# FPGA Based Research on Safety Information Transmission Mechanism of Rail Transit

Hao Wu[1, a], Jian Wang[1,b] and Pengfei Cai[1,c]

[1] Shanghai Metroit Company, Building 3, No. 1, Old Humin Rd., Xuhui District, Shanghai, China

[a]wuhao@metroit.cn, [b]wangjian@metroit.cn, [c]caipengfei@metroit.cn

**Keywords:** information transmission, information safety, transmission mechanism, rail transit

**Abstract.** In recent years, with the rapid development of China High-speed Rail and magnetic levitation transportation, the domestic rail transit industry has entered a high-speed, high efficiency, high safety and high reliability stage. Signal safety is the core of safe and reliable operation of rail transit. In order to guarantee the safe and reliable transmission of rail transit signals, China has already had its own proprietary safety information transfer protocol of RSSP-1 and RSSP-2. At the application level of the protocol, however, it can only achieve the communication between the train control center. The application environment of the protocol, which requires the safety computer with high performance, is usually achieved by high-level language. Based on the analysis of the safety information transmission mechanism, it is the first time to propose that using the FPGA to achieve the safety information transmission protocol, which is original and expands the application scenarios of rail traffic safety communication protocol. Due to the erase and reconfiguration ability of FPGAs, the cost of safety information transmission engineering can be reduced to a great extent, and it has a high value on research. In this paper, the design of communication frame protocol is given from two aspects: sender and receiver. Its reliability and function was tested, and the test results showed that the safety information transmission interface based on the FPGA fully meets the design requirements. The system can not only achieve the function of fail- safe but also can meet requirements of reliability on the rail transit system.

## Introduction

### Overview of Safety Information Transmission

As the name suggests, the transmission of safety information consists of two elements, safety and information transmission. The information transmission refers to the transmission of information between entities. The elements of information transmission include information transmission entities, messages, information transfer protocols, and media or channels for transmission. Information transmission entity type is also very broad, it can be people, equipment and equipment, and even processes and processes. In the field of rail traffic signals, the focus is on the transmission of messages between devices.

For safety, the difference between Safety and Security should be identified. The concept of safety introduced in the relevant international standards refers to a state in which the persons or things are not subjected to unacceptable harm. Security is also a state in which people or things are not subject to intentional and malicious damage or loss. It can be found that security is subjectively with more stringent restrictions and emphasizing the harm of intentional and malicious, and objectively expand the harm of the audience which can be the loss of property. While Safety only emphasizes the harm to people, and the damage must be achieved to a certain extent. In the field of rail traffic signal safety information transmission, security is concerned with Safety which means the risk introduced by the communication process whether will causes harm to the personnel is considered.

This paper mainly studied the safe transmission of the rail transit signal in the closed system. The closed network is defined in GB / T24339.1 as the number or the maximum number of connected devices is fixed, and the characteristics of the transmission system is known and fixed, and the system can ignore the risk of unauthorized access.

As the environment, in which the rail transit information transmission system often works, is complex and harsh electromagnetic, the channel is susceptible and may generates incorrect coding which makes the data error in the transmission process.

According to the threat sources on the transmission system which is stated in the GB/T24339.2, the threat of closed transmission systems is presented as below:

Data frame repetition
Data frame loss
Data frame insertion
Data frame order confusion
Data frame error
Data frame transmission timed out

It requires high safety in the field of rail transit, if there were threats which cannot be detected effectively and timely, the consequence would be unacceptable. Safety information transmission is proposed for the above threat source on closed transmission system, in which the information receiver can efficiently and accurately identify the threat source and take appropriate measures when a variety of threats are likely to inject into the channel. So as to ensure the information truly, completely, real-time and orderly transmission, and ultimately ensure the operation of rail traffic safely, orderly and efficiently.

The core of the safety information transmission is the safety information protection algorithm. According to different applications and different application requirements, several different safety communication protocol emerged in recent years. These safety communication protocols have the same points and different points. Different points reflected in the different needs of defensive tailoring, while the same points are reflected in the information in the transmission process, which all meet the following requirements:

Source information of the sender(authenticity)
Information frame correctness (integrity)
Information Timeliness (Timing)

**safety information transmission system architecture**

The overall structure of the safe communication system is shown in Fig 1. It uses the safety-related communication technology, and adding a safety layer to the OSI communication hierarchy is necessary. That uses the safety-related process and safety coding provided by safety layer to provide process protection for data transmission between orbital signaling devices.

