A Safety Management and Signaling System Integration Method for Communication-Based Train Control System

Fei Yan¹ · Chunhai Gao² · Tao Tang³ · Yao Zhou⁴

Received: 25 September 2016/Revised: 7 February 2017/Accepted: 18 February 2017/Published online: 2 March 2017
© The Author(s) 2017. This article is published with open access at Springerlink.com

Abstract The safety and the correctness of signaling system not only relate to the safety and efficiency of the rail transit operation, but also link with the life safety of passengers. In order to guarantee the safety of a signaling system for metro, the safety certificate for the trial operation with carrying passengers must be obtained. In this paper, a suitable safety management and signaling system integration model are explored according to the CENELEC standards and applied in China. With taking account of the strict safety requirements for the Communication-Based Train Control (CBTC) system, a safety assurance and assessment method based on safety verification and validation process was put forward. This method was applied in every phase of the CBTC system development life cycle to monitor and control each activity in the life cycle and to review each document in system development process. At the same time, this method is also used to ensure the traceability of relevant documents and to test all the functions of the whole system sufficiently and completely. So that the safety operation of train control system can be ensured. Up to now, the independently developed CBTC

system with the safety management had been applied in many urban rail transit lines of Beijing, such as Yizhuang Line, Changping Line, Line No. 14, and Line No. 7. The CBTC signaling systems of these projects have been authorized by the safety certification from a third party, e.g., Lloyd Register which is a British company and famous for the safety verification and validation process.

Keywords Rail transit system · CBTC · Safety management · Signaling system · Safety verification and validation · System safety assurance

1 Introduction

While technology is changing faster than the engineering techniques to cope with the new technology are being created, software is pervasive in our society: Its scope is widening more and more in many critical domains such as avionics, space, railway, automotive, nuclear, medical, and air traffic control. As a consequence, it is of utmost importance to assure the society at large that deployment of a given software-intensive system does not contribute to pose an unacceptable risk of harm. For metro system, communication-based control system now has been widely used in new building metro lines. And most of operational functions are realized by software.

Lessons learned over centuries about designing to prevent accidents may be lost or become ineffective when older technologies are replaced with new ones. Digital technology has created a quiet revolution in most fields of engineering, but system engineering and system safety engineering techniques have not kept pace. Digital systems introduce new failure modes that are changing the nature of accidents.

✉ Fei Yan
fyan@bjtu.edu.cn

¹ National Engineering Research Center for Rail Traffic Operation and Control, Beijing, China

² Beijing Traffic Control Technology Co., Ltd., Beijing, China

³ State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China

⁴ School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China

Editors: Jiaqi Ma, Yihui Wang, Xiaolu Rao, Shane Wu and Alireza Khani

Traditional methods in safety engineering therefore struggle to keep up with the development of new technologies and usages of the same. The main drawback of such methods is that they are founded on an assumption of a certain degree of predictability and decomposability. These approaches have lately been labeled “Safety I.” New concepts, such as resilience engineering, have gained attention. A common foundation for these concepts is that they all focus on adaptive capacity to stay in control when facing unforeseen disturbances or events, labeled “Safety II.”

With the rapid development of urban rail transit systems, it is urgent to develop high-performance train control system with high safety, high reliability, and high efficiency to ensure the safety of train operations. The Communication-Based Train Control (CBTC) system is the trend for the most advanced train control system all over the world.

Compared to the traditional train control system based on track circuits, the CBTC system has the following characteristics: (1) the CBTC system could supply much larger capacity to support the continuous bidirectional train–ground communication; (2) the safety computers platform has been used in both the ground equipment and the on-board equipment to handle train status and control commands, to realize the continuous interval control, route control, speed protection, and automatic driving; (3) the train position can be achieved with high precision; (4) the number of the cables, train control equipment, and first-stage costs, and operational and maintenance cost could be reduced; (5) the CBTC information can be superimposed on the existing signaling system to facilitate the transformation of the existing line and to enable the interconnection of urban rail transit lines.

The CBTC system consists of ground zone controllers (ZC), the on-board equipment, the bidirectional train–

ground information transmission system, and the train positioning system (as shown in Fig. 1). In particular, ZC, the core of the CBTC system, calculates the movement authority (MA) 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 MA received in real time. If the speed of the train exceeds the speed limit in the MA, the on-board equipment will automatically implement the common brake or emergency brake to ensure the train stops in front of the safety point. The train–ground information transmission system could adopt wireless communication, cross-ground induction loop, waveguide, or other media to achieve the bidirectional communication. 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 [1].

