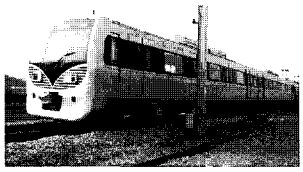
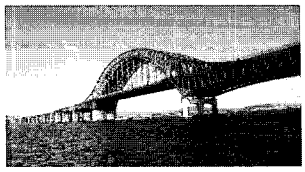
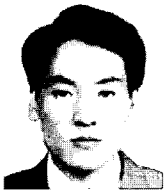




위험도 평가 기반의 철도시스템 안전관리

- 철도사고 위험(Hazard)분석 및 위험도(Risk)평가 체계 구축



왕종배 >>
한국철도기술연구원
안전기술연구팀 책임연구원

박찬우 >>
한국철도기술연구원
안전기술연구팀 선임연구원

1. 서 론

우리의 삶은 우리의 안전에 영향을 주는 상이한 시스템 망(網)으로 서로 얽혀있다. 이들 시스템은 각기 독특한 구조와 구성요소(부품) 들을 가지며, 각각의 시스템마다 재난 위험도를 나타낼 수 있는 고유의 위험들을 포함하고 있다. 우리는 항상 시스템이 제공하는 편익(benefit)과 그에 대비하여 나타나는 재난 위험도의 수용 사이에서 거래를 하고 있다고 할 수 있다.

일반적으로 모든 위험을 제거하는 것은 불가능하기 때문에 현실적인 목표는 수용 가능한 재난위험도 수준으로 시스템을 개발하는 것이 되며, 이것은 위험의 제거나 감소를 위하여 잠재위험을 확인하고 그들의 위험도를 평가하여 그에 따른 교정조치(안전대책)를 시행하는 것으로 이루어 질수 있다.

위험은 언제나 존재하지만 그 위험도는 반드시 수용 가능해야하며 그렇게 할 수 있어야 한다. 그러므로 안전은 예측 가능하고 수용 가능한 위험도의 수준을 나타내는 상대적인 용어로서 "시스템 안전은 완전한 수치라기보다는 오히려 비용, 시간 그리고 운영효과(시행)에 종속되는 재난 위험도 관리의 최적화된 수준"을 의미한다.

국방, 항공, 원자력과 같이 시스템이 복잡하고 재난 위험도가 높은 분야에서는 재난 위험도를 사전에 확인하고 이를 제거하거나 관리하는 정식 과정으로서 MIL-Std-882와 같은 시스템 안전 프로그램(SSP)을 수립하여 공학, 설계, 교육, 관리정책 그리고 환경에 대한 위험을 제거하는 정식적인 방법 · 절차와 관리 · 감독 체계를 구축하여 적절한 시스템 안전관리를 실행하고 위험도 기반의 안전목표 달성을 보장하고 있다.

철도와 같은 교통시스템에서도 재난 위험도 관리 활동의 출발점으로서 위험원(Hazard) 분석 및 위험도(Risk) 평가가 필수적이며, 확인된 위험은 최종적으로 해결될 때(수용 가능 위험도)까지 설계, 제작, 운영 및 유지보수의 수명 주기에 걸쳐 연속적인 순환과정을 통해 관리해야 한다. 즉, 위험요인의 판별, 관련 위험도의 정량적인 평가, 비용-효율적인 안전개

❑ 위험(Hazard) 분석/위험도(Risk) 평가에 기반한 철도시스템 안전관리 체계

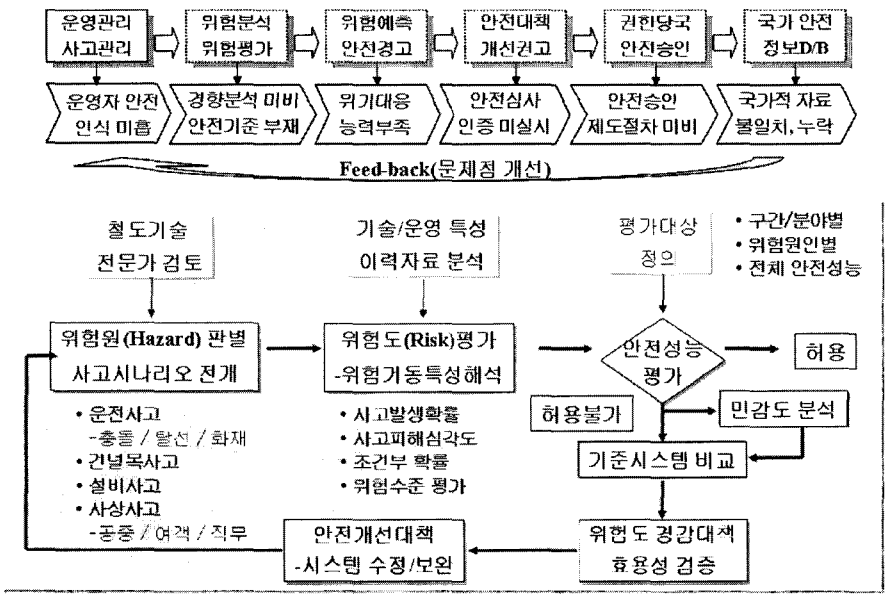


그림 1. 위험도 기반의 철도시스템 안전관리 체계

선 대책의 검토 및 실행 그리고 이에 대한 주기적인 문제점 개선 활동을 통해 일정한 안전수준을 지속적으로 유지하거나 향상시키는 일련의 순서를 가진 프로그램 활동을 기반으로 해야 한다.

본 고에서는 위험도 평가 기반의 철도시스템 안전관리의 절차를 소개하고자 하며, 이를 위해 본고에서는 2장에서 시스템 안전특성 및 안전관리 절차를 소개하고, 3장에서 시스템 안전관리와 재난의 연관성을 고찰해 본다. 다음으로 4장에서 철도사고 위험(Hazard)분석 및 위험도(Risk)평가 체계 구축을 위한 세부 절차를 조사하고, 마지막으로 5장에서는 본고의 결론을 정리하였다.

