Suggestions of Development Methodology for Railway Software

Eui-jin Joung[1] and Kyung-ho Shin[2]
[1, 2] Train Control & Communication Research Department, Korea Railroad Research Institute
#360-1, Woram-dong, Uiwang-si, Gyeonggi-do, 437-757, Korea
E-mail: [1] ejjoung@krri.re.kr, [2] khshin@krri.re.kr

Keywords: railway software, safety criteria, development methodology

Abstract: One of the main concerns of railway system is to secure safety. Nowadays digital technology has been rapidly applied to safety critical system. The digital system performs more varying and highly complex functions efficiently compared to the existing analog system because software can be flexibly designed and implemented. The flexible design makes it difficult to predict the software failures. For this reason, the safety criteria are suggested to secure the software safety for the field of railway system. Following them, the railway software has to be examined whether it is properly developed according to the safety criteria and certification process. Also because the articles suggested in safety criteria are written in legal term, it is difficult to apply the criteria to develop railway software. This paper suggests and discusses a development methodology to solve these issues.

1. Introduction

One of the main concerns of railway system is to secure safety. Nowadays digital technology has been rapidly applied to safety critical system. The digital system performs more varying and highly complex functions efficiently compared to the existing analog system because software can be flexibly designed and implemented. The flexible design makes it difficult to predict the software failures. For this reason, the safety criteria are suggested to secure the software safety for the field of railway system. Following them, the railway software have to be examined whether it is properly developed according to the safety criteria and certification process. We describe the procedure to deduce the railway software safety criteria in the section 2. The safety criteria are written in a legal term, it is difficult to apply directly the criteria to develop the railway software. In the section 3, we also suggest the railway software development methodology to easily access the criteria to the railway software industry.

2. Railway Software Safety Criteria

Railway software safety criteria have to be described not to contradict other international standards. The following Figure represents the areas to secure the quality of railway software and the classification of the related standards. There are three areas related to the software quality, such as domain standards, process related standards, and product related standards.

As the safety related standard of railway system, there are representatively electrical and electronics standard, IEC 61508, and railway related standard, IEC 62278 and IEC 62279. IEC 62278 is described the railway RAMS (Reliability, Availability, Maintainability, and Safety) and IEC 62279 represents the railway software as those transformed from the European CENELEC standard, EN50128 into the international standard. Of course safety critical software standards of other domains such as nuclear, aerospace, defense, etc are reviewed to understand the characteristics of safety critical software.

As the process area, there are CMMI (Capability Maturity Model Integration) and ISO/IEC 15504 (so called SPICE: Software Process Improvement and Capability dEtermination) which manage the maturity of the software process. The failure due to the software are recognized as the systematic failure. The unadquatable system interface and process between human and machine, and between hardware and software is inducing the systematic failure. To avoid the failure, well defind process has to be prepaired and the process has to be also assessed whether it controls the software errors. The standards referred in the process areas give us the guide to evaluate the process maturity level.

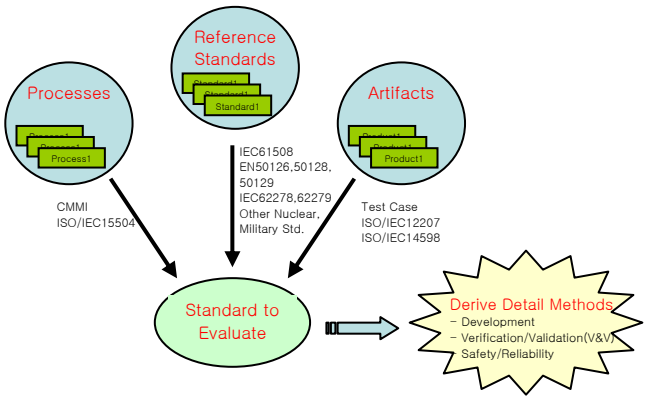

Figure 1. The categorized standards related to deduce the safety criteria of the railway software

As the product area, there are ISO/IEC 9126 which defines the software quality characteristic and ISO/IEC 14598

which covers the quality evaluation of software products. While the standards of the process area are suggested in the assumption that high qualified software is coming from the well defind process, the standards of the product area are just focusing the software artifact itself. If there is no error detected during the software test in each lifecycle steps, we consider the software has desirable quality in the related test. The standards referred in the product area are described the software quality charicteristic that have to be ensured the software quality, and the evaluation procedure to assess the software quality. [1]-[7]

After reviewing several standards describe above, we finally suggest railway software safety criteria described below.