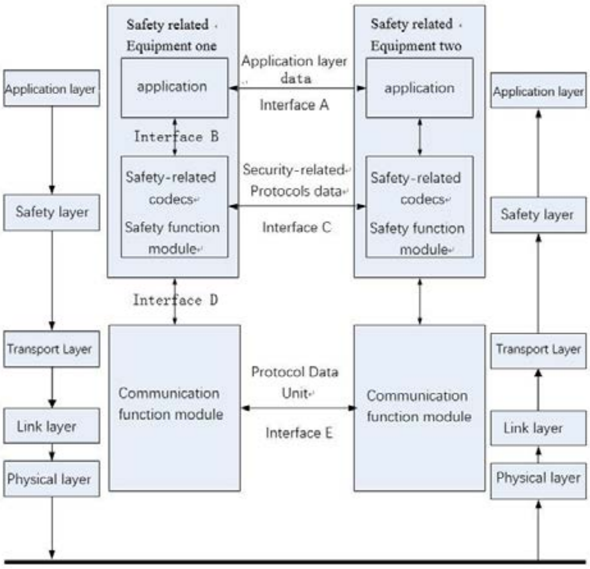
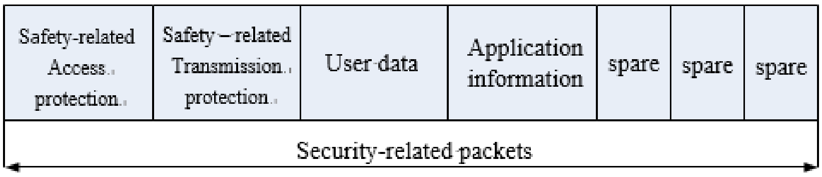


Fig.1 The overall structure of the safe communication system

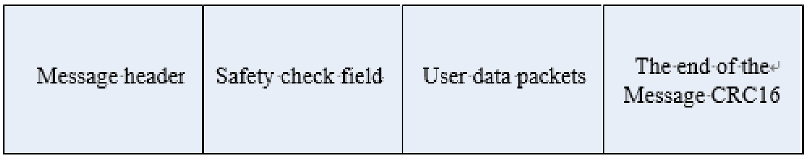
Here interface A is the application protocol of the safety information transmission, interface B is the interface between the application program and the safety function module, interface C is the interface between the safety function modules. In the field of rail transit in China, the safety interface is conventionally designed according to the EN50126 standard and RSSP-1 protocol to achieve the communication protection against threat in the transmission system. Interface D is the interface between the safety function module and the communication function module, and interface E is the interface between the communication function modules (e.g. CAN, RS485, etc.). Among all layers of the information transmission, the safety layer is the research object of this paper, and the function of safety module mainly includes safety transmission protection and safety access protection. According to these two main functions, the measures of protecting information safety can be obtained, which means the telegrams can be safety-related information by marked relevant sign respectively and transmit in the system. The required model for safety information is showed in Fig 2.



| Safety-related Access protection | Safety – related Transmission protection | User data | Application information | spare | spare | spare |
|---|---|---|---|---|---|---|
| Security-related packets | | | | | | |

Fig 2. Safety-related information model

The structure of the telegram in the RSSP-1 safety communication protocol of china is shown as the following Fig 3.



| Message header | Safety check field | User data packets | The end of the Message CRC16 |
|---|---|---|---|

Fig.3 The structure of the telegram in the RSSP-1

Here the header of telegram is checked and processed by the communication function module and the safety function module together, the field of safety checking is processed by the safety function module, and user data packets are processed by the application validation.

## Design safety communication interface using FPGA

RSSP safety communication protocol is mainly used in the communication between the train control center in China railway industry. In the past, the research on RSSP is based on the high-level language such as C language or C ++, and it has mature method of design and implementation. However, because the train control center is similar to the server side of the communication system, the application of RSSP is limited. The significance of which using FPGA to achieve the RSSP-1 safe communication protocol, is to expand the application scenario and scope of RSSP protocol. For example, in the future, using the similar RSSP-1 protocol in which FPGA is the core of each communication node to build a more comprehensive rail transit signal network. The reliability and safety of system will be greatly strong with increasing few cost of equipment.

### RSSP-1 safety communication protocol based FPGA

In this section, the design of safety communication protocol for RSSP-1 railway signal using FPGA is discussed. The design block diagram is showed in figure 4. In order to simplify the design, bus mode is not considered. According to the communication protocol and frame processing flow, the sender and receiver are respectively designed. The sender is divided into four parts: sender master, RSD frame transmission, SSR frame transmission and SSE frame check.

