Development of train detection system by microwave balises, based on Safety Integrity Level and Safety Life cycle.

Tatsuya Sasaki, Noriyuki Nishibori
Railway Technical Research Institute
Hiroyumi Ogushi
Japanese West Railway Company
Takayuki Kasai, Yasuko Hidaka
Nippon Signal Co., Ltd

1. Introduction

Superannuated signal systems are still used on less busy lines of Japanese Railways, which have a problem in track circuits, on low short circuit sensitivity due to small density of trains. On the other hand, in order to cope with system requirements for higher safety, a safety guideline for computerized train control and protection systems was finalized by a specialists committee inclusive of the members of Railway Technical Research Institute, Japan, in 1996. The guideline covers the concepts of a Safety Integrity Level to indicate the class of safety, and a safety life cycle (from the conceptual design to decommissioning) of safety-related equipment to ensure the required security level.

The Guideline also recommends preliminary safety analysis of the Safety Life cycle. Therefore, we followed the Guideline in developing the solutions to these problems. This system differs from the rail-dependent train detection method, as it adopts microwave balises transmission between train and station equipment. The components of the system are a transmitter transponder placed to sandwich the rail, an on-board transmitter and a controller at stations. Therefore, the fail-safe technologies of this system are basically the same as those of existing closed-loop train detection systems except that a closed-loop configuration is achieved by wireless transmission. This system continuously detects trains between two adjacent points by a point detection method, because the pair of transmitters at the head and tail of the vehicle can transmit and receive information at the same time; the direction of train running is judged by the order of signal reception by different on-board transmitters, and the train is identified by this information.

With regard to the preliminary safety analysis, we extracted hazard analysis factors which might cause a system failure as safety requirements. We applied Fault Tree Analysis (FTA) to this analysis of the system with emphases placed on the train running direction by the point detection method. The hazards in this function are the failure of detection level (i.e. decision or non-decision), as well as on-board transmitter and train running direction errors. The causes of these failures have been detected. A precise specification has been prepared by these analyses. This system has been found not to cause events of risk.

In addition to the reliability of transmission, the interlocking and blocking functions have been verified by a field test at a Japanese Railway Company (JR).

2. System configuration

2.1 Equipment configuration

COMBAT comprises a microwave balise (interrogator, wayside responder and on-board responder) and a processing unit. The interrogator and wayside responder are installed close to the entering signal and starting signal, holding the track line in between. On local traffic lines, there is no room to allow installation of the equipment (construction gauge) between the tracks of up and down trains within the station yard. Since up and down trains do not travel at the same time close to the turnout point of the track (close to the starting signal), it is installed holding the up and down train tracks in between. For the reasons discussed above, when a standard turtle shell-shaped station as on a local traffic line is used as a model, interrogators and wayside responders are installed at four positions at each station, as shown in Figure 1. Each interrogator is connected with the processing unit. Two on-board responders are installed at each of the front and rear ends on the cars in units of train composition.
2.2 COMBAT specifications

Table 1 shows the COMBAT specifications.

<table>
<thead>
<tr>
<th>Type</th>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microwave balise</td>
<td>Regulations of Radio Law</td>
<td>Specific low power radio equipment(*)</td>
</tr>
<tr>
<td></td>
<td>Frequency</td>
<td>2.450GHz</td>
</tr>
<tr>
<td></td>
<td>Antenna power</td>
<td>10mW</td>
</tr>
<tr>
<td></td>
<td>Modulation method</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interrogator</td>
<td>Not modulated</td>
</tr>
<tr>
<td></td>
<td>Responder</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interrogator</td>
<td>Direct Sequence spread spectrum</td>
</tr>
<tr>
<td></td>
<td>Transmission rate</td>
<td>51.18kBPS</td>
</tr>
<tr>
<td>Processing unit</td>
<td>CPU configuration</td>
<td>Bus synchronous duplex system</td>
</tr>
<tr>
<td></td>
<td>Address data bus</td>
<td>32 bits</td>
</tr>
</tbody>
</table>

(*) Japanese radio law legislation

3. Microwave balise

The following describes the microwave balise which plays a major role in the implementation of train detection by COMBAT. The following describes the features of the microwave balise:

3.1 Features

1. Radio transmitter-receiver which uses a microwave balise.
2. Excellent performance against noise is ensured by the use of a spread spectrum communications system.
3. PN codes permit one interrogator to have simultaneous communications with multiple responders.
4. Stable communications are ensured by the use of circular polarized waves in a polarized wave system.
5. Improved functions at the receiving end eliminate the existence of a dead section, and provide an extensive communications range.
6. Safety is achieved by combining the radio equipment with the fail-safe processing unit.
7. There is almost no deterioration in performance when used under various meteorological conditions including rainfall and snowfall.
8. It conforms to the standard specification (RCR STD-29 : Japanese radio low) in the specific low power radio equipment.
3.2 Communications performance

Figure 2 shows the communications area for "interrogator to wayside responder" and "interrogator to on-board responder".

