열차제어시스템 안전성 확보를 위한 리스크 평가 방법 분석
Risk Assessment Method for Guaranteeing Safety in the Train Control System

조현정*, 황종규**, 윤용기**
Jo, Hyun-Jeong Hwang, Jong-Gyu Yoon, Yong-Ki

ABSTRACT

Recently, failures of equipments 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 have to progress for guaranteeing safety during the system life-cycle. In this paper, we examine the methods for risk analysis and assessment of safety activities and propose optimized one method for risk assessment. There are original risk assessment methods; risk graph and risk matrix method under the qualitative analysis, IRF(Individual Risk Formula) calculations and statistical calculations method under the quantitative analysis. Best-Practice(BP) risk analysis method is proposed for combining advantages of the qualitative and the quantitative analysis. In the comparison of risk graph and risk matrix method for safety estimation, BP method has no applications published up to now, but we can expect that this method will be utilized widely for the risk assessment due to various strong points.

---

1. 서론

최근 들어 전자, 컴퓨터, 통신 기술이 발달하면서 열차제어장치들도 과거의 기계식/전기식에서 전자식으로 바뀌어 가고 있다. 그림 1과 같이 컴퓨터화된 열차제어시스템의 사용이 증가함에 따라서 장치들의 고장이 대규모 인명피해나 경제적 손실과 직결되는 경우가 발생하고 있다.

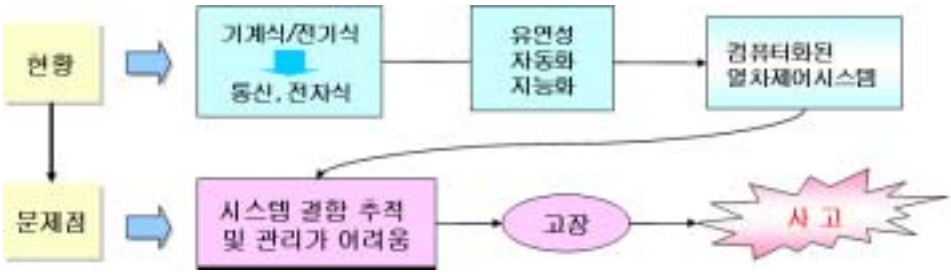


그림 1 열차제어시스템의 전자화에 따른 문제점

---

* 한국철도기술연구원 열차제어연구팀
E-mail : hjjo@krri.re.kr
TEL : (031)460-5458 FAX : (031)460-5449
** 한국철도기술연구원 열차제어연구팀

따라서 열차제어시스템의 안전성 확보를 위한 절차를 수행하는 체계인 안전성 활동을 시스템의 수명주기 전반에 걸쳐 진행하여야 한다. 본 논문에서는 안전성 활동 중에서 리스크 분석 및 평가를 위한 방법에 대해 알아볼 것이며, 그 중에 최적화된 새로운 방식을 한 가지 소개하고자 한다.

2. 리스크 분석 및 평가

전체적인 시스템 안전성 활동 과정은 위험성을 관리 및 제어하는 과정이다. 이것에 의해 위험요소의 확인, 사고위험성 평가, 허용 불가능한 위험원의 제어를 통하여 안전성이 달성된다. 리스크 분석은 시스템 위험도를 추정하고, 도출된 위험원을 제거하거나 완화시킬 대책을 수립하는 과정으로 시스템의 안전성 확보를 위한 기본적인 토대를 제공한다. 리스크는 사고의 발생확률과 사고가 발생했을 경우 심각도의 곱으로 정의한다.

$$\textit{리스크(Risk)} = \textit{발생확률(Probability)} \times \textit{심각도(Severity)}$$

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 리스크는 시스템의 안전성 활동을 통해 허용범위 내로 존재하도록 시스템 수명주기 전체 단계를 거쳐 위험원이 제어 및 관리되어야 한다.

리스크 분석 전체과정은 그림 2에서 나타낸 것과 같이 시스템 정의에서부터 시작하여, 위험원 도출, 결과 분석, 리스크 평가, Tolerable Hazard Rate(THR) 할당, 위험원 제어의 모든 과정을 포함한다. 즉, 안전성 평가 활동의 목표가 사고의 발생빈도와 심각도를 나타내는 리스크를 허용 가능한 수준으로 만드는 안전성 확보라 할 수 있으므로, 아래 그림 일련의 과정이 안전성 활동 체계 전반이라 해도 과언이 아니다.

