A Real-time Train Safety and Collision Prevention System

Hao Cai

Professor of Computer Science

Department of Computer Science, University of Shantou,

Shantou, China

Weihang Wu

Senior Consultant

Lloyd's Register Rail (Asia) Ltd, Beijing, China

SUMMARY

This paper discusses the lessons learnt from the investigation of recent train collision accidents such as the "7•23" Yong-Wen accident in China, and a number of common system design faults and safety limitations of many existing signalling systems are identified. Although the European Train Control System (ETCS) and Chinese Train Control System (CTCS) have been developed to standardise different safety systems currently used by European and Chinese railways, especially on high-speed lines, it is evident that there is still a long way to go in order to fully implement such ETCS or CTCS into current railway infrastructures of different countries. As a result, the train collision risk associated with existing railways using various train protection systems and safety technologies is still relatively significant and should not be considered to be negligible.

This paper proposes the introduction of an innovative Real-time Train Safety and Collision Prevention System (RTSCPS) as a medium-term cost effective solution to addressing the current safety risk associated with existing signalling systems. The underlying safety principle of the RTSCPS is to determine the current position of existing in-service trains in a real time manner using reliable GPS (Global Positioning System) equipment and to identify possible train collision scenarios on the basis of the calculation of the running trajectory of each train using the known train/line profile data. The RTSCPS will be interfaced to the control centre and thus a timely early warning can be given to the controller.

The system architecture of the RTSCPS is described and the development approach discussed. Technical issues on high availability, real-time performance and human computer interface design as well as development cost and installation are then discussed. The potential risks associated with the RTSCPS such as loss of warning (e.g. due to failure of GPS equipment) and false warning (e.g. due to environmental interference) are also analysed.

The RTSCPS is independent of existing signalling systems and can be treated as the additional safety system to improve safety of existing railway. Failure of the RTSCPS will not compromise the level of safety in existing railway.

INTRODUCTION

Railway transport continues to become more and more high-speed and high-density. While transport efficiency is improving, ensuring safety is increasingly becoming a prominent issue. The safety of the railway transport directly links to the lives and wellbeing of a large number of passengers. Safety is a crucial and urgent issue that needs to be addressed. The use of train control systems is an effective means of improving traffic safety and efficiency, but such large-scale control systems (especially software-based systems) are becoming increasingly complex with more functionality. To guarantee their correctness is also getting more and more difficult. The failure of these systems has led to immeasurable losses to the society and people's life. It has become an urgent problem that needs to be resolved.

Some examples of major railway disasters occurred recently, in particular and "the 7·23" Yong-Wen railway accident in China. According to the investigation of these accidents and the analysis of the current status of those Train Control System (TCS) used for train control, besides the poor safety management, the failure of the control system software is one of the major reasons that caused the system failure.

There are four major technical defects in the design of TCS:

- Existing TCS purely utilizes the Automatic Train Protection (ATP) and interlocking mechanisms [4,5] to avoid train collisions. When the subsystems associated with ATP malfunction (e.g. lightning causing the track circuit transmission damage), the system safety protection mechanism might be defeated or significantly weakened causing accidents.

- From the viewpoint of the system design, system safety has not been fully taken into account as part of the overall system design, such as eliminating certain equipment failures and errors with the appropriate redundancy mechanism and inherent fail safety design [12].

- There are major design flaws in the human-computer interface [12]. The TCS design does not take sufficient consideration of the high integration between software systems and users of such systems. When the TCS data acquisition fails, very limited information is displayed to the train operation controllers, vehicle attendant and equipment maintainers. This makes it difficult for the train control center staff to gain a full understanding of the situation on the ground in a short period of time. Because there is very limited and unreliable information available and it is very difficult to know exactly what is going on when some signalling systems failed. The TCS controlling center, and ground electrician, and train drivers are completely in chaos during the failure of the signalling systems. The design faults of the TCS make it easy for the users of these systems to make more mistakes which would eventually lead to catastrophic disasters.

- There are also issues on the quality control of the core software and hardware systems throughout the system development process [12]. System development has not followed the development methods and processes required for high integrity software / hardware system, or conducted quality assurance and safety reviews according to the relevant high integrity industry standards.

- The trend in modern industrial development with increasing dependency on computer and software systems challenges the traditional method of system safety engineering. The defects of the requirements, the design faults and the incorrect implementation are the main causes to the failure of large scale high integrity computer systems.

