Method forVerifying System Requirement Specifications Based on Train Control System Safety Requirements

Koji IWATA
Senior Researcher, Train Control Systems Laboratory, Signalling and Transport Information Technology Division

A high level of safety is required for train control systems. It is important to apply all required safety measures to train control systems without any omissions. As many more functions are required in recent train control systems than before, it is necessary to divide the design phase into the conceptual design phase and the detailed design phase, in order to avoid system design complexity. In this paper, in order to conduct this appropriately, the template of safety requirements and a method of verifying the specifications of the system requirements with this template are proposed. The procedures are illustrated by applying the proposed method to CARAT (Computer And Radio Aided Train control system) as an example. Moreover, to apply this method efficiently, a support tool was built to verify safety requirements, and which displays safety verification items to be checked in the system requirement specifications automatically.

Keywords: train control system, system safety requirements, safety

1. Introduction

More than 20 years have passed since electronic interlocking devices based on microcomputers were introduced [1]. As CPU performance improves, there has been an increase in the variety of the functions implemented by the software on the FS-CPU boards (Fail-Safe CPU boards) dedicated to equipment requiring a high level of safety. As a result, systems have a growing number of functions which improve their availability and maintainability, etc. than before. The number of types of equipment connected to networks is also increasing, while the size of this equipment is getting smaller. Devices, which are installed outside the equipment rooms, such as signals, can also have processors [2].

On the other hand, international standards, such as IEC 62278, IEC 62279, IEC 62280, IEC 62425, are published, and it becomes more important to define system lifecycles and SIL (Safety Integrity Level) according to the required safety levels, to apply safety analysis, and to take appropriate safety measures.

In train control systems, it is important to define the whole system specifications without any omissions in order to ensure safety. The latter specifications are positioned high up in the system lifecycle and play an important role to ensure system safety and availability. Given the manifold increase in train control system functions aimed at securing safety, it is important to define safety measures of train control systems as a whole, not only including software but hardware as well, and to manage individual safety function requirements systematically. It is also necessary to establish a mechanism for realizing these requirements in the systems exactly. As it is necessary to show safety check lists automatically in order to manage these safety requirements appropriately, we propose a template for safety requirements and a method of verifying specifications from the viewpoint of safety with this template.

2. Causes of train control system failures

The causes of train control system failures were analyzed on the basis of data recorded by the electronic interlocking devices. Figure 1 shows the results of failure record analysis in the test compared with the current commissioning systems at about 5 months of the development phase of devices categorized as terminal control parts. Results indicate that half of the number of the failures can be attributed to system requirement specifications, demonstrating the importance of making system requirement specifications clear and of applying appropriate measures.

System requirement specification errors were traced back to the software specifications used with the hardware,
and the specifications defining the input-output control timing between different kinds of equipment, etc., illustrating the importance of making these specifications clear.

3. Method for verifying specifications based on safety requirements

The definition of specifications at the conceptual design phase can greatly affect the detailed design phase further down in the process. Failure record analyses also show that many failures stem from errors in defining system requirement specifications. This singles out the conceptual design phase as being critical. The safety requirements for this phase are made up of requirements contained in train control system guidelines [3] and those specific to each type of safety technology. These defined requirements can complement those which have been lacking until now.

3.1 Proposed template for safety requirements

One of the unique features of the proposed safety requirement template is that it is systematically configured. More specifically, in consideration of the order of the measures to be applied, they are classified into the inherent safety measures and the additional safety measures (Fig.2).

Safety requirements are defined on the basis of the individual functions making up the train control systems. Inherent safety measures, which remove the hazardous event in the systems by control logics or hardware configurations, are defined in the inherent safety measures field. Additional safety measures, for detecting faults or errors during input, process and output, and the safety controls, which are activated after detection of faults or errors, are defined in the additional safety measures field. It is important to keep the status on the safe side after detection of faults or errors.

Each field of inherent safety measures and additional safety measures shown in Fig. 2 has input, process and output fields. These measures are linked with constraint conditions shown in FTA (Fault Tree Analysis), and fault detection measures shown in FMEA (Failure Mode and Effects Analysis).

This template clarifies the measures to be applied and include not only those stemming from fault or error detections, but also those linked to control logics. This process helps to avoid omitting any of the measures to be applied.

3.2 Verification of specifications based on safety requirements

Figure 3 illustrates the proposed method to verify the system requirement specifications, using the safety requirements template (Fig.2).

(1) Step 1: Definition of system configurations and function block diagrams

This step defines each function block making up the train control systems, input and output between these functions, and system configurations are defined. The safety requirements of each function are defined using the template shown in Fig.2.

(2) Step 2: Verification based on safety requirements of each function

System requirement specifications are checked per individual function. More specifically, it is checked whether the train control system safety requirements relating to the system to be developed are defined in the system requirement specifications or not.