![Figure 2. Communications range](image)

4. Concept of train detection by COMBAT

The COMBAT train detecting function consists of point detection and block detection. The following describes these two detecting methods.

4.1 Point detection

In the COMBAT train detection, detection of the presence of, and up or down direction of, trains is carried out at the site where the ground-based microwave balise is installed.

1. Detection of train clear/occupied state

Train clear/occupied state is detected without contacting the train. A closed loop composed of radio communications is used in order to ensure the fail-safe capacity equal to or greater than that of the conventional track circuit.

The closed loop is composed of the interrogator and wayside responder with the track line sandwiched in between. This ensures that communications are normally established by the closed loop, as shown in Figure 3 when the track is clear of a train. When a train passes by, communications are interrupted as shown in Figure 4, and a detection logic is actuated. So the closed loop is also shut off in the event of trouble (Figure 5), and the track is assumed to contain a train (on the safety side), thereby ensuring safety.
Figure 3. No train passing by

Figure 4. Train passing by (normal interruption)

Figure 5. Failure (abnormal interruption)
(2) Direction detection

The forward direction of the train is detected by a pair of on-board responders. They store the train ID and installation position on the car as unique information. The forward direction of a train is specified at the detecting point according to the information on the receiving sequence and installation position. The forward direction of a train is detected at the wayside detecting point according to the sequence of reception by two on-board responders. In this case, continuity is required in switching signal reception. If continuous switching is not possible, an incorrect direction will be detected when the train runs forward and then backward close to the wayside detecting point (interrogator). The symbol <1> in Figure 7 shows the result of signal reception when the train passes by the detecting point taking the route of "a → b → c → d → e". The system cannot distinguish this case from the case where it passes by the detecting point taking the route of "a→ b → c → d → c" (changing the direction on the way). In our new system, continuity is ensured by simultaneous signal reception with two on-board responders, and correct detection of the direction is provided (<2> in Figure 6).
4.2 Block detection

The COMBAT train detection system constitutes a detection block with the microwave balise as a boundary. Entry/exit of the train to/from the block is detected according to the result of detection of the train existing/non-existing and direction shown in 4.1. This allows logically continuous train detection to be realized,
and use of the train ID ensures highly reliable detection (Figure 7). The following describes the entry/exit of the train to/from the block to the block and the train tracking logic.

1. Detection of entry

   Interruption of closed loop was assumed as a requirement (unconfirmed entry) for detection of entry into the block, as shown in 4.1 (1), with considerations given to fail-safe features. For the concept of this train detection, a unique ID is assigned to the train in order to ensure highly reliable train detection, and train tracking by the ID which moves between blocks was implemented (Figure 7). For train tracking, transition is made from unconfirmed entry to ID confirmed entry when the train ID is acquired at each detecting point (signal received from the on-board responder in Figure 8). Then the train having entered the block is identified.

2. Detection of exit

   Detection of exit from the block is carried out only for the train having agreement between confirmed ID and train tracking logic. Exit from the block on the rear side of the train is identified on the condition that the closed loop is established after reception of the signal from the on-board responder mounted on the rear end of the car.

   In this case, in order to improve the reliability of the exit condition, the rear end of the car is identified by detection of the train direction using the on-board responder, as discussed in 4.1 (2) (Figure 6). In this way, the block from which the train has exited is identified.
(3) Train tracking logic

Train tracking logic uses the following two theories to improve safety and reliability of train detection.

<1> Integrated management of train IDs in all blocks and carries out supervision to ensure that only one ID is present in the entire section.

<2> Supervision to make sure that block transition of the train ID is carried out only between the adjacent blocks.

5. A Priori (Preliminary) Safety Analysis

5.1 Safety Life Cycle

High-level safety is required for a train detection device which is part of safety control system. In developing the Computer and Microwave Balise Aided Train Detection System (COMBAT), therefore, we followed the concept of safety guidelines which are based on IEC 1508. The guideline consists of two concepts, the safety life cycle and the safety integrity level that represents safety grades (Figure10). The guidelines define the safety function of the safety control system to be realized by the management and technological activities over the entire safety life cycle. The safety guideline cites the processes of conceptual design, a priori (preliminary) safety analysis, design, manufacture, operation, maintenance and modification to define the activities implemented in the safety life cycle. The safety integrity level specifies levels 0 to 4, of which the level 0 means irrelevant to safety and level 4 the highest safety level. By following the safety (levels) defined by the integrity level, therefore, it is possible to ensure safety efficiently with each device as a unit. We extracted hazards by the hazard analysis of system functions, and created the principles to maintain safety and requirements therefor by analyzing hazards that might lead to (that will cause) accidents.

