Risk assessment method for guaranteeing safety in the train control system

H.-J. Jo, J.-G. Hwang & Y.-K. Kim
Train Control System Research Team,
Signalling and Electrical Engineering Research Department,
Korea Railroad Research Institute (KRRI), Korea

Abstract

Recently, failure of equipment has been linked directly to human casualties or financial losses from the increasing use of train control equipment utilizing computers. These systems have to progress to guarantee safety during the system life-cycle. In this paper, we examine the methods for risk analysis and assessment of safety activities and propose an optimized method for risk estimation. In the comparison of the risk graph and the risk matrix method for safety estimation, the proposed BP (Best Practice)-risk method combines the most beneficial properties of commonly used approaches.
Keywords: risk analysis, train control system, Best Practice risk.

1 Introduction

Vital control systems, such as train control systems, are computerized for guaranteeing the safety of trains and take charge of controlling train speeds and direction, especially preventing train collisions, located about the side of rails. Such train control systems require higher reliability than the general industrial controlling systems. These systems have to guarantee safety during the system life-cycle. Risk assessment is an important phase to increase safety from determining the risk presented by the identified hazard. In this paper, we investigate several methods for risk analysis and estimation of safety activities in the life-cycle, and then we draw a comparison between original methods to suggest an optimized one in the application to train control systems. In the result of the comparison, we propose the risk analysis method called BP-risk analysis

WIT Transactions on The Built Environment, Vol 96, © 2007 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/UT070531

combining the advantages of qualitative and quantitative analysis [1]. In addition, we attempt to apply the BP-risk method to ATC (Automatic Train Control) system handling speed restriction in Korea.

2 Risk analysis and estimation

Risk is the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm [2]. Risk is defined as the product of the hazard severity times the hazard probability. Risk is utilized to control and manage the hazard within tolerable levels from safety activities. The risk oriented approach of established standards such as IEC 61508, EN 50129, is to allow a maximum level of risk of a product that is acceptable to railway authorities or standards [3]. This level of risk is called tolerable risk. Risk analysis is the total process of identifying safety risk. This involves system definition, hazard identification, consequence analysis, risk estimation, THR (Tolerable Hazard Rate) allocation, and hazard control. There are original risk assessment methods; risk graph and risk matrix method under the qualitative analysis, IRF (Individual Risk Formula) calculations and a statistical calculations method under the quantitative analysis shown in Figure 1 [4]. The statistical calculation is a quantitative method based on accumulated data for accidents of advanced railway countries to measure risk statistically. BP-risk analysis is the compromise method between qualitative and quantitative analysis.

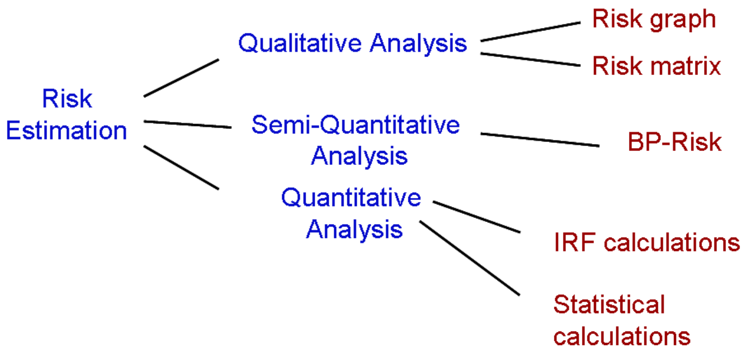


Figure 1: Risk assessment methods.

2.1 Risk matrix

Risk matrix is the method to determine risk class from a matrix form for hazard frequency and severity as in Table 1. We are able to confirm that the risk can be within a tolerable level or the risk has to be controlled below than tolerable level by a safety action. For the consequence scale, the following assumption is made: 1 fatality = 10 Major Injuries = 100 Minor Injuries; the frequency and severity classifications are contiguous overlapping bands as opposed to discrete values.

Table 1: Risk matrix.

Frequency	Total risk levels			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	Marginal	Critical	Catastrophic
	Severity levels of hazard Consequence			

Table 2: A calibrated frequency – consequence matrix.