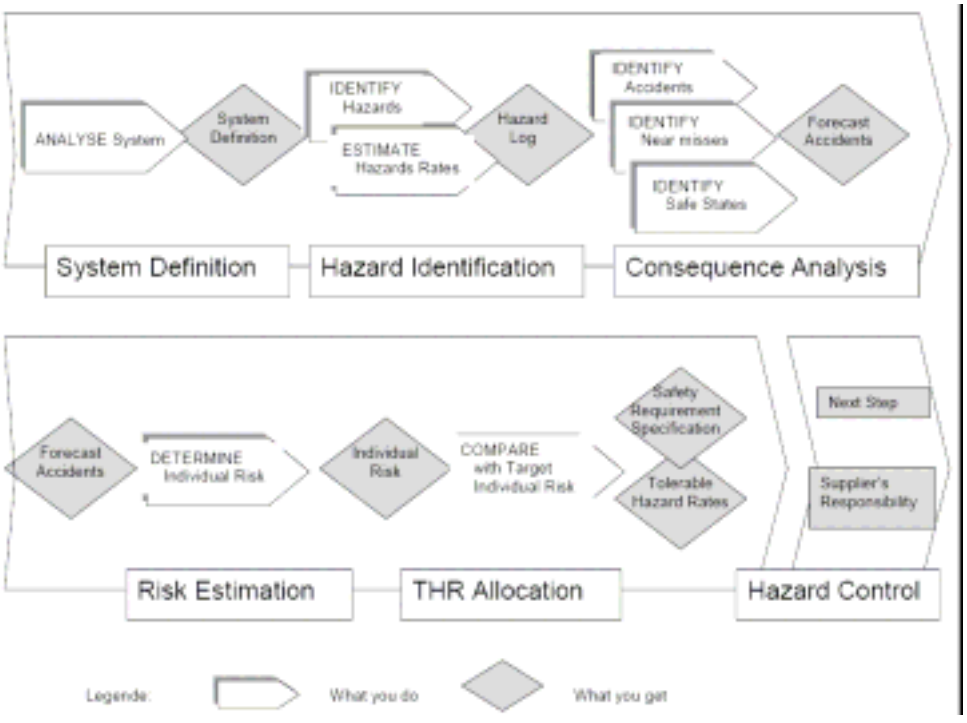


그림 2 리스크 분석 과정

리스크 평가를 위한 방법으로는 그림 3에 나타낸 것들을 제안할 수 있다. 먼저 정성적인 분석에 해당되는 리스크 그래프 방식과, 리스크 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 리스크를 통계적으로 계산하는 정량적인 방식이다. 이와 같은 정성적인 분석과 정량적인 분석의 특징을 혼합하여 절충한 새로운 방식이 Best-Practice(BP) 리스크 분석 방식이다.

그림 3 리스크 평가를 위한 방법들

2.1 정성적인 리스크 매트릭스 방식

리스크 매트릭스는 위험원의 발생빈도와 심각도를 표 1과 같이 매트릭스 형태로 배치하여 리스크 등급을 결정하는 방식이다 [1]. 리스크 등급은 일반적으로 I부터 IV까지 리스크의 크기와 빈도에 의한 테이블로 결정된다. 이 리스크 등급에 의해 해당 리스크가 수용가능한지 아니면 안전대책을 통해 수용가능 수준 이하로 제어해야 하는지를 결정할 수 있게 된다. 도출된 리스크 등급별 안전무결성레벨(SIL : Safety Integrity Level)을 할당하여 SIL 레벨별로 IEC 기준에서 정하는 THR을 할당하는 방법도 적용되고 있다. 여기서, SIL은 '안전관련 시스템이 목표된 시간과 환경에서 안전하게 기능을 수행할 확률'이라고 정의된다. 이와 같은 리스크 매트릭스 방식의 장점과 단점은 표 2와 같다.