In the a priori (preliminary) safety analysis of COMBAT, we compared the conventional system and a hypothetical system using COMBAT and extrapolated possible configurations of the equipment to comply with the present railway infrastructure regulations.
5.2 Hazard Analysis

5.2.1 Extraction of Hazards

We assumed events in which normal functions don't hold (abnormal events) and specified the hazards arising in each category.

(1) Transmission performance
   (a) Faulty transmission between interrogator and responder on the ground
   (b) Faulty transmission between interrogator to/from on-board responder

(2) Detection of direction
   (a) Faulty transmission of train direction information
   (b) Faulty transmission between interrogator to/from on-board responder

(3) Train occupancy management
   (a) Faulty detection of the state of train clear/occupation
   (b) Faulty detection of train entry
(c) Faulty detection of train exit
(d) Faulty memory of train occupation
(4) Parallel track management

5.2.2 Specification of Hazards
To specify hazards, we extracted causes of improper (inappropriate, incomplete, or defective) control of the train in the detection block that will lead to a derailment or collision. It is possible to eliminate dangerous elements, therefore, by designing the detection system (detection device) in consideration of the specified hazards. We applied fault tree (FT) analysis to develop the system (Figure 11).
1: Error of detection of train clear / occupied state.
2: Train clear at detection block.
3: Malfunction in detection of exit of train from the block.
4: Malfunction of entry of the train to the block.
5: Device trouble.
6: Electrical power failure.
7: Failure during division or amalgamation.
8: Malfunction of restoration management.
9: Malfunction of detection of entry.
10: Malfunction of detection of exit.
11: Illegal interruption.
12: Unconfirmed entry
13: Non-received from the on-board responder.
14: Abnormal receiving responder
15: Interruption detection delay by the management speed defect of detection job
16: Malfunction of direction of detection (forward direction at head side)
17: Malfunction of direction of detection (backward direction at rear side)
18: Malfunction of direction of detection (forward direction at rear side)
19: Installation position defect
20: Closed-loop interruption defect by the body
21: Detect responder as on-board responder
22: Regular sign disturbance
23: Transmission circuit defect
24: Rationality check
25: Failure

Key
26: The combination of the basic matter
27: a matter
28: A switchover to the part of relates
29: OR
30: AND
31: An occurrence matter with the condition

Figure 11. FTA
5.3 Hazard Analysis for Direction Detection

We performed hazard analysis for all functions of the device. Since this device is based intermittent detection, it is required to detect train direction correctly, even if it moves back and forth at the detection point. We will concentrate below, therefore, on the analysis of direction detection which is one of the most important factors to ensure safety.

<table>
<thead>
<tr>
<th>Fault</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition transition defect</td>
<td>1. It is unusually received from on-board responders.</td>
</tr>
<tr>
<td></td>
<td>2. It is unusually received from responder on the ground.</td>
</tr>
<tr>
<td></td>
<td>3. A transition defect from the management device defect.</td>
</tr>
<tr>
<td></td>
<td>4. A logic mistake after the direction detection defect.</td>
</tr>
<tr>
<td></td>
<td>5. The transition which was dependent on the management order</td>
</tr>
<tr>
<td>On-board responder defect</td>
<td>1. Identification defect of on-board responder</td>
</tr>
<tr>
<td></td>
<td>2. Position defect of on-board responder</td>
</tr>
<tr>
<td>Mistake of train identity</td>
<td>It is mistaken for the information on other trains.</td>
</tr>
<tr>
<td>Direction fixed defect</td>
<td>1. A receiving condition defect from on-board responder</td>
</tr>
<tr>
<td></td>
<td>2. Do not receive from on-board responder</td>
</tr>
<tr>
<td></td>
<td>3. The defect of contents of a frame on-board responder</td>
</tr>
</tbody>
</table>

5.3.1 Extraction of Hazards in Direction Detection

The direction is judged based on the transition of the receiving condition from two on-board responders. An abnormal event occurs when the transition is abnormal or improperly processed.

5.3.2 Specification (Identification) of Hazards in Direction Detection

Defects in the receiving condition to determine the direction may occur at the on-board transponder A or B, or at both transponders simultaneously. The duration of an improper receiving condition may or may not affect direction detection. In the a priori safety analysis, therefore, we identified the events on the danger side that will affect the direction detection. With regard to these events, we summarized the judgement conditions for point detection and those for block detection that make the basis of the logic of train detection in the detailed detection logic design. As a result, we were able to confirm that events on the danger side would not occur even when the receiving condition of on-board responders was abnormal.