Frequency	Total risk levels			
10^{-1} per hour Frequent	10^{-3}	10^{-2}	10^{-1}	1
10^{-2} per hour Probable	10^{-4}	10^{-3}	10^{-2}	10^{-1}
10^{-3} per hour Occasional	10^{-5}	10^{-4}	10^{-3}	10^{-2}
10^{-4} per hour Remote	10^{-6}	10^{-5}	10^{-4}	10^{-3}
10^{-5} per hour Improbable	10^{-7}	10^{-6}	10^{-5}	10^{-4}
10^{-6} per hour Incredible	10^{-8}	10^{-7}	10^{-6}	10^{-5}
	Insignificant Minor Injuries	Marginal Major Injuries	Critical 1 Fatality	Catastrophic >=10 fatalities
	Severity levels of hazard consequence			

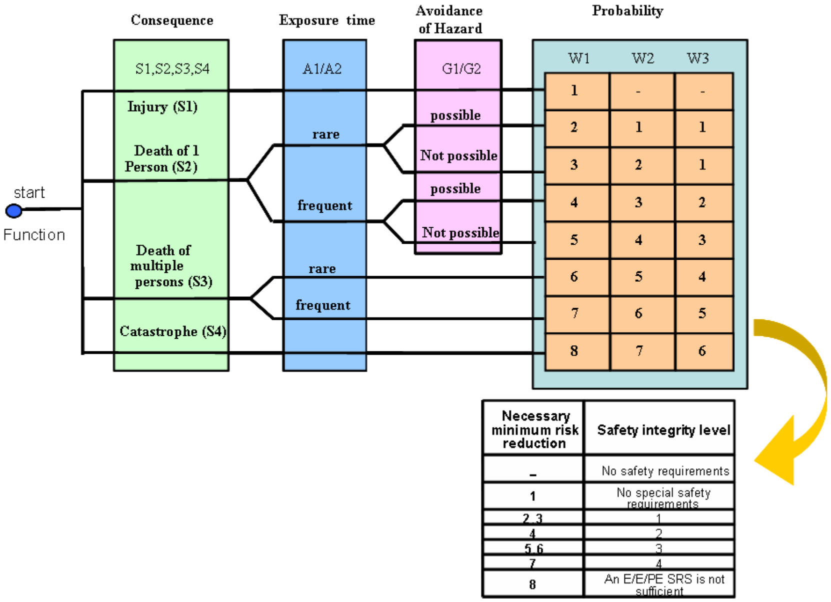
By the risk matrix method, safety targets can easily be derived, but this would result in a very coarse measure for the individual risk of fatality arising from a hazard caused by failure or mal-operation of a signalling system. Also, this method tends to overestimate risks because users often consider the maximum damage and tend towards the view of making no distinction between hazards and accidents and some important parameters as a reduction factor are missing. This can lead to higher safety requirements if hazard avoidance might be possible.

2.2 Risk graph

Until the release of IEC 61508, the DIN standards such as DIN19250 and DIN0801 developed for applications to safety-related systems are utilized in Germany. The DIN 19250 standard defines the relationship between risk and the required German Requirement Class. The standard uses a risk graph with consequence, frequency and exposure, probability of avoiding hazard, and the probability of unwanted occurrence as inputs. The DIN 0801 defines the techniques and measures that are required to meet each of the German

Requirement Classes. These techniques and measures are dependent on the requirement class and are used to control the effect of hardware failures and systematic failures.

In the risk matrix method, just frequency and severity are considered but the risk graph uses additional parameters. Then the risk graph can be regarded as a better analysis of risk method than the risk matrix and often applied to risk assessment in European train control systems. In Figure 4, risk classes are estimated by using these parameters, SIL (Safety Integrity Level) can be allocated to the measured classes. Specified W scale of final results from risk graph is provided with SIL for safety-related systems. This method is easy to use and comprehensive. However, it has disadvantages in that the categories of the parameter are only verbally described and there is no explicit consideration of the duration time of the hazard. That means that although it is very useful, it does not fulfil all engineering requirements completely. For this reason the Best-Practice approach has been developed.



W1	W2	W3
1	-	-
2	1	1
3	2	1
4	3	2
5	4	3
6	5	4
7	6	5
8	7	6

Necessary minimum risk reduction	Safety integrity level
–	No safety requirements
1	No special safety requirements
2,3	1
4	2
5,6	3
7	4
8	An E/E/PE SRS is not sufficient

Figure 2: Risk graph case.