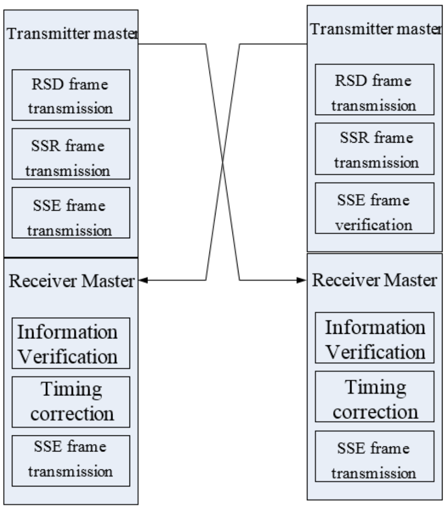


Fig.4 Block Diagram of RSSP-1 safe communication protocol for FPGA design

**Sender design**

The block diagram of sender design is showed in figure 5.

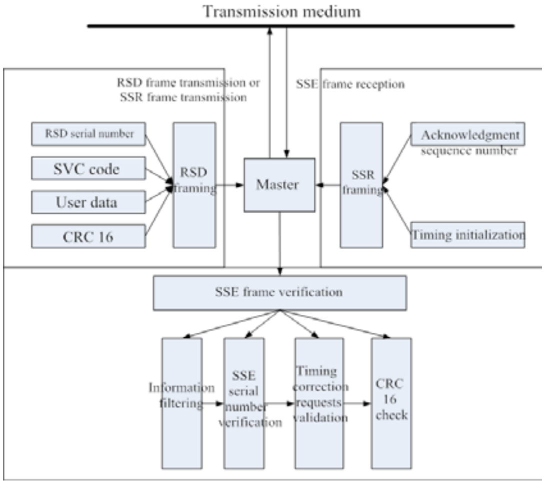


Fig.5 Block diagram of sender design

Its main function modules are designed as below:

Sequence number generation module

The sequence number generation module includes the RSD sequence number, the response sequence number and the SSR sequence number module at the receiver. The sequence number is 4 bytes in each telegram. The sequence number increases with the increasing of the transmit cycle count value.

SVC code module

According to the formula SVC=CRC^SID^T（N）^SCW the SVC value is obtained. Since there are two SVC channels, SVC_1 and SVC_2 are calculated independently. In the formula, CRC is the CRC32 calculated only for the user data packet; SID is the source identifier of the channel. T (N) is the value of timestamp based on a 32-bit linear feedback shift register, the initial value of T(0) is equal to SID, N is the RSD sequence number, and SCW is the constant.

User data module

RSD frames need to transfer the application data content of a total of 2054 bytes CRC16 module The end of telegram CRC16 shall be generated based on the header of telegram, the field of safety checking, and the user data packet. The CRC16 generator polynomial can be expressed by G（x）$=X^{16}+X^{11}+X^{4}+1$. The initial value is zero.

Framing module

Framing module refers to framing module of RSD frame, SSR frame and SSE frame.

Information filtering module

This module is mainly used to determine the type of received information frame and whether to receive the information. There are three types of telegram in the RSSP-1 safety information transmission protocol, mainly includes RSD, SSE and SSR, and the corresponding bytes are 0x80, 0x90, 0x91.

Timing correction request module

Timing correction request SEQENQ = SID ^ T (Ne), the sender extracts 4 bytes of SEQENQ as a part of the initialization channel of the reply SSE frame timing.

SSE sequence number verification module

As with the sequence number generation module, SSE sequence number verification module also has a cycle counter, during the timing correction process, the sender will retain the SSE frame sequence number after receiving the SSE frame.

Timing initialization module

According to the formula INITIAL=SEQENQSIDT（Nr）DATAVER the initial value was gotten. In the formula, SEQENQ is the timing correction request of the corresponding channel in the SSE frame, Nr is the serial number of the responder, and DATAVER is the data version of the channel.

### Receiver design

The receiver is the same as the sender. It has the filtering verification (RSD information frame, SSR information frame) and the transmission of information frame (SSE information frame). The block diagram of Receiver design is showed in figure Fig.6