Beijing Jiaotong University set up an independent innovation project to carry out the research about the CBTC core technology and key equipment by the way of Industry–University Research (IUR) proposed by the Chinese government. The demonstration of the independent innovation CBTC project was carried on the Beijing Yizhuang Line, which was formally approved and started its operation on December 30, 2010. [2].

By referring to the advanced safety standards from other countries and the actual situations of domestic rail transit engineering in China, the safety management and certification activities have been designed special for rail transit project in China and carried out and tested in practice.

Mature safety management concepts of the rail transit were formed in electronic and electrical standard IEC61508 [3], aviation industry standard ARP4761 [4], and the related European railway signal standards CENELEC [5–7]. According to these standards, British railway safety and standards board (RSSB) built the safety risk model (SRM) based on the accumulated data of railway operation for decades to evaluate the safety state of railway operation and to provide guidance [8]. The European commission proposed the SAMRail [9] and SAMNET [10] projects, which aimed at railway risk management promotion in 2002 and 2003. These projects have unified the railway safety operation strategy and established general safety targets and indicators and finally formed the railway operation safety performance indicators and safety target allocation methods [11], based on the common safety target, the common safety indicator, and the common safety method.

Fig. 1 CBTC system structure

2 Challenges in Innovation of CBTC Systems

CBTC system is a kind of train control system which adopts advanced communication and computer technologies to continuously control and monitor the operation of trains. CBTC systems were independently studied and developed by Siemens, Alstom and Thales according to the development process of the safety-critical control system.

In China, we started to study CBTC in 1995 and have experienced more than 20 years' development since the beginning of 1995. The CBTC system consists of the control, communication, network, integration, transportation organization, material technology, and other multidisciplinary integrated system technologies. All related research works were carried out in accordance with the requirements of the whole life cycle.

The structure diagram of the CBTC system developed by us is shown in Fig. 2. The data transmission between trackside equipment and on-board equipment is achieved by the data communication network. In addition, the CBTC on-board equipment controls the operation of trains and the CBTC trackside equipment sends data to the ATS system, which supervises and controls the train through the interlocking systems.

The real-time two-way communication between on-board equipment and wayside equipment is the cores of the CBTC system, which can provide a large amount of information transmission with fast transmission speed to achieve moving automatic block easily. So the expansion of information utilization and function in CBTC system can greatly improve the ability of the interval and the capacity of the tracks. The flexible organization of two-way

operation and one-way continuous operation reduces the number of wayside equipment, which makes the CBTC system easy to install and maintain. Moreover, it is also easy for the CBTC system to adapt to different speeds, different traffics, and different types of traction train operation control, etc. Wireless communication methods are mainly divided into wireless AP transmission mode, waveguide transmission mode, and leaky cable transmission mode as well as inductive loop mode.

2.1 Complexity of the CBTC System

To solve the technical problems of the CBTC system in principle is not equal to achieve the feasibility; there is a long distance between reliability and safety in engineering. Rail transit CBTC signaling technology's research and development, engineering and industrialization is a typical complex system. As an intelligent complex safety control system, CBTC systems are required to realize a safe and reliable operation in different weather conditions along the whole life cycle, as well as to achieve the collaborative control (among human, trains, and railroad) with complex multivariate parameters characteristics.

Urban rail transit operations are affected by the weather and the passenger flow, and in such situation we need to ensure a continuously safe and efficient operation for 30 years. Even when there is rain/snow or trains are overloaded, e.g., 150%, the CBTC system must provide safe and reliable services. The CBTC system is a complex safety critical system with perfect function and clear hierarchy according to the CENELEC international safety standards. The SIL4 level train control equipment must adopt the risk-control development method and the fault-tolerance redundancy computer platform in the whole life cycle. Hence, the traditional R & D methods and safety analysis theory are facing difficulties to ensure the safe operation of the CBTC system.

The failure propagation model based on the complex scenarios of train operation and the system design and development method that covers the whole life cycle is significant for the system safety requirements. The safety management system and the integrated research and development platform should be set up to meet CENELEC standards of the highest safety integrity level SIL4. Furthermore, the train and ground two signal dedicated, portable safety computer platform, and CBTC complete set of technical equipment should be developed. Moreover, the mechanism and evolution law of the hazard causations (accident causes) and the establishment of the hazard log and safety integrity level requirements can eventually control the system risk within acceptable limits.

