ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 1246 -1251
doi: 10.18178/wcse.2017.06.217

An Improved Safety Control System for Rail Transit

Guantao Hu [1+]

System Safety Department, Zhejiang United Science and Technology Co., Ltd, Hangzhou, China

Abstract. An improved safety control system is designed and is composed of the reference signal generating unit, the processing unit, the output unit, and the dynamic & static read-back unit. A synchronization vote mechanism within dual channel is adopted to realize the safe and reliable output for this system. The processing unit is composed of a short-time detection pulse generation module, an output module, a short-time pulse decoding module and a static decoding module for realizing short-time detection pulse generation and decoding of the extraction signal. Testing results present this system has the characteristics of fast detection, high fault detection coverage and low failure rate, which can meet the requirements of safety and reliability in rail transit field.

Keywords: safety control system, reliability, safety, synchronization vote, read-back check

1. Introduction

In the field of rail transportation, the safety output system usually controls the corresponding signalling devices (such as signals, switch machines, propulsion control systems, train doors etc.) by driving external safety relays, because of the high reliability and safety. Therefore, beside the relays with high safety and reliability, their control systems must have a high requirement on the safety and reliability [1].

At present, there are two safety output methods commonly adopted in the railway industry. One is the static output mode that the control system directly outputs a high voltage to energize the external relay when needed. Another way is the dynamic output mode that the control system outputs a pulse signal with a certain frequency to charge the capacitors, which supply power for the external relay, when needed. In the second method, the asymmetry of charge and discharge can assure the capacitor voltage at a stable value to drive the external relay [2].

The biggest problem of first method is when the output circuit is stuck at a permanent state (on or off) the system can't detect this failure immediately and resulting in error output, which may lead to dangerous situations (derailment or collision). On another hand, the main issue of second method is low reliability and availability and high maintenance costs. Therefore, there are many improvement spaces in the existing control system in fault detection, anti-interference and reliability and availability [3].

In this paper, an improved safety control method for rail transit is proposed and implemented by adopting dual-channel drive, cross-check, coupled pulse detection and synchronization vote.

2. Improved Safety Output System

The improved safety output system is based on 2oo2 voting system with a reference signal generating unit, a dual channel processing unit, a dual channel output unit, and a dual channel static & dynamic read-back unit as shown in Fig. 1. In practical engineering applications, the multichannel output is realized by the output unit and read-back unit with multiple paths.

The reference signal generation unit is to generate a reference signal for the processing unit A and B

[+] Corresponding author. Tel.: + 86 13396539778.
E-mail address: huguantao@unitedmne.com.

which use this signal to synchronize each other and generate a dynamic pulse for checking the output circuit.

The output unit (A and B) are to drive the external relay by outputting a voltage which couples the short-time pulse detection signal.

The read-back unit (A and B) are to check the output circuit, acquire the read-back signal and send back to the processing unit.

The processing unit (A and B) are to control the system output, generate the coupling short time detection pulse, and determine the output state of dynamic and static detection. The processing unit is the core of the entire safety control system.

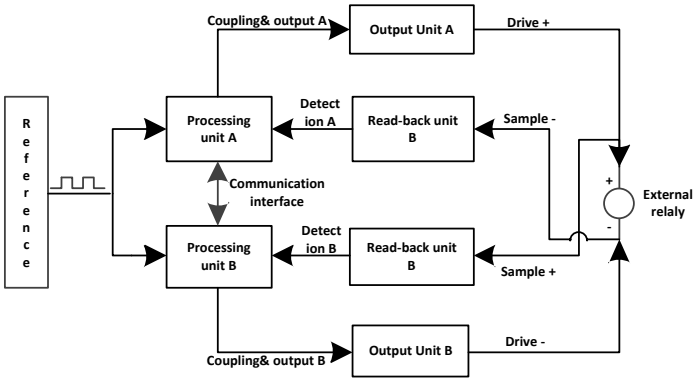

Fig. 1: Architecture of safety control system

2.1. Reference Signal Determination

The reference signal is a 50% duty cycle square wave. The frequency of this signal should not be too high or too low. The appropriate signal frequency is between 10Hz and 200Hz. In order to prevent interference, the power frequency should not be selected as the reference signal, such as 50Hz in China, 60Hz in USA.

2.2. System implementation

The dual-channel processing unit (A or B) exchanges information through the Fast Ethernet for achieving dual-channel data synchronization and voting.

Channel A and Channel B controls one terminal of the relay's coil respectively. Only when the output from the both channels is identical, the relay can be activated.

Cross-check mechanism is adopted in the read-back check, that is, channel A checks the output state of channel B, and vice versa. When one channel has failure, the other channel can detect such failure immediately.

