IJR International Journal of Railway
Vol. 2, No. 3 / September 2009, pp. 127-130

The Korean Society for Railway

Research on Safety-related Communication of Railway Automatic Block Between Railway Stations System

Pei-yan Yun* **and Jin Guo****

Abstract

The system improves the safety and efficiency of railway transport, combining the advanced axle-counter with single-track semiautomatic block. Using computer, to accomplish relay-based semiautomatic block logic operation and axle-counter to check section status, it will further increase the performance of railway transport. Safety-related communication is one of the important topics in railway signal system. By referring to relevant safety-related communication standards, to research on safety-related communication of Micro-computer automatic block between Railway Stations System, the thesis introduces the basic requirements, concept model, codes, and the process, etc.

Keywords : *Micro-computer automatic block, Axle-counter, Safety-related communication*

1. Introduction

Micro-computer automatic block with axle-counter between railway stations system combined inter-station block and the axle-counter equipment, interval checking interlock control integration, the abolition of artificial arrival confirms that improve range traffic safety. Will be the station interlocking system, interval occlusion of equipment and range of joint monitoring equipment operator axis, inter-occlusion achieve automatic stations, improve transport efficiency. To occlusion of operation, the state of occlusion devices, including real-time action-axis equipment records, archiving for computer monitoring equipment to provide fault diagnosis information. Interval for the TDCS (Transport & Dispatch Control System) system is idle and occupied by the source of information for the realization of basic preparation CTC (Centralized Traffic Control) ready.

Inter-Block System automatically stops the full use of computer network data transmission capacity, change the previous occlusion devices have blocking action of positive and negative electric code transmission method, so that inter-station transmission equipment has been site traffic circle and equipment status information among the other station equipment seized intact situation. Occlusion information between the original station is only through the loop transmission, information is also required of the other axis accounted for channel transmission, the system of information transmission between stations should be able to achieve through the exchange of optical fiber and rail network dedicated channel transmission. Increase the starting signal, stop signal, the train position, blocking each other station equipment, such as station moves between the traffic information to traffic officers a more accurate plan, command and train operation.

Automatic station stops between the occlusion system between the communications and security are closely related. Automatic weather station because of the abolition of the artificial inter-occlusion to confirm integrity of the clearing interval train steps, how to determine the basis of the number of train axle clearance interval is required on an urgent problem. The most central point is how to send the correct inter-Axes. How to ensure that the system of information transmission between station security? Clearly, if we can not guarantee that information transmitted between station security, but also no way of guaranteeing the safety of rail transport.

2. Network Of Railway Automatic Block Between Railway Stations System

Automatic station stops between the occlusion system

* Institute of Information Science and Technology, Southwest Jiaotong University, No.111, Erhuanlu Beiyiduan, Chengdu, 610031, P.R.China
E-mail: yunpeiyan@hotmail.com
**E-mail: gj60@sina.com

between the network transmission channel through the railway network dedicated to exchange of 2 M interface can also be two special cables or fiber-optic ring network constitute the structure, station between two adjacent DC has physical access, continuous 4~5 stations can be cited a circuitous route. Station through the wide area network for inter-axis information, blocking information and other information transmission.

Stations from machine A, machine B and monitoring of machine components and through 10 M/100 M constitute LAN Ethernet switch, the various stations of the LAN through the WAN router to connect constitute. Occlusion machine A machine with B Hot Standby dual agency structure, to monitor the machine moves the process of recording equipment and the information transfer process, machine A, machine B and monitor the machine through the LAN information transmission, information transmission using standard TCP / IP protocol.

Through inter-network communication transmission station, a station occlusion machine A, machine B can stop occlusion and machine A, machine B set up information exchange between the links, constitute a redundant channel, so that A, B Station occlusion between any machine malfunction or interruption of communications, does not affect the occlusion of two stations operating. Station network structure as shown in Fig. 1.

3. The Required Safety For Communication

Authenticity, integrity and correct time of data shall be ensured. As the safety processes have no access to the internal functionalities of non-trusted circuits being part of the non-trusted transmission system the safety processes shall perform checking in addition to that provided by this equipment to ensure that faults do not go undetected.

Faults may occur when memory is contained in protocol circuits or in non-safety-related equipment. A safety-related message, stored in non-safety-related equipment, could be transmitted again at the wrong time. Protection against this fault shall be provided.

To maintain the required safety for communication between safety-related equipment the following requirements shall be fulfilled.

(1) If the source is not uniquely identified in the transmission system, authenticity shall be provided by adding a source identifier to the user data.

