IJR International Journal of Railway
Vol. 2, No. 3 / September 2009, pp. 113-117

The Korean Society for Railway

Risk Management Qualitatively on Railway Signal System

Ya-dong Zhang* and Jin Guo**

Abstract

Risk management is an important part of system assurance and it is widely used in safety-related system. Railway signal system is one kind of safety-related system and its most important goal is to guarantee the safety of railway system. The method based on risk management can find and solve the security issues of railway signal system more effectively. This paper introduces the basic conception of risk management, studies the whole process of risk management and related tools and techniques and discusses some key points qualitatively combining with the particularity of railway signal system.

Keywords : *Safety, Risk, Hazard, System lifecycle, Risk management, Railway signal system*

1. Introduction

Today in the field of railway signal system, the method based on technique specifications is usually adopted to ensure safety [1]. This method can guarantee the safety of railway signal system in a large extent. However, with the development of science and technology, this method exposes many problems. The method based on technique specifications can not meet the requirement of the high-speed development of railway. It is required to find other more effective and scientific methods to guarantee the safety of railway signal system. Here this paper introduces the qualitative method based on risk management combining with the particularity of railway signal system. The method based on risk management can guarantee the safety of railway signal system more effectively.

2. The Basic Conception of Risk Management

Risk management is an important part of system assurance.

It includes the processes of analyzing risks, evaluating risks, making decisions on accepting or altering risks, restricting risks and monitoring risks.

The core of risk management is how to guarantee the safety of safety-related system through managing system risks. It can minimize the chance of failure and maximize the chance of success.Risk management is a durative process through all the system lifecycle [2]. The system lifecycle is a very important conception in the safety-related system. It includes 14 phases as shown in Fig.1.

3. The Whole Process of Risk Management

The risk management includes the processes of hazard

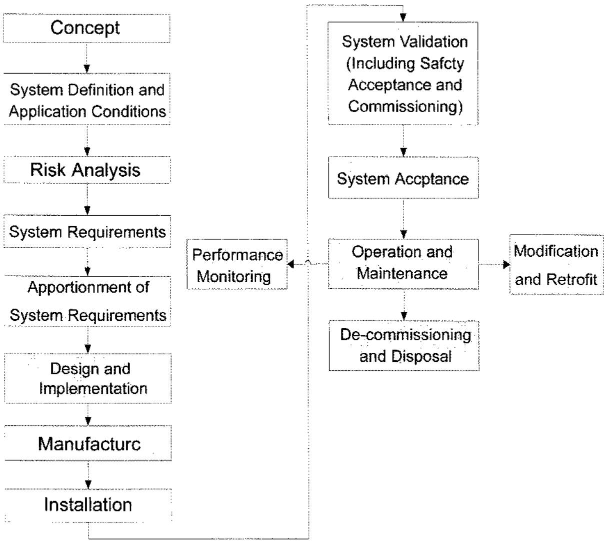
Concept
System Definition and Application Conditions
Risk Analysis
System Requirements
Apportionment of System Requirements
Design and Implementation
Manufacturc
Installation
System Validation (Including Safcty Acceptance and Commissioning)
System Accptance
Operation and Maintenance
Performance Monitoring
Modification and Retrofit
De-commissioning and Disposal

