Applicability Analysis of Software Testing for Actual Operating Railway Software

Jong-Gyu Hwang[1], Hyun-Jeong Jo[1] , Baek-Hyun Kim[1], Jong-Hyun Baek[1]

[1] Korea Railroad Research Institute, 176 Cheoldo Bangmulgwan-ro, Uiwang-si, Gyeonggi-do, 437-757, South Korea
{jghwang, hjjo, bhkim, jhbaek}@krri.re.kr

Abstract. Many function of train control system is being operated by according to the development of computer technology. The source code testing to validate safety becomes to be more important, and related international standards highly recommend inspections on the source code also. For this purpose, studies in relation to the development of source code validation tool were started from several years ago. To verify the developed testing tool, the applicability test was performed for the railway signaling system being. This paper represents the result of application test for this actual source codes.

1 Introduction

Train control system which is in charge of the most core function in a railway system is changing from the existing electrical device to the computer-based control system in accordance with the development of the recent computer technology. Accordingly, many parts of the main functions of train control system are operated by the software, and the dependence on software has been increased continuously. As the train control system software becomes more complex, the importance of software taking up in the railway signaling system is increasing further.

Safety requirements for railway signaling system software were internationally standardized by IEC 61508[1] and IEC 62279[2] recently. There are several efforts to study for software testing tool, but those are not suitable for railway signaling system software like vital one required high level safety[3][5]. And also, the validation on software is mainly dependent on the document for development process, and the quantitative analysis by testing is being accomplished only for a fraction of it.

It is the situation where the software testing is highly required in the international standards in relation to the system software. Especially, in the “A.4 software design and development” of [2], it is required that the “design & coding standards" must be observed in the design and development of SW-SIL(Software Safety Integrity Level) 3 or 4 grade software highly recommended. Provided, however, the guideline to coding standard is presented in the inside of document for international standards in a qualitative form, and it takes the form of compliance by determining coding standards by actual project. Accordingly, the coding standard with which the train control system software must comply was drawn in Korea through the analysis on [1]&[2] which

are international standards in relation to the software safety, and the studies on this drawn coding standard, MISRA-C which is the software coding standard for embedded control system being applied to the motor industry[4], and the automated validation tool to support the drawn coding standard were performed[5].

This paper performed tests through the application to train control system being applied to the existing actual domestic railway sites through automated testing tools for coding standard of railway signaling system software, and analyzed their results. The existing system which was the target for application is the system having been applied before international standards were introduced in Korea. We would like to check the effectiveness of validation tool being developed through the test and analysis on result for the software of this system, and to consider the effect of study on static testing technology for software on the railway industry in the aspect of validation on safety.

2 Coding rules validation tool

Train control system software for which a high safety grade is required shall be verified and validated whether it was developed to be suitable for the coding standard presented in [1]&[2]. In relation to it, international standards require the compliance with coding standard. However, although it is required to check the coding standard like this, the coding standard is not presented in the corresponding standard, and international organizations in relation to the railway, etc. does not define the relevant coding standard also. However, overseas railway system software assessment agencies generally apply the MISRA coding standard which is applied to the automobile field. In relation to it, the studies which have drawn the coding standard suitable for railway field from regulations presented by the IEC 61508 and IEC 62279. Through these studies, the coding standard to apply the domestic train control system software was drawn, and it is being prepared as the national standard.

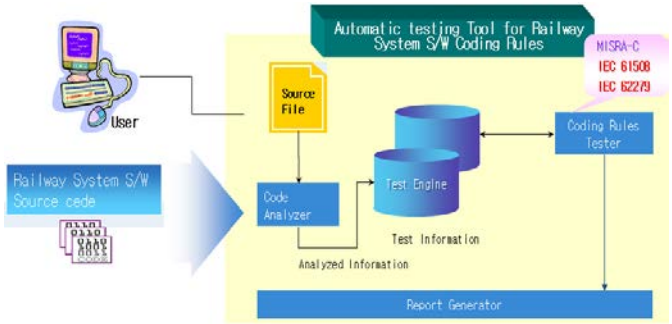

Fig. 1. Outline of the automated testing tool for software coding standard

Inspection technology on the source code coding rules is to test the train control system software to judge whether it is suitable for the required rules to a certain extent by checking whether the train control system software complies with coding standards required by relevant rules, etc. Inspection result like this can validate the risk of mal-

functioning of system due to the software error in advance by detecting not only violations against standards but also potential errors embedded in the source code.

