Vol. 10, No. 2, pp. 27-31, December 2011

INTERNATIONAL JOURNAL OF SAFETY
www.kosos.or.kr

Review of Safety Activity Process for Safety Enhancement of Railway Signaling System

Jong-Gyu Hwang

Korea Railroad Research Institute, Uiwang-si 437-757, Korea

(Received October 18, 2011; Accepted December 10, 2011)

Abstract : As safety-related regulations for signaling systems are standardized to IEC 61508 and 62425, and others at the international level, safety activities and its verification are required. And also there is need to develop technologies for safety improvement to secure safety signaling systems in terms of technologies for safety activities on each life-cycle. In this paper it is reviewed the safety activity processes and technologies each steps of proposed processes respectively for railway signaling systems.

Key words : safety activity procedure, hazard identification, railway signaling system

1. Introduction

The electronic and computerized railway signaling systems have replaced the existing mechanical systems, resulting in intelligent and automatic high-performance systems. For the existing electrical systems, empirical approaches and engineer's intuition are mainly used to detect any faults, assuring a certain degree of safety in the railway signaling systems. However, the new computerized railway signaling systems do not allow the safety assurance based on such empirical approaches to detect faults. Therefore, IEC(International Electrotechnical Commission) requires more rigorous safety activities to assure the safety in the railway signaling systems [1]-[5]. 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 signaling systems.

The safety activity requirements for railway signaling systems were established as the international standards by the IEC. Further, the IEC standards describe the documentation requirements necessary to demonstrate such safety activities [6][7]. The safety assessment of the railway signaling systems is done by performing safety activities and analyzing/evaluating the results. Therefore, it is necessary to analyze and establish the safety activity system and tools appropriate for railway signaling systems [8][9]. In this paper, it is analyzed the railway signaling system safety activity process and its applying techniques for railway signaling systems.

*Corresponding author: jghwang@krri.re.kr

2. Int'l std. related safety activity

The embedded system such as railway signaling system is very difficult to identify the inherent faults for occurrence of accidents during lifecycle. And also all inherent faults or cause is not deduced the accidents. So the identification of faults for occurrence of accidents is important and the deduced faults have to be eliminated or suppressed tolerable level. Those faults are called as a hazard in this paper like Fig. 1.

This section briefly explains safety activity system to be presented through railway signaling system safety-related standards. Fig. 2 is the one showing safety-

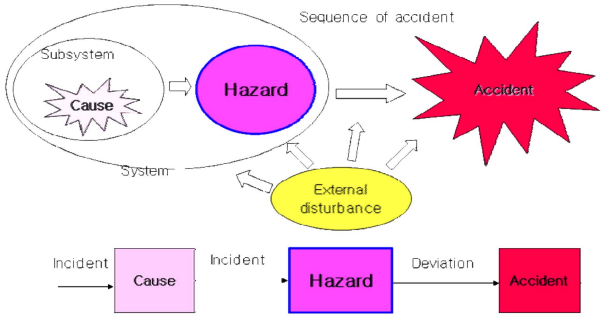

Fig. 1. Accident occurrence mechanism.

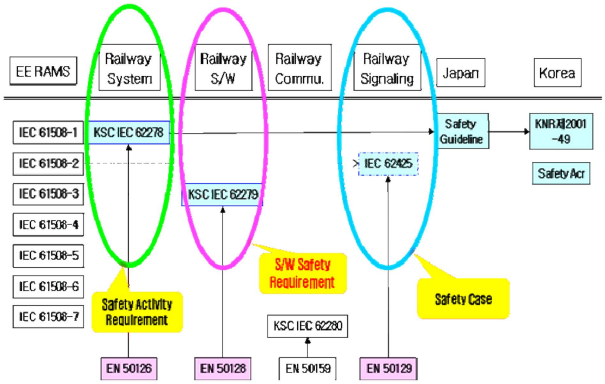

Fig. 2. Safety-related international standards for railway signaling systems.

related standards, which are standardized internationally by being divided largely into various parts such as system, S/W, communication and Safety, etc. with IEC 61508 which is the standard for electric/electronic system as their base.

In Korea, the technical guideline for safety is presented by KORAIL as a recommendation with IEC 61508-1 as its base. As shown in Fig. 2, the direct international standards in relation to the safety activity of Railway Signaling System are IEC 61508, IEC 62278 and IEC 62425. Among them, the former two standards are for the entire RAMS, and the last one is the standard in relation to the safety activity.

