열차제어시스템의 위험도 평가를 위한 적용 방법 분석

조현정, 황종규, 양도철
한국철도기술연구원

Analysis of Application Methods for Risk Assessment in Train Control Systems

Hyun-Jeong Jo, Jong-Gyu Hwang, Do-Chul Yang
Korea Railroad Research Institute (KRRI)

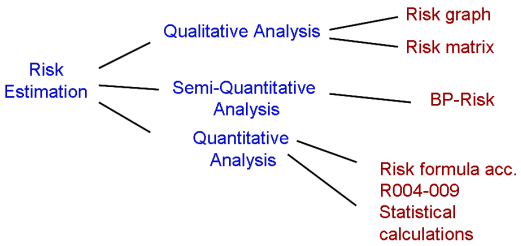
Abstract - 최근 들어 컴퓨터화된 열차제어시스템의 사용이 증가함에 따라서 장치들의 고장이 대규모 인명피해나 경제적 손실과 직결되는 경우가 발생하고 있다. 따라서 열차제어시스템의 안전성 확보를 위한 절차를 수행하는 체계인 안전성 활동을 시스템의 수명주기 전반에 걸쳐 진행하여야 한다. 본 논문에서는 안전성 활동 중에서 위험도 분석 및 평가를 위한 방법에 대해 알아볼 것이며, 그 중에 최적화된 새로운 방식을 한 가지 제안하고자 한다. 정성적인 분석과 정량적인 분석의 특징을 혼합하여 절충한 제안하고자 하는 방식이 Best-Practice(BP) 위험도 분석 방식이다.

1. 서 론

열차제어시스템(train control systems)은 열차의 속도제어 및 진로제어 등을 담당하며, 특히 열차의 충추돌 방지의 기능을 담당하는 열차의 안전운행을 최종적으로 책임지는 바이탈 시스템이다. 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 열차제어시스템의 안전성 확보를 위한 절차를 수행하는 체계인 안전성 활동을 시스템의 수명주기 전반에 걸쳐 진행하여야 한다. 본 논문에서는 안전성 활동 중에서 위험도 분석 및 평가를 위한 방법에 대해 알아볼 것이며, 그 중에 최적화된 새로운 방식을 한 가지 소개하고자 한다. 또한, 제안하는 BP 위험도 분석 방식을 적용하여 국내 ATC(Automatic Train Control) 시스템에 적용한 사례를 제시할 것이다.

2. 위험도 분석 및 평가

위험도는 사고의 발생확률과 사고가 발생했을 경우 심각도의 곱으로 정의한다. 사고의 발생확률과 심각도의 곱인 위험도는 시스템의 안전성 활동을 통해 허용범위 내로 존재하도록 시스템 수명주기 전체 단계를 거쳐 위험원이 제어 및 관리되어야 한다. 위험도 분석 전체과정은 시스템 정의에서부터 시작하여, 위험원 도출, 결과 분석, 위험도 평가, Tolerable Hazard Rate(THR) 할당, 위험원 제어의 모든 과정을 포함한다. 즉, 안전성 평가 활동의 목표가 사고의 발생빈도와 심각도를 나타내는 위험도를 허용가능한 수준으로 만드는 안전성 확보라 할 수 있으므로 위험도 분석 과정이 안전성 활동 체계 전반이라 해도 과언이 아니다.



<그림 1> 위험도 평가를 위한 방법들

위험도 평가를 위한 방법으로는 그림 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 Best-Practice(BP) 위험도 분석 방식이다.

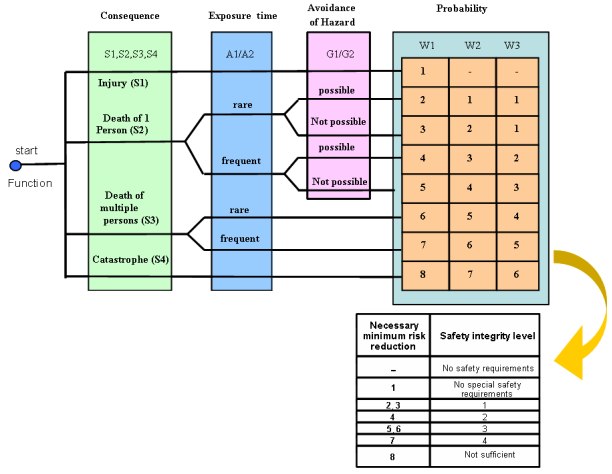
2.1 정성적인 위험도 매트릭스 방식

위험도 매트릭스는 위험원의 발생빈도와 심각도를 표 1과 같이 매트릭스 형태로 배치하여 위험도 등급을 결정하는 방식이다[1]. 위험도 등급은 일반적으로 I부터 IV까지 위험도의 크기와 빈도에 의한 테이블로 결정된다. 이 위험도 등급에 의해 해당 위험도가 수용가능한지 아니면 안전대책을 통해 수용가능 수준 이하로 제어해야 하는지를 결정할 수 있게 된다. 도출된 위험도 등급별 안전무결성레벨(SIL : Safety Integrity Level)을 할당하여 IEC 기준에서 정하는 THR을 할당하는 방법도 적용되고 있다. 이와 같은 위험도 매트릭스 방식의 장점은 비교적 쉽게 THR이 유도될 수 있다는 것과 사용하기 쉽다는 점이다. 이에 반해 위험도 매트릭스의 결과는 사용된 시스템 레벨과 참고문헌의 양에 의존해야 하며, 몇몇 중요한 파라미터들이 누락된다는 단점이 존재한다.

