열차제어시스템 안전성 확보를 위한 위험도 분석 방법 적용

조현정† · 황종규
한국철도기술연구원 전기신호연구본부 열차제어연구팀
(2007. 6. 29. 접수 / 2007. 9. 12. 채택)

Risk Analysis Method Applied to Train Control Systems for Safety Assurance

Hyun-Jeong Jo† · Jong-Gyu Hwang
Signaling & Electrical Engineering Research Department, Train Control System Research Team,
Korea Railroad Research Institute(KRRI)
(Received June 29, 2007 / Accepted September 12, 2007)

Abstract : Failures of equipments for train control systems are linked directly to extensive damages of human lives or financial losses from the increasing uses of train control equipments utilizing computers. Then safety activities for assuring safety and reliability are needed during the system life-cycle. Risk analysis is important phase to increase safety from determining the risk presented by the identified hazard. In this paper, we investigated several methods for risk estimation of safety activities, and then we drew a comparison between original methods to suggest optimized one in the application to train control systems. In the result of the comparison, we had plan to propose the risk analysis method called Best-Practice(BP) risk method combining advantages of the qualitative and the quantitative analysis. In addition, we attempted to apply the BP-risk method to domestic train control systems handling in Korea.
Key Words : risk analysis, risk estimation, train control systems

1. 서 론

최근 들어 전자, 컴퓨터, 통신 기술이 발달하면서 열차제어장치들도 과거의 기계식/전기식에서 전자식으로 바뀌어 가고 있다. 컴퓨터화된 열차제어시스템의 사용이 증가함에 따라서 장치들의 고장이 대규모 인명피해나 경제적 손실과 직결되는 경우가 발생하고 있다. 따라서 열차제어시스템 안전성 확보를 위한 활동을 시스템의 수명주기 전반에 걸쳐 진행하여야 한다[1]. 본 논문에서는 안전성 확보 활동 중에서 위험성 분석을 위한 방법에 대해 알아볼 것이며, 그 중에서 국내 열차제어시스템에 적용하기 위한 최적화된 방식을 제시하기 위해 기존의 위험성 추정 방법들의 장단점을 비교 분석하였다. 비교 분석 결과를 바탕으로 여러 방법들에 비해 정성적인 방식과 정량적인 방식을 절충하여 강점을 가지고 있는 BP 위험도 분석 방법을 국내 열차제어시스템에 적용하고자 한다.

† To whom correspondence should be addressed.
hjjo@krri.re.kr

2. 위험도 분석 및 위험도 추정

전체적인 시스템 안전성 확보 활동 과정은 위험성을 관리 및 제어하는 과정이다. 이것에 의해 위험요소의 확인, 사고위험성 평가, 허용 불가능한 위험원의 제어를 통하여 안전성이 달성된다. 위험도 분석은 시스템 위험도를 추정하고, 도출된 위험원을 제거하거나 완화시킬 대책을 수립하는 과정으로 시스템의 안전성 확보를 위한 기본적인 토대를 제공한다. 위험도는 사고 발생확률과 사고가 발생했을 경우 심각도의 곱으로 정의한다. 사고의 발생확률은 시스템 고장이 사고를 유발할 수 있는 확률을 의미하며, 사고의 심각도는 사고로 야기되는 손실을 의미한다. 이러한 발생확률과 심각도는 정성적 또는 정량적으로 정의되고 평가되어질 수 있다. 사고의 발생확률과 심각도의 곱인 위험도는 시스템의 안전성 확보 활동을 통해 허용범위 내로 존재하도록 시

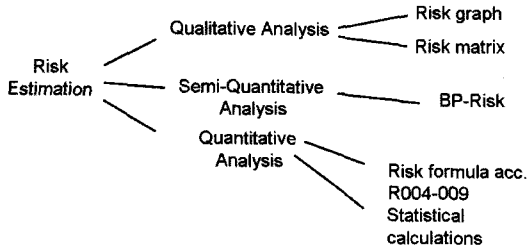

Fig. 1. Classification of methods for risk estimation.

스템 수명주기 전체 단계를 거쳐 위험원이 제어 및 관리되어야 한다.