Fig. 2 is the one expressing the structure of safety case to prove the safety activity of railway signaling system described in IEC 62425. That is, it shows that the safety in railway signaling system in IEC 62425 shall be implemented and evaluated through three large axes called as quality management, safety management and technical supporting evidence for safety. Among of them, the last two contents are the results of safety

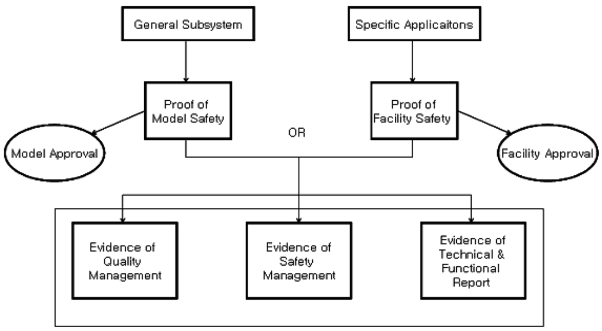

Fig. 3. Structure of the safety demonstration based on IEC 62425.

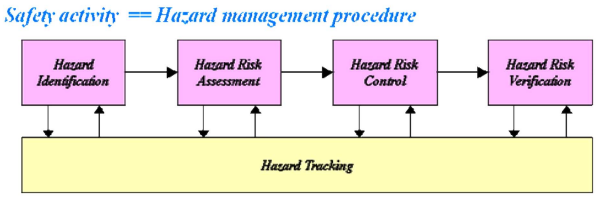

Fig. 4. Hazard management procedure.

activity during safety lifecycle.

3. Safety activity process

As explained in the previous section, the safety activity of railway signaling system becomes very important activity in the aspect of securing safety of system. This section will review and suggest these safety activities of railway signaling system.

The former European safety-related standards on railway systems were transformed into the international standards by the IEC, which requirement the safety activity 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 Korea, such international standards have recently been introduced, making the people recognize the need for safety activity. As a result, some research programs on such safety activity have been initiated.

In general, the safety activity of the railway signaling system is conducted by the manufactures to get a safety assessment and certificate by ISA(Independent Safety

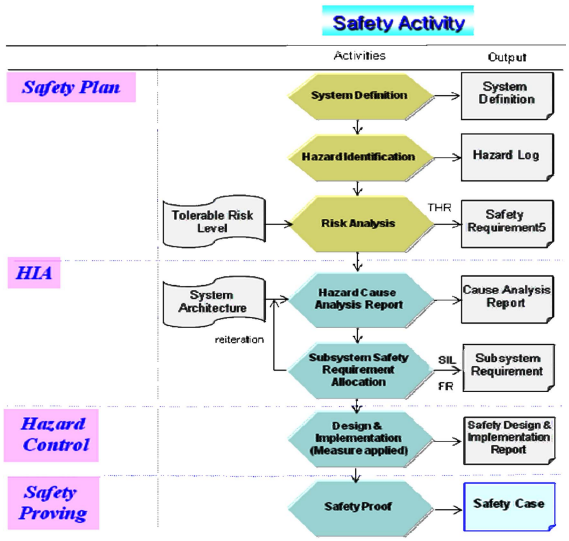

Fig. 5. Safety activity with system lifecycle.

Assessor). The basic system requirements for safety activity 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 performed by the manufacturers are specified in IEC 62425.

There are various stages of safety activity stage in accordance with each stage of system life cycle, and among them, there are overlapping parts according to the stage. This thesis presented the safety activity suitable for railway signaling system as shown in the following figure, and the figure displayed each stage of system life cycle presented in IEC 62278.

The safety activity system was presented through this thesis, and the main output by stage was marked. That is, the Hazard Log which is the result of safety activity and one of the most important documents is created at the Hazard derivation stage which is the second stage, and it is the document which must be updated continuously at previous stage of safety activity. And the safety requirement of system is to be prepared as the result of risk analysis stage, and finally, the safety case for proving the safety is to be prepared at the final stage.

Fig. 4 is the figure displayed with summarized safety activity procedure as its center without comparison with system life cycle, which is the same procedure as that of Fig. 5. That is, the safety activity procedure for

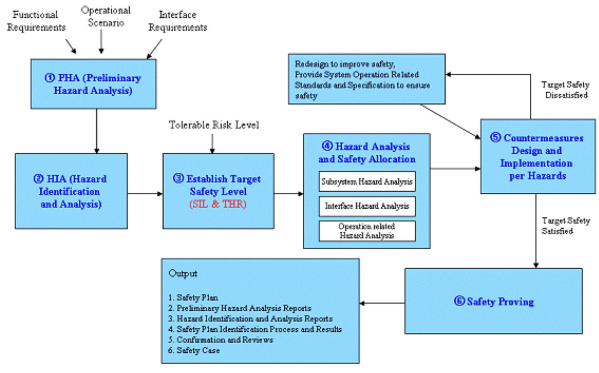

Fig. 6. Summarized safety activity procedure.