표 1 리스크 매트릭스

	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
발생가능성이 미약함 (Remote)	IV	III	III	II
발생가능성이 없음 (Improbable)	IV	IV	III	III
발생가능성이 거의 희박(Incredible)	IV	IV	IV	IV

- 리스크 등급 I (Intolerable) : 허용할 수 없는 수준
- 리스크 등급 II (Undesirable) : 부적절한 수준(불가능한 수준의 대응과 가격대 성능비가 심하게 불균형을 이루어야만 허용할 수 있음)
- 리스크 등급 III (Tolerable) : 허용 가능한 수준(리스크 감소의 비용이 성능향상을 초과하는 경우에 허용할 수 있음)
- 리스크 등급 IV (Negligible) : 무시 가능한 수준

표 2 리스크 매트릭스 방식의 장·단점

장 점	단 점
- 사용하기 쉽다. - THR이 쉽게 유도될 수 있다.	- 모든 경우에 대해 측정되어야 한다. - 위험원의 수를 정확히 고려해야 한다. - 결과는 사용된 시스템 레벨과 참고문헌의 양에 의존한다. - 이 방법은 리스크를 과대평가하는 경향이 있다. - 몇몇 중요한 파라미터들이 누락된다.

2.2 리스크 그래프 방법

독일의 DIN 표준들(DIN19250과 DIN0801)은 안전관계 시스템들을 위해 개발되어 IEC61508이 발표되기 전까지 적용되었다. DIN19250 표준은 리스크와 필수 독일 요구사항 등급(German Requirement Class) 사이의 관계를 정의한다. 이것은 결과, 빈도와 노출시간, 위험원을 회피할 확률, 입력과 같은 4가지 파라미터들을 적용하여 필요한 요구사항 등급을 정의하는 리스크 그래프를 사용한다. DIN0801은 각 요구사항 등급을 충족시키는데 필요한 기법과 대책들을 정의한다. 이 기법과 대책들은 요구사항 등급에 따라 다르고, 하드웨어 고장과 시스템 고장의 결과를 제어하는데 사용된다.

리스크 매트릭스 방법에서는 심각도와 발생빈도만을 고려하였으나, 리스크 그래프에서는 여기에 추가적인 파라미터들을 더 고려하여 유럽 열차제어시스템의 리스크 평가에 많이 적용되고 있다. 그림 4와 같이 이러한 여러 파라미터들을 고려하여 리스크 등급을 평가하고, 이 도출된 등급에 SIL을 할당하는 방식을 적용한다 [2]. 리스크 그래프의 최종결과인 특정 W scale(즉, W_1, W_2 또는 W_3)은 안전 관계 시스템의 안전무결수준(즉, 1,2,3,4)을 제공하고, 이 시스템에 요구되는 리스크 감소에 대한 대책을 의미한다. 이와 같은 리스크 그래프 방식의 장점 및 단점은 표 3과 같다.