<표 1> 위험도 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

2.2 위험도 그래프 방법



<그림 2> 위험도 그래프

위험도 매트릭스 방법에서는 심각도와 발생빈도만을 고려하였으나, 위험도 그래프에서는 여기에 추가적인 파라미터들을 더 고려하여 유럽 열차제어시스템의 위험도 평가에 많이 적용되고 있다. 그림 2와 같이 이러한 여러 파라미터들을 고려하여 위험도 등급을 평가하고, 이 도출된 등급에 SIL을 할당하는 방식을 적용한다 [2]. 위험도 그래프의 최종결과인 특정 W scale은 안전 관계 시스템의 SIL을 제공하고, 이 시스템에 요구되는 위험도 감소에 대한 대책을 의미한다. 이와 같은 위험도 그래프 방식은 비용 측면에서 효율적이며 시스템 기능 레벨에 적용할 수 있다는 장점이 있는 반면, 위험도 그래프에 내재하는 위험도 수용이 명백하지 않고 매개변수의 카테고리가 구두로만 설명된다는 단점이 있다.

2.3 IRF 계산 방식

일반적으로 개별 위험도 또는 총체적인 위험도가 계산될 수 있으며, IRF를 구하는데 다음 식 (1)이 사용될 수 있다 [3].

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

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

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

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. 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-Risk 방식

위와 같은 다수의 위험도 평가 방법들은 많은 비용과 시간을 요하며, 고도의 전문지식을 필요로 한다. 최근 독일에서는 다른 위험도 평가 방식의 단점들을 보완한 새로운 Best-Practice(BP) 위험도 분석 방법을 도입하여, 철도신호분야에 적용하고 있다 [4]. BP-Risk 방식의 적용절차는 다음과 같다.

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. 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.

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

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

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

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(a), 속도(v), 사고유형(t)으로 분해될 수 있다. 상수 c와 더불어, 심각도 $s_i = c \bullet a_i \bullet v_i^2 \bullet t_i$이 된다. 각 부분 위험도의 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.

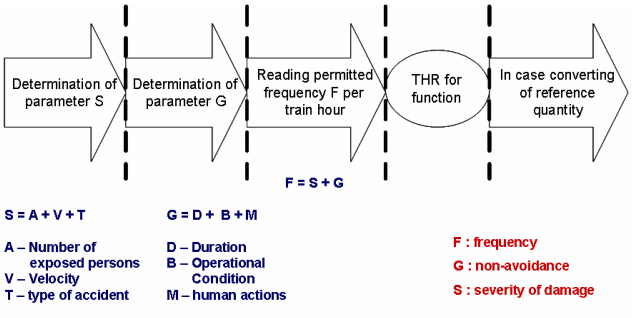
$$C_i = [\log_b(R_i)] \approx [\log_b(f_i)] + [\log_b(g_i)] + [\log_b(s_i)] \quad (5)$$

위의 식 s_i의 경우 $S_i = A_i + 2 \bullet V_i + T_i$가 된다. 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 3으로부터 취할 수 있다.

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

$$S = A + V + T \quad (6)$$

여기서, A는 위험에 노출된 사람의 수, V는 속도, T는 사고유형을 나타낸다. 모든 시스템 고장이 반드시 사고를 일으키는 것은 아니기 때문에 non-detection 또는 non-avoidance 확률(G)이 추정되는 것이다.



<그림 3> BP-Risk 방식의 기본순서

G는 식 (7)에서의 매개변수들로 나뉠 수 있다. 모든 매개변수들은 시스템 경계 밖에 있어야 한다는 것에 주의한다.

$$G = D + B + M \quad (7)$$

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

$$S + G + U \quad (8)$$

국내 ATC의 속도 제한 조작을 예로 들면, ATC는 train-borne system이므로 열차에 계속적으로 영향을 미치는 기능(U)은 0으로 추정된다. 이처럼 각 변수에 대한 구체적인 값을 정의한 표를 참고한다면, $S+G$ 값을 구할 수 있으며 최종적으로 이에 해당하는 THR을 도출할 수 있다. 이러한 결과를 안전요구사항과 비교하여 위험도 분석을 통한 안전성 확보를 이룰 수 있다. 이와 같은 BP-Risk 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-risk가 더 효율적이며, 정량화된 위험도 분석과 비교하여 약 40%의 작업량을 감소시키는 것을 기대할 수 있는 큰 장점을 지닌다. 마지막으로 BP 위험도 방식에 쓰인 모든 매개변수들은 다른 정성적인 방법들보다 더 정확하게 설명된다는 것과, 특히 심각도의 매개변수는 세 개의 하위 매개변수들로 구성되어 BP 위험도 방식을 사용하면 보다 더 우수한 평가를 가능하게 해준다는 이점이 존재한다.

3. 결 론

본 논문에서는 열차제어시스템의 안전성 확보를 위해 요구되는 안전성 활동의 핵심 단계인 위험도 분석 및 평가를 위한 기법들에 대해서 구체적으로 서술하고 비교해 보았다. 지금까지 철도신호시스템에서 안전성 입증을 확인하기 위해 기존의 위험도 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 위험도 매트릭스와 위험도 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.

[참 고 문 헌]

[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.