Vol. 6, No. 2, pp. 38-42, December 2007

INTERNATIONAL JOURNAL OF SAFETY
www.kosos.or.kr

Analysis of Safety Assessment Methodology for Railway Signaling Systems

Jong-gyu Hwang*, Hyun-jeong Jo and Yong-Ki Yoon

Train Control System Research Team, Korea Railroad Research Institute, Uiwang-si 437-757, Korea

(Received July 12, 2007; Accepted December 5, 2007)

Abstract: As railway signaling system is computerized, the significance on safety demonstration and assessment has been increased. Therefore, railway signaling system should reflect the needs for safety assessment technique. Various studies on safety assessment technique for railway signaling have been made in Europe and standardization of the requirements for safety acceptance has been initiated by IEC. In order to develop and establish the safety assessment techniques for railway signaling in Korea, we try to review safety assessment activities for signaling system via reviewing relevant case studies and consulting with experts. And also we propose the safety assessment activity/methodology for Korean railway signaling system.

Key words: railway signaling systems, safety assessment, vital communication protocol, IEC 62280

1. Introduction

As existing electrical and mechanical railway signaling systems are replaced with the system using electronic and computer technologies, system capability has improved in such a way that the system is intellectualized and automated. But it is becoming difficult to tracing and managing fault of the compurised systems. So Railway signaling system is a vital system which is directly connected to massive life damage or economical loss due to its features; therefore strict safety activity and evaluation methodology must be required. So safety assurance is needed to prevent these accidents. Then safety activities for assuring safety have to be carried out during the system life-cycle, and safety assessment must be required in the viewpoint of safety activity. And also risk analysis and estimation method are very important in safety activity & assessment.[1-[3].

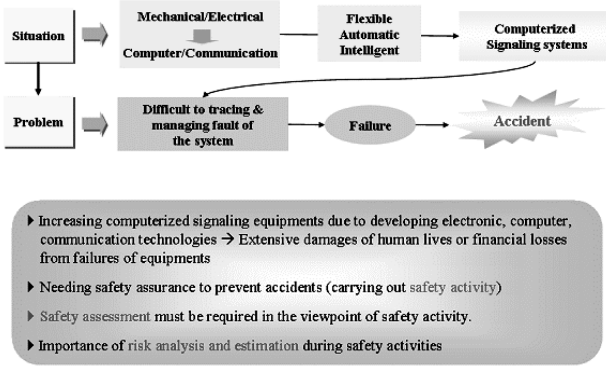

Fig. 1. Needs of safety activity and assessment.

There are international standards, established by IEC [2,3,7], for railway signaling system safety activity requirements and documentation requirements, required to demonstrate those safety activities. Railway signaling system safety assessment is performed by analyzing and evaluating system safety activity process and its results. In order to establish safety evaluation techniques for railway signaling system, therefore, railway signaling system applicable safety activity techniques and analytical methods should be required[4-8].

In this paper, we suggest railway signaling system safety activity techniques for railway signaling system and its specific execution techniques at each activity phase. We also analyze safety assessment task based on suggested safety activity techniques and identify necessary study case required to ensure safety assessment techniques.

*Corresponding author: jghwang@krri.re.krr

2. Review of Safety Assessment for Railway Signaling Systems

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

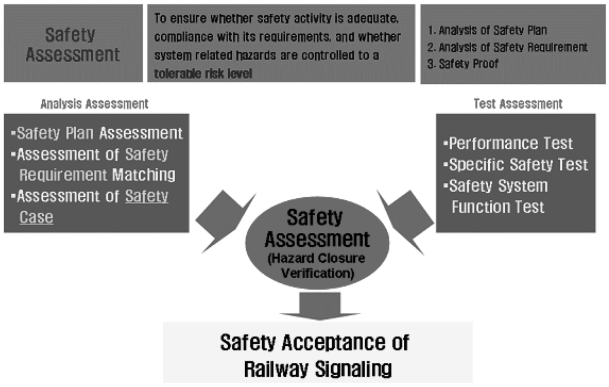

Fig. 2. What is safety assessment?

2.1 What is 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 signaling systems. In foreign countries, the manufacturers of the railway signaling 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 signaling systems according to the IEC standards. In Korea, such international standards have recently been introduced, making the people recognize the need for safety activity and assessment. As a result, some research programs on such safety activity and assessment have been initiated.