2. 시스템 안전특성 및 안전관리 절차

시스템 안전의 기본 목적은 사망, 부상, 시스템 손실 그리고 환경에 대하여 피해를 초래할 수 있는 위험을 제거하는 것이며, 재난 위험도의 감소는 재난 발생의 가능성이나 재난 심각도의 감소에 의하여 이루어진다. 과거 경험으로 볼 때 시스템의 설계와 개발 단계에서 안전에 대한 사전 예방을 하는 것이 사고나 재난이 발생한 이후에 시스템에 안전을 부가하는 것보다 훨씬 더 저렴하다는 것을 알고 있다. 따라서 시스템 안전은 잠재적인 재난이 초래할 수 있는 더 큰 피해와 손실을 막을 수 있는 초기 투자이다.

시스템 안전관리는 시스템 안전업무를 올바르고 종합적으로 달성하기 위한 프로그램 관리 요소로서 이것은 시스템 안전 요구사항의 확인(검증)을 포함해야 한다. 시스템 안전의 목적은 (발생 전에)무엇이 잘못될 수 있는지를 이해하고 발생 가능성의 감소와 피해 경감을 위한 예방관리 체계를 확립하는 것으로서, 이것은 위험 확인과 위험도 경감을 통하여 달성된다. 따라서 시스템 안전프로그램(SSP, System Safety Program)은 시스템 설계의 초기단계 부터 시스템의 개발 및 완성, 운영 및 유지보수 등 수명주기 전체를 통하여 지속적으로 실행되어야만 최소 비용으로 목표를 달성할 수 있다.

2.1 시스템 안전의 특성 및 속성

그림 2는 시스템의 일반적인 개념으로서 해당 시스템은 목적을 가지며 (영역)경계와 환경에 의하여 둘러싸여 있고 하부시스템 사이의 인터페이스와 함께 많은 하부시스템들을 포함하는 시스템을 보여준다. 본질적으로 시스템이란 시스템 목적 달성을 위해 서로 연계하는 하부시스템들의 조합이다. 하부시스템은 시스템 목적달성에 기여하는 특정기능의 시행을 위해 시스템 내에 연계된 장비, 부품, 직원, 설비, 공정, 문서, 절차 그리고 소프트웨어를 포함하는 시스템의 부분집합이다.

시스템 안전관리를 효과적으로 수행하기 위해서는 시스템에 관계하는 특성과 속성을 완전히 이해하는 것이 필수적이다. 이것은 시스템을 구성하는 것이 무엇이고, 어떻게 운영되며, 시스템 분석 도구, 시스템의 수명주기 그리고 시스템 개발공정에 대한 이해를 포함하는 것이며, 시스템 위험분석은 시스템의 기능, 하부시스템, 인터페이스, 경계 및 환경과 전체적인 시스템 그 자체를 포함하는 모든 시스템 형태에 대한 이해를 필요로 한다.

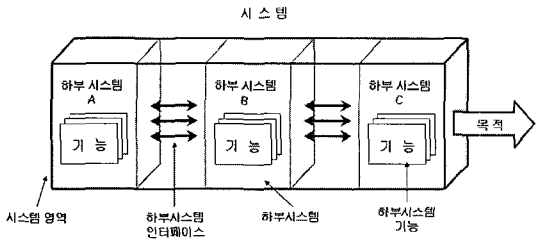


그림 2. 시스템 모델 및 속성

오늘날 철도 시스템과 같이 복잡성과 재난 위험도가 큰 시스템에서 재난과 사고를 의도적으로 막기 위해서는 시스템 안전이 필수적이다. 따라서 철도시스템의 안전관리는 "모든 위험(Hazard)에 관하여 허용할 수 없는 정도의 위험도(Risk)가 없는 것"이며, "만일 어떤 특정한 위험(Hazard)에 관하여 위험도(Risk)가 크다면 이것을 허용할 수 있는 수준까지 감소(개선)시키는 것"이다. 이때 사용재료의 고유 위험, 환경의 영향 그리고 운영 요구사항 등의 복잡성을 고려해야 하며, 더욱이 프로그래밍 오류와 같은 소프트웨어 인터페이스, 인적 오류 그리고 하드웨어 고장 등은 시스템 안전에서 반드시 고려해야 할 추가적인 사항이다.

다음은 시스템 구성요소별 속성에 대한 기본적인 안전 고려사항을 제시한 것이다.

- 하드웨어 고장 모드, 위험한 에너지 자원
- 소프트웨어 디자인 오류, 디자인 불일치
- 직원 인적 오류, 인적 부상, 인적 관리 인터페이스
- 환경 날씨, 외부 장비
- 절차 지시, 업무, 경고 노트
- 인터페이스 잘못된 입력/출력, 예상치 못한 복잡성
- 기능 실행 실패, 잘못된 실행
- 설비 구축 결함, 양립성 부족, 수송 결함

2.2 시스템 안전관리 절차

그림 3은 8개의 주요 단계들로 구성되는 MIL-Std-882에 따른 시스템 안전 관리 절차를 나타낸 것이다. 우선 안전계획 단계에서 재난 위험도 관리를 위하여 특정위험의 분석 및 보고를 포함하여 안전업무의 모든 사항들을 기술하는 공식적인 문서인 시스템 안전 프로그램(SSP)을 수립해야 한다. 그리고 실행 활동으로서 위험원의 확인과 그들의 위험도 평가, 위험도 감소 방법의 확인과 필요한 결정사항의 적용을 통한 위험도 감소의 확인이 이루어진다. 이때 위험도 감소 방법은 시스템 안전 요구사항(SSRs, System Safety Requirements)으로서 시스템 설계와 운영에 반영된다. 끝으로 확인된 모든 위험은 위험조치기록(HARs, Hazard Action Record)으로 변환하여 위험추적시스템(HTS, Hazard Tracking System)을 구성하고 이들 위험이 종결될 때 까지 HTS내에서 지속적으로 추적해야 한다.