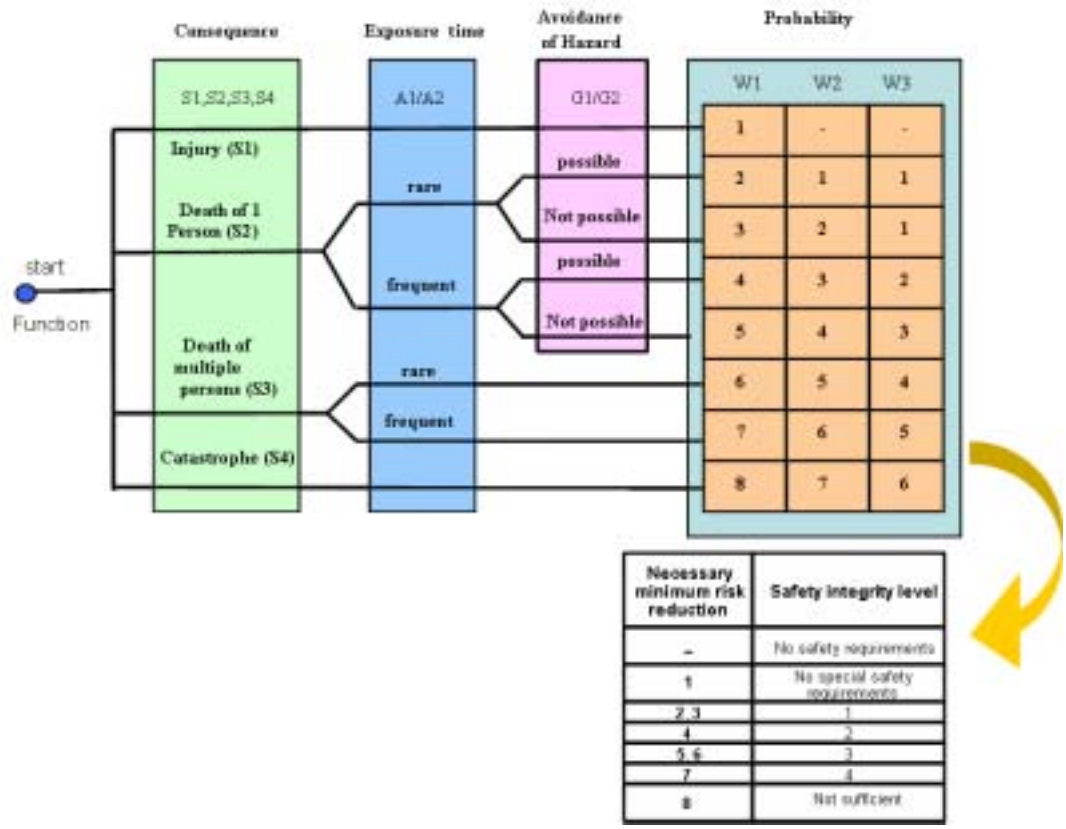


그림 4 리스크 그래프

표 3 리스크 그래프 방식의 장·단점

장 점	단 점
- 모든 기능에 사용하기 쉽다. - 효율적이고 납득할 수 있는 비용 - 시스템 기능 레벨에 적용	- 매개변수의 카테고리들은 구두로만 설명된다. - 절차의 구성은 이에 대한 어떤 근거도 제시하지 않고 수립되었다. - 리스크 그래프에 내재하는 리스크 수용은 명백하지 않다. - DIN19250에 의한 리스크 그래프는 독일 외의 다른 국가에서는 받아들여지지 않는다. - 위험원의 지속시간에 대한 고려는 명확하지 않다.

2.3 IRF 계산 방식

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

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

여기서, 매개변수 k는 모든 사건유형, j는 위험원을 i는 각각의 개별성을 나타내준다. (1)의 식을 하나의 위험원으로 단순화시키면 아래 식 (2)와 같다.

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

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 리스크 분석을 할 때, 리스크 분석과 시스템 위험원 분석사이에 명확한 경계는 없다. Risk formula를 이용하면 다음과 같은 장점과 단점을 갖는다.

표 4 Risk formula 방식의 장·단점

장 점	단 점
- 위험원의 지속시간과 개개인의 노출시간 또한 고려될 수 있다. - 매개변수들은 수학적인 문맥에서 사용되어 분명하고 정확하게 정의된다.	- 이 방법은 HR이 계산에 사용되기 때문에 의도된 시스템 구조의 영향을 받는다. - 많은 노력이 필요하다.

2.4 BP-Risk 방식

모든 리스크 평가 방법은 고유의 장점을 가지고 있으며, 대체로 전문가들에 의해 인정되고 있다. 그러나 다수의 리스크 평가 방법들은 많은 비용을 필요로 하고, 많은 시간을 요하며, 고도의 전문지식을 필요로 한다. 최근 독일에서는 다른 리스크 평가 방식의 단점들을 보완한 새로운 Best-Practice(BP) 리스크 분석 방법을 도입하여, 철도신호분야에 적용하고 있다 [4]. BP-Risk 방식의 적용절차는 그림 5와 같다.

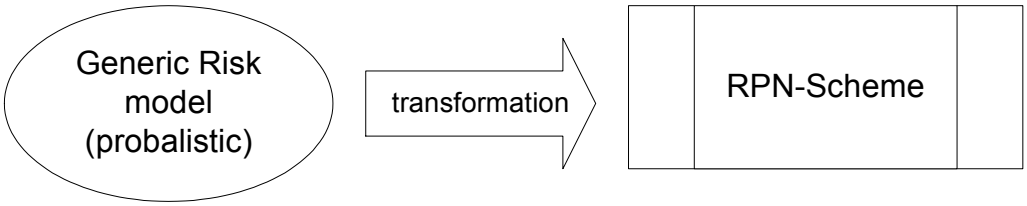


그림 5 BP-리스크 transformation

1단계 : 모델에 대한 관련 매개변수 및 가정과 더불어, 일반적인 확률적 모델이 정의된다.
2단계 : 확률적 모델에 수학적인 변환을 가하면 정성적인 모델 RPN(Risk Priority Number)-scheme이 된다. 이 단계에서 정량적인 매개변수들은 선택된 매개변수 범위로 나누어진다.
3단계 : 에러를 최소화하고, 의미있는 구두설명을 확실히 할 수 있도록 매개변수 범위가 조정되어야만 한다.

