Development of safety criteria for railway software

E.-j. Joung & K.-h. Shin
Train Control Research Team, Korea Railroad Research Institute, Korea

Abstract

Safety critical systems are those in which a failure can lead to serious and irreversible consequences. Nowadays digital technology has been rapidly applied to critical systems such as railways, aerospace, nuclear power plants, and vehicles. The main difference between an analog system and a digital system is that the software is the key component of the digital 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. This paper reviews safety standards and criteria for safety critical systems such as railway systems and introduces the framework for the software lifecycle. The licensing procedure for the railway software is also reviewed.
Keywords: railway software standard, quality management procedure, product oriented view point, process oriented view point.

1 Introduction

Railway systems put a great emphasis on safety more than any other component. It is true that software is increasingly used for functional realization of railway systems. Software has a certain congenital uncertainty to predict failures. The development of railway software has so far been inclined to function realization. In the case of using software without any safety certification, and if this use led to accidents, we will get severe and great damage. To deal with the situation, safety standards for railway software need to be suggested, and a verification and certification framework should be established to ensure that the software is developed with safety standards. We research other fields including nuclear power plants, aerospace, defenses in terms of quality management procedures, and review an appropriate safety management system for railway software.

WIT Transactions on The Built Environment, Vol 96, © 2007 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/UT070561

Section 2 describes the railway safety regulation framework in Korea, section 3 explains the procedure to derive railway software safety standards, and the composition of railway software safety standards. In section 4, we exam quality management procedures of other industries, and describe that of the railways. In section 5, we draw a conclusion suggesting the direction of progressing tasks hereafter.

2 Railway safety act and safety standard

The purpose of the project "Establishment of safety standards and management system for railway safety critical software", which is hosted by Korea Railroad Research Institute (KRRI) from 2004 to 2008, as one development project of Korean Ministry of Construction & Transportation (MOCT), is to develop a safety regulatory system to secure software safety of computer-based controllers used in railways. In other words, the project aims at setting up safety standards of railway software as the subordinate laws of the railway safety act, the implementing ordinance, and the implementing regulation as in figure 1 below, and developing supporting directives for their translation. The safety standard to be enacted should not be separated from the existing international standard IEC/ISO, the domestic one KS, and the one of industrial undertakings IEEE, and should put them together.

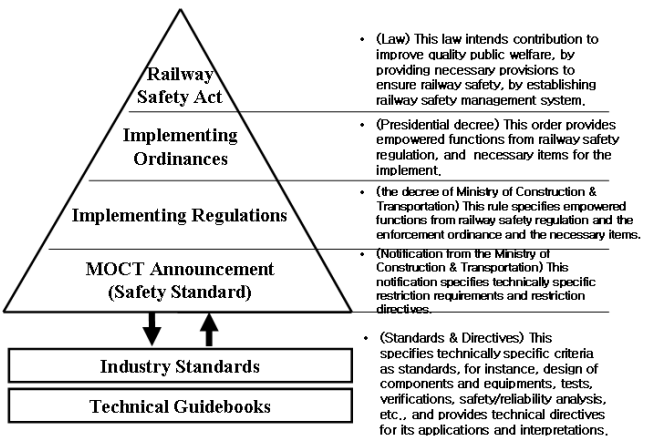

Figure 1: Structure of railway safety act.

3 Railway software safety standards

Software adds more difficulties to assure its accuracy because of its complexity. Many accidents have been reported since the 1990s due to software errors. To secure software safety of those systems, a number of countries and authorities propose plans to ensure its safety and reliability.

We can solve schedule delay, excess cost, customer dissatisfaction caused during software development, by improving the quality of the product itself, and managing the process of product development.

We can consider two points of view to improve reliability and safety of railway software; one is from a focus on the product, to manufacture a good product by accurate tests, and to assess its accomplishment; the other is from a focus on process, to set up a good organizational structure to make a good product.

