철도시스템 기본위험분석모델 개발 방안에 관한 연구
A Study on the Development of Preliminary Hazard Analysis Model for Railway System

왕종배** 박찬우* 박주남*

Wang, Jong-Bae Park, Chan-Woo Park, Joo-Nam

Abstract

To improve safety management of railway and cope with the factors to threat technical and social safety, we need to establish railway safety management system based on analysis of hazards and assessment of risk for railway system. So we have to conduct PHA(Preliminary Hazard Analysis) first to understand weak points and factors to possibly threat safety using analysis of related data such as past accident/incident data and safety regulation and classification standards of hazards/causes of railway accidents. Therefore in this research, we led types/dangerous events/causes of risks/factors of risks from hazard log developed based on railway accident classification and hazards of railway accident. PHA model for domestic railway system will be used in risk analysis and risk assessment of railway accident.

1. 서론

철도 안전관리와 기술기반을 선진국 수준으로 제고하고, 기술적·사회적 안전 위협요소에 대응하기 위하여 철도시스템 위험(Hazard) 분석 및 위험도(Risk) 평가기술을 기반으로 하는 국가적인 철도안전관리시스템의 구축이 요구된다. 이를 위해서 철도의 위험관리는 우선 사고/장애 이력자료와 안전규정/기준 등의 관련 자료 분석과 철도사고 위험/원인 분류기준을 통하여 철도사고를 유발할 수 있는 취약요인과 안전 위협요소를 사전에 파악하는 기본위험분석(PHA)이 선행되어야 되어야 한다.

따라서 본 연구에서는 국·내외의 사고/장애 이력자료와 안전규정/기준 등의 관련 자료 분석을 통해 도출된 철도 사고분류와 철도사고 위험요인을 통하여 개발된 철도사고 위험목록(hazard log)을 통하여, 기본위험분석(Preliminary Hazard Analysis, PHA)의 철도사고의 형식/위험사건/위험원인/위험요인을 도출하였으며, 위험사건 별 안전대책을 도출하기 위한 연구를 수행하였다.

이를 위해 본 논문에서는 2장에는 예비위험분석에 대하여 소개하고, 3장에서는 예비위험분석에서 철도시스템의 위험조건과 위험사건을 정의하며, 제 4장에서는 이를 통해 본 연구에서 수행된 기본위험분석 모델을 소개한다. 마지막으로 제 5장에서는 결론 및 추후 연구방향을 제시한다.

* 한국철도기술연구원 책임연구원, 정회원

** 한국철도기술연구원 선임연구원, 정회원

2. 예비위험분석(Preliminary Hazard Analysis: PHA)

현재 제안되고 있는 많은 국제안전규격들의 첫 번째 특징은 위험도 평가(risk assessment)에 토대를 한 안전성 입증에 있다. ISO/IEC 가이드 51에 규정된 안전의 기본 개념은 위험도 평가를 바탕으로 하고 있다. 그림1은 가이드51에 표시된 안전성 평가의 순서를 나타낸다. 설비 혹은 시스템은 의도된 사용방법 외에 합리적으로 예견 가능한 오류사용을 배려하여 위험원(hazard)을 판별하고, 위험도의 크기를 어림잡아 그 위험성이 허용 가능한지의 여부를 평가하여 만약 허용가능하지 않으면 위험성 저감 대책을 실시하여야 한다. 또한 충분히 허용 가능한 위험도 수준일 때를 안전하다고 정의한다.

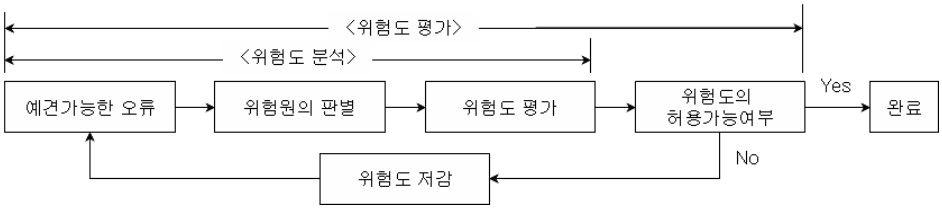

그림1. 위험도 평가 절차

예비위험분석은 그림1에서 위험원판별 및 위험도 평가 단계의 예비평가 단계에서 사용되는 분석방법으로써, 시스템 위험분석의 초기단계에 핵심 안전위험 부분을 확인하고, 위험조건의 초기 평가와 필요한 위험조건 관리 및 후속 조치를 판단하기 위하여 수행된다. 일반적인 예비위험분석의 절차 및 방법은 그림2와 같다.