이 방법을 적용하기 위한 원칙은 모든 컴포넌트들과 기능적인 인터페이스를 설명하는 정확한 시스템 정의에 있다. 시스템의 기능들은 인간과 기술의 상호작용 의해 공급되는 것으로 간주된다. 시스템 기능에서 생긴 부분적인 리스크들이 첨가될 수 있고, 다음의 식 (3)과 같이 전체 리스크 R은 부분적인 리스크를 모두 합한 것보다 더 크지 않다는 사실이 가정된다.

$$R \leq \sum_{i=1}^{n} R_i \qquad (3)$$

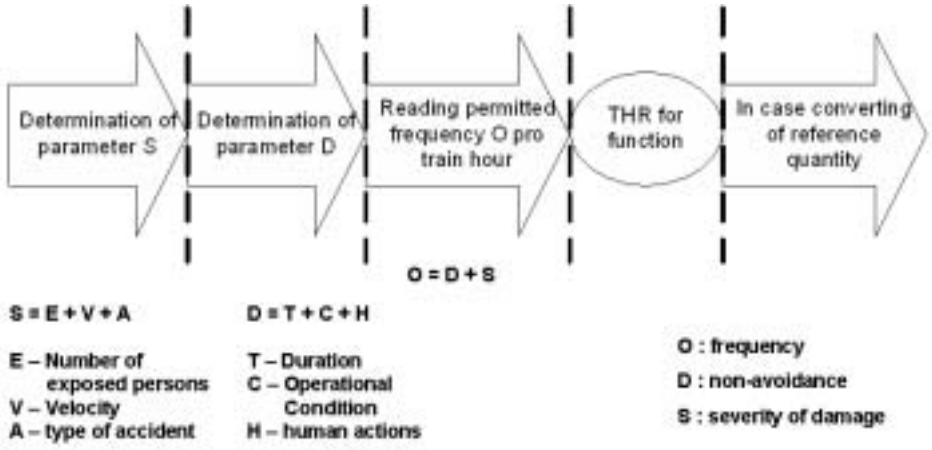
접근법은 고장이 발생한 경우에 각 시스템 기능의 영향을 평가하는 것이다. 일반적인 영향, 상태, 회피 확률들이 고려되어야만 한다. 부분 리스크의 경우 가장 간단한 접근법이 선택된다. 부분 리스크는 아래 식 (4)에 있는 파라미터의 곱에 의해 좌우되며, 결과는 아래와 같다.

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

여기서, f는 발생빈도, g는 검출되지 않거나 회피되지 않을 확률, s는 손상의 심각도를 나타낸다. 이 매개변수들은 차례로 세분될 수 있다. 예를 들면, 심각도(s)는 노출된 사람(e), 속도(v), 사고유형(a)으로 분해될 수 있다. 상수 c와 더불어, 심각도 $s_i = c \cdot e_i \cdot v_i^2 \cdot a_i$이 된다. 각 부분 리스크의 임계상태는 R_i의 변환에 의해 결정될 수 있다. 보다 더 정확한 변환은 식 (5)처럼 밑을 b로 하는 로그를 취한 후 나오는 어림수의 정수를 취함으로써 실현된다. 밑은 일반적으로 $\sqrt{10} \cong 3.2$인데, 이것은 정확한 필요조건으로는 부적절하다.

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

위의 식 s_i의 경우 $S_i = E_i + 2 \cdot V_i + A_i$가 된다. 속도 변수 V는 본보기로 표시되어야 한다. 열차가 낼 수 있는 속도는 0부터 200km/h의 범위로 추정된다. 속도 5~200km/h 범위를 로그를 취해서 고려해보면 3.2에서 7.2까지 나온다. 이 값은 영점이나 그 밖의 선호하는 점으로 맞출 수 있다. 마지막으로 할 일은 미리 정해진 값에 할당될 수 있는 실용적이고 유일한 속도 등급을 찾는 것이다. 다음의 예시가 변환과정을 명백하게 보여준다. 고려중인 시스템은 열차이고, 1시간의 train mission을 고려 단위로 한다. 모든 시스템 기능의 평가는 전형적인 손상 심각도, 평균 운영 매개변수들의 분류, 위험원을 회피할 가능성에 대해 수행된다. 기본적인 순서는 그림 6으로부터 취할 수 있다.