1 The state of the art

Traditional software engineering approaches such as object oriented design (OOD) methods represented by using the Unified Modeling Language (UML) break down a system into smaller modules and subsystems. Such a method would simplify the design and development of a complex system and system's development and testing are based on the more manageable modules. To a certain extent, they can improve overall software quality and reliability. However, in practice when developing large and complex systems, there is difficulty of applying such methods to addressing the linkage between the abstract design and the realization of that design. Very often the resulting graphical design models are either too abstract or too specific. For the design which is too abstract, it is difficult to transit from design to specific system implementation. As for the design which is too specific, designers have to spend a great deal of time and effort in constructing the graphical design models from system requirements.

The linkage between design models and implementation has also significant impact on software quality. For example, the "7•23" incident report points out that the deficiency of the design documentation and inconsistencies between the design and implementation have greatly affected the quality of the software. This is mainly due to possibility of human errors when manually translating from the symbolic or graphical design models into the implementation, eventually leading to the introduction of defects into the design and quality of software products.

In the security or safety-critical system industries, formal methods has been increasingly used in the design and development of large-scale safety-critical software systems, such as a number of European safety critical control systems [2] and the French High-Speed Rail Control system developed by GEC-ALSTHOM Transport [14]. Formal methods is an effective and important way to improve the quality of large-scale software and reduce the cost of software development, such as the methods represented by Z [1, 13], B and CSP [9] etc. Due to its simplicity, together with the support tools, Most formal methods allows system

designers to invest the main energy in the actual function of the system and application logic, and greatly helps the system implementer to complete the transition from design to concrete implementation. Due to its precise description and definition of system functions and requirements, formal methods can also help system testers to test the correctness of the implemented system, which can greatly reduce the defects in the delivered software products, to better ensure the safety of the system.

Often we see systems architectures where the software is split into two: the software which performs the safety critical functions and then a "safety monitor" that double checks that the output from the main software to ensure the output is safe. These safety monitor applications are where Z is very good because:

a) safety monitors are generally small

b) safety monitors normally involve checking a lot of logical conditions

c) safety monitors don't normally have a lot of algorithms.

2. The approach

In this research project, we will develop and improve the complex safety-critical software and hardware systems engineering approach, and apply the methods to develop a real-time train safety and collision prevention system, hereinafter referred to as RTSCPS (Real-time Train Safety and Collision Prevention System). This will progressively develop and refine the theoretical and practical foundation in the area of safety-critical software system development. Using concepts from a number of European safety critical control systems, the RTSCPS will make up for the safety defects of the existing train control system. The system is independent of the existing TCS and ATP systems to provide further protection for traffic safety. The architecture is shown in Figure 1. Dashed portion is the main portion of the extended function.