입력자료	· 철도시스템에 대하여 일반적으로 고려되는 가능한 사건들의 리스트 · 시스템 연구의 경계 규정 · 시스템 운영 및 유지보수 단계의 정의 · 위험조건의 심각도 수준(gravity) 정의 · 시스템에 대한 설명 - 시스템의 기능 흐름도(Functional Flow Diagram) - 기존 시스템에 대한 제품분해구조(Product Breakdown Structure: PBS)
⇩	
예비위험 분석	① 철도시스템에 대하여 일반적으로 고려되는 가능한 사건들 중에서 하나의 잠재적 사건을 선택 ② 수명주기에 따른 잠재적 사건의 발생 가능성 조사 ③ 잠재적 사고를 일으키는 모든 불안전 사건의 규정 ④ 불안전 사건의 기술 ⑤ 각 불안전 사건과 관련된 영향의 규정 ⑥ 각 불안전 사건과 일치하는 위험수준의 평가 ⑦ 안전기준의 정의 - 각 불안전 사건을 제거하거나, 최소화하거나 또는 통제하기 위하여 수행되어야 하는 대책에 관한 제안 ⑧ 안전대책의 수행 후에 기대되는 빈도 수준의 평가
⇩	
출력자료	· 불안전 사건들의 리스트와 관련된 위험조건의 심각도 수준과 발생빈도 · 잠재적으로 위험한 요소들의 리스트 · 각 위험요소에 대한 안전기준의 정의

그림2. 예비위험분석 단계 및 절차

3. 위험조건과 위험사건의 정의

그림2의 예비위험분석에서 위험조건의 확인과 평가는 위험조건의 중요성, 위험조건 확률 및 운용 제약 조건을 고려하여 이루어지며, 받아들여질 수 있는 수준까지 관련된 위험을 줄이거나

위험조건을 제거하기 위하여 필요한 안전 대책 및 대안들이 포함하며, 철도시스템에서 일반적으로 고려되는 위험조건은 표1과 같다.

표1. 철도시스템 수명주기 및 기술특성상의 제반 위험조건

1. 위험부품	a) 기체/액체/고체상태 인화성 물질 b) 레이저 c) 폭발물 d) 질식, 중독, 부식 유발 물질 e) 고온 또는 저온 유체 f) 위험 건설자재 g) 압력시스템 h) 전원 i) 이온화 또는 반이온화 방사원 j) 수력 도르래, 또는 회전기계 k) 회전 또는 기타 기계적 동작에 의한 에너지원 l) 배기가스 m) 장애물 n) 위험한 표면 o) 절단면/천공부위	3. 운영 위험	a) 실족 b) 충격과 진동(지진 포함) c) 극고온/저온, 극고압/저압, 악천후 d) 소음 e) 독성/부식성 물질 등의 노출 f) 화재/폭발 g) 곤충, 쥐, 곰팡이 등의 설비 손상 h) 이물질, 먼지 i) 낙뢰 등 전계 방전 j) EMI k) 이온화 또는 반이온화 방사 (레이저 포함) l) 전원공급 차단, 유압시스템 고장 m) 배기가스
2. 인터페이스	a) 재료간 상호적합성 b) EMI/EMC c) 부주의 d) 발화 및 화재/폭발 전파 e) H/W 및 S/W 제어	4. 적대적 행위	a) 적대적 행위 b) 능동 보호시스템 동작실패 c) 수동 보호시스템 비효율성 d) 손상 방지
5. 교육훈련 및 비상절차	a) 평상시/훈련시/전시 운영 b) 인적오류 고려 c) 교육훈련의 효과/신뢰성 d) 건강 e) 사용자 실수 f) 설비배치, 조명 등 인간공학적 요인 g) 독성물질, 소음 및 복사에너지 등의 노출위험 h) 긴급지원체계 i) 충돌안전, 탈출, 구조 등 생존성 j) 복구 및 구원운전	7. 설비	a) 지원장비 b) 교육 c) 위험물 저장규정 d) 위험물 취급규정 e) 위험물 시험규정
6. 손상제어 대책	a) 손상 방지 b) 수리 c) 위험 억제 d) 탈출, 구조	8. 안전관련 장비, 보호수단 및 고장억제 대책	a) 화재 진압 시스템 b) 독성 물질 통제 c) 전원공급, 공조시스템 d) 개인보호장비 e) 환기 f) 방음벽 g) 경보 및 경고
9. Common mode failure 방지	a) 시스템 이중화 및 분산 b) 인터록 c) fail-safe 설계	10. 시스템 안전 지침 및 기준 준수여부	a) 업무종사자의 시스템 숙련도 b) 사건 기록/감시 c) 운영자 실수 d) 설계 결함 e) 관리감독 소홀 f) 대체부품 결함
11. S/W로 작동되는 전자장치	a) 바이러스 b) 보안문제		