The product-oriented approach is to identify faults in a product itself by examining it. This approach is currently only applied on a black box test. After defining appropriate software properties and sub-properties, and completing the test case, the test (black box test) is performed. Korea have GS (Good Software) and ES (Excellent Software) as certification marks given by product testing [1,2.]

The process, in software development, indicates resources (people, equipment, technology, and methodology), activities, methods, and directives in practice which are used for achieving targets within an organization. Process inspection is to evaluate whether a process meets targets. The benefits from it help us to determine the organization capability to develop products, and to provide important indications to improve quality of a process. Typical examples of the approach are CMMI (Capability Maturity Model Integration) of SEI (Software Engineering Institute) and ISO/IEC 15504 (SPICE: Software Process Improvement Capability dEtermination) [3,4].

To ensure software safety of railway systems, which is one of the safety-critical industries like nuclear power plants, both aspects should be taken into account. The whole process can be arranged as in figure 2.

The Reference Standards here are the standards made after considering domain properties of railway systems, which can be divided into two kinds of standards – a process-related one and a product-related one [5–8].

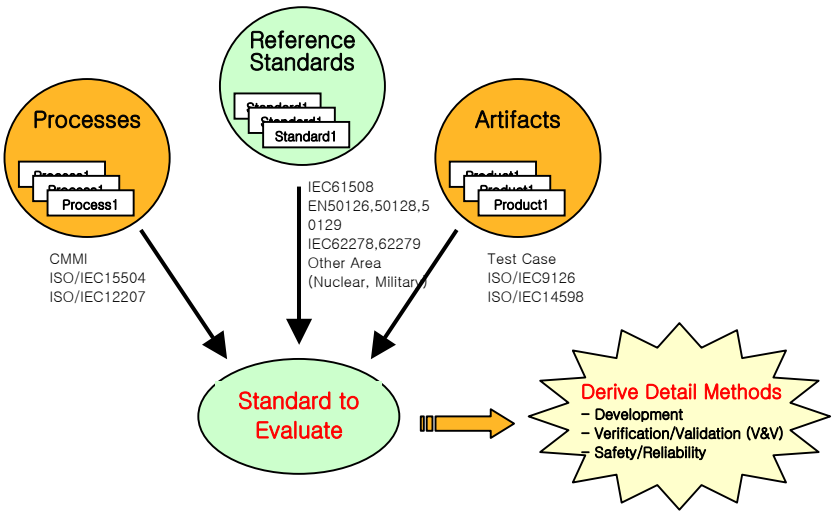

Figure 2: Aspects for establishing safety standard.

3.1 Standard applied to derive railway safety standard

Figure 3 below illustrates the relationship between the safety act and industrial standards to be referred respectively, dividing the life-cycle process, plan, requirement specification, design, test, installation etc, when writing a software safety standard.

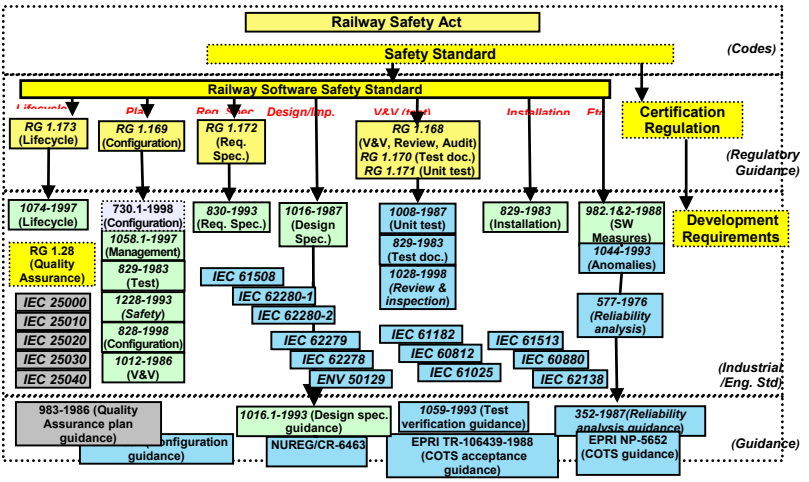

Figure 3: Relationship between railway software safety standard and industrial standards.