위험도 분석 전체과정은 시스템 정의에서부터 시작하여, 위험원 도출, 결과 분석, 위험도 추정, Tolerable Hazard Rate(THR) 할당, 위험원 제어의 모든 과정을 포함한다. 즉, 안전성 평가 활동의 목표가 사고의 발생빈도와 심각도를 나타내는 위험도를 허용 가능한 수준으로 만드는 안전성 확보라 할 수 있으므로, 위험도 분석 과정이 안전성 활동 체계 전반이라 해도 과언이 아니다. 위험도 추정을 위한 방법으로는 Fig. 1에 나타낸 것들을 제안할 수 있다. 먼저 정성적인 분석에 해당되는 위험도 그래프 방식과, 위험도 매트릭스 방식을 들 수 있으며, 정량적인 분석에는 CENELEC 규격의 R004-009에서 제시하는 IRF(Individual Risk Formula) 계산 방법과 통계적 계산 방법(Statistical calculations)을 꼽을 수 있다. 통계적 계산 방법은 독일 등과 같은 철도선진국에서 사건, 사고에 대한 자료를 데이터베이스로 구축하여 축적된 데이터를 바탕으로 위험도를 통계적으로 계산하는 정량적인 방식이다. 이와 같은 정성적인 분석과 정량적인 분석의 특징을 혼합하여 절충한 새로운 방식이 BP 위험도 분석 방식이다.

2.1. 정성적인 위험도 매트릭스 방식

위험도 매트릭스는 위험원의 발생빈도와 심각도를 Table 1과 같이 매트릭스 형태로 배치하여 위험도 등급을 결정하는 방식이다[1]. 위험도 분류(III와 IV)는 허용할 수 있는 위험원이다. 확인된 모든 위험원에 대한 분석, 발생확률, 그리고 발생에 따른 결과를 단계적으로 수행해야 한다. IEC의 권고안에 의하면 위험도 분류 I을 위험도 분류 III이하로 감소시키기 위해서 SIL4(Safety Integrity Level 4: 안전무결성레벨 4)의 안전대책을 적용하여 개발되어야 한다고 제시하고 있다. 이와 같은 정성적 분석 방법인 위험도 매트릭스 방식은 비교적 쉽게 THR이

Table 1. Risk matrix method

	사소한 위험 (Negligible)	중요하지 않은 위험(Marginal)	중대한 위험 (Critical)	치명적인 위험 (Catastrophic)
빈번한 발생 (Frequent)	II	I	I	I
가능성 있는 발생 (Probable)	III	II	I	I
종종 발생가능 (Occasional)	III	III	II	I
발생가능성 미약함 (Remote)	IV	III	III	II
발생가능성 없음 (Improbable)	IV	IV	III	III
발생가능성 거의 희박 (Incredible)	IV	IV	IV	IV

- 위험도 등급 I (Intolerable) : 허용할 수 없는 수준
- 위험도 등급 II (Undesirable) : 부적절한 수준
- 위험도 등급 III (Tolerable) : 허용 가능한 수준
- 위험도 등급 IV (Negligible) : 무시 가능한 수준

유도될 수 있다는 것과 사용하기 쉽다는 점 때문에 사용자들의 호응이 높아 널리 사용되어 인지도가 좋은 편이다. 그러나 사용빈도에 비해서 커다란 약점이 내포되어 있는데, 그것은 위험도 매트릭스 방식이 누구나 용인할 수 있는 확고한 구성 원칙에 근거하지 않고 구체적 응용 분야에서의 경험에 근거한다는 점이다. 따라서 위험도 매트릭스의 결과는 몇몇 중요한 파라미터들이 누락되어 활용된 변수들이 조밀하지 않다 보니 사용자로서는 측정해야 할 대상이 너무 많아지기 때문에 차라리 되는대로 대충 평가를 내리는 결점이 존재하여 이러한 단점을 보완할 필요성이 있다.