2.3 IRF calculations

In general, an individual or a collective risk can be calculated. To calculate the individual risk of fatality IRF the following formula can be used:

$$IRF_i = N_j \sum_{Hazards\_H_j} \cdot \left((HR_j \cdot D_j + HR_j \cdot E_{ij}) \cdot \sum_{accidents-A_k} C_{jk} \cdot F_{ik} \right) \qquad (1)$$

where all types of accidents are *1...k*, all hazards are *1...j*, Individual risk is *i*. Simplified for one hazard there are the following dependencies:

$$IRF = N \cdot HR \cdot (D + E) \cdot \sum_k C_k \cdot F_k \tag{2}$$

where *HR* is the hazard rate of protection system, *N* is the frequency that a person is using the system, *D* is the duration time of the hazard, *E* is the duration time that a person is exposed to the hazard, C_k is consequence probability of occurrence for an accident, and F_k is the probability of fatality for a single individual. Because the *HR* is needed to calculate the IRF there is no clear border between risk and hazard analysis when conducting a quantitative risk analysis. IRF parameters are used in a mathematical context and therefore clearly and exactly defined. However this method needs much effort and is not independent from the intended system architecture because the hazard rates are used in the calculations.

2.4 BP-risk analysis

Each risk analysis method has its own benefit and is more or less recognized by experts and authorities. Many approaches are cost-intensive and time-consuming and require a high degree of expertise. Siemens introduced the risk analysis method BP that combines the most beneficial properties of commonly used approaches. It has been independently assessed by the Federal German Railway Authority (EBA) which has found no impediments to application in the railway signalling domain. The new BP-risk approach is based on a variation of the RPN (Risk Priority Number) concept [5]. The application procedure of BP-risk method has three steps as shown in Figure 3.

1. A generic probabilistic model is defined, together with the relevant parameters and assumptions about the model.
2. The probabilistic model is mapped by mathematical transformation with guaranteed properties (accuracy, monotony and similarity) to a qualitative model (RPN-scheme). Within this step the quantitative parameters are discretely mapped onto parameter ranges.
3. To minimise rounding errors and to ensure a meaningful verbal description the parameter ranges must be adjusted.

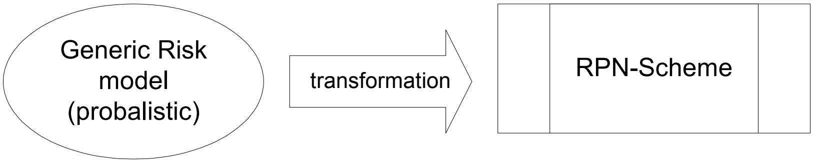


Figure 3: BP-risk transformation.

The principle of the BP-risk application is that precise system definition is needed from components used with interaction with the environment and clearly separated functional interfaces. A system is considered whose functions are supplied by the interaction from humans and technique. It is assumed that the partial risks, coming from the system functions, can be added and that the total risk R is not greater than the sum of all partial risks [6].

$$R \leq \sum_{i=1}^{n} R_i \tag{3}$$

The approach is to evaluate for each system function the consequences in case of failure. The typical influences, conditions, and avoidance probabilities must be taken into account. The partial risk is influenced multiplicatively by the following parameter and results in $R_i = f_i \cdot g_i \cdot s_i \cdot$

Where, f is frequency of occurrence, g is probability of non-detection or non-avoidance, and s is severity of damage. These parameters in turn can be refined. For instance the severity (s) can be broken down into a function of exposed persons (a), speed (v) and accident type (t). The severity results in $s_i = c \cdot a_i \cdot v_i^2 \cdot t_i \cdot$ The criticality of each partial risk can be determined by transformation of R_i. More precisely the transformation is realised by taking the logarithms to the basis b and subsequently integer rounding as eqn. (4).

$$C_i = [\log_b(R_i)] \approx [\log_b(f_i)] + [\log_b(g_i)] + [\log_b(s_i)] \tag{4}$$

Then the example of s_i becomes $S_i = A_i + 2 \cdot V_i + T_i$. For every system function an assessment is performed of the typical damage severity, a classification of the average operational parameters and of the possible avoidance of the hazard. The principle sequence can be taken from the following diagram in Figure 4. In short, the parameter s is out of three partial parameters: number of the exposed persons (A), velocity (V), accident type (T).