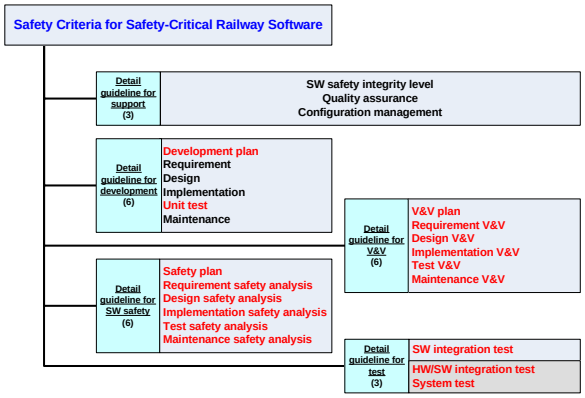

Figure 2. The structure of railway software safety criteria

The safety criteria suggested in this paper are classified to the five areas such as support, development, verification & validation (V&V), test and safety analysis. The criteria of the development, V&V and safety are parally related together, and the test criteria are decribed as a kind of acceptance test. The support criteria is related to the other criteria to control all the management activities.

All of the criteria have to be referred to the development company when developing a railway software. The criteria with red character in the figure 2 is for the assessment organization.

Figure 3 is an example extracted from the criteria. The clause is a part of the activity at the design step in the development lifycle. It is composed of the article, comment and referrence as an evidence describing related standards and regulations. As described in the figure 3, the criteria is described as a kind of legal statement. It is just described not how to do but what to do. So the process which has to specifically follow wasn't addressed. This situation can cause a lot of confusion in case of applying the software safety criteria. Therefore we need to prepare the development methodology which systematically regulates the conducting work for each step of life cycle which develops, verifies & validates, tests railway software and analyzes the safety of railway software.

Clause 4 (Railway software design activity)

The software developer should do software design activity to develop the software according to the software life cycle.

[Comment]

This clause is written referring to the content of IEC 62279 and IEEE Std 7-4.3.2, IEEE std 1074. Software design specification is the specification changing the software requirements into the software architecture, software components, interface and the matters related to the required data in the implementation phase.

[Reference]

- IEC 62279 Railway application : Software for railway control and protection system
- IEEE Std 7-4.3.2 IEEE Standard Criteria for digital computers in safety systems of nuclear power generation stations
- IEEE Std 1074 IEEE Standard for Developing software life cycle process

Figure 3. An example of railway software safety criteria

3. Railway Software Development Methodology

The development methodology of safety related railway software is made to provide methods which can be applied when safety critical software is developed.

This methodology is composed of documents for processes, templates and techniques. The process documents show each step which is composed of the activities which are included at each step. The template documents are to set the format to write the input and output materials which is defined in the process documents. The technique documents are to gather the items which more technical contents are described than the activities which are described in process documents. We consider several aspects to develope the methodology of the safety critical railway software. First we review the needs of the railway software developers and reflect the characteristics of safety critical software. Also we develope the methodology to meet the related international standards.

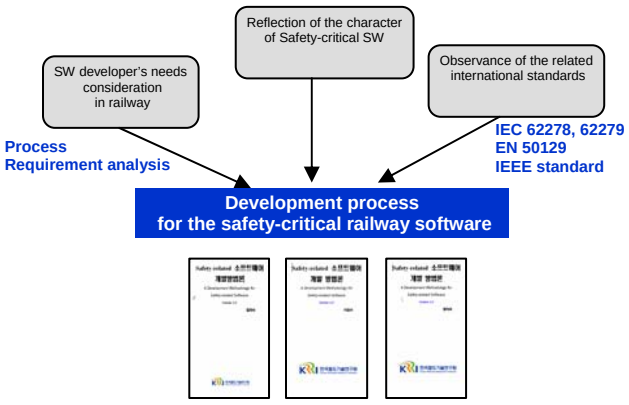

Figure 4. Aspects to develope the development methodology for the safety related railway software