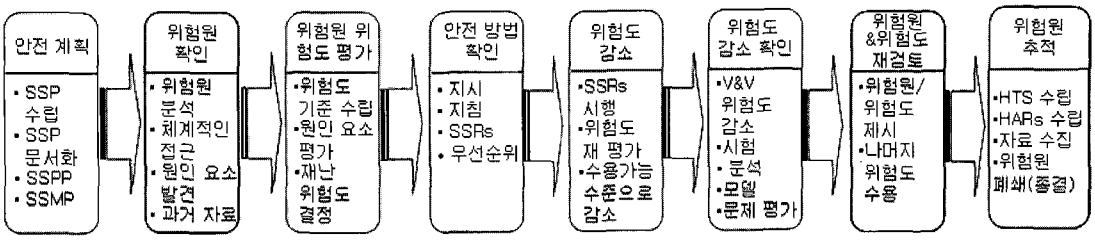


그림 3. 시스템 안전관리 절차(MIL-Std-882)

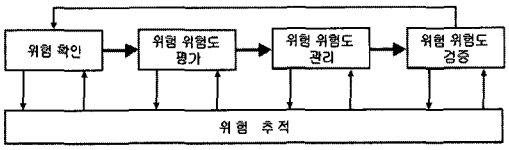


그림 4. 핵심 시스템 안전관리 절차

시스템 안전관리의 핵심은 위험도 관리로서 그림 3과 같이 위험의 확인, 재난 위험도의 평가 및 지속적인 위험추적을 통하여 위험도의 허용수준을 관리하는 것이다. 이것은 폐회로 공정으로서 피드백 과정을 반복 시행하여 위험도가 수용 가능할 수준이 될 때까지 위험을 추적하고 위험도를 확인하는 것이다.

3. 시스템 안전관리와 재난

그림 5에서 위험과 재난은 상태 변화로 연결된 같은 현상의 분리된 두 개의 상태이다. 위험원은 스펙트럼의 한쪽 끝 "잠재적인 사건"에서 다른 한쪽 끝 "실제사건"으로 의 상태변화를 기반으로 이동할 수 있다.

위험원으로부터 재난으로의 상태의 변화는 (1)수반되는 원인인자와 (2)결과적인 재난 위험도라는 두 가지 요소들에 근거한다. 원인인자는 위험원을 구성하는 인자들이며, 재난 위험도는 재난의 발생가능성과 발생되는 재난손실의 심각성이다.

재난은 자발적으로 발생하지 않으며, 시스템 설계에 부여된 설계 결함의 결과이다. 이런 의미에서 재난은 예상 가능한 사건들이며, 만약 해당 위험원을 제거하거나 경감한다면 그에 상응하는 재난 또한 제거되거나 통제할 수 있다. 따라서 위험원의 확인과 위험도 관리를 통한 시스템 안전관리는 재난 예방의 핵심인 것이다.

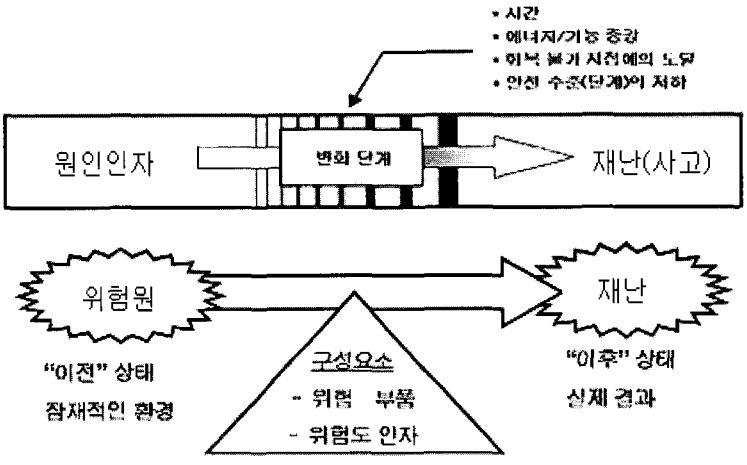


그림 5. 위험-재난의 관계성(상태변화)

4. 위험도 평가(Risk Assesment)

현재 많은 국가의 안전관리의 특징은 위험도 평가(risk assessment)를 토대로 하고 있다. 위험도 평가는 어떤 시스템의 수명주기(건설, 운영, 유지보수, 교환, 갱신 및 폐기)동안 발생하는 사고가 초래하는 특정기간 동안의 손실(loss)의 평균값을 측정한 것이며, 손실은 인명피해, 재산, 시간 등을 포함한다. 이것은 특정기간 위험원의 발생빈도와 초래되는 손실(예, 등가사망자)을 곱하여 계산할 수 있다. 즉, 위험도(예상 손실/특정기간)는 어떤 위험사건의 빈도(사건발생 건수/특정기간)와 위험사건이 초래하는 손실(예상 손실/특정기간)의 곱으로 표현된다.

철도 분야에서는 일반적으로 손실을 등가사망자(Equivalent Fatalities)로 표현하며, 등가사망자란 인명손실의 측면에서 손실을 표현하기 위하여 사망자수, 중상자수, 경상자수를 사망자수로 단위를 일원화하여 표현한 것을 의미한다. 예를 들어, 10명의 부상을 1명의 사망자로 환산하고, 100명의 경상자를 1명의 사망자로 단위를 환산하여 인명손실을 사망자수로 표현하여 한 것을 의미한다. 아래는 등가사망자로 표현된 위험도 평가 사례를 나타낸다.

그림 6은 영국철도의 표준 안전관리절차서인 Yellow Book에 표시된 안전성 평가의 절차를 나타낸다. 시스템 안전관리는 위험원을 판별하고, 해당 위험원이 야기하는 사고 또는 재난의 위험도를 평가하여 위험도가 허용 가능한지의 여부를 조사하고 만약 허용가능하지 않으면 위험도 저감 대책을 실시하여야 한다.

