Safety assessment methodology of railway signalling systems in Korea

J.-G. Hwang, H.-J. Jo & Y.-G. Yoon
Train Control Research Team,
Korea Railroad Research Institute (KRRI), Korea

Abstract

As existing electrical and mechanical railway signalling systems are replaced with systems using computer technologies, system capability has improved in such a way that the system is intellectualised. The railway signalling system is a vital system that is directly connected to massive life damage or economical loss due to its features. Therefore strict safety activity and assessment methodology are be required. There are several international standards for railway signalling system safety activity requirements, which are required to demonstrate those safety activities. Signalling system safety assessment is performed by analysing and evaluating the system safety activity process and its results. In this paper, we suggest railway signalling system safety activity techniques for the railway signalling system safety assessment and its specific execution techniques at each activity phase. We also analyse safety assessment tasks based on suggested safety activity techniques and identify the necessary case study required to ensure the safety of assessment techniques.
Keywords: railway signalling systems, safety assessment, RAMS.

1 Introduction

Electronic and computerized railway signalling systems have replaced the existing mechanical systems, resulting in intelligent and automatic high-performance systems. For the existing electrical and mechanical systems, empirical approaches and the engineer's intuition are mainly used to detect any faults, assuring a certain degree of safety in the railway signalling systems. However, the new computerized railway signalling systems do not allow the safety assurance based on such empirical approaches to detect faults. Therefore,


WIT Transactions on Information and Communication, Vol 39, © 2008 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK080491

IEC (International Electrotechnical Commission) requires more rigorous safety activities to assure the safety of the railway signalling systems [1,2,5,7]. In addition, such safety activities have to be evaluated by an ISA (Independent Safety Assessor) in order to assure a certain degree of safety in the railway signalling systems.

The safety activity requirements for railway signalling systems were established as the international standards by the IEC. Further, the IEC standards describe the documentation requirements necessary to demonstrate such safety activities. The safety assessment of the railway signalling systems is done by performing safety activities and analysing/evaluating the results [3,4,6]. Therefore, it is necessary to review and analyse the safety activity system and tools appropriate for railway signalling systems, in order to establish the techniques for safety assessment of the railway signalling systems. In Korea, many researchers have investigated the methodologies to evaluate the safety of the railway signalling systems, which will be discussed in this study.

2 Overview of safety assessment technology for railway signalling systems

The safety assessment of the railway signalling systems is performed through safety activities and verification of results from such activities. Therefore, analysis of the safety assessment of railway signalling systems is very important in developing the safety assessment technology. Analysis of the safety assessment of railway signalling systems was performed through investigation and analysis of international standards and technical advice from foreign safety assessment consultants.

2.1 What is a safety assessment?

The former European safety-related standards on railway systems were transformed into the international standards by the IEC, which require the safety activity and assessment for the railway signalling systems. In foreign countries, the manufacturers of the railway signalling systems also perform the safety activities according to the international standards. In addition, there are independent safety assessors to perform the safety assessment of the railway signalling systems according to the IEC standards. In Korea, such international standards have recently been introduced, making people recognize the need for safety activities and assessment. As a result, some research programs on such safety activities and assessment have been initiated.

In general, the safety assessment of the railway signalling system is conducted by the ISA (Independent Safety Assessor). The basic system requirements are determined by the purchasers and the operators, but the safety requirements other than system function and performance requirements have to comply with IEC 62278, IEC 62279, and IEC 62425 in European countries. Such safety-related standards provide the requirements for safety approval procedures and supporting documents to assure the safety of the railway systems. Among those standards, IEC 62278 is a framework standard that defines basic concepts

and safety procedures for railway signalling systems as well as overall railway systems. In addition, this standard describes the definition of SIL (Safety Integrity Level) and IEC 62425 provides detailed requirements for SIL. The activities to be performed by the manufacturers and the assessors are specified in IEC 62425.

2.2 Safety activity and the safety assessment system

Fig. 1 shows the risk-based safety activity and safety assessment process for the railway signalling system. The assessment system consists of system definition, PHA (Preliminary Hazard Analysis), HIA (Hazard Identification and Analysis), risk analysis and SIL allocation. The safety assessment of the railway signalling system is a process of verifying if various required documents are prepared, if such documents are appropriate, and if the identified hazards are minimized to an acceptable level through safety activities. Therefore, in performing the safety assessment, it is necessary to analyse the safety activity system for the railway signalling system and the documents prepared through such safety activity and their quality level. In this study, some methodologies were selected according to the system shown in figure 1; PHA for hazard analysis at step ①, FMEA and HAZOP for hazard identification and FTA (and ETA as a supplementary step, if necessary) for hazard analysis at step ②, and BP-risk method and SIL allocation method based on THR derived from BP-risk according to SIL matrix (IEC 62278).