2.2. 위험도 그래프 방법

위험도 매트릭스 방법에서는 심각도와 발생빈도만을 고려하였으나, 위험도 그래프에서는 여기에 추가적인 파라미터들을 더 고려하여 유럽 열차제어시스템의 위험도 분석에 많이 적용되고 있다. Fig. 2와 같이 이러한 여러 파라미터들을 고려하여 위험도 등급을 평가하고, 이 도출된 등급에 SIL을 할당하는 방식을 적용한다[2]. 이와 같은 위험도 그래프 방식은 시스템 기능 레벨에 적용할 수 있다는 장점이 있는 반면, 위험도 그래프에 내재하는 위험도 수용이 명백하지 않고 매개변수의 카테고리가 구두로만 설명된다는 단점이 있다.

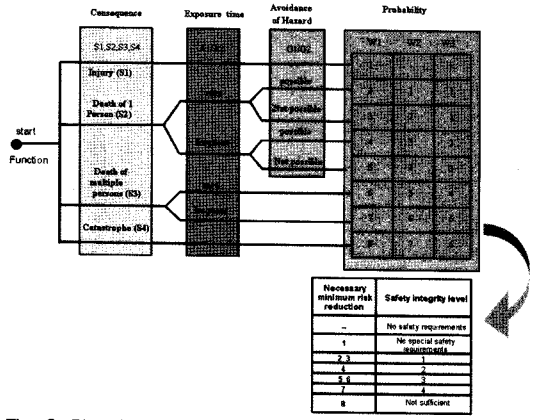

Fig. 2. Risk Graph.

2.3. IRF 계산 방식

일반적으로 개별 위험도 또는 총체적인 위험도가 계산될 수 있으며, IRF(individual risk of fatality)를 구하는데 다음 식 (1)이 사용될 수 있다[3].

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

여기서, 매개변수 k는 모든 사건유형, j는 위험원을 i는 각각의 개별성을 나타내준다. 식 (1)을 하나의 위험원으로 단순화시키면 식 (2)과 같다.

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

여기서, HR은 보호 시스템의 위험원 비율, N은 사람이 시스템을 사용하는 빈도, D는 위험원의 지속시간, E는 사람이 위험원에 노출되는 지속시간, C_k는 사고 발생 확률, F_k는 한 사람의 치사율을 의미한다. IRF를 계산하는데 HR이 필요하기 때문에 정량적인 위험도 분석을 할 때, 위험도 분석과 시스템 위험원 분석사이에 명확한 경계는 없다. Risk formula를 이용하면 위험원의 지속시간과 개개인의 노출시간이 고려되면서 수학적인 문맥에서 사용되어 정확하다는 장점이 있지만, 사용하기 복잡하며 노력이 많이 필요하여 시간과 비용에서 비효율적인 단점이 있어 자주 사용되지 않는다.

2.4. BP 위험도 분석 방식

위와 같은 다수의 위험도 분석 방법들은 많은 비용과 시간을 요하며, 고도의 전문지식을 필요로 한다. 또한 대체로 정량적 위험도 분석의 실행 과정에 접어들면 모델링한 변수의 개수가 증가함에 따라 비용이 증가할 뿐 아니라 결과의 정확도도 대체로 떨어지는 것을 알 수 있다. 그 이유는 정량 분석에 필요한 데이터가 충분히 확보되지 않기 때문이다. 최근 독일에서는 다른 위험도 추정 방식의 단점들을 보완한 새로운 Best-Practice(BP) 위험도 분석 방법을 도입하여, 철도신호분야에 적용하고 있다[4]. BP 위험도 방법은 정량적 위험도 분석 방식을 최대한 단순하면서도 정확하게 하기 위해 제안하는 새로운 방식이며, 본 접근법을 제시하는 목적은 심각도 및 발생확률을 효율적으로 파악하기 위함이다. 원칙적으로 본 기법은 다음과 같이 3단계로 구성된다.

1단계 : 주요 변수와 가설들이 포함된 일반적인 확률적 모델을 정의한다.

2단계 : 수학적 전환 방법을 통해 확률론적 모델을 정성적 모델인 RPN (Risk Priority Number)-scheme으로 변환한다. 이때 정량적 변수들은 따로 분리하여 매개 변수 범위로 나누어서 표시한다.

3단계 : 매개 변수 범위를 조정하여 최적화한다. 그 목적은 분리 시의 오류를 최소화하고 나중에 이를 설명할 수 있게 하기 위함이다.