5.4 Specification for Safety Requirements

In the specification for safety requirements, we clarified the principle of safety functions according to the definition of the operation on the safety side based on the results of hazard analysis. We also determined a format for the requirements for safety integrity level and a written procedure to control design documents. The aforementioned guideline prescribes the requirements to ensure the safety of safety devices using micro-electronic technology. Since the specification of the requirements for the safety functions of COMBAT is based on these
requirements, we adopted a CPU of redundancy composition centering on a bus comparison and collating circuit as a fail-safe system configuration. We also designed the system to assume that a train exists in the relevant block when a failure has been detected and we defined operations to ensure safety for detailed items of each hazard.

Table 3 Definition on the safety side movement in the hazard occurrence

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Definition on the safety side movement</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>The defect concerned with the closed-loop</td>
<td>Interception of closed-loop</td>
<td>Occupied state</td>
</tr>
<tr>
<td>The defect concerned with the direction detection</td>
<td>Direction not specified</td>
<td>Occupied state</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Train identification is uncertain.</td>
</tr>
<tr>
<td>The defect concerned with control of a train existing</td>
<td>Train detection but not identified</td>
<td>Detection &amp; non-identification maintained</td>
</tr>
</tbody>
</table>

In the specification of safety requirements, we determined the safety integrity level, redundancy configuration and means to realize fail-safe composition of devices.

In IEC 61508, the definition of safety integrity level is a key among the processes in the early stage. Safety integrity levels are specified by the gap between a target safety level (i.e., tolerable risk) and the original system level without additional safety measures (i.e., original risk), and hazard and risk analyses are the basis for these quantitative analyses. In order to compensate for the risk gap with appropriate safety measures, the safety integrity level is defined. The question is how we are able to manage these processes quantitatively.

Hazard analysis specifies factors which might cause failure to the system concerned. Usually FTA is applied to this analysis. FTA's main concept is to specify failure causes in a top-down manner. However, the important thing is that there is no guarantee that FTA covers all the possibilities which cause failure. Bottom-up approaches, such as FMECA, should also be included and the specialists' reviews are crucial. The benefit of using both of these analyses is that the confidence in insight into the system concerned is enhanced and that it is disclosed where safety measures are necessary. Especially in a case of completely new systems, such as a train control system by radio, there are no other practical alternatives which specify failure causes.

After identification of hazard, IEC 61508 requires risk analysis, which allocates quantitatively probability of occurrence of harm and the severity of that harm to each hazard. It is, however, not easy to estimate the probability of the occurrence because of the variety and complexity of objects which train control systems deal with, and for the same reasons statistics gained from actual use and experience tend to be insufficient. Especially in the case of new systems, it is difficult to specify the value when we face train control systems which we have not had before. Databases must be assembled.

As mentioned above, there is some uncertainty in quantitative risk analysis. It looks rather
practical to allocate the top safety integrity level to railway signaling systems and adopt the fail-safe principles. For non-safety critical parts, less high safety integrity should be allocated mainly because of cost. In this context, IRSE’s table which provides the safety integrity levels proposed by major European railways is applicable (IRSE, 1992). Hazard analysis can be utilised so as to specify all safety measures corresponding to each hazard cause, rather than for quantitative risk analysis. This approach is more appropriate for railway signaling systems because a deterministic way has more value than numerical probability random failure.

We set the level 4, since COMBAT is a railway signal system that adopts the fail-safe principle to prevent accidents of derailment and collision.

6. Field monitored traveling test

Dynamic field monitored test was carried out at Kanno Station on the Kakogawa Line, and the evaluation shown in Table 2 was made.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Period</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 3</td>
<td>Nov. 2000 to March 2001</td>
<td>Verified train control system including operation management by a station system consisting of train detection logic, interlocking logic and a center system.</td>
</tr>
</tbody>
</table>

* 1ID: A responder device which allows one-to-one communication with the responder.
* 2ID: A responder device which allows simultaneous communication with multiple responders.
7. Afterword

In the developmental process, we designed the system to reflect the results of the a priori (preliminary) hazard analysis, tested it on a JR line, and confirmed that the system is safe and has satisfactory basic performance.

We expect that the system will be put to practical use soon.
References:


(3) Sasaki, Nishibori, Ohgushi, Kawachi and Kasai: "Development of Train Detection System by Microwave Balises," 2000, Industrial System at the National Meeting of Institute of Electrical Engineers of Japan, 4-231

(4) Nishibori, Sasaki, Kawai, Ohgushi, Kawachi and Kasai: "Field Test of a Train Detection Device based on Microwave Balise (COMBAT) and Implementation of Train Detection by Non-contact Train Tracking Technique," 37th Railways Cybernetic Symposium Session, 8, 620

(5) Nishibori, Sasaki, Kawai, Ohgushi, Kasai, and Toyoda: "Development of Tracking Train Detection Device (COMBAT) by Using Wireless Communication" 2001 IEEE/ASEME JOINT RAIL CONFERENCE