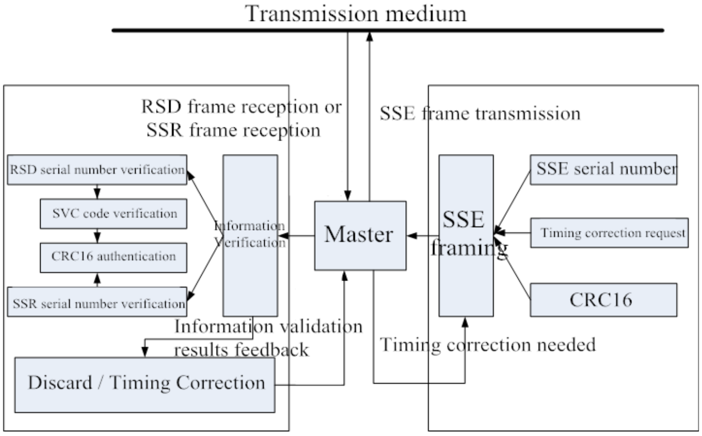

Transmission medium
RSD frame reception or SSR frame reception
SSE frame transmission
RSD serial number verification
SVC code verification
CRC16 authentication
SSR serial number verification
Information Verification
Master
SSE framing
SSE serial number
Timing correction request
CRC16
Information validation results feedback
Timing correction needed
Discard / Timing Correction

Fig.6. Block diagram of Receiver design

Its main function modules are designed as below:

RSD frame sequence number verification

The verification of the RSD frame sequence number by the receiver is based on the number of local cycles. The locally stored sequence number is associated with the number of local increment cycles. When the RSD frame information is received, the sequence number is extracted and compared. If the difference of the sequence number is between the tolerant range, the data was received, or the timing sequence was determined an error, and it needed to be verified.

SSR frame sequence number verification

Checking whether the sequence number of the requester in the SSR frame is the same as the sequence number of the SSE frame sent by the previous Ne, and the initial expressions of the initial channels 1and initial channels 2 are collated according to the responder serial number Nr.

## Implement safety communication interface

### Overall design schematic diagram

The complete design of the safety communication interface based on the FPGA is showed in Figure 7

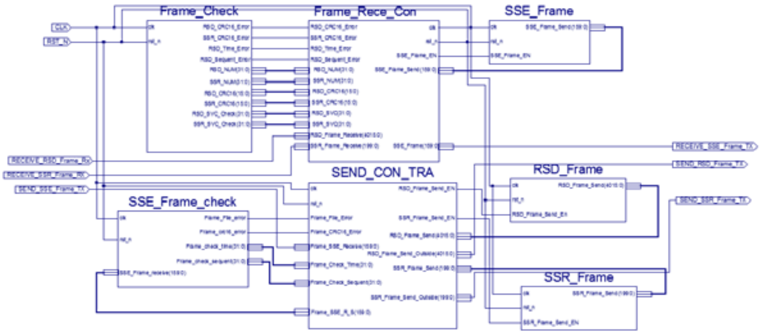


Fig.7 Overall design schematic diagram

## Functional verification

In order to test the function of system protocol, the simulation software of station communication is developed. The information transmission is completed through the serial port. The fault injection method is used to carry out the functional verification of the safety information transmission interface, includes artificially injected frame repetition, frame loss, frame insertion, frame order confusion, frame error, and frame transmission timeout. Due to space limitations, the simulation software screenshots is not showed here, and the verification results are shown in table 1.

Table 1:Functional verification result of the safety communication interface

| Number | Fault injection operation | expected results | actual results |
|---|---|---|---|
| 1 | Frame repetition | After receiving the SSE frame packet, the SSR packet is sent in response, then it repeats the previous situation | Consistent with expected results |
| 2 | Frame loss | After receiving the SSE frame packet, the SSR packet is sent in response | Consistent with expected results |
| 3 | Frame insertion | After receiving the SSE frame packet, the SSR packet is sent in response | Consistent with expected results |
| 4 | Frame order confusion | After receiving the SSE frame packet, the SSR packet is sent in response | Consistent with expected results |
| 5 | Framing error | After receiving the SSE frame packet, the SSR packet is sent in response | Consistent with expected results |
| 6 | Frame transmission timed out | After receiving the SSE frame packet, the SSR packet is sent in response, then it repeats the previous situation | Consistent with expected results |

The test results show that the system can protect against duplication, deletion, insertion, reordering, destruction and delay under the application of RSSP-1 protocol. The timing correction mechanism can guarantee the system to respond to the threat in safety information transmission.

## Reliability analysis

In order to solve the problem of the reliability of the safety communication interface designed by FPGA, the work efficiency model provided by GJB299C "Electronic Equipment Reliability Prediction Manual" was used to predict the reliability of XILINX's high-performance platform FPGA devices.