Fig. 2 CBTC system structure diagram

2.2 Distributed and Collaborative Control of the CBTC System

The equipment of the CBTC system is distributed in the train, trackside, station, and control center. Those devices are connected by many different types of fiber optic cable and have numerous interfaces. For example, to equip 1-km track route, there are dozens of kilometers fiber optic cable laying, thousands of connection points and nearly ten thousands components. The failure of any component will affect the stability of the CBTC system since it is required to have high reliability.

The CBTC system relies on wireless communication technology to achieve train–ground communication, which could use wireless LAN technology based on ISM band. There are some problems in this technology, such as vulnerable to interference and the frequent handoff because the wireless transmission environment consists of the underground tunnel and the ground section in urban rail transit systems. So the single transmission mode is difficult to meet the high reliability requirements for the CBTC train–ground communication.

Since the doors open automatically, the safety protection of passengers is an important requirement for the CBTC systems. In addition, the CBTC system is also closely related to the operations staff; for example, dispatchers need to use the ATS equipment, and drivers need to use ATP/ATO equipment. Therefore, CBTC system is very important to improve the service quality of the operation.

2.3 Multivariate Parameters Adjustment

Moving block signaling system can achieve a larger line capacity when compared with the fixed block signaling system because a train can be allowed to move to the tail of the front train with a certain safety distance. The CBTC system with moving block could secure safe, fast, reliable, punctual, comfort, and energy-efficient operation of trains.

The objectives for the operation of trains are contradicted with each other, such as the safety and the fastness. For passengers, they want trains to run as fast as possible; however, the speed of trains is limited by the signaling systems, train characteristics, etc., to ensure the safety. So the CBTC systems need to find a trade-off between these objectives to achieve the maximum capacity allocation.

Compared with the traditional signaling system, the control precision of the CBTC system is greatly improved. For example, the train positioning error can be limited within centimeter level. The parking control precision of a train with hundreds of tons can be less than 30 cm. The solution of each problem requires careful theoretical deduction and a large number of field tests. Besides, the location of the train needs to be sent to ZC by wireless

communication to generate MA. The delay of wireless communication impacts the correctness and precise position of the train because the train always moves forward. When ZC calculates the MA for next train, it needs to consider the delay.

3 Processes of Safety Management and System Integration for CBTC

In order to deal with the challenge of CBTC system development, we try to find best practice in the world. As we know, the biggest safety challenge of CBTC System is that system safety cannot be simply achieved by testing and need to take safety management measures to deal with the human errors and software failures. And the systematic features of CBTC system need a proper integration method along its product life cycle. The safety management system during the railway development, construction, operation, maintenance is the effective way to conduct the risk control and set up the implementation framework of railway safety management.

European EN series standards are important guideline in the railway industry, but simply apply the method described in it cannot solve the management and technical problem encountered in our project process. In the practice, we summarized our own methodology.

3.1 European Safety Standards and Principles

SC9XA Committee of the European electrification Standards Committee (CENELEC) established a set of standards which includes IEC62278, IEC 62279, IEC 62280 and IEC 62425 (as shown in Fig. 3) for rail transit train control system based on computer control [12, 13]. Because these standards have strong pertinence and better practicality, they have been promoted in many countries and been adopted by the IEC Committee as an international standard.

IEC62278 (EN 50126) defines the reliability, availability, maintainability, and safety (RAMS) for rail transit train control system and the relationships among them. In

Fig. 3 International safety standards for rail transit

addition, it also standardizes the credibility system's framework of the life cycle and the works that need to be done at every stage of the life cycle to ensure the RAMS of the system. IEC62425 (EN 50129) makes the IEC62278 improved according to safety case of train control and system safety integrity level, etc. Furthermore, IEC62279 (EN 50128) is the safety-related design standard for train control system software and it complements the content of software engineering under the framework of IEC62278. IEC62279 also provides the technology and management for different safety-level software design. IEC62280 (EN 50159) is a rail transit communication system safety standard, which involves two parts: open communication system and closed communication system.

In rail transit, IEC62278 recommends three international common safety principles: the Globalement Au Moins Aussi Bon (GAMAB) principle of France, the Minimum Endogenous Mortality (MEM) Principle of Germany and the British As Low as Reasonably Practicable (ALARP) principle. GAMAB requires all new systems must provide the best safety performance, and at least it should be equivalent to the safety performance of the existing similar systems.

MEM principle means that the application of the new system cannot increase the probability of casualties. In Germany, casualties caused by rail transit systems are below the country's lowest natural mortality rate (the natural mortality rate for the 5–15 years old is the lowest, which is 1/20000 per year in Germany). Thus, the rail transit system in general set the safety objectives $RM = 10^{-5}$ catastrophic risk/person years.