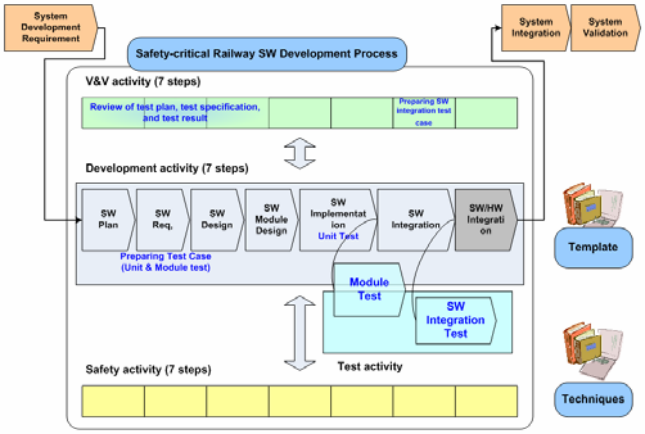

Figure 5. Software development methodology for the safety related railway software

The figure 5 shows the software development process for the safety related railway software. The development process of the safety related railway software is composed of the following seven steps.

1) Step of planning establishment of railway software
2) Step of requirement specification of railway software
3) Step of design of railway software
4) Step of module design of railway software
5) Step of implementation of railway software
6) Step of integration of railway software
7) Step of integration of hardware and software in the railway software

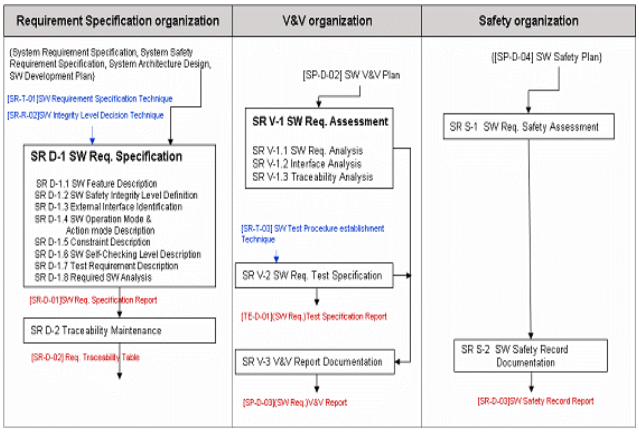

Figure 6. An example of process document for the safety related railway software

An example of the process document for the requirement specification of railway software is described in Figure 6. The process document represents the role and activity among those who responsible for requirement specification, V&V and safety. Also it specifically describes the input and output documents and the detail conduction for each step. For the development methodology of general software, those who responsible for V&V include the role of safety. System verifier and validater review the software safety in the view of quality management. Otherwise, for the railway system which considers safety as an important factor, the role of safety is devided from that of V&V. The safety documents developed by company are transferred to the ordering organization or the third independent safety assessment organization to review the adoptiveness with the required safety criteria.

4. Conclusions

To apply uncertain software to the safety critical system such as railway, nuclear, aerospace, defense, etc, safety has to be drastically inspected. Each safety critical systems prepare their quality assurance system according to the each system characteristic. In case of the railway software it needs the access of the process view point and product view point to develop the good qualified software and secure safety. In the view of improvement of process maturity, it is to be followed the various procedures and process suggested in the CMMI and ISO/IEC 15504 (SPICE) to secure the software quality. It improves the maturity of software development organization. And in the product view, it is considered the process which improves the software quality as development and verification by the formal method or conducting the test according to the test case derived in the early stage of development.

This project suggests the software safety criteria considering the process to improve the software quality in the view point of process and product. It suggests the development methodology for the safety related railway software which is composed of process document, template document, and technique document to raise the site applicability of the given safety criteria. In the future, the development methodology will be extended to the ordering and assessment methodology.

References

[1] IEC 62278, "Railway application − The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)", March, 2002

[2] IEC 62279, "Railway application − Software for railway control and protection system", June, 2002

[3] CENELEC EN50129, "Railway application − Safety related electronic systems for signaling", April, 2000

[4] ISO/IEC 15504 "Information Technology-Process Assessment-Part 1 ~ 5"

[5] ISO/IEC 12207 "Information Technology- Software lifecycle processes"

[6] ISO/IEC 9126 "Information Technology-Software Quality Characteristics and Metrics-Part 1,2,3"
[7] ISO/IEC 14598 "Information Technology-Software Product Evaluation-Part 1 ~ 6"