표 1. 위험도 평가 사례

	위험사건 기술	빈도(건수/년)	심각도(등가사망자/년)	위험도(등가사망자/년)
1	두 열차간의 충돌	1.8	3.32	5.8
2	선로 장애물과의 열차 충돌-탈선 없음	49.7	0.006	0.3
3	정거장내 두 열차간의 충돌	6.0	0.025	0.15
4	차막이 장치와의 충돌	40.9	0.029	1.2
5	건널목에서 도로차량과의 충돌	21.5	0.28	6.1
6	열차 탈선	14.3	0.30	4.3
	상기 6가지 위험사건의 전체 위험도 =			17.9

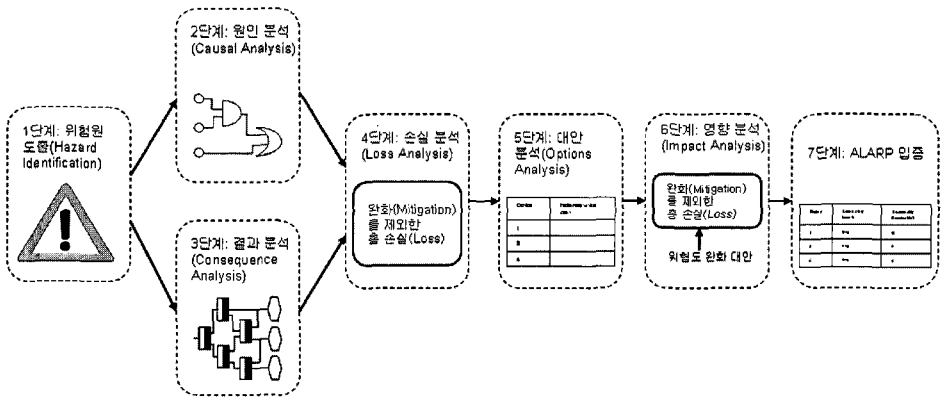


그림 6. 위험도 평가 절차

4.1 위험원 판별(Hazard identification)

위험도 평가의 첫 번째 단계인 위험원 판별은 시스템 안전관리의 토대를 제공한다. 따라서 체계적이고 이해 가능한 위험원의 판별 없이는 위험도 평가의 효과를 현저히 반감시킬 수 있으며, 시스템의 안전에 대한 잘못된 이해를 형성할 수 있다. 위험원과 위험원을 구성하는 원인요인(casual factor)을 정의하기 위해서는 위험원의 속성, 재난에 대한 그들의 관계 그리고 시스템 설계에 미치는 영향 등을 이해하는 것이 필요하다. 따라서 위험원을 판별하기 전에 관련 시스템의 영역과 시스템 주변 환경과의 상호관계를 정의해야 한다(그림 7 참고).

위험원을 판별할 때는 지금까지 고려되지 않았던 잠재적인 위험원의 상호작용에 대해 항상 고려해야 한며, 정상상태와 운영단계만으로 국한시키지 말고 철도에 설치된 시점부터 유지보수, 업그레이드를 포함하여 최종 사용중지까지의 시스템 전 생애에 걸친 모든 측면을 고려해야 한다. 위험원 도출은 전문 지식 및 이전 경험을 바탕으로 예비위험분석(PHA, Preliminary Hazard Analysis), HAZOP(Hazard and Operability Studies) 등의 기법을 통해 수행될 수 있다. 그림 8은 역구내 충돌사고의 위험원 판별 사례를 나타낸다.

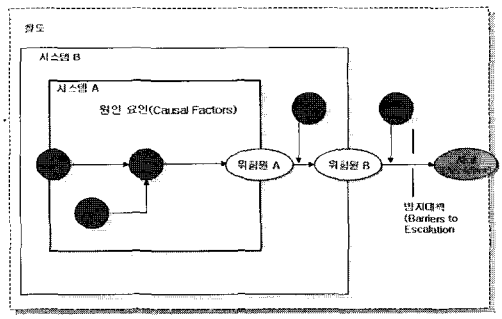


그림 7. 시스템 경계 설정 및 위험원 판별

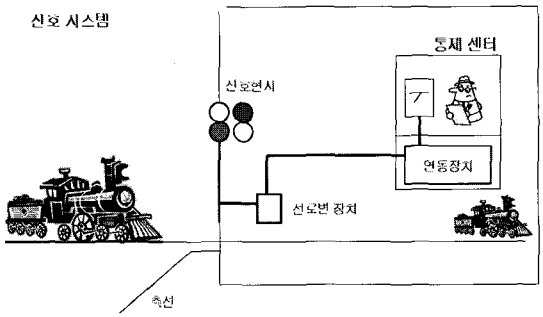


그림 8. 역구내 열차 충돌사고 위험원 판별 사례

역구내 열차 충돌사고 위험원 판별 사례

시스템 구성		원인요인	위험원	방벽-차단	사고발생
신호 시스템	신호기	신호등기구 고장	정지조건에서 진행신호 현시	이중화 (Fail-safe)	열차충돌 (역구내) -여객열차 (고속/일반) -화물열차 (일반/특수)
	선로변 장치	선로변장치 고장			
	케이블	케이블 단선			
	연동장치	연동장치 오출력			
	제어장치	전원공급 차단			
	관제사	교통관제 오류			
	· · ·				
차량 시스템	운행제어장치	지상신호 미검지	폐색구간 오진입	자동정지	
	제동장치	제동장치 고장			
	기관사	기후/전방시계 불량			
	· · ·			측선대피	

시스템 안전관리의 설계단계에서 수행하는 예비위험분석은 광범위한 정성적 분석으로서, 관리대상이 되는 핵심 위험원을 판별하고, 위험원의 초기 평가와 위험요인의 관리 및 후속 조치를 판단하기 위하여 수행된다. 철도 인명사상 사고에 적용된 예비위험분석의 사례는 그림 9와 같다.

상세 설계정보를 얻을 수 있고 대형사고 가능성으로 상위레벨의 보증이 요구되는 분야에서 위험원 판별을 위해 HAZOP 기법이 적용될 수 있다. HAZOP는 다양한 전문가 집단에 의한 시스템적이고 창의적인 위험원 판별방법이다. 전문가 집단은 시스템의 상세 설계정보를 수집하고, 인터페이스(interface)를 포함하여 각 시스템의 구성요소를 조사한다. 전문가 집단은 시스템 목적을 고려하고 길잡이 말(Guide words)을 이용하여 설계 목적에서 벗어나는 오동작을 파악한다. 아래의 표는 "역에서 열차 정지 후 차량