The ALARP principle means that a reasonable and feasible method is adopted to reduce the risk as far as possible in the case of cost. This principle divides the risk into three levels, as shown in Fig. 4. The focus of the ALARP principle is to make a final overall judgment about the risk associated with the system and try to make every

risk acceptable or tolerable. In addition, the overall risk of the system should be reduced as much as possible.

From a formal perspective, the GAMAB principle and the MEM principle clearly define the safety requirements in the form of the risk acceptance thresholds, which is represented by the “existing similar system” and “minimum national population natural mortality” and have a strong universality and objectivity. The limitation of the MEM principle is that it does not consider the differences in risk perception among different types of systems. For example, the acceptance of the risk for rail transit and civil aviation, highways and other means of transport systems could be different.

The ALARP principle encourages the maximal reduction of risk to improve safety by taking the cost into account. To a certain extent, it promotes the research and application of risk reduction technology. Compared with the GAMAB and MEM principles, the ALARP principle is more stringent since it needs to analyze a variety of risk reduce measures and then choose the most reasonable solution during the design process. British Health and Safety Executive (HSE) issued a number of regulations on the interpretation and constraints of the ALARP principle and provided many court cases as references. Rail transit regulatory authorities also issued the ALARP principle guidance, the engineering safety management (Yellow Book) and other industry standards to provide detailed application procedures and steps for the ALARP principle in system design, operation, maintenance, and safety demonstration.

During the development process of the CBTC system for China practice, the requirement analysis, risk analysis, system design, product realization, system testing, and other works were carried out according to the CENELEC standard. The “standards, methods, processes, people” of each task is analyzed based on its own characteristics. The final product obtained the SIL4 safety certification from a foreign third-party certification company, and it can be applied in the actual project.

3.2 The General Method of Safety Management for Rail Signaling System

The life cycle of a system refers to the various stages of the whole process from the initial concept to retirement and tasks at each stage (as shown in Fig. 5). The entire phase includes a plan, management, control, and supervision of a safety-related system. System life cycle (Lifecycle System) is a description of the process of system development and usage. System life cycle provides a unified framework for planning, management, control and supervision of the quality, and the performance, construction period, cost and other aspects of the system. System safety is the result of

Fig. 4 ALAP principle

Fig. 5 Life cycle of the system

many factors working together, and these factors are distributed in all the system life cycle stages. In particular, the factors involved in different stages are different. Therefore, we need to carry out the system safety work in system life cycle to control and monitor the different factors at different stages. The system life cycle that includes the system safety work is called the safety life cycle, also called Safety Lifecycle.

From the activities of the whole life cycle, it could be found that the management concept-based risk is adopted to control the risk of the system within the system or project life cycle. In the process of the actual rail transit project implementation, the whole life cycle is usually divided into 5 milestones, as shown in Fig. 6. The objective of the first milestone is to generate the system requirements, and this includes the first 4 phases. The second milestone needs to distribute the safety requirements to subsystems and give detail design outline. Before the third milestone, implementation and installation of the system need to be finished. The main activity of milestone 4 is system certification and safety inspection. The final milestone is to state commercial operation.

3.3 The Processes of Safety Lifecycle for CBTC

In October 2004, Beijing Scientific and Technological Committee carried out the project “Communication based

on Urban Rail CBTC system research” for the first time. The team at Beijing Jiaotong University was assigned to develop the automatic train protection (ATP) and automatic train operation (ATO) system which was once dependent on technology import and restricted the further development of signaling system in China.

By the end of 2007, the team overcome the difficulties of the CBTC system’s key technologies and completed the integrated test of the whole CBTC system. The function and performance test were carried out on the 1.3-km test line of Beijing metro afterward. Finally, the CBTC systems were checked and accepted by the experts. Moreover, the various functions and performance indicators have reached the international advanced level. The resulting CBTC system also broke the technical monopoly in China [14].

The system design theory was established and the self-developed complete sets of systems and equipment were developed, which include: (1) the system design theory of moving block; (2) the design method of safety critical system in the whole life cycle; (3) self-developed safety computer platform; (4) technology and equipment based on the integrated design, e.g., the two-level scheduling model and three kinds of control level [11].

In view of the complexity of CBTC system, we use the scene analysis method to analyze. According to the EN50129, combined with the actual characteristics of the Beijing metro project, a safety life cycle model for the self-developed CBTC products was established and the details are shown in Fig. 7 [15].