(3) Step 3: Verification of consistency between train control system application functions and the FS-CPU boards

Consistency of safety requirement specifications for multiple functions in the train control systems is verified. More specifically, specifications verified in Step 2 are checked for consistency, based on input and output relations between functions, and those between FS-CPU boards and train control system applications.

![Fig. 3 Verification of specifications based on safety requirements with proposed safety requirements template](image)

4. Case study on the proposed method for verifying specifications based on safety requirements

To illustrate the proposed verification procedure it was applied to the conceptual design phase of CARAT (Computer And Radio Aided Train control system) [4] by way of example, which has essentially the same functions as JRTC.
(Japan Radio Train Control System) [5] recently published as a Japanese Industrial Standard. In this system, the train position is calculated by on board control processing units and transmitted to the ground control processing units; based on this information train interval controls and route settings are conducted.

4.1 Step 1: Definition of system configurations and function block diagrams

Figure 4 shows the function block diagram applied to the CARAT. Table 1 lists the functions related to the FS-CPU boards and the train control system applications. In this example, all train control system application functions are installed on one FS-CPU board in the on board control processing unit or one FS-CPU board in the ground control processing unit (Fig.4).

4.1.1 Overview of each function

(1) Train control system application functions

Functions of the train control system applications are shown in Table 1 (from F1 to F6). The movement authority setting function (F4) in the ground control processing unit is described as follows:

(a) Acquisition of train positions, route status and other conditions

All train positions are received from each of the on board control processing units in the control area of the ground control processing unit. Conditions of route settings and other conditions are also inputted.

(b) Setting of movement authorities

Movement authorities of each train in the control area are set based on all train positions, status of route settings and other conditions.

(c) Transmission of movement authorities

Movement authorities are transmitted to the on board control processing unit of each of all trains.

(2) FS-CPU board functions

FS-CPU board functions are as shown in Table 1 (from F7 to F19). For example, as for the overview field of the process part function (F8), it is prescribed that output values are calculated based on the defined calculation process with the input and memorized values.

4.1.2 Definition of safety requirements

Safety requirements are as defined in the inherent safety measures (control logics or hardware configurations) field, and the additional safety measures field. Each field has input, process and output fields.

(1) Train control system application function

The process field for the movement authority setting function (F4) as for the inherent safety measures (control logics or hardware configurations) and the additional safety measures are illustrated in Table 2. In this example, safety requirements defined as the additional safety measures are the same as part of the inherent safety measures, differing however in purpose because diagnosis in the additional safety measures is applied as a backup in order to confirm no effects caused by latent faults or errors. In case

<table>
<thead>
<tr>
<th>ID</th>
<th>Category</th>
<th>Function name</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Train control system application</td>
<td>Train interval control and route setting</td>
</tr>
<tr>
<td>F2</td>
<td>Speed detection</td>
<td></td>
</tr>
<tr>
<td>F3</td>
<td>Speed check and brake control</td>
<td></td>
</tr>
<tr>
<td>F4</td>
<td>Movement authority setting</td>
<td></td>
</tr>
<tr>
<td>F5</td>
<td>Interlocking</td>
<td></td>
</tr>
<tr>
<td>F6</td>
<td>Support for maintenance work</td>
<td></td>
</tr>
<tr>
<td>F7</td>
<td>FS-CPU board</td>
<td>Input, output, process, comparison check</td>
</tr>
<tr>
<td>F8</td>
<td>Input</td>
<td>Process</td>
</tr>
<tr>
<td>F9</td>
<td>Output</td>
<td></td>
</tr>
<tr>
<td>F10</td>
<td>Comparison check</td>
<td></td>
</tr>
<tr>
<td>F11</td>
<td>System management</td>
<td>Redundancy management</td>
</tr>
<tr>
<td>F12</td>
<td>Mode(operation or maintenance)</td>
<td>Management</td>
</tr>
<tr>
<td>F13</td>
<td>Power on process</td>
<td></td>
</tr>
<tr>
<td>F14</td>
<td>Power off process</td>
<td></td>
</tr>
<tr>
<td>F15</td>
<td>Reinitialization process</td>
<td></td>
</tr>
<tr>
<td>F16</td>
<td>Maintenance</td>
<td>Download of program or data</td>
</tr>
<tr>
<td>F17</td>
<td>Changeover of version</td>
<td></td>
</tr>
<tr>
<td>F18</td>
<td>Test support</td>
<td></td>
</tr>
<tr>
<td>F19</td>
<td>Operation record and failure management</td>
<td></td>
</tr>
</tbody>
</table>
faults or errors are detected through diagnosis as shown in the additional safety measures field of Table 2, safety controls are applied (for example, output of a red aspect).