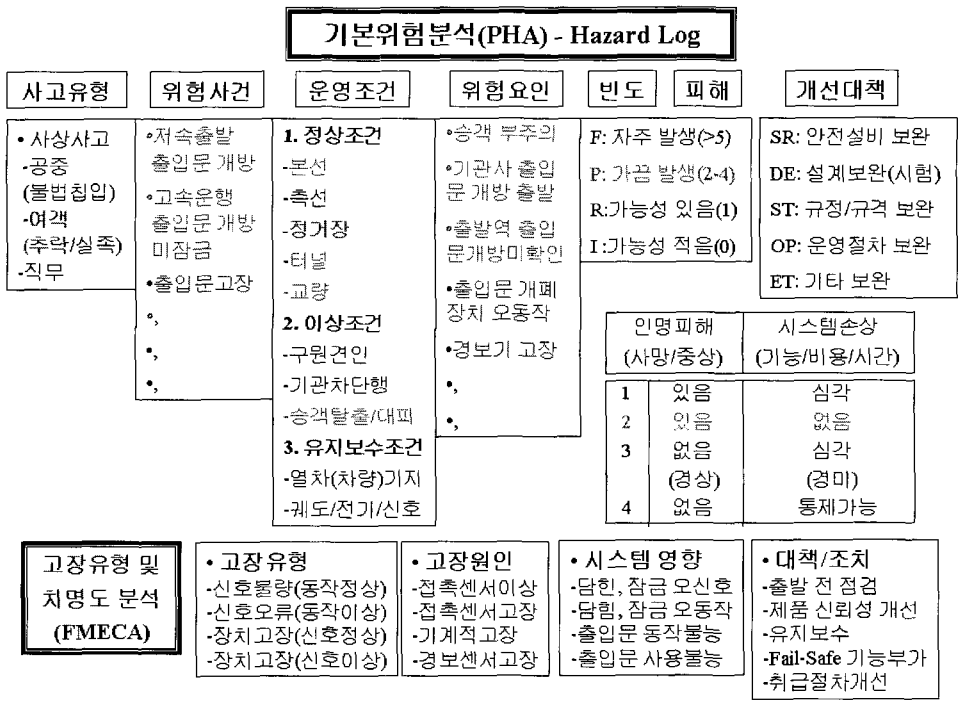


그림 9. 철도 인명사상 사고에 적용된 예비위험분석(PHA) 사례

표 2. 열차 시스템의 HAZOP 기법의 적용 사례

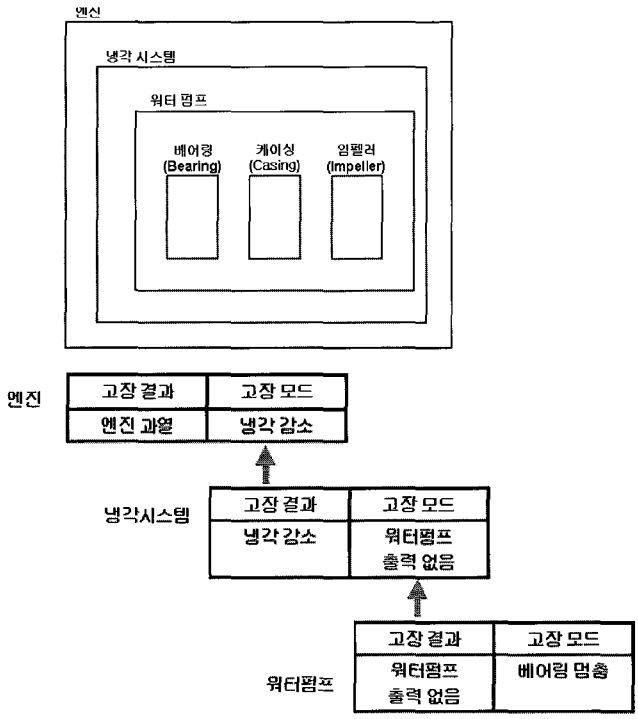
설계목적	역에서 열차 정지 후 차량 출입문 자동 개방		
Guide word	오작동(위험원)	원인 요인	Effect(영향)
NO	문이 열리지 않는다.	기계적 결함	승객 하차할 수 없음
MORE	문이 너무 일찍 열린다.	Operator error	승객 사상 우려
	(열차가 운행 중 이거나	조작자 실수	
	플랫폼에 접근하지 않은 경우)		
LESS	한 쪽 문만 열린다.	기계적 결함	승객 하차 제한으로 혼잡 초래, 사상 우려
AS WELL	열차의 양 쪽 문이 열린다.	제어 회로 고장	잘못된 문으로 내리는 승객의 사상 우려
PART OF	less의 경우와 동일함	-	-
REVERSE	N/A	N/A	N/A
OTHER THAN	반대쪽 문이 열린다.	제어 회로 고장	잘못된 문으로 내리는 승객의 사상 우려

출입문 자동 개방"이라는 설계목적을 가진 열차의 HAZOP 기법의 적용 사례를 나타낸다.

4.2 원인분석(Causal Analysis)