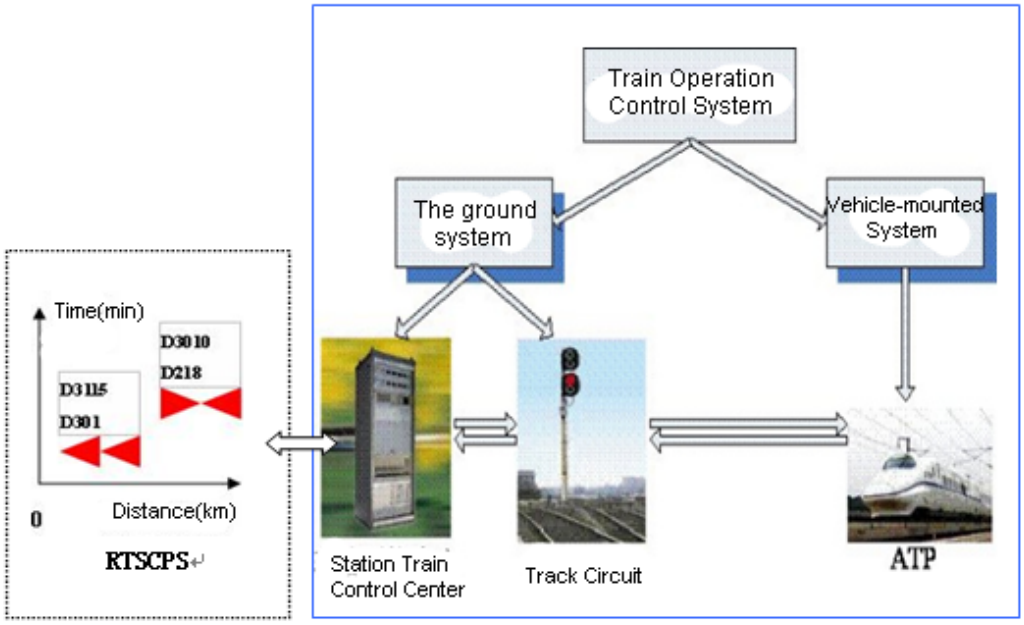

Figure 1 Real-time train safety and collision prevention system architecture

The RTSCPS will be based on the real-time data from reliable GPS systems installed on locomotives and the ground data, including real-time absolute train position, speed, line profile data, road, bridge and tunnel location data, permanent or temporary speed limit and other important information, and will calculate the trajectory of the train in a real time manner. Through the resulting train trajectories, the important early-warning information about collision that may occur between trains, the locomotive overspeed, and the route deviating from the plan will be given. The RTSCPS provides timely early-warning to station control center and offers the basis to train scheduling decisions, in order to completely avoid train collisions and to ensure that the trains operate as scheduled.

Regarding the train control center at both central and local station levels, the RTSCPS will provide a better and well-understood human-computer interaction interface to the central train operation controllers. It is easier for control personnel to schedule trains and manage safety, thereby minimizing human errors and reducing the incidents of train operation. When an error or hazard occurs, the integrated safety management strategy and optimisation of human-computer interaction will take the system to a safe state, both improving train operating efficiency and avoiding the accident.

The RTSCPS also examines the driving instructions and ground control instructions issued by the central control personnel before they are executed. The examination ensures traffic safety and avoids train collision. The system automatically backup central control instruction, core and safety-related data, which provides the basis for system diagnostics and safety analysis.

Real time train safety and collision prevention system mainly consists of the following four main modules (see Figure 2): data acquisition and processing, data analysis, human-computer interaction and automatic data backup. Data acquisition and processing module have direct responsibility for collecting，processing and caching data from the automotive system and ground system, including real-time train operation and associated track information. Based on the information of the data acquisition and processing module, the data analysis module calculates the trajectory of the train, to detect possible collisions between trains and send locomotives overspeed warning information.

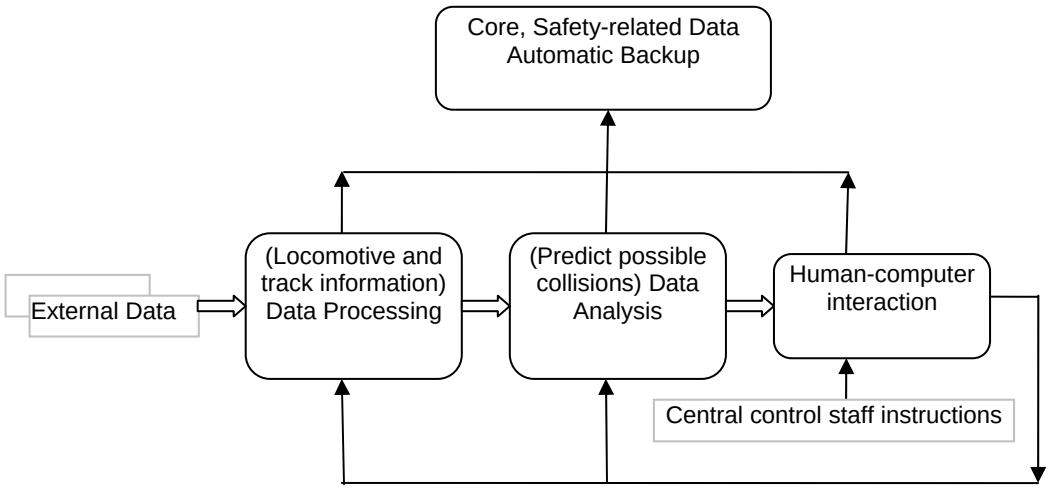

Figure 2 Real time train collision prevention system

Human-computer interaction module accepts instructions from the central train operational controllers, displays possible collision between trains, locomotive overspeed and other important warning information, at the same time also tests the instruction which will be given by central control personnel. Before central control personnel require train drivers to run at a certain speed in a certain track, it can be tested whether this instruction will lead to possible collisions between trains and other safety risks in human-computer interaction module. After ensuring that all is safe, central control staff gives instructions to train drivers and confirm and record the occurrence of the directive via the human-computer interaction module.