(2) Integrity shall be provided by adding a safety code to the user data. The safety process shall not rely on the transmission code generated and checked by integrated circuits being part of the non-trusted transmission system.

(3) The timeliness of user data shall be provided by adding time information (e.g. time stamps, sequence numbers, ...) to the user data. The time delay which is allowed depends on the application.

(4) If necessary the sequence of messages shall be checked by the safety process.

The following definitions are given:

Definition: RH is the hazardous failure rate of the complete transmission system; RHW is the hardware failure rate of the non-trusted transmission system; PUS is the probability of undetected failure due to the performance of the safety code; PUT is the probability of undetected failure due to the performance of the transmission code; fM is the maximum frequency of messages for one receiver; fW is the frequency of wrong (corrupted) messages; T is the time span, if more than a defined number of corrupted messages were received within this time, the safe fall back

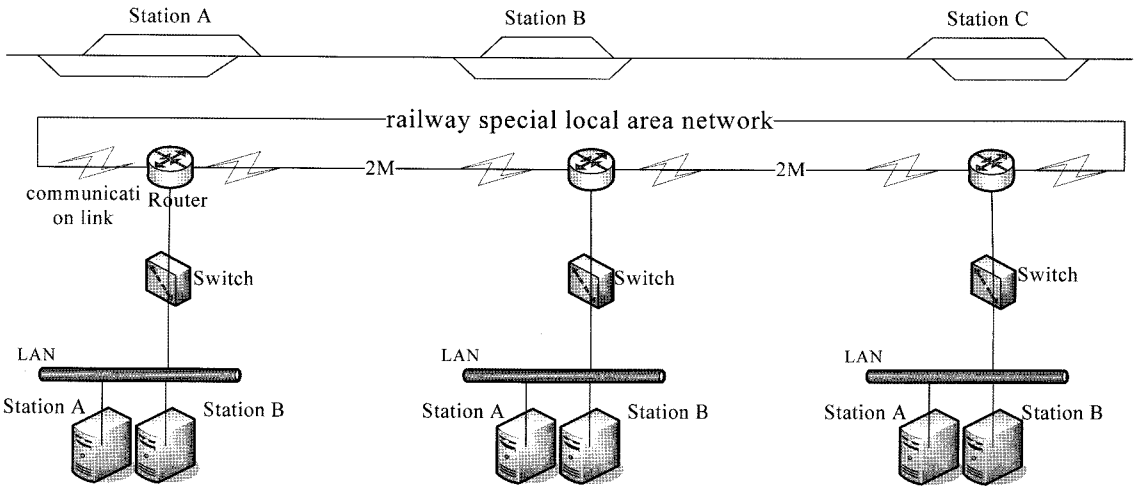

Fig. 1 network between stations

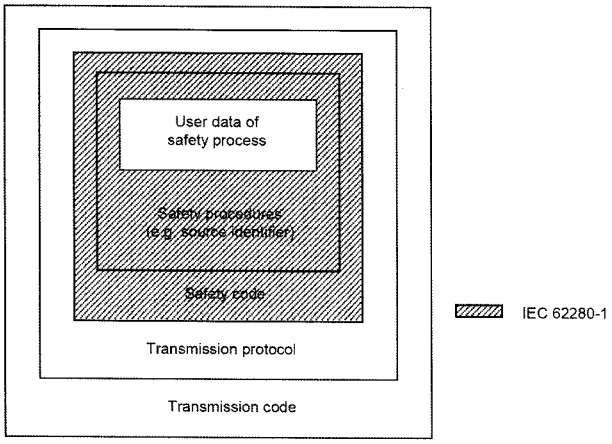

Fig. 2 Model of message representation on the transmission media

state will be entered; k1 is the factor for hardware faults including safety margin; k2 is the factor which describes the percentage of hardware faults that result in undetected disabling of transmission decoding; m is the safety factor included within k1; n is the number of consecutive corrupted messages until the safe fall-back state is entered.

With these definitions the following inequations have to be fulfilled:

$$R_{HW} \times P_{US} \times K_1 \leq R_{H1} \text{ (hardware faults)} \quad (1)$$

$$P_{UT} \times P_{US} \times f_W \times R_{H2} \text{ (EMI)} \quad (2)$$

$$K_2 \times P_{US} \times \frac{1}{T} \leq R_{H3} \text{ (transmission code fault)} \quad (3)$$

The sum of all three rates shall not exceed RH:

$$R_{H1} + R_{H2} + R_{H3} \leq R_H \quad (4)$$

Because it cannot be assumed that the failure is a random failure, it is necessary to take into account a safety margin m in the factor k1. The factor k1 shall be calculated according to the following formula:

$$k_1 \geq n \times m \quad (5)$$

The factor m represents the safety margin with $m \geq 5$.