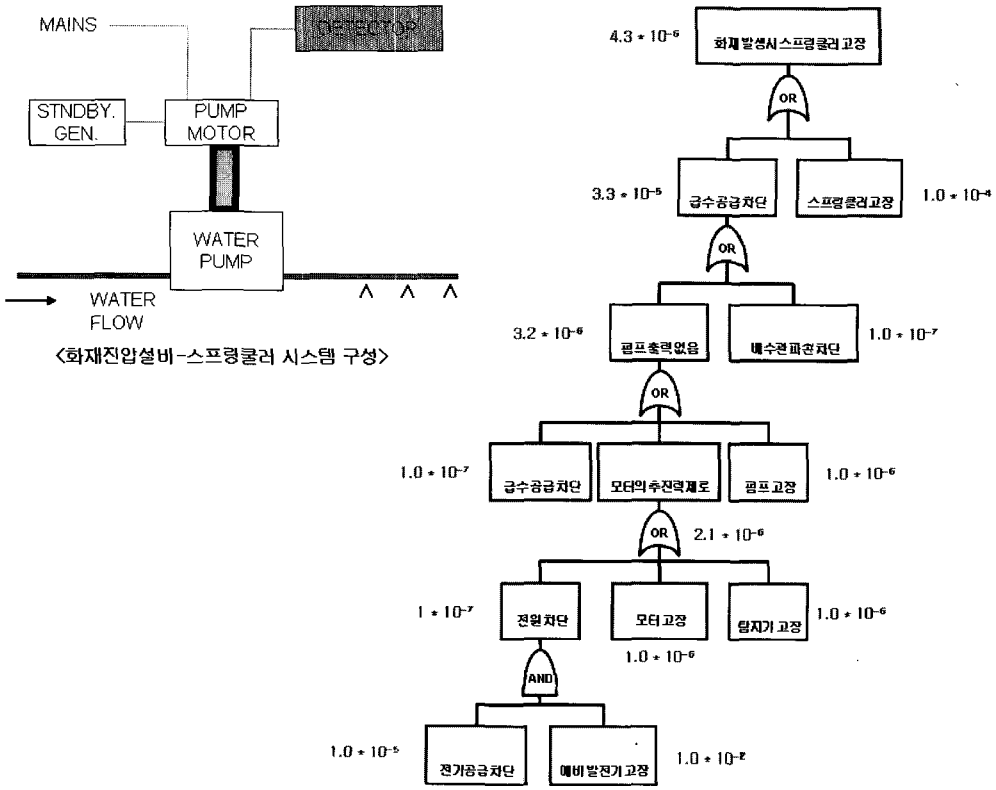
일단 위험원을 판별했다면 각 위험원의 발생확률을 평가하고, 발생확률의 저감방법을 찾기 위해 각 위험원의 원인분석을 수행 한다. 원인 분석은 정성적, 정량적으로 이루어질 수 있으며, FMEA(Failure Modes and Effect Analysis), FTA(Fault Tree Analysis) 등 대부분의 원인분석 기법은 각 위험원의 원인들 간의 관계를 이해하고 표현하기 위하여 위험원을 초래하는 원인의 도식적인 표현을 사용한다.

원인 분석방법으로 잘 알려진 FMEA는 시스템 계층구조의 하위 계층에서 상위 계층으로 상향식으로 순차적으로 분석을 실행한다. FMEA 분석 시 대상 계층의 고장 원인에 따른 결과를 기록하고, 대상 계층의 고장결과를 상위 계층의 고장 원인으로 기술한다. 이와 같은 과정은 전체 시스템의 위험원의 원인을 분석하기 위하여 기능적 계층을 따라 상향식으로 반복적으로 이루어진다. 그림 10은 FMEA를 적용한 원인분석의 예를 나타낸다.



항 목	설 명	모 드	원 인	국지적 결과	보상 규정	최종 결과
1	베어링	이상 정지	제조 결함	출력 없음	과열 경고	과열
2	케이싱	파손	충돌	냉각제 손실	과열 경고	과열
3	임펠러	파손	피로	출력 감소	과열 경고	과열

그림 10. FMEA를 적용한 원인분석의 예



<화재진압설비-스프링쿨러 시스템 구성>

그림 11. FTA를 적용한 스프링쿨러 시스템의 고장 원인분석의 예

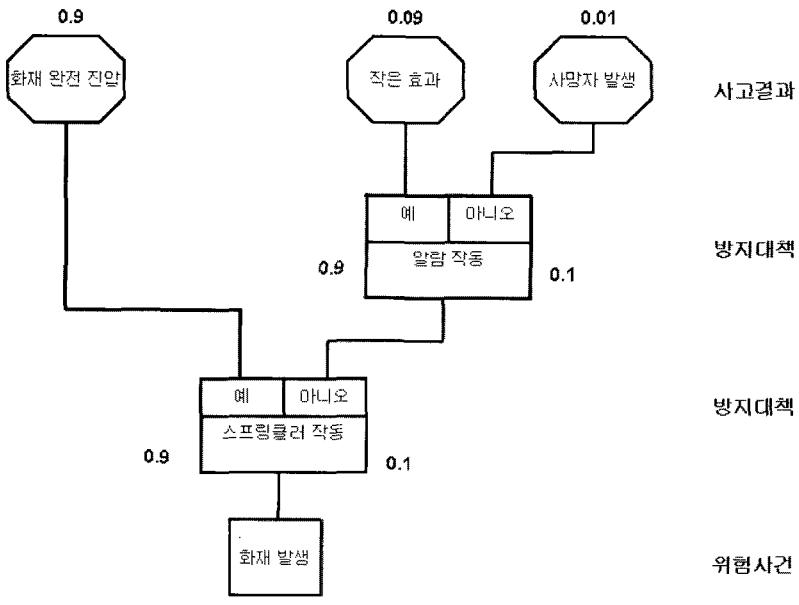


그림 12. 원인-결과 다이어그램(Cause Consequence Diagrams)을 적용한 결과분석의 예

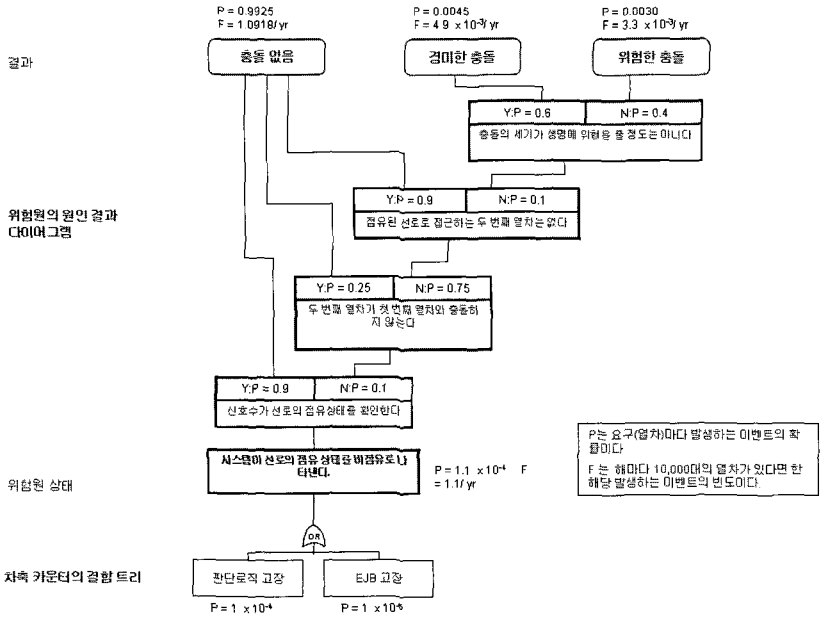
FTA(Fault Tree Analysis)은 하향식 원인 분석 또는 귀납법적 시스템 오류 분석 기법으로 알려져 있다. FTA는 상위의 위험원을 최상위 위험사건으로 시작해서 해당 위험사건에 대해 있을 수 있는 모든 원인을 분석한다. FT(Fault Tree)는 최상위 위험사건을 발생시키는 위험사건들을 계층적으로 조합하여 도식적으로 표현한 논리적인 모델이며, 정량적, 정성적 분석 모두에 사용될 수 있다. 그림 11은 FTA를 적용한 스프링쿨러 시스템의 고장 원인분석의 예를 나타낸다.