매개변수 S는 식 (6)과 같이 세 가지 부분변수로부터 구할 수 있다. 각 매개변수는 스케일 값을 가질 수 있다.

$$S = E + V + A \tag{6}$$

여기서, E는 위험에 노출된 사람의 수, V는 속도, A는 사고유형을 나타낸다. 모든 시스템 고장이 반드시 사고를 일으키는 것은 아니기 때문에 non-detection 또는 non-avoidance 확률(D)이 추정되는 것이다. D는 식 (7)에서의 매개변수들로 나뉠 수 있다. 모든 매개변수들은 시스템 경계 밖에 있어야 한다는 것에 주의한다.

$$D = T + C + H \tag{7}$$

여기서, T는 위험원 지속시간, C는 동작 조건, H는 인간의 교정행위를 나타낸다. 고장빈도는 기능이 고려중인 항목에 영향을 미치는 기간에 따라 결정되므로, $S+D$는 식 (8)처럼 환산값(U)에 의해 조정될 필요가 있다.

$$S + D + U \tag{8}$$

$S+D$를 조정하는데 몇 가지 방법이 있다는 사실에 주의해야 한다. 아래의 표에 조정을 간단히 하기 위한 환산값이 표 5에 제시되어 있다.

ATP의 속도 제한 조작을 예로 들면, ATP는 train-borne system이므로 열차에 계속적으로 영향을 미치는 기능(U)은 0으로 추정된다. 각 변수에 대한 구체적인 값을 정의한 표를 참고한다면, $S+D$ 값을 구할 수 있으며 최종적으로 이에 해당하는 THR을 도출할 수 있다. 이러한 결과는 ETCS(European Rail Control System) 안전 요구사항과 비교할 수 있고, 요구사항을 정확하게 따르는 값이다.

표 5 환산값 U의 정의

U	Type of function	Type of impact	Comments
-1	Functions impact the train continuously	Central Function	Central function of an 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

이와 같은 BP-Risk 방법은 아직까지 정식으로 공표된 적이 없고, 시작된 지 얼마 안 된 방법이라는 단점만 제외하면 다음과 같은 장점을 지니고 있다.

- BP-리스크는 절차인데, 그것은 엔지니어링 규칙에 따라 구성되어왔고, 이해하기 쉽다. 명백하게 정의된 요구사항에 따라 구성되어 왔다.
- 비록 리스크 분석의 일부분만 단순화되지만 정량적인 방법과 비교하면 BP-risk가 더 효율적이다. 정량화된 리스크 분석과 비교하여 약 40%의 작업량을 감소시키는 것이 기대될 수 있다.
- BP-리스크는 일반적인 리스크 분석 또한 허용한다.
- 리스크 공식의 모든 매개변수들이 사용되어 왔다. 매개변수들은 다른 정성적인 방법들보다 더 정확하게 설명된다. 특히 심각도의 매개변수는 세 개의 하위 매개변수들로 구성되는데, 이것이 보다 더 우수한 평가를 가능하게 한다.

3. 결론

본 논문에서는 열차제어시스템의 안전성 확보를 위해 요구되는 안전성 활동의 핵심 단계인 리스크 분석 및 평가를 위한 기법들에 대해서 구체적으로 서술하고 비교해 보았다. 지금까지 철도신호시스템에서 안전성 입증을 확인하기 위해 기존의 리스크 평가 방법들은 각각이 가지고 있는 장점에 따라서 적절하게 사용되어져 왔으나, 좀 더 정확하고 효과적으로 고장을 분석하기 위해서 기존의 방법들의 단점을 보완한 새로운 BP-Risk 방식이 제안되었다. 안전성 평가를 위한 리스크 매트릭스와 리스크 그래프의 사용에 비해 아직 BP-Risk의 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 Reliability, Availability, Maintainability and Safety (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.