The maximum frequency of wrong messages fW shall be estimated either by the worst case estimation fW = fM, or by limiting the maximum rate or number of wrong messages where safe counters and/or safe timers are implemented. If more than one wrong message within a definite time interval is received, the safe communication shall be aborted and the safe fall back state shall be entered. A mathematical derivation proves that a certain limit cannot be exceeded.

In cyclic transmission the frequency fM is well-defined. In the case of non-cyclic transmission, the maximum possible frequency must be taken. By using proper CRC, the maximum value of PUT may be estimated as

$$PUT = 2^{-b} \quad (6)$$

where b denotes the number of redundancy bits.

4. Safety-related Communication Methods For The System

Between the transmission station of the system state of the occlusion, the number of axes and other important information is to protect an important part of traffic safety, in accordance with the International Electrotechnical Commission IEC61508 (electrical / electronic / programmable electronic safety-related system security standard) definition, the transmission channel security level should be SIL4 level (safety integrity level, Safety Integrity Level); communications messaging security should be on secure communications to meet the foregoing requirements, therefore, between the transmission station of the item using the following measures:

(1) The transmission identification

The role of identification was to prevent non-licensed users to interfere with network communications.

The system used for identification of double test: first, check the sender's IP address for the current permit communications IP, followed through to the system settings for each station to determine the identity ID. Such as the system has at least A, B, C three stations, if A, B two points received from the communication station C data packets, you can determine this from the C stands for the interference packet.

(2) Check the integrity of information

Check the integrity of the role of information is subject to interference was to prevent tampering, insert and delete.

The use of Cyclic Redundancy Check code (such as CRC32) technology in the sending end and receiving-side validation code, through the use of a pre-agreed to get information to generate polynomial identification code, together with the information to send to the recipient, the recipient of received information re-calculation, will be the identification code with the received identification code to compare if the two are not the same, you can determine the information has been tampered with.

(3) Information in real-time test

System can detect the occurrence of delayed data. Because this system uses TCP / IP protocol, TCP is con-

nection-oriented end-to-end reliable protocol, and to ensure the order of transmission of data packets. So do not need to add a sequence number.

However, the data delay may occur because of the situation so required in the data add timestamps to protect transmission of real-time information.

(4) Detection of communication interruption

Because communication lines are not reliable enough, outside influence might cause communication interruption, required detection system detected.

By setting a delay to wait, such as scheduled during this period of delay, the detected hardware failure or line instability has led to communications connection is lost, then think communications interruption.

(5) The state of security protection

For communication failures that could lead to dangerous conditions, the establishment of a security state, can protect the system has a transmission-level fault-oriented security features.

In the transmission information to set a security status symbol, if there is an open-signal station in the hair after the communication failures such as interruption of communication lines, because we set the detection interrupt communications security communication function, then, after Detection of communication interruption should the safety Set status symbol to indicate the fault status at this time the risk of side-oriented, and can use the corresponding operation. The examples given here can be directly to the blocking state to "state failure." Can also be required under different circumstances to protect, for example, do not deal with occlusion, such as aircraft idling.

5. Conclusion

According to the railway signal system communication about safety standards to Computerized Automatic Block System of inter-station communication station security as the research object, this paper occlusion system to protect the security of communication between stations measures. These security measures can achieve communication between the communicating transmission station of the identity authentication, information integrity and real-time validation, communications interruption detection and state security settings. According to the calculation available through secure communications and secure communications encoding process protection, you can check undetected communication rate to 2×10^{-10}, can protect the transmission system with fault-oriented security features. Research results show that the proposed secure communication measures can effectively protect the safety of the railway.

Reference

1. Wen-yan Zhong, Jin Guo and Li-fang Liu. (2004). "Research on Computerized Automatic Inter-Station Block," *Proc. the China Association for Science and Technology.*, Vol.1, pp.236-238.
2. International Electrotechnical Commission. (2002). "IEC62280-1: Railway applications–Communication, signaling and processing systems–Part 1: Safety-related communication in closed transmission systems," *Commission Electrotechnique Internationale.*, pp.18-35.
3. Babak Dehbonei and Fernando Mejia. (1995). "Formal Development of Safety-critical Software System in Railway Signaling," *Prentic Hall*, pp.227-252.