Dynamic pulse decoding and static decoding are applied in read-back check. Dynamic pulse decoding module first collects the short-time coupled pulse signal from the output signal, second decodes and finally determines whether stuck-on or stuck-off failure happens. Static decoding module collects the actual output state, and determines whether the actual output state is consistent with the expected state.

The processing units within Channel A and Channel B use heterogeneous architecture. Channel A uses the POWERPC architecture, and Channel B uses the ARM architecture to reduce common cause failures.

2.3. Application of the system

Fig. 1 shows the 2oo2 voting structure of the safety control system. The voting structure is the most important method for assuring the system safety during system design. Only when the outputs of channel A and channel B are identical and the check states (including static and dynamic) of channel A and channel B are also identical, the system is in normal operation mode, otherwise the system will enter fail-safety state.

In actual engineering application, such as automatic train protection system, computer based interlocking system; 2x2oo2 system (one normal, one standby) is commonly used to achieve high reliability and availability in rail transit [4]. As a part of the whole safety platform, the safety control system finally presents within a 2x2oo2 architecture, which has been proven that it can greatly improve the overall

reliability of the system [5]. Fig. 2 shows the voting structure with 2x2oo2 architecture of the safety control system.

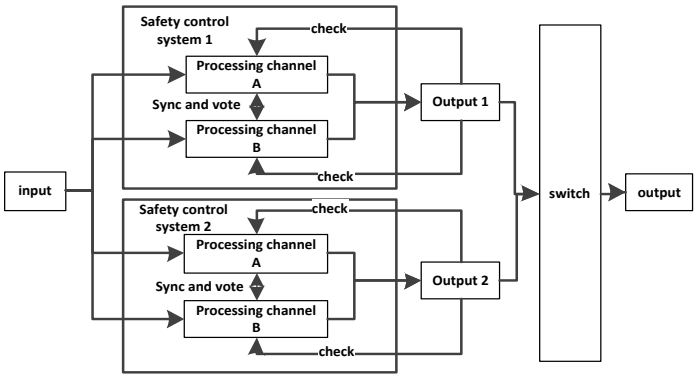

Fig. 2: Voting Structure of Safety Control System

2.4. Mechanism of safety control flow

The mechanism of safety control flow is shown in Fig. 3. The processing unit (A or B) generates the short-time detection pulse based on the reference signal generated by the reference unit, couples this signal to the output signal, collects the short-time detection pulse data and the static detection data through the read-back unit; the processing unit sends the collected static and dynamic detection data to the other processing unit for checking whether the detected data collected by the two processing units to be consistent with the pre-set state. And if not, the system will enter fail-safety state.

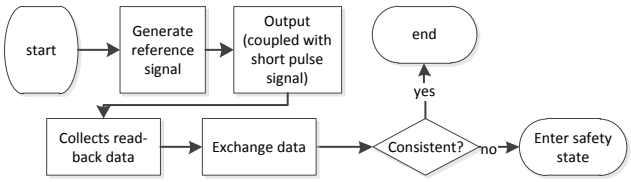

Fig. 3: Mechanism of Safety Control Flow

3. Main Functions of Safety Control System

The main functions of the safety control system include: short-time detection pulse generation; detection pulse coupling output; output read-back check. These main functions are described in the sections as below.

3.1. Short-time detection pulse generation function

The short-time detection pulses S1, S2, S3, and S4 are generated based on the Sref signal of the reference signal generation unit.

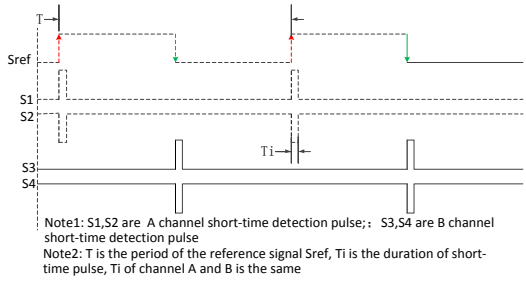

Fig. 4: Phase Relations between Sref and Short-time Detection Pulse

The specific method is: at the rising edge or falling edge of the Sref signal, short-time detection pulse will be generated. Channel A generates the short-time detection pulses S1 and S2 at the rising edge of the Sref signal, Channel B generates the short-time detection pulses S3 and S4 at the falling edge of the Sref signal. The phase relationship between the short-time detection pulse and the reference signal Sref is shown in Fig. 4. In the figure, " ↑ " means the rising edge of the reference signal and " ↓ " means the falling edge of the reference signal, T is the cycle time of the reference signal and Ti is the duration of the short-time

detection pulse. Ti is a critical parameter. If an improper value of Ti is selected, it will cause the malfunction of the external relay (for example, error drop-off). According to the actual relay connected, Ti is chosen usually less than 1ms.

