Safety Analysis and Design for the Switch Control Unit of All-electronic Computer Interlocking System

Tao He
Key Laboratory of Opto-Electronic Technology and Intelligent Control, Ministry of Education, Lanzhou Jiaotong University, Lanzhou, 730070, China
e-mail: hetao@mail.lzjtu.cn

Abstract

The switch control unit module is a critical core control module of the all-electronic computer interlocking system. Switch in the wrong place as the top event, use the Relex software for quantitative analysis of the importance of analysis method and found a key part of the module designs. The weak link in the system design through the use of the ‘2-Vote-2’ modular architecture analysis showed that the system has reached the security requirements of the railway signaling system.

Keywords: railway signaling, computer interlocking, All-electronic, Three-phase AC switches

1. Introduction

All-electronic computer interlocking system has good maintainability, so it is development direction of railway signal control system. Because internal structure of all-electronic computer interlocking system is relatively complex, it is quite necessary to use the safety analysis technology to design, and the fault tree analysis (FTA) [1, 2] is one of commonly used and effective methods to analyze system safety. In the railway signal control system, the crash, derailing and such high risk events are the top of the fault tree event. After analyzed the top event, the failure will come down to switch and signal equipment failure. In the switch control unit, the bottom events are ‘switch position error’ or ‘switch wrong turning’. For ‘switch wrong turning’ has been studied, this paper will use the alternating five-wire system switch indication circuit as the example. This paper’s focus is to analysis and design ‘switch position error’.

2. Working Principle of Switch Indication Circuit

The indication circuit module of the switch unit model is showed in Figure 1. The circuit consists of indication transformer, normal detection circuit, reverse detection circuit and control switch K11 to switch K15 of indication circuit.

Normal detection circuit and reverse detection circuit are into the CPU, which are analyzed by software, control switch of indication circuit is controlled by CPU. Figure 1 shows the equivalent circuitry of the switch in normal location. The working principle and process design of the circuit:

Step 1: CPU closes control switches K11, K13, K14 of the indication circuit, at the same time disconnects K12, K15, and records collected waveform of the normal detection circuit.

Step 2: CPU closes control switches K12, K13, K15 of the indication circuit, at the same time disconnects K11, K14, and records collected waveform of the reverse detection circuit.

Step 3: Refer to Table 1, the waveforms of the normal detection circuit and the reverse detection circuit are considered simultaneously, then current position information of switches are obtained synthetically.

3. Switch Indication Circuit Safety Analysis

As mentioned above, the FTA method is used in switch indication circuit safety analysis. Set the switch in the wrong place as the top event. According to the analysis, the risk of failure of the circuit has two causes, event A indicates that when the switch is in middle position, but
collected result is in normal, event A1 indicates that when the switch is in middle position, but collected result is in reverse, event B indicates that when the switch is in normal, but collected result is in reverse, event B1 indicates that when the switch is in reverse, but collected result is in normal. According to the symmetry of the circuit, the event A and A1 have the same safety as well as B and B1, so the paper takes the event A and B as the safety analysis objects.

![Figure 1. The equivalent circuitry of the switch in normal location](image)

Table 1. Waveform feature comparison matrix of the indicating circuit

<table>
<thead>
<tr>
<th>Waveform Feature of The Normal Detection Circuit</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waveform Feature</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Reverse</td>
<td>No</td>
<td>No</td>
<td>Reverse</td>
<td>No</td>
</tr>
<tr>
<td>Normal</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Symmetrical waveform</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Note:
(i) A——The asymmetric waveform that the upper half-wave is smaller, the lower half-wave is larger.
(ii) B——The asymmetric waveform that the upper half-wave is larger, the lower half-wave is smaller.
(iii) C——The symmetrical waveform that both of the upper and lower half-wave are smaller.
(iv) D——The symmetrical waveform that both of the upper and lower half-wave are larger.