First, the working efficiency model of safety communication interface digital circuit can be expressed by: $\lambda_{\mathrm{p}} = (C_1\pi_\tau + C_2\pi_E)\pi_Q$

$\lambda_{\mathrm{p}}$ --- Work failure rate

$C_1$ --- Circuit complexity failure rate

$\pi_\tau$ --- Temperature coefficient

$C_2$ --- Encapsulation complexity failure rate

$\pi_E$ --- Environmental coefficient

$\pi_Q$ --- Quality coefficient

The FPGA, which is selected to design the safety information transmission connection, is more than 1 million doors XC2VP30 FPGA device in this paper. $C_1 = 0.0012*10^{-6} / h$ can be obtained by looked up the table, the shell temperature of FPGA device is $T_C = 70^\circ C$ during the prediction. In the worst state, the power of the device is P = 1.4W. Then, looking up the table, temperature coefficient can be obtained as $\pi_\tau$ =3.443 and the packaged form of the device is a BGA package, it is also can be obtained that the encapsulation complexity failure rate is $C_2 = 0.0076*10^{-6} / h$, and environmental coefficient $\pi_E$ =7.0 can be knew given the environment in which the most of the safety communication interfaces is designed to work in this paper belong to the environment of severe ground moving. The quality level of the device is industrial grade, and $\pi_Q$ =6 can be obtained by looked up the table. Finally the result can be expressed by

$\lambda_{\mathrm{p}} = (C_1\pi_\tau + C_2\pi_E)\pi_Q = 0.34*10^{-6} / h$

Thus, the mean time between failures MTBF= $2.94*10^6 h$ can be calculated, which meet the reliability of the design requirements of $10^6$h .

## Conclusion

In the paper, the safety information transmission mechanism in rail transit is studied. Based on the protocol of RSSP-1in the field of rail transit in china, the safety information transmission interface for the sender and the receiver is designed. The function of the safety information transmission interface based on FPGA is verified by the fault injection method. The results show that FPGA based safety information transmission interface can respond to the threat generated by safety information transmission, and the reliability is calculated according to GJB299C. The MTBF value shows that the reliability meets the requirement of mean time between failures in rail transit.

## Acknowledgments

This paper is supported by Shanghai Science and Technology Giant Project (No. 1601HX69300).

## References

【1】 CENELEC EN50159-1.Railway applications: Communication，signaling and processing systems-Part 1: Safety related communication in closed transmission systems[S], 2001(3).

【2】 CENELEC EN50159-2.Railway applications: Communication，signaling and processing systems-Part 2: Safety related communication in open transmission systems[S], 2001(3).

【3】 CENELEC EN50126-1.Railway applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety(RAMS)[S], 1999.

【4】 CENELEC EN50126-2.Railway applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety(RAMS)[S], 2007.

【5】 Esposito Rosada, Lazzaro Annando, Marmo Pietro, Sanseviero Angela. Formal Verification ofERTMS EURORADIO Safety Critical Protoc01. Ansaldo Segnalamento Ferroviado S.p.A.

【6】 J. D. Lee, J. I. Jung, J. H. Lee, J.G Hwang, J. H. Hwang, S. U. Kim, Verification and conformance test generation of communication protocol for railway signaling systems，Computer Standards＆Interfaces in Elsevier 29.2007.143-151.

【7】 Systems safety-related communication in transmission systems[Z]

【8】 Ming Yang，Design and Simulation of Safety Communication Protocol in CBTC System [D]. Zhejiang University, 2012,6.

【9】 Zhen Chen，Application Research of Railway Signal RSSP-1 Safe Communication Protocol on Safety Information Transmission between Existing Stations [D]. Beijing Jiaotong University, 2013,6.

【10】GJB/Z 299C-200X Electronic Equipment Reliability Manual.

【11】GB24339.1 Railway applications - Communication, signaling and processing systems-Part 1: Safety-related communication in closed transmission systems [S], 2009.

【12】GB24339.2 Communication, signaling and processing systems for rail vehicles-Part 2: Safety-related communication in open transmission systems [S], 2009.

【13】Operating Base Signal [2010]No.267. RSSP-1 railway signal safety communication protocol[S]. Ministry of Railways of the People 's Republic of China, 2010.

【14】Operating Base Signal [2010]No.267. RSSP-2 railway signal safety communication protocol[S]. Ministry of Railways of the People 's Republic of China, 2010.

【15】Changzong Zheng, Xiaobin Liu, Dengke Xu, et al. Research on Railway Signal Safety Protocol[J]. Railway Communication Signals，2011,47（10）:66-69.

【16】Jin Guo, Xiaoming Wang. Railway signal base [M]. China Railway Press, 2010.

【17】Ying Zhou. Reliability Design Based on FPGA [D]. Beijing University of Posts and Telecommunications, 2012.