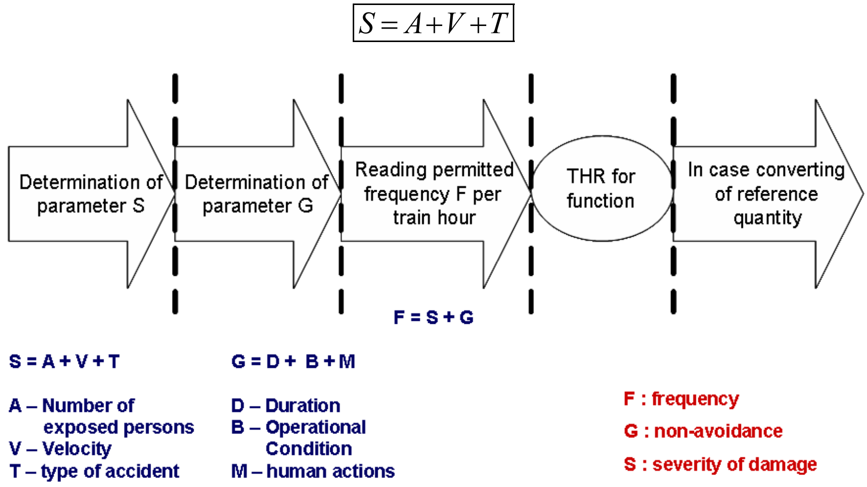

S = A + V + T
Determination of parameter S
Determination of parameter G
Reading permitted frequency F per train hour
THR for function
In case converting of reference quantity
F = S + G
S = A + V + T
G = D + B + M
A – Number of exposed persons
V – Velocity
T – type of accident
D – Duration
B – Operational Condition
M – human actions
F : frequency
G : non-avoidance
S : severity of damage

Figure 4: BP-risk principle sequence.

As shown above, each parameter can be mapped to scale values. Table 3 describes possible values for the other parameters. Not every system failure leads necessarily to an accident. Therefore, the probability of non-detection or non-avoidance (G) is to be estimated. Similarly, G can be broken down into the following parameters: duration of hazard (D), operational conditions (B), corrective action by human (M).

$$\boxed{G = D + B + M}$$

Table 3: Description of three parameters made up of severity S .

A	People exposed	Comment / Examples
1	single person	
2	few people	Accident at level crossing
3	several people	
4	many people	All passenger of one or few cars
5	very many people	All passenger of a train
V	**Velocity**	**Comment / Examples**
1	very low	Walking pace
3	low	During Shunting
4	moderate	Fall-back or unsupervised mode
5	medium	Branch line
6	high	Regional line
7	very high	Main line
T	**Accident type**	**Comment**
1	Collision	Collision with persons or objects inside the structure gauge. Excluded are passengers, railway vehicles and accidents at work.
2	Impact	Impact means the collision of a railway vehicle with a road vehicle (level crossing).
3	Derailment	
4	Crash	Crash means a rear-end collision of two railway vehicles.

In Table 4 three parameters: (D), (B), (M) can be derived by experience, tests and statistic analyses. The following THR values in Table 5 results from S+G and are calibrated on the basis of different risk analyses and statistic evaluations. The failure frequency depends on the period of time in which the function has an effect on the item under consideration. Train-borne functions (e.g. speed indicators) operate continuously whereas trackside functions (e.g. balises, points, etc.) operate normally in defined time intervals. Therefore, S+G needs to be adjusted by the conversion value (U), $S+G+U$. In order to simplify the adjustment, Table 6 shows conversion values.

Table 4: Description of three parameters for non-detection probability G.