Fig. 1 System Lifecycle

[*] Southwest Jiaotong University, China
E-mail: zyd308@163.com

[**] Southwest Jiaotong University, China
E-mail: gj60@sina.com

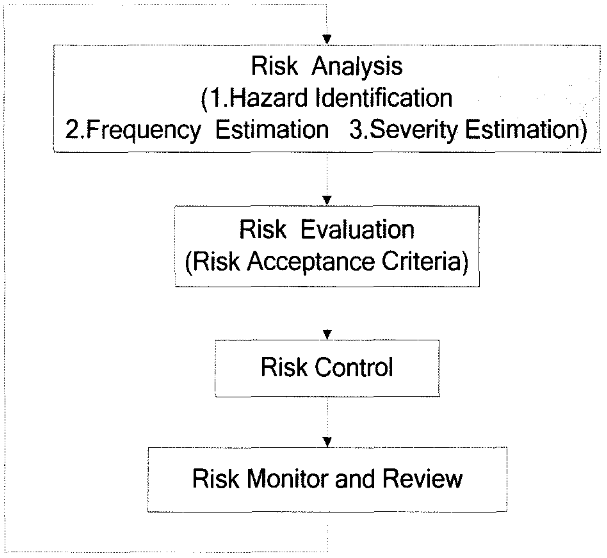

Fig. 2 The whole process of risk management

identification, frequency and severity estimation, risk evaluation, risk control and monitoring and reviewing risk. The whole process of risk management is shown in Fig. 2.

3.1 Hazard Identification

Hazard identification is the first step of risk management. Hazard is a source of potential harm or a situation with a potential to cause loss. Through hazard identification, it should find out and record all hazards of railway signal system. It also should number, give description for every hazard and record the cause and effect of hazards using a hazard log.

3.1.1 Tools and Techniques

During the process of hazard identification, it should make use of various tools and techniques to recognise the hazards of railway signal system. There are a number of tools and techniques summarized as follows:

(1) HAZOP Studies [3]

HAZOP is the shortened form of Hazard and Operability. It is developed by ICI from the idea of Method Study and widely used in various industries to explore causes and consequences of deviations from normal operations to identify hazards and operability problems. The form of HAZOP is brainstorming session. HAZOP is undertaken by a formal, systematic and critical examination of the process and engineering intentions of a design. The examination is structured around a specific set of guidewords, which ensure complete coverage of all possible problems while allowing sufficient flexibility for an imaginative approach. The guidewords should be tailored to the railway signal system concerned before starting a HAZOP study.

(2) Hazard Review

This is a qualitative review of a facility to identify hazards that may be present. Hazard review is desk study that looks at previous risk assessments, accident histories, previous experience, guideline codes and practices.

(3) Literature Review

Literature review is usually performed as part of the Hazard review. It should form part of risk assessment especially where little information is available and it is usually performed at concept stage.

(4) Accident Investigation

Accident reports are a very good source of hazard information. In a review of accident reports, it is important to review near misses and those with minor outcomes as well as the more serious ones.

(5) Hazard Checklist

Hazard checklist is a written list of questions designed to prompt the consideration of a full range of safety issues. It should be developed by individuals who understand the design and operating procedures.

(6) Site Inspection and Audit

Site inspection and audit is visual inspection of a facility. It is typically combined with hazard checklist. Through reviewing previous site inspections and audits to see if hazards can be identified. Not only restricted to hardware but also procedures and practices. It only works for existing facilities not very useful for novel and new designs.

These tools and techniques mentioned above have their own characteristics. In order to identify hazards of system comprehensively, especially the complex system like railway signal system, it needs to use above tools and techniques synthetically in the process of identifying hazards.

3.1.2 Different phases hazard analysis

In the different phases of system lifecycle, it should identify and analysis hazards of system in greater depth.

(1) Preliminary Hazard Analysis (PHA)

The aim of PHA is identifying potential hazards arising from the railway signal system at a high level. It needs to be performed as early as possible in the design and presents the design controls requiring attention early.

(2) System/Subsystem Hazard Analysis (SHA/SSHA)

SHA/SSHA is a similar process to the PHA. It focuses on specific system/subsystems. SHA/SSHA is conducted after the PHA.

(3) Interface Hazard Analysis (IHA)

IHA identifies the interfaces (functional analysis) of system. It needs to consider two problems: how can other systems affect this system and how can the system affect other systems? It also need consider operation, mal-operation, failure and incorrect specification.

(4)Operation and Support Hazard Analysis (OSHA)

OSHA should consider the risk to the operator and maintainer. The risk arises from normal, abnormal operations and routine, scheduled, unscheduled maintenance. It also needs to consider specifics of the operator/machine interfaces and specific tasks to be performed.