3.2. Short-time detection pulse generation function

It is necessary to determine the correct signal to be coupled to the output signal according to current output, the specific coupling principle is:

Current output is logic "1" that means to energize the external relay, signal S2 shown in Fig. 4 should be coupled to the output signal from Channel A, signal S3 shown in Fig. 4 should be coupled to the output signal from Channel B. If the output circuit has no failures, the correct signals of Channel A and Channel B are shown in Fig. 5. OUTA in the figure represents the output signal of Channel A, and OUTB represents the output signal of Channel B.

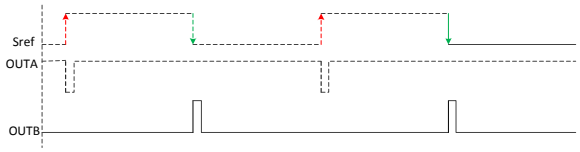

Fig. 5: Relations between Output Signal and Reference Signal as Output Logic is “1”

Current output is logic "0" that means to de-energize the external relay, signal S1 shown in Fig. 4 should be coupled to the output signal from Channel A, signal S4 shown in Fig. 4 should be coupled to the output signal from Channel B. If the output circuit has no failures, the correct signals of Channel A and Channel B are shown in Fig. 6. OUTA in the figure represents the output signal of Channel A, and OUTB represents the output signal of Channel B.

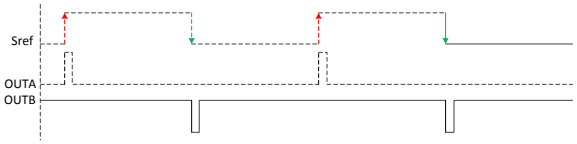

Fig. 6: Relations between Output Signal and Reference Signal as Output Logic is “0”

3.3. Output read-back check function

Output read-back check function is to determine whether the output is correct or not. It will check whether the stuck-on or stuck-off failures are happened and the output is identical with the expected state. This design will use two detection methods to realise this.

3.3.1 Dynamic pulse decoding

Dynamic pulse decoding can decode the read-back signal, so that the processing unit can determine whether the output circuit has adhesion failures. From the circuit shown in Fig. 1, Read-back detection circuit in Channel A checks adhesion failure for the output circuit of Channel B, and vice versa. According to Fig. 5 and Fig. 6, Channel A should detect the short-time pulse at the falling edge of reference signal Sref, and Channel B should detect the short-time pulse at the rising edge of reference signal Sref. The dynamic pulse decoding method is described below (Channel A as an example). Dynamic pulse decoding principle in Channel A is shown in Fig. 7. ConA signal from the processing unit would control the enable end of tri-state gate for collecting the short-time pulse from Channel B, and it (ConA) is a signal with coded information. If the Channel A processing unit can acquire the Channel B dynamic pulse, when is located in time of short-time pulse from Channel B output signal, the short-time pulse detection in Channel B is passed, otherwise failed.

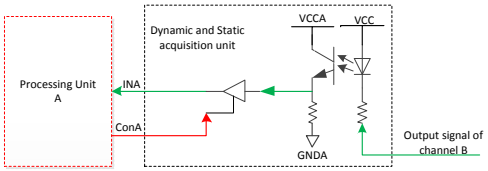

Fig. 7: Dynamic Pulse Decoding Module in Channel A

The relations among the dynamic detection signal (ConA), the Channel B output signal (OUTA) and the reference signal (Sref) is displayed in Fig. 8 (Channel B output logic is "1"), and the short-time pulse signal outputted by the Channel B is amplified for convenience. The detection concept for Channel B is the same as Channel A, and not described in words detail at here. The Channel A dynamic detection signal (ConA) can be encoded into 8bit, 16bit or 32bit, and also could be added CRC code for improving the anti-interference ability. In order to prevent mutual interference between adjacent channels, different channels can adopt different encoded dynamic pulses.

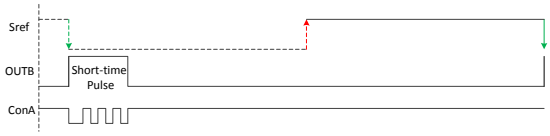

Fig. 8: Relations among Reference Signal, Dynamic Detection Signal (ConA) and Short-time Pulse

3.3.1 Static decoding

The processing unit cyclically decodes the read-back signal based on the reference signal Sref to determine whether the actual output of the circuit coincides with the expected output. This paper will still take Channel A as an example to state the decoding concept. The read-back principle shall be referenced as Fig. 7. ConA signal from the processing unit would control the enable end of tri-state gate for collecting the output signal from Channel B, and it (ConA) is a signal with coded information. If the processing unit A acquires the signal corresponded to ConA (detection signal sent by the processing unit A) in a Sref period, it can be seem that the actual circuit output is consistent with the expected output of the processing unit A.