To guarantee safety, it is most important to maintain the reliability of control logics, given that rational checks shown in the additional safety measures are unable to detect all errors.

(2) FS-CPU board function

Table 2 shows FS-CPU board functions (for example, process function (F8)), inherent safety measures (control logics or hardware configurations) and additional safety measures. Note that, after faults or errors are detected through the diagnosis shown in the additional safety measures field of Table 2, safety controls (such as halt of processes, and stop of outputs) are applied, and system output, containing faults or errors, is cut out.

Table 2 illustrates how control logics or hardware configurations are as important as detection of hardware faults and safety controls to secure safety.

4.2 Step 2: Verification based on safety requirements of each function

Checks are carried out by checkers to determine whether train control system safety requirements built during Step 1 are defined in the system requirement specifications.

4.3 Step 3: Verification of consistency between functions of train control system applications and FS-CPU boards

(1) Consistency between train control system applications

Consistency between train control application system requirement specifications is verified. Relations between input and output of various functions are based on the function block diagram defined in Step 1 (Fig. 4).

For example, in the consistency between speed check and brake control function (F3) and the movement authority setting function (F4), movement authorities, which are transmitted from F4, are verified in terms of the definitions of movement authorities, and related rational checks inter alia.

(2) Consistency is then checked between train control system application functions and FS-CPU board functions. Information linking functions is based on relations between FS-CPU boards and train control system applications, defined in Step 1. For example, the definition in the FS-CPU boards that the data, such as 0, 1, is classified into safety status and dangerous status is checked for consistency with the status in the train control system applications, which are installed in the FS-CPU boards.
5. Support tool for verifying specifications based on safety requirements

When system requirements are drawn up, they are checked against the safety requirements defined according to the template shown in Fig.2. The number of verification items in the system corresponding to the functions shown in Table 1 is as follows:

As for Step 2, 7 fields (Fig. 2) multiplied by 19 functions equals 133 fields.

As for Step 3, 7 fields multiplied by 6 functions for the train control system application equals 42 fields, and these fields are compared with the 13 FS-CPU board functions. As a result, 546 fields are verified in this step. Consistency between input and output of train control system application functions, means checking 5 interfaces between the functions defined in Fig.4 multiplied by 7 fields twice (dual directions) which equals 70 fields. Moreover, to verify that there are no effects between the 13 FS-CPU board functions, \( \binom{13}{2} = 78 \) times 7 fields equals 546 fields. Note that, as the detailed verification items are defined in each field, the number of verification items can potentially be very high.

These results show that the method may be useful for applying the safety measures appropriately to define the safety requirements systematically, but also demonstrates the need for support tools. Such a tool was therefore built to offer greater efficiency and effectiveness.

The support tool can display the verification items automatically, and is built with Microsoft Access 2010. For example, as for Step 2, the items which have been verified can be marked in the check box. Each safety requirement is linked to a chapter or section No. in the targeted system requirement specifications. They are also linked to constraint conditions in FTA, in order to make the purpose of the safety measures clear (Fig.5). As for Step 3, verification items for consistency between train control system application functions are automatically displayed based on the input or output relations. Table 3 shows these relations between functions defined in function block diagrams. Verification items for consistency between system require-

Fig. 5 A screen shot of support tool for verification of specifications based on safety requirements

<table>
<thead>
<tr>
<th>Function name (ID)</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train position calculation (F1)</td>
<td>F3</td>
<td></td>
</tr>
<tr>
<td>Speed detection (F2)</td>
<td>F3</td>
<td></td>
</tr>
<tr>
<td>Speed check and brake control (F3)</td>
<td>F1, F2, F4</td>
<td>F4</td>
</tr>
<tr>
<td>Movement authority setting (F4)</td>
<td>F3, F5</td>
<td>F3, F5</td>
</tr>
<tr>
<td>Interlocking (F5)</td>
<td>F4, F6</td>
<td>F4, F6</td>
</tr>
<tr>
<td>Support for maintenance work (F6)</td>
<td>F5</td>
<td></td>
</tr>
</tbody>
</table>
ment specifications of the train control system applications and FS-CPU boards are also automatically displayed, based on the relations between FS-CPU boards and train control system applications, defined in Step 1. Verification items for consistency between functions related to FS-CPU boards are also automatically displayed.

6. Conclusions

A high level of safety is required for train control systems. It is important to apply all required safety measures to train control systems without any omissions. To achieve this, a template of safety requirements and a method for verifying the specifications of the system requirements using this template are proposed. The procedures were illustrated by applying the proposed method to CARAT. Efficient application of this method however requires a support tool, which was developed and built. This tool displays safety verification items to be checked in the system requirement specifications automatically. These defined safety requirements are reusable for the same type of control logics, and also contribute to safety technology progress.

References