In general, the safety assessment of the railway signaling 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 signaling 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 per-

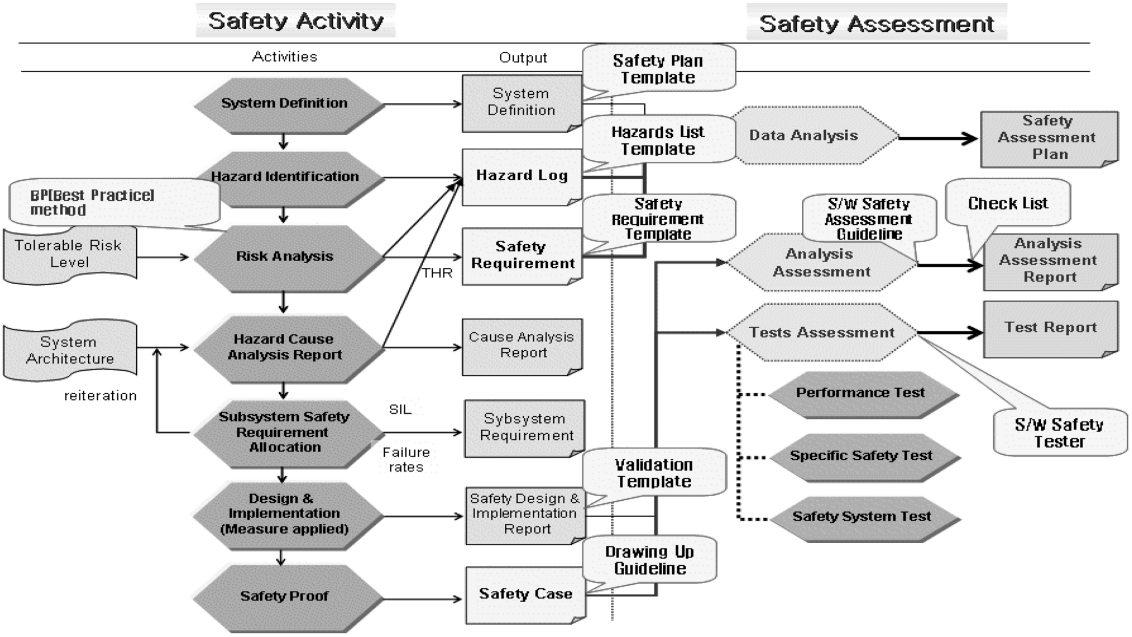

Fig. 3. Safety activity technique for railway signaling system.

formed by the manufacturers and the assessors are specified in IEC 62425.

2.2 Safety Activities for Railway Signaling Systems

Railway signaling system safety activity is done via analyses and evaluations on system safety activity process and its results. Therefore, analysis for railway signaling system applicable safety activity technique must be preceded in order to establish railway signaling system safety assessment technique. In this paper, we suggest safety activity technique for railway signaling system and specific execution technique at each phase by analyzing relevant standards.

Since traditional way to ensure system safety, ensuring system safety via experimental fail-safe, turned out to have various limits, current electronic railway signaling systems choose system life cycle safety activity and its assessment to ensure its safety. Safety activity can be defined as hazard control process including documentation of supporting evidence, performed via systematic and scientific methods. In other words, safety activity is a comprehensive process including hazard identification, hazard risk evaluation, establishing risk plan to remove or mitigate risk, removing hazard at design and implementation phase and assuring that hazard risk is controlled to a tolerable level[4-6].

We suggest safety activity technique as shown in figure 3 through this paper. It aims for safety demonstration by identifying railway signaling system potential hazards and performing hazard analysis and assessment and by demonstrating that identified hazards are controlled to a tolerable level via safety activity. In other words, safety activity technique suggested here consists of ① Preliminary Hazard Analysis (PHA phase), ② Hazard Identification and Analysis (Detailed PHA phase), ③ Target Safety Establishing phase, ④ Hazard Confirmation and Analysis (HIA phase), ⑤ Design & Implementation phase, and ⑥ Safety Assessment and Acceptance phase. Safety activity can be divided into life cycle hazard controlling activity (to a tolerable level) and demonstration activity.