이 방법을 적용하기 위한 원칙은 모든 컴포넌트들과 기능적인 인터페이스를 설명하는 정확한 시스템 정의에 있다. 시스템 기능에서 생긴 부분적인 위험도들이 첨가될 수 있고, 다음의 식 (3)과 같이 전체 위험도 R은 부분적인 위험도를 모두 합한 것보다 더 크지 않다는 사실이 가정된다.

$$R \le \sum_{i=1}^{n} R_i \quad (3)$$

각각의 시스템 기능이 기능 장애를 일으킬 경우에 발생할 피해를 예측하는 것이 원칙이며, 전형적인 환경요인, 제반조건, 피해 방지가능성 등 기능장애와 피해 '사이'에 존재하는 요인들을 평가한다. 부분적 위험도에 대한 평가는 최소한 단순화시켜야 하며, 다음 식 (4)의 3가지 변수의 곱에 해당하는 값이 부분적 위험도에 영향을 미치는 것이라 가정한다.

$$R_i = f_i \cdot g_i \cdot s_i \quad (4)$$

여기서, f는 발생빈도, g는 검출되지 않거나 회피되

지 않을 확률, s는 손상의 심각도를 나타낸다. 이 매개변수들은 차례로 세분될 수 있다. 예를 들면, 심각도(s)는 위험에 처한 사람(a), 속도(v), 사고유형(t)으로 분해되어 $s_i = c \cdot a_i \cdot v_i^2 \cdot t_i$이 된다. BP 위험도 분석 방식을 활용할 경우, 사용자는 피해의 정도에 따라 피해 잠재성을 예측할 필요 없이 간단히 예측할 수 있는 변수를 활용하기만 하면 된다. 각 부분 위험도의 임계상태는 R_i의 변환에 의해 결정될 수 있다. 보다 더 정확한 변환은 밑을 b로 하는 로그를 취한 후 정수를 취함으로써 실현된다. 식 (5)의 s_i 경우, $S_i = A_i + 2 \cdot V_i + T_i$가 된다. 다음의 예시가 변환과정을 명백하게 보여준다. 고려중인 시스템은 열차이고, 대상 시간은 1시간이다. 각각의 시스템 기능에 대해 전형적인 피해 수준을 파악하고 운행에 필요한 통상적 주변 요인들을 분류하며 나아가 피해 방지 방법도 알아본다. 기본적인 순서는 Fig. 3으로부터 취할 수 있다.

$$C_i = [\log_b(R_i)] \approx [\log_b(f_i)] + [\log_b(g_i)] + [\log_b(s_i)] \qquad (5)$$

매개변수 S는 3개의 부분변수로 구성되고, 이 3개의 부분변수를 합산하여 $S = A + V + T$라는 변수를 도출한다. A는 위험에 노출된 사람의 수, V는 속도, T는 사고유형을 나타낸다. 같은 유형의 사고라 하더라도 그 결과에는 커다란 차이가 있을 수 있다. 그 차이를 결정짓는 가장 결정적인 요인은 바로 속도이다. 각 변수의 스케일 값을 결정하는 방법을 자세히 알아보기 위해 속도의 경우를 예로 들어 설명하면 다음과 같다. 요즘 철도통행에 있어 통용되는 속도 범위는 대개 0~300km/h 수준이다. 그런데 초고속으로 주행하다가 일어난 사고들의 경우, 그 결과들 사이에 별 차이가 없다. 따라서 0~200m/h까지만 대상으로 삼더라도 별 무리가 없을 것으로 판단된다. 이제 실제적이면서도 분명한 속도를 선정하여 이를 스케일 값에 배당해야 한다.

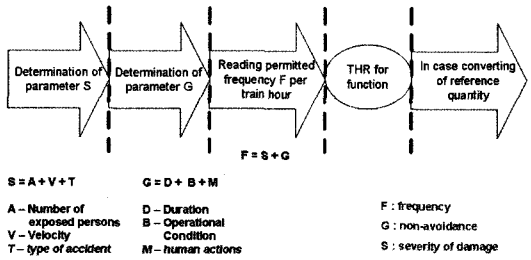

Fig. 3. Principle sequence of BP-risk method.