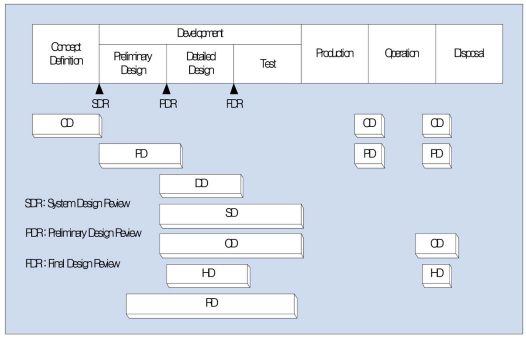

Fig. 7. Hazard analysis type according to system lifecycle.

securing and proving the safety of railway Signaling system is to draw potential hazard of railway signaling system preferentially and perform the analysis and assessment on it, and finally, the safety proof can be accomplished by proving whether this drawn hazard was controlled to be set below permissible level through safety activity. That is, they are composed of preliminary Hazard analysis stage, Hazard derivation and analysis stage, Safety target establishment stage, Hazard validation and analysis stage, stage for design and implementation of risk measures by Hazard, and final Safety Validation and Verification stage. The safety activities are composed of stages which manage and control the hazard of railway signaling system through system life cycle, and finally make it controlled below permissible level and prove it.

As a mentioned above, there are several steps in safety activity during system lifecycle, and also several methods and techniques in each safety activity steps. It is important to select the suitable methods for each step to ensure the safety when safety activity is performed for specific railway signaling systems. Fig. 6 represents the hazard analysis type, such as CD, PD, DD, SD, OD, HD and RD. Those hazard analysis types are allocated to the safety activity steps respectively like figure 5.

- CD : Conceptual Design hazard analysis type
- PD : Preliminary Design hazard analysis type
- DD : Detailed Design hazard analysis type
- SD : System Design hazard analysis type
- OD : Operations Design hazard analysis type
- HD : Health Design hazard analysis type
- RD : Requirements Design hazard analysis type

And also there are several methodologies and techniques for each hazard analysis types like table 1, which is recommended hazard analysis methods for IEC 62425 standards. It is important to apply the suitable method and technique for each hazard analysis types for

Table 1. Relation between Hazard Analysis Type and Methods

Tech-nique	Type	Identify Hazard	Identify Root Causes	Lifecycle Phase	Qualitative/ Quantitative
PHL	CD	Y	N	CD~PD	Qualitative
PHA	PD	Y	P	CD~PD	Qualitative
SSHA	DD	Y	Y	DD	Qualitative
SHA	SD	Y	Y	PD~DD~Test	Qualitative
O&SHA	OD	Y	Y	PD~DD~Test	Qualitative
HHA	HD	Y	Y	PD~DD~Test	Qualitative
FTA	SD, DD	P	Y	PD~DD	Qualitative/ quantitative
ETA	SD	P	P	PD~DD	Qualitative/ quantitative
FMEA	DD	P	P	PD~DD	Qualitative/ quantitative
HAZOP	SD	Y	P	PD~DD	Qualitative
FaHA	DD	P	P	PD~DD	Qualitative
FuHA	SD	P	P	CD~PD~DD	Qualitative

the reason. There are many followed methodologies for hazard analysis besides of above mentioned IEC 62425. Table 1 is shows the relation between hazard analysis types and methodologies. This table is represents the applying yes or not of hazard identification, hazard analysis type, lifecycle phases, qualitative or quantitative approaches for each techniques respectively.

- *PHL : Preliminary Hazard List*
- *SSHA : Subsystem Hazard Analysis*
- *SHA : System Hazard Analysis*
- *O&SHA : Operation & Support Hazard Analysis*
- *HHA : Health Hazard Analysis*
- *FaHA : Fault Hazard Analysis*
- *FuHA : Functional Hazard Analysis*

In this study, some methodologies and techniques were selected for railway signaling systems like figure 5. The PHL technique is applied for hazard identification, PHA, SSHA and IHA methodologies are applied to risk analysis steps, BP-risk method and THR allocation are selected for risk estimation steps, and FTA method is selected for causal analysis step and next SIL level is allocated each functions and hazards. The HAZOP-KR (HAZOP for Korean Railway) technique is proposed and applied for PHA methodology. This technique is proposed to apply the Korean railway signaling system by modification and fitting of existing HAZOP