Among several IEC standards regarding the safety of the railway system, the IEC 62425 standard defines the safety assessment as the analytical process with a view to determining whether a system satisfies specific requirements and

Figure 1: Safety activity and the safety assessment system.

whether the system operates as intended. Foreign safety assessment organizations perform the safety assessment activities for the railway signalling systems according to the definition of the IEC 62425 standard. From the analysis of various standards regarding the safety of the railway system, investigation of prior research activities and technical advice from foreign safety assessment organizations, the objectives in performing the safety assessment of the railway signalling systems can be summarized as follows:

- Verifying if the system requirements are adequate
- Verifying if the system requirements, codes, and standards are complied with
- Verifying if system risks are removed or reduced to acceptable levels
- Analysing and verifying the master safety plan
- Analysing the hazards log

2.3 Safety assessment process

As described above, the safety assessment of the railway signalling systems is to verify if a system is able to accomplish the intended purposes and if all potential hazards are identified and removed or reduced to an acceptable level. Such removal or reduction of those potential hazards can be confirmed only by verifying the adequacy of measures for removal or reduction and the realization and performance of the functional system requirements. In other words, serious hazards may be mistakenly omitted or underestimated in the process of identifying and controlling the potential hazards. Such problems may be solved to some degree through the safety management.

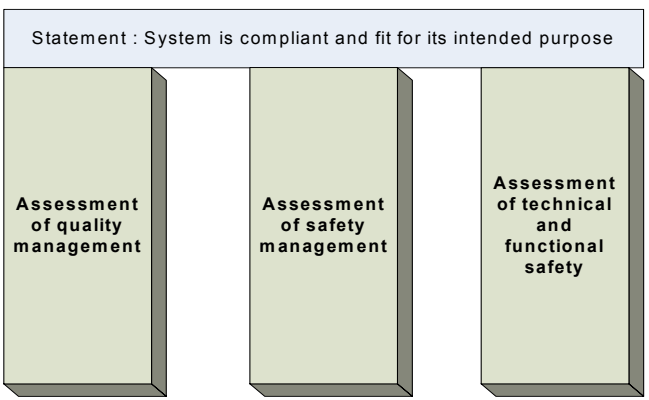

Figure 2: Assessment tasks.

In addition, the project system will not be designed and made as only one system to be tested, but it will be made and operated for the manufacturer's continuous assessment based on the same procedures. Therefore, it is important that the system manufacturers assure that the future systems have the same quality as that of the system under test and assessment. In performing the safety

assessment of the railway signalling systems, verification and validation of such quality control system are highly important. In other words, the safety assessment of the railway signalling system comprises the assessment of the technical and functional safety as well as the assessment of system quality and safety management. Accordingly, as shown in fig. 2, the safety assessment of the railway signalling systems consists of the assessment of technical and functional safety, the assessment of quality management, and the assessment of safety management.

3 Definition of safety assessment of railway signalling systems

As described above, the safety assessment of the railway signalling systems consists of the assessment of quality management, the assessment of safety management, and the assessment of technical and functional safety. The safety assessment in these three aspects is intended to verify if appropriate safety activities and procedures are complied with and determine whether the identified hazards are removed or reduced to acceptable levels.

Prior to the safety assessment, the master safety plan for the project system has to be evaluated for its adequacy and the master document for safety measures summarizing the safety activities and the results has to be verified for compliance with the master plan. Therefore, in performing the safety assessment of the railway signalling systems, checks are carried out to ensure that the planned project activities were performed according to the practices and procedures specified in the safety plan. The safety assessment through analysis and verification of safety plans, safety requirements, the master document for safety measures, and other related documents is called the "Analysis Assessment Approach", which is an essential part of the safety assessment of the railway signalling systems.

This analysis assessment approach can be divided into two assessment activities; assessment of safety management procedures and practices assessment of whether the identified hazards relating to the relevant railway signalling system project are removed or reduced to acceptable levels through the design and manufacture processes. Verification and validation of safety management practices, quality control, and organizational structure can be done through examination of documents. However, analytical procedures and additional tests are required to verify whether the identified hazards are actually removed or reduced to acceptable levels. The safety of the railway signalling system can be verified and assessed through these activities. In addition, for the analysis assessment approach, the system safety requirements will be reviewed, the specifications will be evaluated for their adequacy in terms of risk control, and the system will be assessed to verify whether it is in compliance with the safety requirements specification. In short, the safety assessment of the railway signalling system begins with the review and verification of the hazards log, safety plan, safety requirements specification, and other documents. In addition, analysis of the master document for safety measures may lead to the request for formal tests to verify the functions. If necessary, additional tests in challenged

conditions may be required to verify the safety of the system. Such assessment can be called the "Test Assessment Approach".