Table 2. Description of the parameter V – Velocity

V	전반적 속도	사례
1	매우 미미한 수준	도보속도
3	미미한 수준	전철(轉轍) 시 주행속도
4	약한 수준	신호에 따른 주행속도
5	중간 수준	지선노선에서의 주행속도(R80)
6	높은 수준	지방노선에서의 주행속도(R120)
7	매우 높은 수준	간선노선에서의 주행속도

Table 3. Parameter A – Number of persons at risk

A	피해자의 수	사례
1	1인	
2	소수	철길건널목에서 발생되는 전형적 사고의 경우
3	여러 명	
4	다수	객차 1량 혹은 그 이상에 승차한 승객
5	매우 다수	기차 안의 모든 승객

Table 4. Parameter T – Accident type

T	사고유형	참고사항
1	대인/대물 충돌	'대인/대물 충돌'이란 표준 궤도를 운행하는 열차가 사람(승객은 제외)이나 장애물에 부딪치는 것을 의미한다. 또 다른 열차와의 충돌은 여기에서 제외되고, 산업재해 대상에서 제외된다.
2	대차 충돌	'대차 충돌'이란 열차와 도로통행 차량이 철길건널목에서 충돌하는 것을 의미한다.
3	선로이탈	'선로이탈'이란 열차 바퀴가 궤도에서 미끄러지거나 위로 뜨는 현상을 의미한다. 열차가 탈선했다가 스스로 다시 제자리로 돌아오는 것도 여기에 해당된다. 열차가 복선 운행하는 경우도 여기에 해당된다.
4	대 열차 충돌	'대 열차 충돌'이란 열차와 열차가 부딪치는 것을 의미한다.

스케일 값 5~200km/h를 로그를 이용해 계산하면 1.6~5.2라는 값이 산출된다. 이때 해당 공식에서 속도의 제곱이 활용된다는 점을 고려하면, 변수는 3.2~10.4가 된다. 다음으로 눈금 0에 값을 맞추는 조절작업을 수행하면 0~7.2라는 스케일 값이 도출된다. 그런데 0은 '아무런 영향을 미치지 않음'으로 해석될 여지가 높기 때문에 1을 눈금의 시작점으로 삼는다. 고찰한 내용을 바탕으로 표로 정리해 보면 그 결과는 Table 2와 같다[5]. 사고발생시 피해를 입을 수 있는 사람의 수를 가리키는 변수 A와 전형적인 피해 사례를 파악하여 사고 유형 평가를 하는 변수 T에 대해 같은 방법으로 스케일 값을 취해 정리하면 Table 3, 4와 같다[5]. 시스템 기능의 장애가 반드시 사고로 이어지는 것은 아니다. 따라서 위험 방지 가능성, 즉 위험이 발생할 확률 및 위험 발생을 초

래하는 요인을 파악해 보아야 한다. 이 때, 3가지 변수를 합산해서 산출되는 위험감소인자 $G=D+B+M$을 활용하도록 한다.

D는 위험 지속시간, B는 가동상의 주변요인, M은 돌발적으로 발생하는 사람에 의한 조작활동을 나타낸다. 관찰대상 단위시간은 1시간 동안의 열차운행이다. 그렇기 때문에 결과를 예측할 시에는 가동 중 시스템 장애가 발생할 때까지 시간이 얼마나 걸리는지를 알아내야 할 필요가 있다. 시스템 장애를 파악하는데 걸리는 시간을 위험 지속시간이라 하고, 이 시간은 직접 테스트를 해서 알아내거나 해당 기능의 표준 운용설명서를 통해 파악할 수 있다. 위험 지속시간은 아래 Table 5와 같이 정하도록 한다[5]. 또한, 운행 상의 주변요건들을 정의하는 변수 B와 위험을 예방할 수 있는 사람의 조작행위를 나타내는 변수 M에 대한 각각의 Table도 정리하였다[5].