3.3.1 Design of Safety Management Process

A general overview of the system/subsystem/device design describes the main functions of the system, as well as the internal and external interface, so that the relevant staff can clearly understand the principles and techniques used in the system.

Safety management process is composed of a number of stages and activities, which are connected to the safe life cycle. The design and validation of the system life cycle can be seen as a “top-down” stage and is accompanied by a “down-top” phase, as shown in Fig. 7, which looks like a V-type.

3.3.2 Safety Organization and the Safety Plan Establishing

The safety management process should be performed under the control of a suitable safety organization via a personal that is competent for the relevant work; Fig. 8 shows the organization structure of CBTC project. According to the requirements of the relevant system’s safety integrity level, there should be a proper independence between different personals.

Fig. 6 Life cycle milestone diagram

Fig. 7 Independent research and development of CBTC product life cycle

A safety plan should be made in the early stage of the system life cycle. This plan should determine the organizational structure of the safety management which involves the entire life cycle, the need for a review of safety plans within the appropriate intervals, and all aspects of the system/subsystem/device (including hardware and software).

In the early stage of the system design, we should create a hazard source log based on the results of hazard analysis (including PHA, SHA, SSHA, IHA, and OSHA) and maintain the hazard log throughout the entire safety life cycle. Safety requirements can be considered from two aspects, i.e., the functional safety requirements and the safety integrity requirements. Safety functional requirements are the actual safety-related functions which the system, subsystem, or equipment is required to carry out.

Safety integrity requirements define the level of safety integrity required for each safety-related function.

3.3.3 Safety Audit, Verification and Validation

At the appropriate stage of the system life cycle, safety audit should be carried out to monitor the safety management process in accordance with the requirements of the safety plan and the relevant standards.

Verifying the content of each phase for the life cycle should meet the safety requirements specified in the previous stage and finally confirm that the system/subsystem/equipment meets the initial safety requirements. According to the opinions of the safety authorities, the assessment staff should be authorized by the safety authorities, be completely independent from the project team, and report directly to the safety authorities. Furthermore, the evidence for a system/subsystem/device meeting the safety acceptance criteria shall be listed in a structured document called “Safety Case.” Before Safety Case sent to independent company, internal verification and validation activities need to be done.

3.3.4 Safety Management for System/Subsystem/ Equipment Transfer, Operation and Maintenance

System/subsystem/equipment should meet the conditions of the safety acceptance before the delivery to the railway authorities. The delivery also includes the submission of “Safety Case” and “safety assessment report.” After the system is put into operation, it should meet the process, support system and safety monitoring requirements that are defined in the safety plan and technical safety report.

Fig. 8 Organization structure for CBTC project

Fig. 9 Process for independent certification

3.3.5 Processes of Safety Certification

Safety certification needs a proper process, as Fig. 9 describes. Before conducting an independent evaluation, a checklist is required about user requirements and related standards. This checklist can provide a systematic method to record the results of independent evaluation and evidence and save as the evaluation document for traceability.

(1) Document Review

In the beginning of the project, the independent safety assessment (ISA) staff will review the project plan, safety plan, quality plan, configuration management plan, test plan, and system requirements specification, etc. The staff then put forward written improvement opinions.

After the integrators and subcontractors finish the development of related subsystems, ISA staff will review the test specifications of the integration testing and system testing for each subsystem, the test plans and test reports and then put forward written improvement opinions.

- (2) On-site audit

According to EN50128, EN50129, and other standards, the ISA staff applies the on-site audit to the systems integrators and the core technology supplier during the stage of the system requirements and system design, as well as the implementation stage and system testing stage from the aspects of the system assurance, software quality assurance and management, etc. The staff then put forward a written audit report. System integrators and core technology supplier need to respond to the audit opinions presented by the ISA staff and provide the relevant evidence. After that, the ISA staff can close their views.

For the problems existing in the audit process, the owners, the independent safety assessment staff, as well as systems integrators and core technology provider will hold a weekly safety meeting to communicate and resolve the problems.

(3) Safety confirmation

In order to ensure the safety of the signaling system after testing, debugging and operation, the single train commissioning, multi-train commissioning, trial operation, operations need to be carried out under special monitoring mechanism. System integrators and core

technology suppliers provide related design documents, test report and safety documents. ISA then conduct the safety assessment by means of document review, on-site audit, and witness testing according to the requirements of EN50128 and EN50129. After that, ISA provides the safety assessment report and publish the safety certificate. When achieving the certificate, the testing, debugging, system operation, etc., could be carried out.