The Fig. 9 (Channel B output logic is "1") shows the relations among the static detection signal (ConA), the Channel B output signal and the reference signal. The detection concept for Channel B is same as Channel A, so without stated again. The ConA can be encoded with 8bit, 16bit or 32bit, and also could be added CRC code to improve the anti-interference ability. In order to prevent mutual interference between Channel A and Channel B, the different channel can adopt different encoded dynamic pulses.

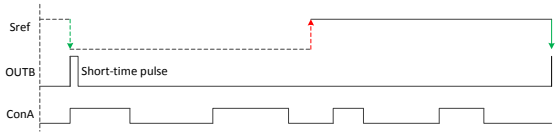

Fig. 9: Relations among Reference Signal, Static Detection Signal (ConA) and Short-time Pulse

The key point of the static decoding module is that the bit-width of the encoded signal per bit is much larger than the width of the short-time detection pulse (4 times or more) regardless of the encoding method used by the ConA signal, and the processing unit avoids the short-time pulse time window when sampling.

4. Realization and Result

The prototype for this safety control system has been designed, implemented, and passed the function and performance test in the laboratory, as shown in Fig. 10. VC1 and VC2 are heterogeneous safety processing boards, VOBs are safety output board, and CPSU is power supply board.

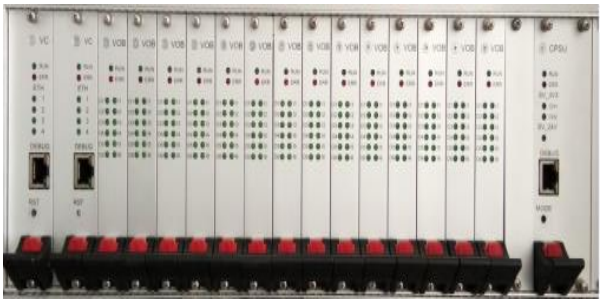

Fig. 10: Prototype of Safety Control System

The safety control system realizes the output and detection function. On one hand the system controls the behaviour of external relay; when the upper-layer command is received. On the other hard it provides detection information to help user for locating the failures.

In actual circuit, the fast optical-coupler is adopted in read-back unit to ensure the response time of the decoder circuit is in micro second level. The response time of the external relay is determined by the relay

itself. The response time of the relay used in experiment is about 1ms; the pulse period of reference signal is 18ms; and the system will enter fail-safety state, when errors are detected in three consecutive cycles. So in the worst case, the system will spend 55ms for getting into fail-safety state, i.e. 54ms data acquisition time for 3 cycles, and plus 1ms hardware response time.

The test result of hardware failure insertion is displayed in Fig. 11. The falling edge of purple line means the hardware fault insertion point, and low level of yellow line means the system entering a fail-safety state. Based on this waveform, the time from fault insertion to system being at safety state is about 55ms, which is consistent with the theoretical analysis value.

Fig. 11: Test Result of Hardware Fault Insertion

Professional software Isograph Reliability Workbench11.0 is used to predict the reliability parameters of each board and the values are listed in Table 1. The MTBF of the safety control system structured with dual 2oo2 is 1136850h and the availability is 99.99995% after calculated.

Table 1. MTBF and MTTR of Each Board

Board name	MTBF(h)	MTTF(min)
VC1	16360	30
VC2	15750	30
VOB	130600	30
CPSU	21340	30

5. Summary

This paper provides a design method for safety control system applied in rail transit. Comparing with the existing output control methods, this safety control system has wide detection range, high detection speed, and low failure rate. It also has higher safety and reliability. Accordingly, it has wide application prospect in the field of rail transportation and other similar safety control fields.

6. Acknowledgements

This work is supported by the funding from the National Science and Technology Infrastructure Program of China under Grant 2015BAG19B03

7. References

[1] International Electrotechnical Commission. IEC Std 61508-2-2010 Functional Safety of Electrical/Electronic Programmable Electr-onic Safety-related Systems[S]. 1997

[2] Lian-xian Zheng. Research on Optimum Design of Driving Circuit for Electromagnetic Relay [J] Technology Innovation and Application, 2013(21):48-48

[3] Yi Yang. Design of safety computer system output module and research on its reliability and safety [D] Zhejiang, Zhejiang University, 2012

[4] Guang-wu Chen, Duo-wang Fan, Zong-shou Wei, Ya-fei Fang, Dual 2 out of 2 electronic computer interlocking system [J]. China Railway Science, 2010, 31(4):138-144.

[5] V Chandra，KV Kumar. Reliability and safety analysis of fault tolerant and fail safe node for use in a railway signalling system. Reliability Engineering & System Safety, 1997, 57(2):177-183.