In short, the safety assessment of the railway signalling system consists of the analysis assessment approach and the test assessment approach. These two approaches lead to the hazard closure verification, resulting in final safety approval. In other words, when the safety assessment is completed through these approaches and the system is finally approved, it means that the identified hazards for the railway signalling system are removed or reduced to acceptable levels. This safety assessment process is summarized in fig. 3.

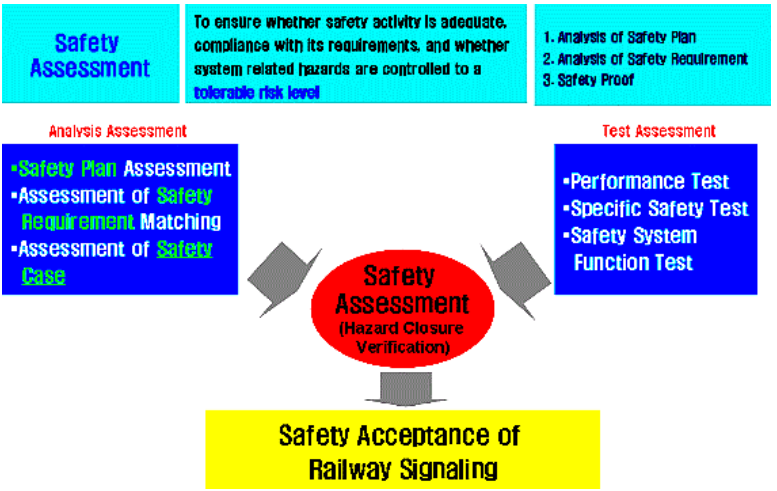

Figure 3: Safety assessment process for railway signalling systems.

4 Proposed methodology for safety assessment of railway signalling systems

As explained in the above section, the safety assessment of the railway signalling systems consists of analysis assessment and test assessment. Most safety assessment is concerned with the analysis of the safety plan, the requirements document, the master document for safety measures, and other documents. After the analysis assessment, the test assessment for additional verification or examination is performed to assess the safety of the railway signalling system. In addition to such classification of two approaches (analysis assessment and test assessment), another classification is possible to reflect the actual assessment activities. In this study, the two-step safety assessment is proposed on the basis of the analysis of assessment activities, practices, and procedures.

The safety assessment at the step of requirements definition (basic step) is to define the scope of the safety assessment activities and to develop the safety assessment plan after analysis of the safety plan and the safety requirements documents. The main purpose of this step is to analyse the safety requirements

specification, system functions and operating environments and to develop the safety plan, including the safety assessment items and criteria, applicable to the whole safety assessment process. At the execution step (detail step), actual safety assessment activities are conducted. Quality control, safety management, and functional and technical safety are assessed according to the safety assessment plan developed at the basic step. All documents, including the master document for safety measures, are used for safety assessment. The risk minimization measures for individual hazards, expected results, and tests are performed at this step to verify whether the identified hazards are removed or reduced to acceptable levels (Hazards Closure Verification).

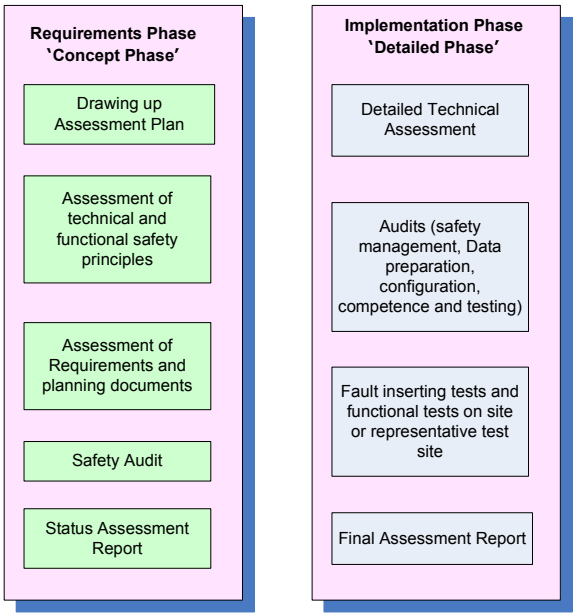

Figure 4: Assessment activities.