Currently, although some of static analysis tools for embedded software source code for general industry are commercialized, the coding standard based static analysis testing that is suitable for software safety requirements required by related international standards, is not performed actually. Therefore, the study was performed as the development of dedicated test tool suitable for international standards in relation to the safety of railway system is necessary[8]. That is, the coding rules suitable for signaling system was drawn by the preceding study, and the tool to inspect it automatically is being developed also. The applicability was analyzed by performing the testing through applying this development tool to the actual train control software.

3 Result of applying software testing for target system

The applicability test was performed to validate its applicability by aiming at the domestic railway train control system software after developing an automated static testing tool for source code to inspect coding standards of train control system software like Fig. 1. First of all, target software to validate the applicability of developed tool was aimed at the software for railway signaling system which was developed prior to the introduction of international standards in relation to the validation of railway system software in Korea and applied to the actual railway sites. Although this target software is being applied to actual railway sites, since the obstacle to train operation has been caused due to the occurrence of software failure recently, it was checked if the static testing tool developed through this study could detect source code parts where this obstacle was occurred. This failed software was the obstacle that was not detected during the validation on test through the simulator or during the operation at the actual railway sites for a long time, and the corresponding part was modified since the obstacle was occurred recently. That is, it is the case where the obstacle was drawn while operating the part for a long time that has not been filtered in the stages of existing conventional software development, validation and operation.

Table 1. Basic information on applicable target systems

	Target system
Language	C/C++
Total number	22 (14 input files/8 include files)
Total number of lines	48,024 lines
Number of comment line (%)	10,778 lines (22.44 %)
Number of function	517
Main function	Route control function

Basic information on the target system is as shown in Table 1, and the system is VxWorks-based embedded software. The SW-SIL 3 level was selected as the criteria of analysis on the result of application to tests, and if summarizing results of applying the test, they are as shown in the following Table 2.

Table 2. Result of applying static testing to A target system software

Information on test performance	Applied standard	IEC 61508, IEC 62279, MISRA 2004, complexity (CC)
Information on summary of result	Total number of items required to be improved	2,310(severity 'very high' : 223, 'high' : 208)
	Number of files including improved items	20 / 22
	Number of standards for which items to be improved were identified / Total number of standards	86 / 142 (severity 'very high' : 7, 'high' : 15, corresponding standards : 22)
	*Standard compliance rate	39.44%
	**Violation density against standard	0.68

* Standard compliance rate= ((Total number of standards - Number of violated standards) / Total number of standards) X 100
** Violation density against standard = Number of violated standards / Valid line

As a result of performing tests shown Table 2, it was analyzed that 2,310 items required to be improved were detected, coding standards necessary to be improved were 86 ea, the coding standard compliance rate was 39.4%, and the violation density against coding standard was 0.68. As a result of analysis, there were many violated coding standards and number of violations, and accordingly, the coding compliance rate was less than 50%. It seems that it is because this software has been developed and used in Korea prior to the beginning of study on static testing technology for software in the aspect of safety.

5 Conclusion

Although functions of railway signaling system which secure the safe operation of train in the railway system are implemented by the computer software recently, the study in relation to the validation on safety of software is in the beginning stage. Related with it, the study in relation to the static testing tool including derivation of the coding standard and validation on coding standard in connection with the validation on safety of railway signaling system software was started from several years ago in Korea. As a part of this study, the applicability test through static testing tools which were developed for the railway signaling system software being operated in the domestic railway sites was performed. As a result of test and analysis for the software of this target system, it was confirmed that they detects violations properly through the static testing tool.

References

1. IEC 61508-3: Functional safety of electrical/electronic /programmable electronic safety-related systems - Part 3 Software requirements, (1998)
2. IEC 62279: Railway Applications - Software for railway control and protection systems, (2002)
3. M. Fewstar, D. Graham: Software Testing Automation: Effective use of test execution tools, ACM Press, Addison Wesley, (1999)
4. MISRA-C Coding Standard: MISRA(Motor Industry Software Reliability Association), (2004)
5. Jong-Gyu Hwang, Hyun-Jeong Jo: Development of automated testing tool for coding standard to check the safety of train control system software, Journal of the Korean Society for Railway, Vol. 12 Issue No. 1, (2009)