고장빈도는 기능이 고려중인 항목에 영향을 미치는 기간에 따라 결정되므로, $S+G$는 환산값(U)에 의해 조정될 필요가 있다. 환산 작업은 간편하게 Table 8을 활용할 수 있으며, 이에 따라 기존 값을 수정하게 되면, S+G값 대신 S+G+U값을 활용해 THR을 Table 9와 같이 도출한다[5]. 도출된 THR 값에 따라서 결정되는 SIL값은 국제표준규격에 제시되는 Table 10에 근거하여 도출될 수 있다. 결과적으로 SIL4를 만족시키기 위한 안전성 활동을 수행하면 대상 시스템의 안전성 확보를 이룰 수 있는 것이다.

이와 같은 BP 위험도 방법은 아직까지 정식으로 공표된 적이 없고, 시작된 지 얼마 안 된 방법이라는 단점만 제외하면 다음과 같은 장점을 지니고 있다. 먼저 BP 위험도 방법은 이해하기 쉽고, 명백하게 정의된 요구사항에 따라 구성되어 왔다는 점을 들 수 있다. 또한, 비록 위험도 분석의 일부분만 단순화되지만 정량적인 방법과 비교하면 BP 위험도 분석 방식이 더 효율적이며, 매우 큰 작업량 감소의 결과를 기대할 수 있다는 장점을 지닌다. 마지막으로 BP 위험도 방식에 쓰인 모든 매개변수들은 다른 정성적인 방법들보다 더 정확하게 설명된다는 것

Table 5. Parameter D – duration of hazard

D	위험 지속시간	설명
1	매우 짧다	시스템 장애를 몇 분 만에 파악할 수 있는 경우. 운행 중 발생한 위험한 상황이 직접적 원인인 경우가 대표적 사례이다.
2	짧다	시스템 장애를 대개 1시간 이내에 파악할 수 있는 경우. 예컨대 무리한 운행으로 인한 경우
3	중간	시스템 장애를 대개 운행 일자를 기준으로 하루 이내에 파악할 수 있는 경우. 예컨대 정기적 기능 검사에 의한 경우
4	길다	지속 시간이 길어질 경우, 반드시 전문가와의 상의 후에 주의 깊게 본 기법을 활용해야 한다.

Table 6. Parameter B – operation conditions

B	운행 상의 주변요건	설명
1	매우 미미한 운행간격	선로 망 평균보다 훨씬 더 낮은 수준
2	미미한 운행간격	선로 망 평균보다 분명히 낮은 수준 (예: 지선노선)
3	일반적 운행간격	선로 망 평균 수준
4	증폭된 운행간격	선로 망 평균보다 분명히 높은 수준 (예: 고속통행노선)

Table 7. Parameter M – human mitigation

M	사람의 조작 행위를 통한 위험 방지 가능성	참고사항
1	거의 매번 가능한 경우	예: 독립된 기술시스템의 가동 혹은 지원이 동반된, 사람의 조작행위
2	대부분 가능한 경우	예: 궤도에 대한 경험과 지식
3	가능한 경우	
4	거의 불가능한 경우	매우 유리한 상황 하에서 우연까지 겹쳐야 위험방지가 가능

Table 8. Converting into different time values

U	기능의 종류	열차에 미치는 영향의 종류	사례
-1	열차에 지속적으로 영향을 미치는 기능	중앙 제어적 기능	열차 운전실에서의 중앙 제어 기능
0		열차 내에서 작동되는 기능	열차 설비
0	열차에 비지속적으로 영향을 미치는 기능	드물다	선로차단기
1		주기적이다	철길건널목
2		종종 있다	전철기, 신호등……

Table 9. Allowable frequency

S+G+U	THR(열차 당, 기능 당)	
25	1,000,000년에 1회	10^{-10}/h
24	300,000년에 1회	4×10^{-10}/h
23	100,000년에 1회	10^{-9}/h
22	30,000년에 1회	4×10^{-9}/h
21	10,000년에 1회	10^{-8}/h
20	3,000년에 1회	4×10^{-8}/h
19	1,000년에 1회	10^{-7}/h
18	300년에 1회	4×10^{-7}/h
17	100년에 1회	10^{-6}/h
16	30년에 1회	4×10^{-6}/h
15	10년에 1회	10^{-5}/h
14	3년에 1회	4×10^{-5}/h
13	1년에 1회	10^{-4}/h

Table 10. SIL allocation through THR value

THR per Hour and per function	SIL
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

과, 특히 심각도의 매개변수는 세 개의 하위 매개변수들로 구성되어 BP 위험도 방식을 사용하면 보다 더 우수한 평가를 가능하게 해준다는 이점이 존재한다.