4.3 결과분석(Consequence Analysis)

결과분석은 각 위험원의 발생으로 야기될 수 있는 사고 및 재난의 최종 결과를 판단하기 위해 진행된다. 결과분석은 원인분석 방식과 비슷하게 정성적, 정량적으로 이루어질 수 있으며, 원인-결과 다이어그램(Cause Consequence Diagrams)과 ETA (Event Tree Analysis) 등 대부분의 결과분석 기법은 각 위험원의 발생에서 초래하는 손실을 표현하기 위하여 도식적인 표현을 사용한다. 그림 12는 화재 발생 시 결과분석의 예를 나타낸다.

4.4 손실 분석(Loss Analysis)

손실분석은 각 위험원과 관련된 잠재적인 안전 손실의 규모를 정량적으로 결정하기 위해 수행된다. 앞



- 중대한 충돌 : EF=사망 30+(중상 50*0.1)+(경상 200*0.05)=36명*1.5£M=54£M
- 경미한 충돌 : EF=(중상 2*0.1)+(경상 6*0.05)=0.23명*1.5£M=0.34£M
- 중대한 충돌 : EF=(경상 2*0.05)=0.01명*1.5£M=0.015£M

	생명가치(£M)	발생빈도/년	연간 손실(£M/yr)
Major Collision	54	0.0033	0.18
Minor Collision	0.34	0.0049	0.0016
No Collision(급제동)	0.015	1.0918	0.016
연간 총 손실			0.20

그림 13. 열차 충돌 사고의 손실분석의 사례

에서 언급했듯이 손실이란 인명피해와 환경적 또는 상업적 손해를 의미하며, 인명피해의 경우 사상자 수를 등사 사망자로 환산하고, 환산된 등가 사망자 수에 기 정의된 사망예방가치(VPF, Value of Preventing a Fatality)를 곱하여 손실을 표현할 수 있다. 여기서, 사망예방가치는 사망자 1인 줄이기 위해 사회가 지불할 수 있는 최대 비용을 의미한다. 영국 철도에서는 2006년 철도전략안전계획(Railway Strategy Safety Plan)에서 사망예방가치로 사망자 1인당 150만 파운드를 사용하였으며, 이는 편익(benefit) 분석 등의 통계분석기법을 이용하여 결정될 수 있다.

4.5 경감대책분석(Options Analysis)

각 위험원에 대한 위험도 완화 대책을 도출하기 위해 브레인스토밍(brainstorming)과 체크리스트(checklist)가 사용된다. 사용된 체크리스트에는 기존에 적용된 것으로 위험도 경감조치들이 기록되어 있다. 브레인스토밍과 체크리스트를 병행 사용하면 리스크 완화 목적으로 사용될 수 있는 중요한 대책들이 모두 도출되었다는 점에 대해 높은 신뢰감을 줄 수 있다. 모든 경감대책이 고려되었다면, 각각의 선택된 대책에 대한 안전 투자비용을 결정한다.

4.6 영향분석(Impact Analysis)

영향분석에서 도출된 각각의 잠재적인 위험도 경감 대책은 추후 분석과정을 거쳐 각각의 대책이 철도 운영 및 손실에 미치는 영향을 결정한다. 이를 위해 위험도 평가 절차의 앞의 4단계가 수행되며, 관련된 원인분석, 결과분석 및 손실분석의 기 개발된 모형을 수정하여 계산될 수 있다.

4.7 ALARP(As Low As Reasonably Practicable) 입증

영국의 "Health and Safety at Work Act (1974)"는 합리적이고 실행 가능한 경우 건강, 안전 복지를 보장하기 위하여 고용자에게 의무를 부여하는 합리적 시행(reasonably practicable)의 개념을 도입했다. 합리적 시행(reasonably practicable)의 개