In the safety assessment of metro projects, ISA will check each of the safety critical system products provided by suppliers to make sure that they have obtained the product safety certification. The safety certification process for the CBTC system is as follows:

- a. Products design
The design and dev med by the design team, and they make a detailed record for the works that completed in each stage of the system design process and development process. The record could be the system and subsystem requirements specification, system architecture specification, etc.
- b. System test
The implementation of the system, subsystems, components, and modules needs to be verified by testing according to the corresponding test specifications at every stage of the CBTC system development [16]. In the testing process, the engineers use the test cases that described in the specifications and test each function and performance individually.
- c. Verification and validation (V&V)
This work is done independently from the project team and is performed by the V&V staff. In each phase of the project life cycle, the V&V staff needs to ensure that the work done at each stage is correct [17] and generates a validation report for each phase.

The safety certification for CBTC covered the certifications in the test line, single train commissioning, multi-train commissioning, trial operation, and the carrying passenger trial operation, etc. At each stage of the whole life cycle of the system, the safety is measured and evaluated by the international advanced and practical standards and scientific methods. In addition, an independent third-party assessment team is hired to carry out safety audits and assessments in each process to ensure the CBTC system with independent intellectual property rights can be used safely and reliably in the application of urban rail transit in China.

4 Conclusions

After absorbing the essence of international safety standards and adapting China urban transit construction practice, the safety management and system integration method

of CBTC system came into being. The method was proved in the process of pilot test on test line, single train commissioning, multi-train commissioning, trial operation on mail line, and the carrying passenger trial operation, and finally the CBTC system and related products developed by Beijing Jiaotong University has obtained the safety integrity level 4 (SIL4) certificate.

After the successful application of independently developed CBTC system, the advanced fully automatic operation system is currently under development and the new technologies will be used in the Beijing Yanfang Line which is expected to be opened by the end of 2017.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Yan F, Tang T (2005) Development of safety technology of rail transit signaling system and the research status of foreign countries. *J China Saf Sci J* 15(6):94–99
2. Gao CH (2014) Research on the core technology of independent innovation CBTC system. *J Modern Urban Rail Transit* 24(1):7–10
3. IEC61508-2010 Functional safety of electrical/electronic/programmable electronic safety-related systems
4. Society of Automotive Engineers (SAE) (1996) Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment (ARP4761). SAE International: Warrendale, PA. [Aerospace Recommended Practice]
5. IEC 62278-2002 Railway applications—specification and demonstration of reliability, availability, maintainability and safety (RAMS)
6. IEC 62279-2002 Railway applications—communications, signalling and processing systems—software for railway control and protection systems
7. IEC62425-2007 Railway applications—communication, signalling and processing systems—safety related electronic systems for signalling
8. RSSB (2011) Safety risk model risk profile bulletin (version 7) [R]. [http://www.rssb.co.uk/risk-analysis-and-safety-reporting/risk-analysis/safety-risk-model-\(srm\)](http://www.rssb.co.uk/risk-analysis-and-safety-reporting/risk-analysis/safety-risk-model-(srm))
9. European Commission-2004 (2004) Safety management in railway, WP.2.2.2: guidance for the safety management system
10. EI Koursi EM, Tordai L (2003) SAMNET: Safety management and interoperability thematic network in railway systems. *WCRR2003*, Edinburgh, pp 198–202
11. Common safety targets, common safety indicators and common safety methods. A joint paper of the Safety Systems Harmonisation Working Group and the Technical Interfaces Working Group of the UIC Safety Platform, Sept'2002
12. CENELEC EN50129-1999 (2003) Railway applications:safety related electronic systems for signalling [S]
13. CENELEC EN50126-1999 (1999) Railway applications:the specification and demonstration of reliability ,availability,maintainability and safety (RAMS) [S]

14. Tang T, Niu YM, Gao CH (2010) Research and innovation of CBTC system for rail transit. *J Munic Technol* S2:349–353
15. Yan F, Gao CH, Tang T (2011) Safety management and assessment mode research for rail transit signalling engineering project. *Urban Rapid Rail Transit* 24(4):12–16
16. Gao CH, Yan F, Tang T (2005) Research on safety assessment method of rail transit signaling system. *J China Saf Sci J* 15(10):74–79
17. Morisio M (2000) Commercial-off-the-shelf (COTS): a survey a DACS state-of-the-art report[R]