Railway signaling system safety activity technique in accordance with risk-based process can be classified as follows; Preliminary Hazard Analysis (HIA) phase, Hazard Identification and Analysis (HIA) phase, and Risk Analysis & SIL Allocation phase, as shown in figure 2. Railway signaling system safety assessment is a process to ensure whether required documents are provided and those documents are appropriate and whether identified hazards are controlled to a tolerable level via safety activity. For safety assessment, therefore, analyses on railway signaling system safety activity technique and document type and level, described during safety activity, should be performed. We select specific methods applied to the technique in figure 4 as follows; PHA for hazard analysis at 1st phase, FTA and ETA, as a supporting method, for hazard analysis at 2nd phase. As for 3rd phase, we suggest SIL allocation method using THR identified via BP-risk and SIL matrix.

3. Proposed Safety Assessment for Railway Signalling System

3.1 Safety Activity

Fig. 4 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), and 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 acceptable level through safety activities. Therefore, in performing the safety assessment, it is necessary to analyze 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 one, 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).

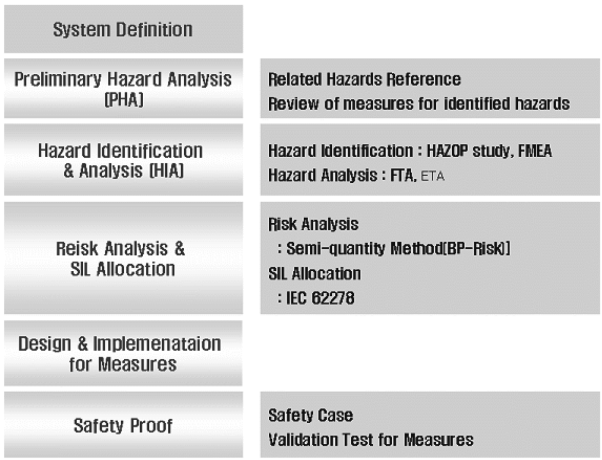

Fig. 4. Safety activity technique proposed.

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 determination whether a system satisfies specific requirements and 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 system requirements are adequate
- Verifying if the system requirements, codes, and standards are complied
- Verifying if system risks are removed or reduced to acceptable levels
- Analyzing and verifying the master safety plan
- Analyzing the hazards log

3.2 Safety Assessment Process

As described in the above, the safety assessment of the railway signaling 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 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.

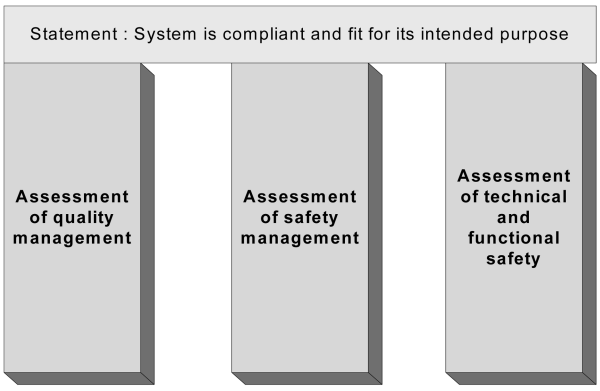

Fig. 5. Assessment Tasks.

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 technical and functional safety as well as assessment of quality system and safety management. Accordingly, as shown in fig. 5, 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.

3.3 Configuration of Safety Assessment

The objective of railway signaling system safety assessment is to ensure whether safety activity is adequate, compliance with its requirements, and whether system related hazards are controlled to a tolerable level. Safety assessment can be divided into analysis task on safety activity and additional task (e.g., fault injection test) evaluation like fig. 3. In other words, safety assessment is done as follows; first, prepare a safety assessment checklist based on safety plan and safety requirements for each safety activity, then draw up a safety assessment plan using this checklist. Finally safety assessment evaluating whether all system related hazards are identified and controlled is performed based on total safety plan specification, which is safety demonstration documents documented according to drown safety assessment plan. Afterwards, final safety is approved via hazard closure verification based on additional test evaluation, such as function confirming test, or fault injection test.