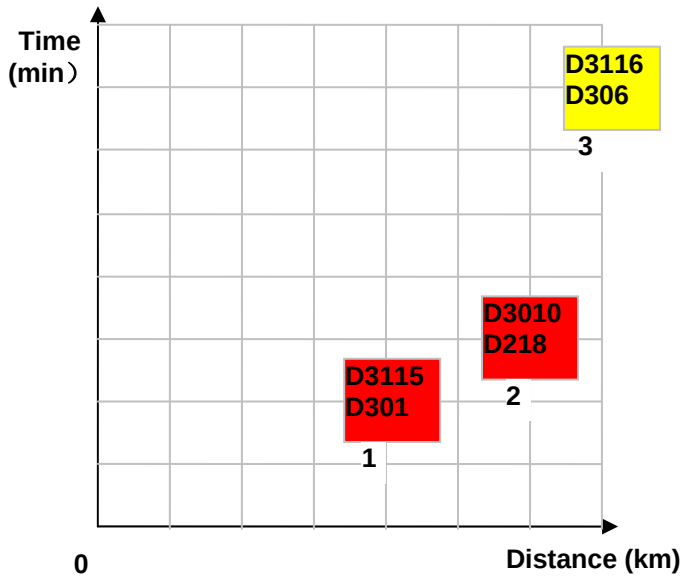

Figure 3 Potential collisions between trains

The potential collisions between pairs of trains are calculated by the data analysis module, and displayed on a human-computer interaction interface. Human-computer interaction interface displays the predicted collisions in Figure 3. The figure displays three collisions that are going to occur. The horizontal axis represents the shortest distance between the two trains, and the vertical axis indicates the shortest time that a crash will occur. In these three pairs of collisions, the first rear-end collision is the most urgent early warning, indicates that train D301 will rear-end collide with train D3115 in 2 minute, and now the two trains are 4000 meters apart. The next emergency early-warning is the No. 2 collision. D218 will head-on collide with D3010 in 3 minutes and now two trains are 6000 meters apart. The 3rd rear-end collision will take place in 7 minutes. Train D306 will rear-end collide with train D3116 and now two trains are at a distance of 7000 meters. After seeing these potential collisions, central control personnel can take corresponding measures, such as adjustment of train scheduling and operation in real time, to avoid accidents.

Before the actual instructions are issued to train drivers, central train operational controllers can test the driving instructions and ground system control instructions (hereinafter referred to as pre- instruction) that they will issue. RTSCPS will analyse these pre-instruction, based on the real-time situation of train and ground systems. For the possible risks or potential crashes, the RTSCPS will display information similar to the information in figure 3. According to the actual situation, central control personnel can adjust or cancel their pre-instructions, dispatching trains effectively and safely.

Automatic data backup modules can automatically store locomotives, track, signals, directives issued by the central train operational controllers and train tracks in real time. Backup important historical information will enable us to do fault diagnosis for each part of the system and provide an effective basis for system safety analysis and continuous improvement of system.

3. Expected benefits

This research project proposes an innovative real-time train safety and collision prevention system (RTSCPS). Based on the Train Control System, RTSCPS can conduct safety analysis for the real-time data of the ground system and train operation when the train runs, to actively search for potential risks, and give early-warning about train collisions and provide the train control personnel with sufficient time and effective method to implement safety measures to avoid accidents.

	Project objective	The existing science and technology	Expected Innovation
Scientific innovation	engineering approach of real-time and high integrity software systems	Traditional development method is based on graphics . Non-critical software development is applied to high integrity software system development.	Formal methods is integrated with the structured safety engineering method. Systematic high-integrity software quality control system.
	human-computer interaction research of real-time high integrity system	Safety strategy is passive. The influences of human behavior and factors on system safety are not fully considered.	Proactive safety strategy. Systematic consideration of human factors in system safety.
Technological innovation	Multiple and effective safety protection for rail transit operation	ATP-based interlocking mechanism for safety protection.	Effective, real-time and comprehensive mechanism for safety protection.

Table 1 RTSCPS science and technology innovation

If real-time train safety and collision prevention system is applied to train operation control system as a practical railway industrial product, it can strengthen the operating safety of the railway system and have huge economic and social benefits. Specific value and innovation are shown in table 1, comparing the existing technology with the innovation of science and technology in this project:

4. Future Works

In this research project, we will use formal methods as the basis and learn and develop the existing risk assessment and risk management methods, integrating them into the high integrity software system development [3, 10]. This research project will establish effective design methods for system safety assurance and utilize appropriate technology and processes to greatly improve the overall system safety.

Modern large-scale software systems usually have a lot of different safety subsystems. We need to ensure system safety integrity through a systematic design method. The "7.23" incident report [12] mentioned that data acquisition unit is more vulnerable to environmental interference. This unit often needs to process data from a number of redundant subsystems with low integrity level before passing the results to subsystems with high integrity to guarantee the safety of the whole system. In this project, we will develop a complete framework for the development of large high-integrity software systems from design to the system realization with integrated system safety engineering. To achieve the conversion from the formal model to the system application architecture, including a valid parallel processing method, safety analysis, train data processing and ground signal processing. Further development of the two-tier fixed priority real-time scheduling method [6, 7, 8], providing theoretical foundation for the development of mixed distributed high-integrity real-time systems and multi-core high-integrity real-time system.