불안전 사건의 확인은 다음과 같은 요소를 고려하여 수행되며, 일반적으로 고려되는 철도시트템의 위험사건은 표2와 같다. 표2는 위험사건은 11개로 세분화 되어 있으나 그 분량이 많아 본 논문에서는 생략하였으며 나머지 6가지에 대한 불안전사건은 한국철도기술연구원 (2005)에서 볼 수 있다.

- 설비의 기능장애 : 기능 없음, 기능 퇴화, 시기를 놓친 기능수행위험 요소
- 설비와 관련된 안전 : 연동, 시스템 중복, 하드웨어 혹은 소프트웨어 실패
- 위험 요소 : 연료, 발사 화약, 폭발물, 유독성 물질, 압력 시스템 등
- Interfaces : 자재 호환성, 전자기적 간섭, 부주의한 활동 등

- 환경적 제약 : 진동, 극한의 온도, 유독성 물질에 노출 등
- 운영과 보전 절차 : 인간의 오류 등

표2. 철도시스템의 불완전 사건 요소

1. 충돌	1.1 차량간 충돌위험 1.2 차량과 선로장애물과의 충돌위험 1.3 차량과 선로구조물과의 충돌위험 1.4 차량과 선로 작업자와의 충돌위험 1.5 차량과 선로상 대피자와의 충돌 1.6 차량과 선로 불입침입자와의 충돌 1.7 차량과 역구내 사람과의 충돌위험 1.8 차량과 다른 차량으로부터 떨어졌거나 치인 사람과의 2차 충돌위험 1.9 차량과 다른 차량으로부터 떨어진 장애물과의 출동위험 1.10자동차와 철도시스템구조물간 충돌 1.11사람과 철도시스템 구조물로부터 떨어진 장애물과의 출동위험 1.12사람과 차량기지에서 이동중인 장비와의 충돌	3. 폭발	3.1 승객 폭발물 소지 3.2 대피 후 폭발물 폭발위험 3.3 열차/역사/차량기지에서 장비의 고장/오조작으로 인한 폭발위험
		4. 추락	4.1 유지보수 작업 중 선로상 추락위험 4.2 대피 중 선로 위로 추락위험 4.3 열차운행 중 선로 위로 추락위험 4.4 불법침입 중 선로 위로 추락위험 4.5 역 구내 추락위험(계단, 에스컬레이터, 플랫폼) 4.6 차량내 추락위험 4.7 차량기지 내 추락위험 4.8 차량과 플랫폼 사이의 추락위험
2. 탈선	2.1 차량시스템의 고장으로 인한 탈선 2.2 선로 이상으로 인한 탈선위험 2.3 과속으로 인한 탈선위험 2.4 분기기 동작 중 탈선위험 2.5 선로 장애물로 인한 탈선위험	5. 감전	5.1 유지보수 작업중 차상 고압 감전 5.2 운행 중 차상 고압 감전 5.3 유지보수 작업중 선로상 고압 감전 5.4 대피 중 선로상 고압 감전 5.5 불법침입 중 선로상 고압 감전 5.6 유지보수 작업중 역구내 고압 감전 5.7 운행 중 역 구내 고압 감전 5.8 차량기지 내 고압 감전