D	Duration of hazard	Comment
1	Very short	System failure is detected within few minutes.
2	Short	System failure is detected within one hour, e.g. due to operational demands.
3	Medium	System failure is detected within one operation day, e.g. due to regular tests.
4	Long	
B	Operational conditions	Comment
1	Very low density	Vastly below average
2	Low density	Under average, e.g. on bunch lines
3	Medium density	Average
4	High density	Above average, e.g. main line
M	Corrective action	Comment
1	Always possible	Corrective action supported by an independent technical system.
2	Often possible	e.g. due to route knowledge
3	Possible	
4	Barely possible	

In comparison to other risk analysis methods, this BP-risk has a lot of advantages, but it has one disadvantage in that it is a relatively new method with no published experience of its use and performance, up to now. BP-risk is a procedure which has been constructed according to engineering rules and which is easy comprehensible. It has been constructed according to clearly defined requirements. In comparison to quantitative methods, BP-risk is more effective.

It can be expected that the amount of work can be reduced by about 40% in comparison to quantified risk analyses. All parameters of the risk formula have been used. The parameters are more exactly described than in other qualitative methods, especially the parameter for severity that consists of three sub parameters which allows a better estimation. BP-risk has the potential for a method which can be uniquely used in the railway domain.

Table 5: Allowable frequency.

S+G	THR (per train and per function)	
25	Once in 1.000.000 years	10^{-10} / h
24	Once in 300.000 years	4 x 10^{-10} / h
23	Once in 100.000 years	10^{-9} / h
22	Once in 30.000 years	4 x 10^{-9} / h
21	Once in 10.000 years	10^{-8} / h
20	Once in 3.000 years	4 x 10^{-8} / h
19	Once in 1.000 years	10^{-7} / h
18	Once in 300 years	4 x 10^{-7} / h
17	Once in 100 years	10^{-6} / h
16	Once in 30 years	4 x 10^{-6} / h
15	Once in 10 years	10^{-5} / h
14	Once in 3 years	4 x 10^{-5} / h
13	Once in 1 year	10^{-4} / h

Table 6: Converting into different time values.

U	Type of function	Type of impact	Comments
-1	Functions impact the train continuously	Central Function	Central function of interlocking
0		Train-borne function	Train-borne equipment
0	Functions impact the train not continuously	Rare	Derailer
1		Regular	Level crossings
2		Frequent	Switches, signals

2.5 Example of BP-risk application to ATC system in Korea

In order to emphasize the usefulness of the BP-risk approach, we shall give an example case of an ATC system handling speed restriction in Korea. In this instance, the hazard is that the ATC controlled train exceed the speed restriction in busy metro lines. The values for $S+G+U$ are determined as followed:

$$\boxed{S=A+V+T}$$

ATC failures can affect very many people, A = 5**.** The speed of ATC that is established on the metro line in Korea for controlled trains is normally 80 km per hour, V = 5. The accident type due to exceeding the speed restriction is a crash from the failure of distance control between trains, T = 4. In results,

$$S=5+5+4=14$$

$$\boxed{G=D+B+M}$$

The failure detection time of ATC systems is assumed as very short, D = 1. ATC systems are normally employed on metro lines with a very high density, more than B = 4. A corrective action of the train master is assumed as often possible, M = 2. Therefore, $G=1+4+2$ =7. Since the ATC is a train-borne system and as the function affects the train continuously (U) is assumed as 0. From this it follows that S+G = 21 and the THR results in 10^{-8} per hour and per train.

3 Conclusion

We have demonstrated and compared various methods of risk analysis and estimation, the important phase of safety activities, for safety guarantee in the train control system. Until now, original risk analysis methods have been used properly to advantage, but we propose the complementary BP-risk analysis method to estimate risk more efficiently. In the comparison of the risk graph and the risk matrix method for safety estimation, the BP method has no applications published up to now, but the new BP-risk analysis method shall be more traceable and comprehensible than other methods. From the example of the proposed method application to ATC systems in Korea, we confirm the advantages of the improved engineering approach to risk analysis with BP-risk. Therefore we can expect that this method will be utilized widely for the risk assessment due to various strong points.

References

[1] Jens Braband and Stephan Griebel, "Engineering a Simple, Yet Rigorous, Risk Analysis Method", Proceedings of the 22nd international system safety conference, 2004.

[2] IEC61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems", 1998.

[3] EN50129, "Railway applications. Communication, signaling and processing systems. Safety related electronic systems for signaling." 2003.

[4] R009-004, "Railway applications - Systematic allocation of safety integrity requirements", 2001.

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

[6] Jens Braband, "Risikoanalysen in der Eisenbahn-Automatisierung, Eurail-Press", Siemens AG, 2005.