3.2 Frequency and Severity Estimation

After hazard identification of railway signal system, it should estimate the frequency and severity of hazards. For the hazard frequency and severity, it can be analyzed qualitatively and calculated quantitatively. Here this paper focuses on the qualitative analysis.

Table 1[4] provides, in qualitative terms, typical categories of probability or frequency of occurrence of a hazardous event and a description of each category for a railway signal system. The categories, their numbers, and their numerical scaling to be applied shall be defined by the Railway Authority, appropriate to the application under consideration.

Table 2[4] describes typical hazard severity levels and the consequences associated with each severity level for all railway systems. The number of severity levels and the consequences for each severity level to be applied shall also be defined by the Railway Authority, appropriate for the application under consideration.

Table 1. Frequency categories

Category	Descriptions
Frequent	Likely to occur frequently. The hazard will be continually experienced.
Probable	Will occur several times. The hazard can be expected to occur often.
Occasional	Likely to occur several times. The hazard can be expected to occur several times.
Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

Table 2. Severity Categories

Severity Level	Consequence to Persons or Environment	Consequence to Service
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment.	
Critical	Single fatality and/or severe injury and/or significant damage to the environment.	Loss of a major system
Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

According to history records of similar railway signal system, components invalidation rate of system, effect of system/subsystem/component invalidation, related expert experience and advice, etc, it can estimate the frequency and severity of hazards. Then according to frequency categories as shown in Table 1 and severity categories as shown in Table 2, it can qualitatively analyze the frequency and severity of hazards and obtain the rank of frequency and severity finally.

3.3 Risk Evaluation

Risk is the likelihood of a specific undesired event occurring within a specified period. Risk includes individual risk, society risk, economy risk and environment risk. It is closely related with frequency and severity of hazards. Here, the paper focuses on introducing the risk matrix method[4] to qualitatively evaluate the risk.

According to the results of qualitative analysis of frequency and severity, it can use risk matrix method to qualitatively analyze risk of railway signal system. Risk criticality matrix is shown as in Table 3.

It shows an example of risk evaluation and risk reduction/controls for risk acceptance. The abscissa of risk criticality matrix is severity of hazard and the ordinate is frequency of hazard. As shown in Table 3, there are 4 grades as listed below:

①Unacceptable: It must adopt risk control measures to reduce the risk.

②Undesirable: It shall only be accepted when risk reduction is impracticable and with the agreement of the railway authority.

③Tolerable: It is acceptable with adequate control and the agreement of the railway authority.

④Acceptable: It does not need adopt any risk control measure and the risk can be ignored. Risks need to be

Table 3. Risk criticality matrix

		1	2	3	4
		Insignificant	Marginal	Critical	Catastrophic
A	Frequent	Undesirable	Unacceptable	Unacceptable	Unacceptable
B	Probable	Tolerable	Undesirable	Unacceptable	Unacceptable
C	Occasional	Tolerable	Undesirable	Undesirable	Unacceptable
D	Remote	Acceptable	Tolerable	Undesirable	Undesirable
E	Improbable	Acceptable	Acceptable	Tolerable	Tolerable
F	Incredible	Acceptable	Acceptable	Acceptable	Acceptable