4. 기본위험분석(PHA) 서 작성

본 연구에서는 국·내외의 사고/장애 이력자료와 안전규정/기준 등의 관련 자료 분석을 통해 도출된 철도 사고분류와 철도사고 위험요인을 통하여 개발된 철도사고 위험목록(hazard log)을 통하여, 기본위험분석(PHA)의 철도사고의 형식과 위험사건을 표3과 같이 도출하였으며, 위험사건별 위험원인과 위험요인을 도출하였다. 충돌사고에 대해 도출된 위험원인과 위험요인을 나타내며, 전체 위험사건에 대한 위험원인과 위험요인은 한국철도기술연구원 (2005)을 참고하기 바란다.

표3. 예비위험분석의 사고형식 및 위험사건 항목

사고형식		위험사건	
열차 충돌 사고	여객 열차	신호지시오류(인적오류)	주행선,역구내, 입환장
		기관사 업무수행불능, 제동실패, 추진실패	
	화물 열차	제어장치결함	차상제어장치고장, 지상신호장치고장
	위험물 열차	이선진입	분기기 고장, 경로설정 오류
		차량분리/구름	차량연결 해제, 제동풀림
	장애물 충돌	선로 장애물, 선로구조물 지장, 도로차량 지장, 궤도장비 지장	
열차탈선 사고	직선, 곡선, 분기	차량결함, 선로결함, 선로장애, 자연재해, 취급오류, 기관사 업무수행 불가, 분기기 고장	
화재 사고	터널, 교량, 역사	차량화재	동력차, 화차, 위험물
		시설화재	
건널목 사고	도로차량 충돌	직전 횡단, 차단기 돌파, 차단기 우회, 차량 정지, 차량 지장, 안전설비 결함	
	보행자 충돌	무단횡단	
사상사고	여객, 공중, 직무	추락, 전도/실족, 출입문 끼임, 충격, 화상, 감전, 질식, 불법행위	

표4. 열차충돌사고의 위험원인과 위험요인

사고형식		위험사건		위험원인	위험요인	비고
열차 충돌 사고	여객 화물 위험물	신호 지시 오류 (인적 오류)	주행선 역구내 입환장	기관사 신호미확인	신호위치, 신호상태	곡선지장, 수목장애
				기관사 신호위반	신호/지시 위반, 주의반응 실패, 안전상태 추측	졸음, 주의태만
				기관사 신호오인	신호착각, 이전신호 망각, 판독 실패/오판	
				신호지시 없음	신호지시 미전달, 신호기 고장	사령, 신호원
				잘못된 신호지시	오류신호전달, 신호기 작동오류	
		기관사 업무수행불능		사상/질병		
				음주/약물		
		제동실패		제동장치 고장		
				제동취급 지연	과속, 선로조건(눈,비,오염물, 낙엽 등)	
				제동취급 오류	제동력부족, 제동취급절차오류	
		추진실패		출발지연/운행정지	출입문 고장, 비상제동체결	
				기동불능	추진장치고장, 추진력부족, 점착력 부족	
		제어장치 결함	차상제어 장치고장	ATS, ATC, ATP	고장신호 미검지, 오류정보 현시	
			지상신호 장치고장	궤도회로/연동장치		
		이선진입	분기기 고장			
			경로설정 오류			
		차량분리/ 구름	차량연결 해제	연결기 풀림, 연결기 파손, 전철기 도중전환		
			제동풀림	구름방지 미설치, 급구배 제동부족		

이상의 결과에서 정의된 철도사고의 형식과 위험사건에 대하여 국내 철도운영기관(한국철도공사, 서울지하철, 도시철도공사 등)의 사고/장애 발생이력을 기준으로 발생빈도 및 피해도 평가를 수행 중이며, 현재 사용 중인 위험도 평가 메트릭스는 그림3과 같으며, 작성된 기본위험분석(PHA)의 예는 그림4와 같다.