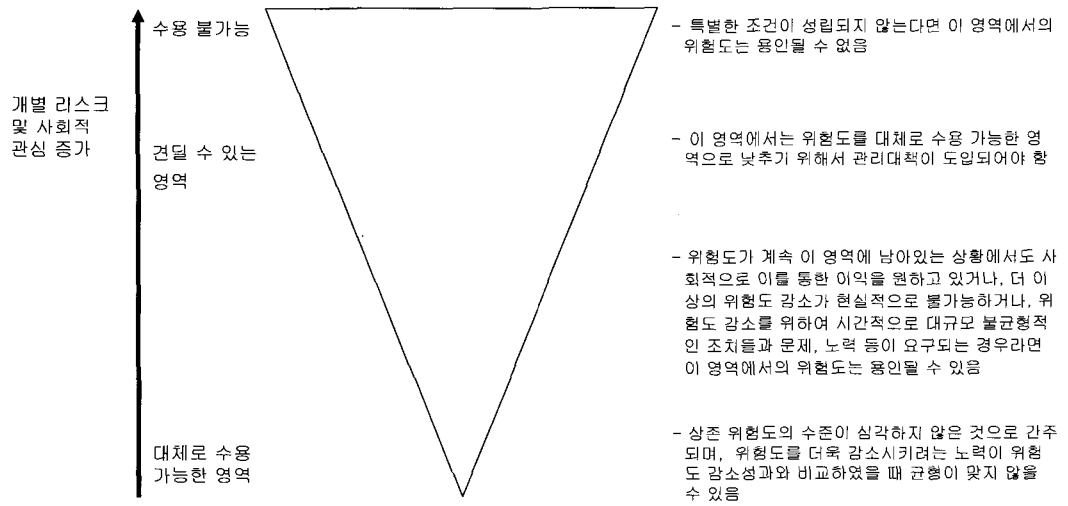


그림 14. ALARP 원칙

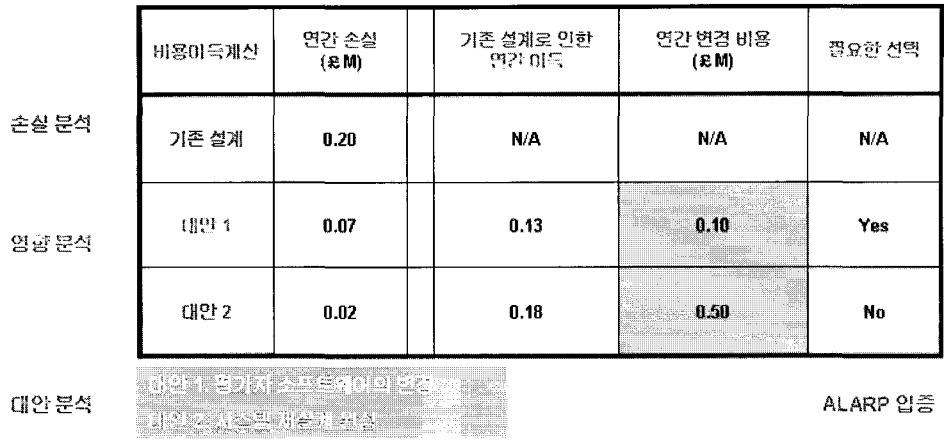


그림 15. 열차 충돌 사고의 경감대책분석과 영향분석의 사례(그림 13 참고)

념에 따르면, 만약 위험원 감소를 위한 방안이 존재하고, 얻어지는 위험원 감소의 이익과 비교하여 비용이 타당하다면, 위험원을 보편적으로 허용할 수 있는 수준까지 반드시 감소시켜야 한다. 이것은 ALARP 원칙으로 정의되며, 이 원칙은 안전규제자가 아래와 같은 두 가지의 목적을 달성하기 위한 수단으로 사용된다.

- 조직이 경제성을 고려하면서 안전개선을 위한 관리활동을 수행할 수 있도록 하는 것
- 모든 조직에 대해서 안전에 대한 판단이 동일한 방법으로 적용되고, "Health and Safety at Work Act(1974)"따라 통제될 수 있도록 하는 것

그림 14는 이러한 ALARP 원칙을 도식화 한 것이며, 위험도의 수용여부를 결정하기 위하여, 아래와 같은 절차를 적용한다.

① 먼저 위험도가 수용 불가능한 영역에 있는지 확인하고, 만약 수용 불가능한 영역에 있다면 이를 수용하지 않는다.

② 위험도가 대체적으로 수용할 수 있는 영역에 있는지를 확인하고, 합리적인 비용으로 위험도를 감소시킬 수 없다면, 위험도를 감소시킬 필요는 없다. 그러나 해당 영역에 계속 남아있는지 확인하기 위하여 감시해야만 한다.

③ 만약 위험도가 이들 두 영역 사이에 걸쳐 있는 경우, 위험도를 감소시키기 위한 합리적으로 실행 가능한 모든 방안을 수행한 후, 이를 수용한다.

그림 15는 그림 13에서 설명된 "열차 충돌 사고의 손실분석의 사례"에 적용된 경감대책분석, 영향분석 및 ALARP 입증의 사례를 나타낸다.

5. 맺음말

우리의 철도가 국가 공공 교통수단으로서 기대되는 서비스를 다하고 「철도안전법」을 중심으로 하는 제도적인 안전관리 체계의 구축과 효율적인 시행기반을 국가적으로 마련하기 위해서는 철도시스템의 제반 위험요인의 분석과 관련 위험도의 정량적인 평가를 통해 비용-효율적인 안전개선 대책을 수립하여 실행하고, 이에 대한 주기적인 문제점 개선 활동을 통해 지속적으로 안전수준을 유지 또는 향상시키는 프로그램 활동을 기반으로 하는 선진 시스템 안전관리 체계로 시급히 전환해야 한다.

지금까지 본 주제에서 다룬 위험도 평가에 기반을 둔 시스템 안전관리 체계와 안전 활동에 대한 사례 분석이 인간의 생명가치를 중심으로 우리의 철도 안전이 나아가야 할 목표와 방향을 설정하는데 시사점을 제시하고, 철도 안전이 국가 교통경쟁력 확보의

근간으로서 올바르게 기능과 역할을 다할 수 있도록 선진 안전관리 체계 구축의 원칙과 절차를 이해하는데 기여할 수 있기를 기대한다.

참고문헌

1. 건설교통부, "철도사고 위험도 분석 및 평가체계 구축", 철도종합안전기술개발사업 연구보고서, 2006
2. 박찬우, 김상암, 왕종배, 홍선호, 곽상록, "개인생명가치추정을 통한 안전개선 비용효과 분석에 관한 연구", 2004년 추계 한국철도학회 논문집, 2004
3. 한국철도기술연구원, "철도안전성능평가 기술개발사업", 철도안전성능 기술개발사업 연구보고서, 2002
4. 왕종배, 박찬우, 곽상록, 박주남, "위험도 평가 기반의 철도안전관리 선진사례 및 기술동향", 한국철도기술, 제 1권 1호, 2005
5. 왕종배, "위험도 평가 기반의 철도시스템 안전프로그램 개발 방향", 한국철도학회지, 제 8권 2호, 2005
6. Clifton A. Erison, "Hazard Analysis Techniques for System Safety", John Wiley & Sons, 2005
7. Railtrack, "Profile of Safety Risk on Railtrack PLC-Controlled Infrastructure", Railway Safety Issue, SP-RSK-3.1.3.11, 2001
8. RSSB, "Engineering Safety Management ISSUE 3 Fundamental and Guidance, Yellow Book3", 2000
9. RSSB, "Railway Safety working for a safer railway", SP-RSK-3.1.3.11, 2, 2003
10. U.S. DOT, Federal Transit Administration, "Hazard Analysis Guidelines for Transit Projects" DOT-FTA-MA-26-5005-00-01, Final Report, Jan. 2000