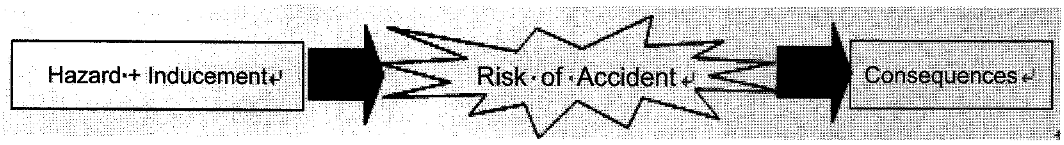

Fig. 3 Sketch map of risk

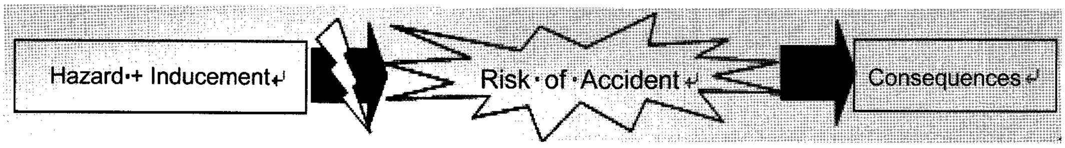

Fig. 4 Risk control measures – preventive measure

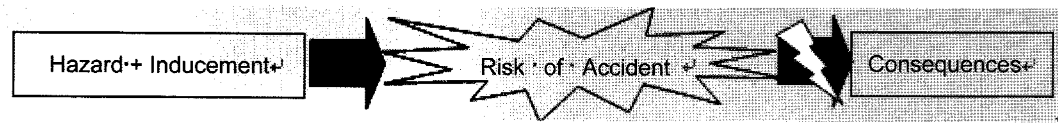

Fig. 5 Risk control measures – mitigation measure

reviewed on a periodic basis or subsequent to any accidents, incidents or near misses.

According to the method based on risk criticality matrix, it can evaluate the risk qualitatively.

3.4 Risk Control

After risk analysis and evaluation, it should consider some control measures and record them to reduce risk if the risk is in the unacceptable region, undesirable or the tolerable region. If the risk is in the acceptable region, the risk can be ignored and it does not need adopt any risk control measures. Control measures should be aimed at either reducing frequency or reducing severity. Here are some ideas about how to consider the risk control measure.

①Removal: Remove the hazard.

②Replacement: Replace the hazardous situation with something less hazardous.

③Separation: Separate the hazard away from sensitive population or equipment.

④Protection: Erect a barrier to protect sensitive population or equipment, or installation of safety devices.

⑤Procedures: Implement working methods that mitigate the hazard.

Hazard is a source of potential harm or a situation with a potential to cause loss. When there is an inducement, it is likely to happen and cause series of consequences. See Fig. 3.

To reduce the risk, it can adopt preventive measures as expressed in Fig.4 to reduce the frequency and mitigation measures as expressed in Fig.5 to reduce the severity.

3.5 Monitoring and Reviewing Risk

After the steps of hazard identification, frequency and severity assessment, risk evaluation and risk control, it also should ceaselessly monitor and review risk. Risk management is a durative process through all the system lifecycle. In the different phases of system lifecycle, it needs to repeat these steps again and again to insure the safety of system.

In every step of risk management, it needs to record the results using a hazard log. Hazard log will be developed to provide a central depository for all hazards to be reviewed and tracked, and to provide a means of monitoring the progress of the hazard controls. The hazard log will continue to be improved along with the development of system lifecycle.

During the process of risk management, it needs to identify safety responsibilities and put them in writing. It must keep records of the transfer of safety responsibilities and make sure that anyone taking on safety responsibilities understands and accepts these responsibilities. It also needs to make sure that anyone who is transferring responsibility for safety passes on any known assumptions and conditions that safety depends on. Only identifying the safety responsibilities, risk management can be performed perfectly.

4. Conclusion

Risk management is an advanced and popular theory in the field of management and engineering. It is an important part of system assurance and widely used in safety-related systems. Here this paper introduces the method based on risk management from qualitative point of view. Through the method based on risk management, it can find and solve the security issues of railway signal system more effectively. However, there are many methods and technologies in this theory that need to be studied and discussed more in future. Through studying this theory in depth and applying it exactly, the safety of railway signal system can be ensured more effectively and comprehensively.

Reference

[1] IEC61508-1997, *Functional safety of electrical/electronic/ programmable electronic safety-related systems.*

[2] IEC62278-2002,*Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)* .

[3] IEC61882-2001, *Hazard and operability studies (HAZOP studies) - Application guide.*

[4] EN50126-1999, *Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).*