The test and assessment step consists of the performance tests, safety tests, and field tests. The safety tests are to test the design and modules for safety functions of a system. For example, the fault insertion test is the representative test in the safety tests. The safety tests are classified into special safety tests and safety system tests.

The test assessment is highly important in performing the safety assessment of the railway signalling systems. There are no standards providing test methods for safety assessment. Such methods may vary depending on the project circumstances, types of documents, and degree of safety and quality. Fig. 5 shows the relationship of safety activities and safety assessment process. The safety activity flow and steps are provided in the left part of the figure, while the safety assessment process and procedures are explained in the right part. As shown in the figure, the safety activity mainly consists of the risk analysis step

and the risk control step and the safety assessment based on the safety activity is divided into the requirements definition step and the execution step. "Data Analysis" represents the requirements definition step at which the safety assessment plan is developed. The execution step is further divided into "Safety Analysis Assessment" and "Test Assessment".

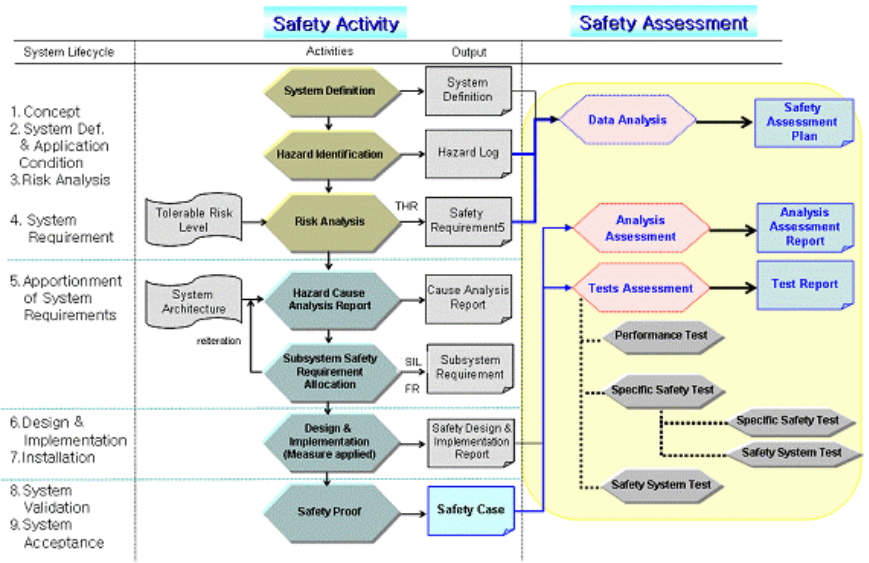

Figure 5: Safety assessment according to safety activity.

In this study, the safety assessment process and steps for the railway signalling systems are proposed and the applicable technologies, templates required at individual steps, assessment guidelines, specifications for development of the software safety assessment instrument, and others are provided as described in fig. 5. In particular, the list of documents to be analysed and verified in the safety assessment of the railway signalling systems and the checklist templates to be used in two safety assessment steps are provided here.

5 Conclusion

The need for safety activity for railway signalling systems in compliance with international standards has been increasingly highlighted. In addition, the need for developing the validation and assessment technologies has been increased. Accordingly, this study proposes the methodology for safety assessment based on the analysis of requirements prescribed in international standards regarding the railway signalling systems.

In addition, the techniques and procedures for the proposed safety assessment process were investigated. For example, major hazards for the railway signalling systems in Korea were listed and analysed and various templates, such as the

safety requirements template and the assessment plan template, were developed. Further, the guidelines on preparation of the master document for safety measures and on software safety assessment are under development. Moreover, the research program is on-going to investigate the strategy to apply the more quantitative BP (best practice) method for list analysis and assessment to the Korean railway signalling systems.

References

[1] IEC 62278, "Railway Applications - The specification and demonstration of RAMS", 2002.
[2] IEC 62425 Ed. 1, "Railway Application: Communications, signaling and processing systems - Safety related electronic system for signalling", 2005.10.
[3] Nicholas J. Bahr, "System Safety Engineering and Risk Assessment", Taylor & Francis, 1997.
[4] Yacov Y. Haimes, "Risk Modeling Assessments and Management", Wiley-Interscience, 2004.
[5] J. Braband and et al, "The CENELEC-Standards regarding Functional Safety", Eurailpress, 2006.
[6] J. Braband and et al, "Risk-orientated Apportionment of Safety Integrity Requirements –An Example", SIGNAL+DRAHT, Vol. 1+2, 2000.
[7] Y. Hirao, "New European Norms from a Japanese Viewpoint", SIGNAL+DRAHT, Vol. 11, 2001