3. 국내 열차제어시스템에 BP 방식 적용

본 절에서는 BP 위험도 방식을 국내 열차제어시스템에 적용하여 그 효율성을 확인하였으며, 각각의 매개변수들의 값을 도출한 결과는 Table 11과 같다. 대상시스템은 최고속도 150 km/h인 국내 철도신호시스템으로 하였으며, 그 기능은 진로제어 및 열차간격을 제어하는 시스템으로 구성하였다. A변수는 사고발생시 피해자의 수가 기차안의 모든 승객이 될 수 있으므로 최대값 5가 도출된 것이며, 속도 V는 간선노선 최대속도이므로 7값이 나오게 된다. 사고유형 T변수는 도출된 위험원에 따라, 선로이탈과 열차끼리의 충돌이 일어날 수 있으므로 4 또는 3의 값이 도출된 것이다. 또한, 위험지속 시간 D변수의 경우는 하드웨어 테스트에 따른 방법으로 시스템 장애를 대게 1시간 이내에 파악할 수 있으므로 2값이 도출된다. 변수 B는 고속통행노선인 경우에 해당하여 열차 운행간격이 조밀하여 4가 되고, 사람의 조작행위로 위험방지를 할 수 있는 가능성 변수 M은 해당 위험원에 따라서 대부분 가능하거나 가능한 경우인 2 또는 3의 값이 나오게 된다. 마지막으로 본 시스템의 연동장치 기능은 중앙제어 방식을 따르기 때문에 환산값 U는 -1이 되는 것이다. Table 11은 이와 같은 실제 대상시스템의 위험원들에 대한 BP 방식 적용 결과 중, 대표적인 위험원 몇 가지를 추려서 도출한 결과를 제시한 것이다.

Table 11. Application results using BP-risk method

#	시스템 위험원	S=A+V+T			G=D+B+M			환산	S+G+	THR
		V	A	T	D	B	M	U	U	
1	잘못된 열차위치	7	5	4	2	4	3	-1	23	10^{-9}/h (SIL4)
2	잘못된 열차방향	7	5	4	2	4	2	-1	23	10^{-9}/h (SIL4)
3	열차제어 손실	7	5	4	2	4	3	-1	24	$4*10^{-10}$/h (SIL4)
4	잘못된 진로설정	7	5	4	2	4	3	-1	23	10^{-9}/h (SIL4)
5	잘못된 열차속도 정보	7	5	3	2	4	3	-1	23	10^{-9}/h (SIL4)

4. 결 론

본 논문에서는 열차제어시스템의 안전성 확보를 위해 요구되는 안전성 활동의 핵심 단계인 위험도 분석 단계의 위험성 추정을 위한 기법들에 대해서 구체적으로 서술하고 비교해 보았다. 지금까지 철도신호시스템에서 안전성 입증을 확인하기 위해 기존의 위험성 분석 방법들은 각각이 가지고 있는 장점에 따라서 적절하게 사용되어져 왔으나, 좀 더 정확하고 효과적으로 고장을 분석하기 위해서 기존의 방법들의 단점을 보완한 새로운 BP 방법이 제안되었다. 안전성 평가를 위한 위험도 매트릭스에 비해 아직 BP 위험도 분석 방식의 이용에 대한 내역은 없지만, 위에서 알아본 바에 따르면 다른 방법에 비해 강점을 지니고 있기 때문에 앞으로 활용 가능성은 매우 크다고 내다볼 수 있다.

참고문헌

1) EN50126, "Railway Applications - The Specification and Demonstration of RAMS", 1999.
2) IEC61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems", 1998.
3) R009-004, "Railway applications - Systematic allocation of safety integrity requirements", 2001.
4) Jens Braband, "Risikoanalysen in der Eisenbahn-Automatisierung", Eurail Press by Siemens AG, 2005.
5) Jens Braband, "Improving the Risk Priority Number Concept", Journal of System Safety, pp. 21~23, 2003.