Incomplete testing is one of the main factors affecting the reliability of the system. For example, the accident report [12] mentions that when abnormal condition occurs, the software design does not correctly implement fail safety measures. If the system tests use the full system coverage for their formal model which includes the tests of the errors which occur in the error condition, the defects of the system can be identified effectively. In this project we will explore reliable, effective and complete overall system testing and verification methods and give a further development of the theory of automated software validation based on formal methods and high integrity languages such as SPARK Ada [1, 2, 13] and their practical application. From the system design, based on the overall requirement of system, the complete coverage test of the correctness of the system realization (source code) function and design integrity, including abnormal state testing and system reliability demonstration, as well as collection, analysis and research of the evidence in the aspects of reliability and safety.

The study of RTSCPS will include the train operation safety (risk) model, data model, information flow model and safe operation model. Subsequently, formalize the definition of system functions and specific implementation mechanism of the system.

CONCLUSION

This paper discusses the lessons learnt from the investigation of recent train collision accidents such as the "7•23" Yong-Wen accident in Chin and a number of common system design faults and safety limitations of many existing signalling systems are identified, and proposes the introduction of an innovative Real-time Train Safety and Collision Prevention System (RTSCPS) as a medium-term cost effective solution to addressing the current safety risk associated with existing signalling systems.

The system architecture of the RTSCPS is described and the development approach discussed. Technical issues on high availability, real-time performance and human computer interface design as well as development cost and installation are then discussed and future works are discussed to implement the proposed Real-time Train Safety and Collision Prevention System (RTSCPS).

Acknowledgement

The authors gratefully acknowledge the help given by Fan Ye during the writing of this paper. This work was funded by the Shantou University funded RTSCPS project (NTF12019).

References

[1] A.W. Roscoe, Cliff B. Jones and Kenneth R. Wood, Reflections on the Work of C.A.R. Hoare, Springer, 2010

[2] Altran-Praxis Ltd, Air Traffic Management, http://www.altran-praxis.com/atm.aspx

[3]British Standard BS: IEC61882:2001 Hazard and Operability studies (HAZOP) – Application Guide. British Standards Institution. "This British Standard reproduces verbatim IEC 61882:2001 and implements it as the UK national standard

[4] China Railway Signal & Communication Corporation, the ATP system of automatic train protection

http://www.crsc.com.cn/jscp/xtjs/csjt/101019a.html, 2010-10-19

[5] China Railway Signal & Communication Corporation , CTCS -3 level train control system

[6] Hao Cai and Andy Wellings, Temporal Isolation in Ravenscar-Java, 8th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC 2005), 5. 2005, ISBN: 0769523560

[7] Hao Cai and Andy Wellings, Supporting Mixed Criticality Applications in a Ravenscar-Java Environments, On The Move to Meaningful Internet Systems 2004: Workshop on Java Technologies for Real-Time Embedded Systems (JRTES), Lecture Note Computer Science 3292, 10.2004 JRTES，Springer ISBN: 3-540-23664-3

[8] Hao Cai, A Virtual Machine for High Integrity Real-Time Systems，The University of York, Ph.D thesis, 2005, YCST 2005/10, The British Library

[9] Hoare, C. A. R. (2004) [1985] (PDF). Communicating Sequential Processes. Prentice Hall International. ISBN 0-13-153271-5

[10] Leveson N.G and Shimeall T.J., Safety Verification of Ada Programs using Software Fault trees. IEEE Software, vol. 8 no. 4, 1991, pp. 48-59

[11] Metro Line 10 " 9 • 27 " accident investigation team, Metro Line 10 " 9.27" accident investigation results, Shanghai Safety Authority 2011.10

http://www.crsc.com.cn/jscp/xtjs/csjt/101019a.html, 2010-09-09

[12] The national production safety supervision and administration bureau, "7.23" Yong-Wen line special major railway traffic accident investigation report.

http://www.chinasafety.gov.cn/newpage/Contents/Channel_5498/2011/1228/160577/content_160577.htm

[13]Woodcock J. (1991) Using Standard Z. Hempstead: Prentice Hall

[14] Zong-Yan QIU, Formal Methods, School of Mathematical Sciences, Peking University, 2010