		발생 빈도			
		발생하지 않음(D)	하(C)	중(B)	상(A)
심각도	사망/다수의 부상(I-1)	A	U	U	U
	사망/부상(I-2)	A	A	U	U
	부상/장애/재산손실(II)	A	A	U	U
	경미한 고장/장애(III)	A	A	A	A

그림 3. 위험도 평가 메트릭스

사고 형식	위험 사건	위험원인	사건유발 요소	위험 요인	결과	심각도	빈도	대 책	이후 빈도	허용
…	…	… … …	… …	… …	… … …	…	…	… … … …	…	…
열차 충돌	후방 충돌	비정상적으로 미끄러운 조건의 레일 (오일/그리스/낙엽 존재)	궤도상에 정지한 다른 열차 존재	궤도	시스템 중요 손상	I-1	B	레일은 정상조건으로 유지/ 관리되어야 함 (오일/그리스/낙엽 제거)	(II) C	A
				환경조건	인명부상 가능성			궤도구간의 여유간격		
								슬립/슬라이드 제어		
								선로 안전을 보장하기 위한 영업열차 운행전의 빗자루 열차 매일 운행		
…	…	… … …	… …	… …	… … …	…	…	… … … …	…	…

그림 4. 예비위험분석서(PHA) 작성 예시

5. 결론

본 연구에서는 국·내외의 사고/장애 이력자료와 안전규정/기준 등의 관련 자료 분석을 통해 도출된 철도 사고분류와 철도사고 위험요인을 통하여 개발된 철도사고 위험목록(hazard log)을 통하여, 기본위험분석(PHA)의 철도사고의 형식/위험사건/위험원인/위험요인을 도출하였으며, 위험사건 별 안전대책을 도출하기 위한 연구를 수행하였다. 향후 본 논문에서 제시된 국내철도시스템 예비위험분석(PHA) 모델은 국내 철도사고의 위험분석과 위험도 평가에 활용에 활용될 수 있을 것으로 판단된다.

감사의 글

본 논문은 건설교통부 “철도종합안전기술개발사업” (2004년 1차년도)으로 수행된 연구내용임을 밝히며, 건설교통부 관계자 여러분께 감사를 드립니다.

참고문헌

1. 곽상록, 왕종배, 홍선호, “철도안전관리 개선을 위한 확률론적 위험도평가 방안 연구”, 한국철도학회지 특별기고, 2003년 2월, 제 6권 4호, pp. 11-18
2. 건설교통부, “철도사고 위험요인(PHA) 분석기술 개발”, 2005
3. 동화출판사, “최신 안전공학개론”, 2002
4. 한국철도기술연구원, “철도사고방지 및 안전확보를 위한 핵심기술개발 연구”, 2003
5. 철도청, "철도청 사고보고 및 수습처리규정", 2003
6. USNRC, "An approach for using probabilistic risk assessment in risk-Informed Designs on plant specific changes to the licensing basis", reg. guide 1.174, 1998
7. Health & Safety Executive, “Railway Regulations 2000”, 2000
8. Network Rail, "Network Rail's Railway Safety Case, version 6", 2004
9. Kalay, S, "An international cooperative research approach to rail defect risk management", proc. of WCRR 2003, U.K. pp. 699-707, 2003
10. U.S. DOT, Faderal Transit Administration, "Hazard Analysis Guidelines for Transit Projects" DOT-FTA-MA-26-5005-00-01, Final Report, Jan. 2000
11. Railtrack, Profile of Safety Risk on Railtrack PLC-Controlled Infrastructure", Railway Safety Issue, SP-RSK-3.1.3.11, 2001