve the safe operation and punctual benefits of trains, and ensure the safety of passengers' personal and property. Fully master the relevant technologies of rail transit integrated automation industrial control system, form an independent technical system, and reach the international advanced level in the field of rail transit automatic driving technology; further improve the automation level of urban rail transit system equipment.

REFERENCES

[1] Liu, D. D., "Application of internet monitoring platform in subway construction safety management," Electronic Technology, 50(9), 28-29(2021).

[2] Wei, Y. X., Li, J. X. and Huang, J. R., "Data security analysis and countermeasures in cloud computing environment," Network Security and Informatization, 66(10), 19-21(2021).

[3] Jiang, M. Y., "Design and optimization of big data triage system under cloud computing platform," Modern Electronics Technology, 39(2), 28-32(2016).

[4] Wang, X. and Zhou, X. M., "Research and simulation of rational triage technology for big data in cloud computing environment," Computer Simulation, 33(3), 292-295(2016).

[5] Wang, F., "Research on the design of big data intelligent operation and maintenance system based on cloud computing," Engineering Technology: Full Text Edition, (3), 44(2017).

[6] He, J., "Research on enterprise crisis management system under big data based on cloud computing technology," Science and Technology Management Research, 319(21), 159-164(2014).

[7] Li, X. F., "Research on big data processing system based on cloud computing technology," Journal of Changchun College of Engineering: Natural Science Edition, 15(1), 116-118(2014).

[8] Meng, C. and Yang, H. P., "Research on big data audit system based on cloud computing service platform," Cooperative Economy and Technology, 4, 170-171(2017).

[9] Jiang, Z., [Research on Cooperative Data Streaming Joint Channel Inquiring Based on Mobile Cloud Computing], Nanjing University of Posts and Telecommunications, Nanjing, (2017).

[10] Gong, L., "Research on security testing and evaluation system and key technologies for cloud computing platform," Information Communication, 162(6), 144-146(2016).

[11] Xie, Y., "Research on the design of big data triage system under cloud computing platform," Electronic Design Engineering, 27(9), 119-122(2019).

[12] Luo, Y., “Design of network operation management system based on cloud computing platform,” Internet Weekly, 757(7), 50-52(2022).

[13] An, K. W. and Zhao, S. H., “Information security risk assessment for the assurance of two integration,” Journal of Xi’an University of Posts and Telecommunications, 15(6) 62-63(2010).

[14] Si, Y. S., [Research on Information Security Risk Assessment Technology], Guizhou University, (2008).

[15] Xiong, Q. and Peng, Y., “Security risk assessment of industrial control systems,” China Information Security, (3), 57-59(2012).