3.4 Analysis of Safety Assessment Tasks

Safety assessment for railway signaling system is usually performed based on safety activity analysis and evaluation. There are several steps to carry on safety activity; those are ① Preliminary Hazard Analysis based on system function requirements and operational scenario ② Safety requirement, hazard list and specific measures are reflected, identification ③ Target safety establishment and allocation via sub-system analysis ④ Sub-system analysis hazard analysis ⑤ Safety plan design and implementation ⑥ Safety Assurance. Generally, it can

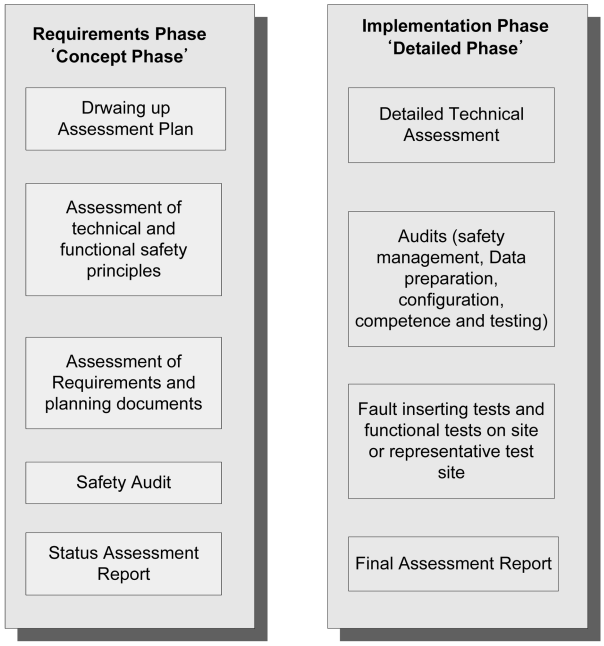

Fig. 6. Safety assessment tasks

be inferred that safety assessment is an activity to ensure all identified hazards are closed via each safety activity process and document validation task.

In this paper, we suggest safety assessment as shown in Figure 3. Safety assessment includes system evaluation whether the system technically and functionally has safety, safety managgement evaluation that makes sure safety activity process is properly performed, and quality management evaluation to ensure system design and manufacturing. Figure 6 shows actual tasks that must be done for safety assessment and those can be divided into fundamental stage and detailed stage. Fundamental stage is a process to establish safety assessment plan based on basic document analysis, such as safety requirements and safety plan. At detailed stage, actual evaluation activities, such as evaluation for safety plan, designed to control hazard risk, and its results, safety management evaluation, and test evaluation.

Figure 6 is safety activity process and safety assessment task for railway signaling system illustrating that safety assessment includes safety analysis assessment and test assessment. Also, the studies that have been carried on so far to ensure safety assessment techniques are separately addressed. To sum up, safety assessment is an activity performed to analyze and evaluate whether any risk is controlled to a tolerable level. Therefore, we try to obtain critical hazard list for railway signaling system and to analyze safety requirement template and safety assessment template. We also carry on some studies on guideline for documentation of total safety plan specification and S/W safety assessment guideline; in addition, study on BP (Best Practice) method application to railway signaling system is in progress. Figure 6 illustrates some research topics necessary for railway signaling system safety assessment and its expected results. We expect that various researches will be carried on this field.

4. Conclusion

In this paper, we suggest safety activity technique for railway signaling study and relevant application technique since the needs for developing standardized railway signaling system safety activity and assessment technique have been increased. In addition, we draw up some research topics required to obtain safety assessment technique by analyzing safety assessment tasks according to railway signaling system safety activity. An in-depth and more specific study for railway signaling system safety assessment based on this paper is expected to carry on continuously.

References

[1] RAILTRACK, “Engineering Safety management Issue 3 Yellow 3, 4”, 2005.
[2] IEC 62278, “Railway Applications - The specification and demonstration of RAMS”, 2002.
[3] IEC 62425 Ed. 1, “Railway Application: Communications, signaling and processing systems - Safety related electronic system for signaling”, 2005.10.
[4] Nicholas J. Bahr, “System Safety Engineering and Risk Assessment”, Taylor & Francis, 1997.
[5] Yacov Y. Haimes, "Risk Modeling Assessments and Management", Wiley-Interscience, 2004.
[6] NASA Dryden Flight Research Center, “Dryden Handbook Code S - System Safety Handbook”, March 1999.
[7] J.Braband and et al, “The CENELEC-Standards regarding Functional Safety”, Eurailpress, 2006.
[8] J.Braband and et al, “Risk-orientated Apportionment of Safety Integrity Requirements -An Example”, SIGNAL+ DRAHT, Vol. 1+2, 2000.
[9] Y.Hirao, “New European Norms from a Japanese Viewpoint”, SIGNAL+DRAHT, Vol. 11, 2001