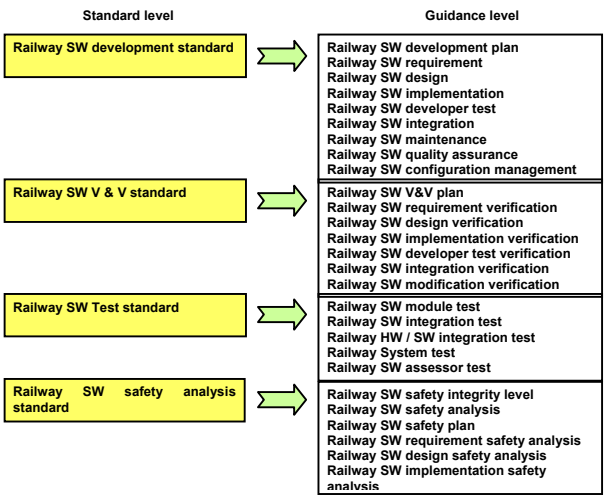

Figure 4: Composition of railway software safety standard.

3.2 Composition of railway software safety standard

The railway software safety standard consists of 4 detailed regulations - development, verification, testing, and safety analysis. The respective regulations describe specific procedures.

4 Quality management procedure of railway software

Stakeholders related to software safety can be divided into software developer, software purchaser, software audit and assessor etc. The quality management procedure describes the duties of each of the above stakeholders to develop, adopt, audit and assess products according to the given railway software safety standards. It proposes a quality management procedure proper to railway software, considering procedures of other industries.

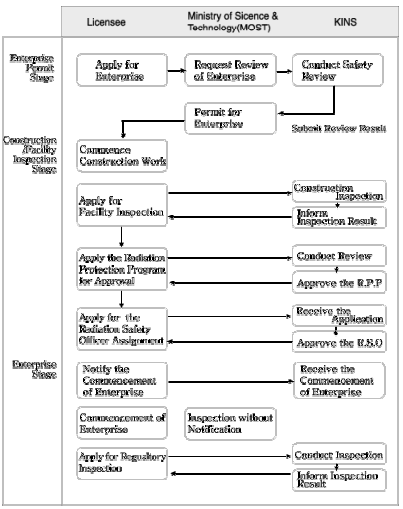

Figure 5: Safety inspection procedure of a nuclear power plant [9].

4.1 Quality management procedures of a nuclear power plant

The general inspection procedure for safety audit and assessment of nuclear power plant is like figure 5, which is carried out by Korea Institute of Nuclear Safety (KINS). The subjects authorized and certified by KINS are grouped into construction and operation permissions of newly constructed nuclear power plants, modification permissions of those that have been permitted once or more times, and approval to reports of specific technical subjects.

KINS first determines its type when a written permission application of nuclear facilities is submitted. When the type is fixed, they check the suitability of the applying documents. When the suitability is confirmed, they determine the