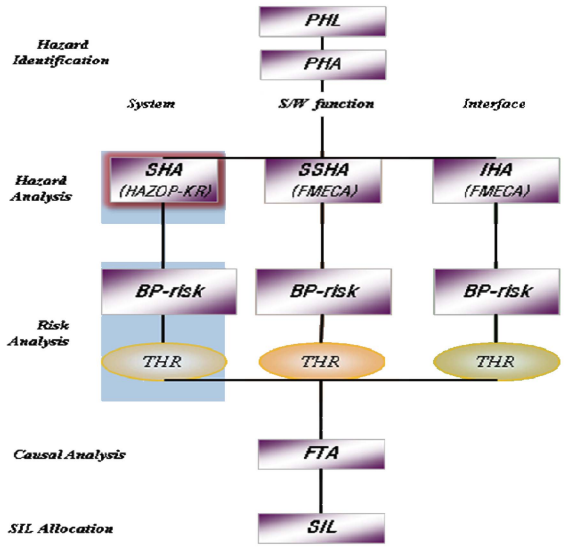

Fig. 8. Selected methodologies for safety activity.

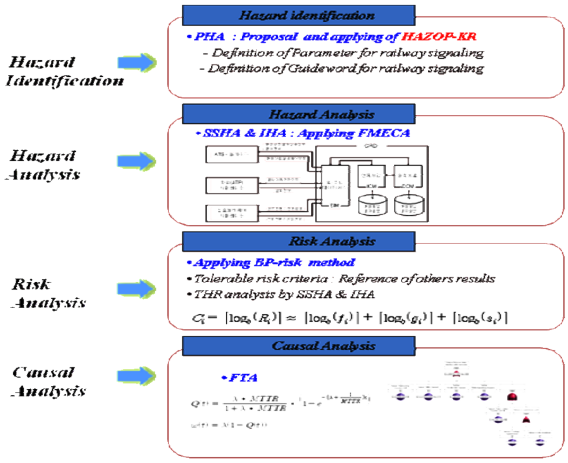

Fig. 9. Applying example for selected safety activity.

study because existing one is suitable to chemical industry [11]. The FMEA technique is selected as a methodology for SSHA and IHA. BP-risk method is applied firstly in Korea as a risk estimation methodology which is proposed for risk estimation technique as a semi-quantitative approach at Siemens company in Germany.

In conclusion, the HAZOP-KR, new HAZOP methodology for Korean railway signaling system, has been proposed and applied firstly the BP-risk method for risk estimation in this study. And also the PHA, FTA, FMECA techniques are applied the CRD system for analysis and establishment of safety activity systems. Fig. 7 shows the selected safety activity procedure with selected techniques and methods for railway signaling system.

3. Conclusion

This thesis reviewed the safety activity procedure and suitable methodologies in compliance with international standards have been increasingly highlighted. This study proposes the methodology for safety activity procedure and techniques based on the system lifecycle, and several new methodologies are introduced as a suitable methodology for safety activity executing for railway signaling system. It is anticipated that the proposed procedure and methodology is able to apply the safety activity for real railway signaling system.

REFERENCES

[1] International Standard, *Functional safety of electrical/ electronic /programmable electronic safety-related systems*, IEC 61508, 1998.

[2] International Standard, *Railway Applications - The specification and demonstration of RAMS*, IEC 62278, 2002.

[3] International Standard, *Railway Application: Communications, signaling and processing systems - Safety related electronic system for signaling*, IEC 62425 Ed. 1, 2005.

[4] J. Braband and et al, *The CENELEC-Standards regarding Functional Safety,* Eurailpress, 2006.

[5] Y.Hirao, *New European Norms from a Japanese Viewpoint*, *SIGNAL+DRAHT, Vol. 11, 2001.*

[6] J.G.Hwang, H.J.JO and Y.K.Yoon, *Analysis of Safety methodology for Railway Signaling Systems*, International Journal of Safety, Vol. 6, No. 2, pp. 38-42, 2007.

[7] Nicholas J. Bahr, *System Safety Engineering and Risk Assessment*, Taylor & Francis, 1997.

[8] J. Braband, *Risikoanalysen in der Eisenbahn- Automatisierung*, Eurail Press by Siemens AG, 2005.

[9] J. Braband, *Improving the Risk Priority Number Concept*, Journal of System Safety, pp. 21-23, 2003.