3.1. Event A: The Switch Has no Indication, But Collected Result is in Normal (or Reverse)

In Figure 1, the equivalent circuit of the rail switch in normal, and the internal circuits of five-wire system switch machine. There are two kinds of situation in the equivalent circuit when the switch has no indication. First, moving contacts in switch machine have just left the group 3 connection point, and did not arrive the group 4 connection point, which was similar with the point A disconnected in Figure 1. Secondly, moving contacts in switch machine have arrived the group 4 connection point, which was similar with the short splice of point A and B in Figure 1. In Figure 1, the switch has no indication, which indicates that the detection circuit detects the waveforms as the upper and lower symmetrical sine wave (disconnected in point A), or detects the signal (short splice of point A and B). In order to make the waveform characteristics of the detection process more obviously, we designed the resistor 2 and resistor 4 for more large resistance, in which signal to noise ratio was also considered. The appropriate resistance of resistor 1, 2 and 4 were designed to 1KΩ, 4.7KΩ and 0.3KΩ respectively. We take different method and circuit to detect the upper and lower waveforms in the detection of the signal. FTA analysis was applied in event A, which use Relex tool5 to perform quantitative analysis. We can set up a fault tree (Figure 2), and calculate the security index of the event A was (3.16E-8)/h if system failure rate and repair rate could meet exponential distribution.
Note:
(i) Top—The switch is in middle position, but collected result is in normal.
(ii) G1—Error checking is in normal under the second condition.
(iii) G2—X2 is disconnected.
(iv) G3—Error checking is in normal under the first condition.
(v) E1, E6—Normal indication checks trouble.
(vi) E2—K14 is off.
(vii) E3—The line is disconnected.
(viii) E4—Connector is disconnected.
(ix) E5—CPU sends the wrong command.

Figure 2. The fault tree of event A

Note:
(i) Top—The switch is in middle position, but collected result is in normal.
(ii) G1—Error checking is in normal under the second condition.
(iii) G2—X2 is disconnected.
(iv) G3—Error checking is in normal under the first condition.
(v) E1, E6—Normal indication checks trouble.
(vi) E2—K14 is off.
(vii) E3—The line is disconnected.
(viii) E4—Connector is disconnected.
(ix) E5—CPU sends the wrong command.

Figure 3. The fault tree of event B
3.2. Event B: The Switch in Normal, Collected Result in Reverse (The Switch in Reverse, Collected Result in Normal)

Refer to 3.1, we can set up the bug tree shown in Figure 3, use the Relex tools for calculation, then get the safety indicators of the event B is (1.11E-16)/h.

4. Module Design

As mentioned before, according to results of the module safety analysis, especially safety index of the event A obviously does not meet the safety demand, hence the need for events in the fault tree of the A component importance analysis, so as to improve the important degree of the larger components. In the Relex software, the main computation is Birnbaum important degree (important degree of probability), Criticality importance (critical degree) and Fussell-Vesely important degree (importance degree of FV)[6]. Calculation of through Relex, the important values of bottom events as shown in Table 2.

### Table 2. The importance of bottom events

<table>
<thead>
<tr>
<th>CODE</th>
<th>Birnbaum</th>
<th>Criticality</th>
<th>FV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.00000000</td>
<td>0.9999928</td>
<td>0.9999928</td>
</tr>
<tr>
<td>6</td>
<td>7.22e-006</td>
<td>7.22e-006</td>
<td>7.22e-006</td>
</tr>
<tr>
<td>2</td>
<td>3.16e-008</td>
<td>1.58e-008</td>
<td>1.58e-008</td>
</tr>
<tr>
<td>5</td>
<td>3.16e-008</td>
<td>7.21e-011</td>
<td>7.21e-011</td>
</tr>
<tr>
<td>3</td>
<td>3.16e-008</td>
<td>4.40e-011</td>
<td>4.40e-011</td>
</tr>
<tr>
<td>4</td>
<td>3.16e-008</td>
<td>7.20e-006</td>
<td>7.20e-006</td>
</tr>
</tbody>
</table>

Note:
(i) Top——The switch is in normal, but collected result is in reverse.
(ii) G1——X4 is disconnected which is a bug.
(iii) G2——the switch is in reverse, but indication has been checked error.
(iv) E1——CPU software checking is wrong.
(v) E2——normal indication checking circuit is off.
(vi) E3——The line is disconnected.
(vii) E4——Connector is disconnected.
(viii) E5——R2 is off.

Figure 4. The fault tree of event a after the circuit improvement

We can be seen from Table 2 that important of the end of the event E1 is much higher than the other events, so it is necessary in the design of the lower ‘positioning said detection of
failure’ of probability. Therefore, in the design of data acquisition circuit used in the ‘2-Vote-2’ module of structure, its FTA as shown in Figure 4. The use of the ‘2-Vote-2’ module of structure, the security indicator of event A can achieve (9.98E-16)/h, at the same time the safety indicators of the event B can achieve (1.68E-27)/h, will bring shown in Figure 1 of the fault tree switch circuit. The available switch position error causes crash or off the Road safety indicators (1.996E-15) / h, to meet the system security index. To risk analysis of the entire signal system, the events A and B security indicators can be used as the basis of data analysis of the overall system security.

5. Conclusion

The five-wire switch module is the key modules in a fully electronic unit, which drivers the S700K series electric switch machine, ZDJ9 electric switch machine and ZYJ series electro-hydraulic switch machine, etc., and has broad application prospects. Through the analysis and design of the module, the module is able to meet the safety requirements of railway signaling systems. The module has been put into formal operation to use to good effect.

References