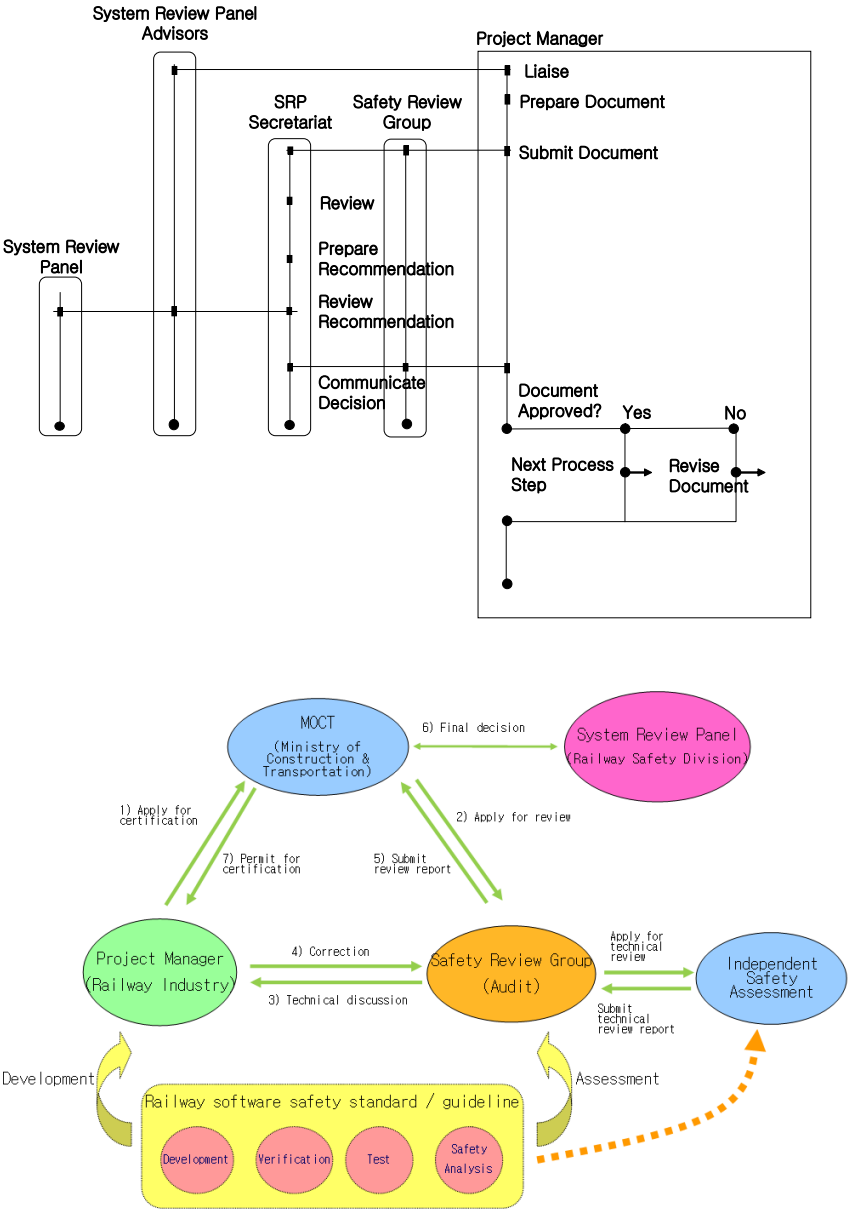

Figure 6: An administrational procedure between safety management authorities [10].

proper scope of inspection according to the type of application, and make an inspection plan appropriate to the documents. The purpose of the inspection is for reviewers to report planned activities and schedules to higher-level managers, and to identify resources, and for participating reviewers to help see the clear picture of inspection criteria and their roles. The inspection activity is carried out in accordance with the plan, referring the acceptable criteria and the inspection procedures.

4.2 Railway quality management procedure

Referring to the procedures of nuclear power plants, an appropriate quality management procedure for railways is suggested.

4.2.1 Safety management procedure of railway

To certify the safety of railway systems, the procedure below is followed. An administrational procedure between project managers, the system review panel, and safety review groups is illustrated.

Project managers prepare related documents, and certify safety after sending them to the system review panel or to the safety review groups.

4.2.2 Role of each organization

Project managers carry out all matters related to safety after obtaining approval from the system review panel. The system review panel deals with all railway safety concerns. Safety review groups handle the works entrusted by the system review panel. An independent safety assessor verifies whether the project managers perform safety actions well in compliance with safety plans.

a. System review panel

The system review panel performs and guides the safety assessment in terms of equipment and component systems through a system life-cycle, from the initial level of concept embodiment and development, to the application, maintenance and termination. The members examine safety records of concerning projects, and supervise the safety management. The documents, which are examined by the system review panel, include the safety case. The panel checks safety assessment schedules, hazard analysis records, risk assessment records, safety requirement specifications, safety assessment reports, safety audit reports, and others. The main accountabilities of the system review panel are as follows:

- To verify the safety case
- To mark on the safety-related documents, and to authorize them
- To disapprove unsuitable, inaccurate, and inappropriate documents with rational evidence
- To recommend systems for safety, to provide them to relevant organizations for their certification
- To discuss systems, equipment, components, system level, to certify formality of the operation process
- To submit verified reports, to issue a certification, for which recommendations are officially written, to concerning organizations

b. Safety review group

Safety review groups carry out safety-related services which are turned over from the system review panel. They check elements which have an impact on performed project safety, and potentially cause effects on it. The documents examined by the groups include the safety plan, safety case, and they also cover the safety assessment schedule, hazard analysis records, risk assessment records, safety requirement specifications, safety assessment reports, safety audit reports and others. The main subjects to be verified are as follows:

- To verify submitted documents
- To approve submitted documents
- To mark whether safety-related documents exist or not, to authorize them
- To disapprove submitted documents which are evaluated as being unsuitable, inaccurate or inappropriate for rational evidence

The responsible works of safety review groups are as follows:

- To change limits of rolling stocks, and track gauges
- To modify upholding modes of gauges
- To introduce stop patterns of new rolling stocks
- To introduce new station
- To consider whether there are any elements influencing the sighting of signaling

c. Independent safety assessment

Independent safety assessment carries out the safety audit and assessment. The safety audit is implemented focusing on the existing management activities used for securing safety, and verifying its compliance. The safety assessment verifies reduction of risks related to systems which are being developed focusing on project products, down to the moderate level.

The safety audit aims at verifying whether management activities for securing safety are performed well and appropriately in compliance with safety plans. If safety plans are not prepared, safety auditors should set them up before the operation of the safety audit. The auditors verify the scope of projects corresponding to safety plans, appropriateness of safety plans, and recommendations of planned tasks, and their improvements.

- Tasks implemented after existing audits
- Plans for the next plans

The safety assessment verifies and makes a decision whether risks, related to systems in the process of development, are reduced to an appropriate level. Assessors check especially the regulations of safety requirements to assess their sufficiency to control risks, focusing on the system safety requirement specification, and verify whether the system meets the regulations.

5 Conclusion

Safety verification is required to apply software to safety-critical systems such as railways, which has potential uncertainty in itself. Other industries such as

nuclear power plants, aerospace, defenses have already set up each quality assurance systems appropriate to their systems. We have two approaches to secure reliability and safety of railway software: one is to secure software quality by improving process maturity, in the process-oriented approach, and the other is to reduce risks in the software itself by developing and verifying with formal methods, and by performing tests derived appropriately in accordance with test cases, in the product-oriented approach. In addition, from another view point, safety audit and safety assessment can also be applied to safety certification. In the case of safety audit, previously recommended process-oriented approaches are more related, which emphasizes the accurate compliance in the safety demonstration process. The safety assessment has a tendency to check the performance of safety analysis, which is a product-oriented approach. Therefore, to secure the safety of railway software being developed hereafter, we need not only to implement safety audits on procedural aspects, but also to secure safety assessment technologies on product quality assurance.

References

[1] ISO/IEC 9126 "Information Technology-Software Quality Characteristics and Metrics-Part 1,2,3", 1991
[2] ISO/IEC 14598 "Information Technology-Software Product Evaluation-Part 1~6", 1999
[3] ISO/IEC 15504 "Information Technology-Process Assessment-Part 1~5", November, 2004
[4] ISO/IEC 12207 "Information Technology- Software lifecycle processes", 1995
[5] IEC 61508, “Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 1~7” December, 1998
[6] IEC 62278, “Railway application – The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)”, March, 2002
[7] IEC 62279, “Railway application – Software for railway control and protection system”, June, 2002
[8] CENELEC EN50129, “Railway application – Safety related electronic systems for signaling”, April, 2000
[9] Ministry of Science & Technology, "2005 White paper of Nuclear Power Safety" 2005
[10] Railtrack PLC, "Engineering Safety Management (Yellow Book) Issue 3", October 2003