안전성활동의 추적성을 위한 초기 위험원 도출 기법에 대한 연구

A Study on Identification of Hazards for Their Tracking and Management

한찬희* 이영수** 안진*** 조우식****

Han, Chan-Hee Lee, Young-soo Ahn, Jin Cho, Woo-Sik

ABSTRACT

The primary purpose of the safety management is to prevent the loss of lives or physical damages arising from potential hazards in the railroad signaling system. Since such potential hazards may occur at any time during the system life cycle from design and development to maintenance, safety management activities have to be continuously taken in the course of the system life cycle. The identification of potential hazards is the early step of the safety management. However, such identification activities have to be continued during the system life cycle. Further, they have to be closely linked with system functions to prevent functional problems. This study provides a systematic approach to identification of potential hazards for their tracking and management during the system life cycle to assure the identification and definition of the most appropriate hazards.

1. 서 론

현재 국내에서는 RAMS에 대한 관심과 요구사항이 증가하고 있는 상황이며, 이에 대한 연구가 활발히 진행되고 있다. RAMS(Reliability, Availability, Maintainability, Safety) 중 RAM에 대한 기술적인 기법과 도구는 이미 오래전부터 실용화 및 적용되고 있으나, 안전성에 대한 적용은 아직 미온적이라 할 수 있으며 현재 여러 가지 시스템에 시험적용중이다. 또한 RAMS에 대한 정량적인 요구사항이 수립되어 철도 시스템 개발 제조사에 제시되고 이를 승인할 수 있는 제도적 기반이 확보되어야 하나 미흡한 실정이다.

안전성활동의 가장 큰 목적은 철도신호 시스템의 잠재적인 위험원으로 인한 사고발생으로 크나큰 재산상의 손실이나 인명피해 사고로의 발전을 차단하고 방지하는데 있다. 잠재적인 위험원은 시스템의 설계에서부터 개발, 그리고 유지보수까지 어느 단계에서든 나타날 가능성이 있기에 안전성 활동 또한 모든 생명주기에서 적용되어야 함은 당연한 일이다. 안전성활동의 가장 초기 활동인 위험원 도출은 이러한 생명주기동안 지속적으로 다루어져야 하며, 시스템 기능과의 연계성을 확보하여 기능적 결함이 발생하지 않도록 관리되어야 한다. 또한 철도시스템은 외부와의 인터페이스로 이루어져 있기 때문에 시스템 위험원의 범위를 정의하는 것 또한 매우 어려운 일이다.

본 논문에서는 이와 같이 안전성활동의 생명주기동안 추적성을 위한 위험원 도출에 대해 체계적인 방법을 제시하여 시스템에 가장 적합한 위험원을 도출하여 정의할 수 있는 단계별 활동 및 절차에 대해 기술하였다.

* 경봉기술(주) 주임연구원

** 경봉기술(주) 수석연구원

*** 경봉기술(주) 수석연구원

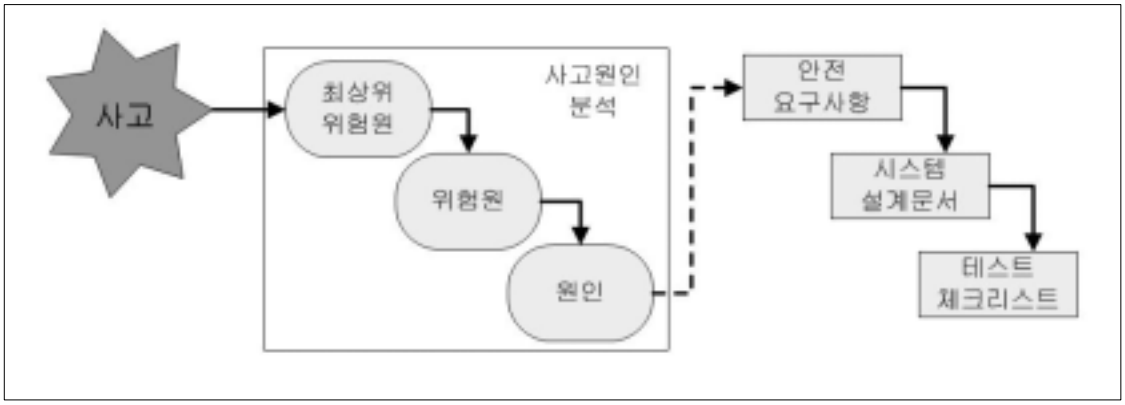
**** 경봉기술(주) 선임연구원

2. 위험원 도출

2.1 위험원 도출 이유

위험원은 '사고를 발생시키는 가장 근본적인 원인'으로 정의할 수 있으며, 위험원을 차단하였을 경우 사고가 발생하지 않는다는 조건이 성립하게 되나, 이러한 조건은 시간과 비용의 한계를 벗어나지 않도록 해야 한다. 위험원을 도출하는 첫 번째 이유는 다음과 같다.

1. 시스템의 기능상 오류나 불능으로 인해 발생되는 사고에 대해 그 원인과 결함에 대해 추적하여 찾아내고 재발을 방지하기 위함이다.



<그림 1 사고에 대한 추적성>

2. 시스템의 기능에 내재되어 있는 리스크를 산출하여 시스템의 안전성을 확보할 수 있는 대책을 수립하기 위함이다.

위험원 도출에 대한 규격에서의 설명은 매우 미약하여 도출 방법이나 절차, 구성에 대해 사용자마다 약간의 차이점을 가지게 되어 위험원에 대한 이해가 매우 어려워질 수 있다.

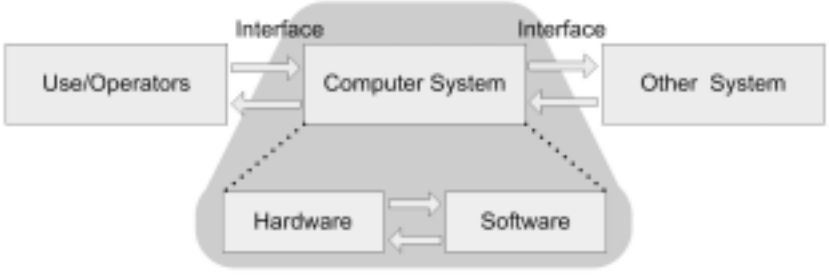
기존의 영국의 Yellow Book에서 제시하고 있는 위험원은 철도환경 전반에 대한 위험원이라 설계 및 개발에 적용하기엔 거리가 있음을 실제 적용 사례를 통해 알 수 있었으며, 보다 밀접한 시스템에 내재된 위험원을 도출하기 위해서는 적합한 방법을 찾아야 했다.

이번 연구에서는 국내 철도업계에서 개발하게 되는 시스템 및 설비의 명확한 위험원을 도출할 수 있는 가이드라인을 제시하여 시스템에 보다 명확한 위험원을 도출하고 이에 대한 대책을 수립할 수 있도록 하였다.

2.2 위험원 도출 범위 정의

위험원을 도출하기 위해서는 우선적으로 '위험원 도출범위'를 결정해야 한다. 위험원 도출범위란 다음과 같은 사항에 대해 결정하는 것이다.

1. 하나의 시스템에 국한된 위험원을 도출할 것인가?
2. 시스템과 관련된 다른 시스템과의 인터페이스나 인적오류까지 포함하는가?
3. 개발 시스템의 소프트웨어 위험원만 도출할 것이냐?



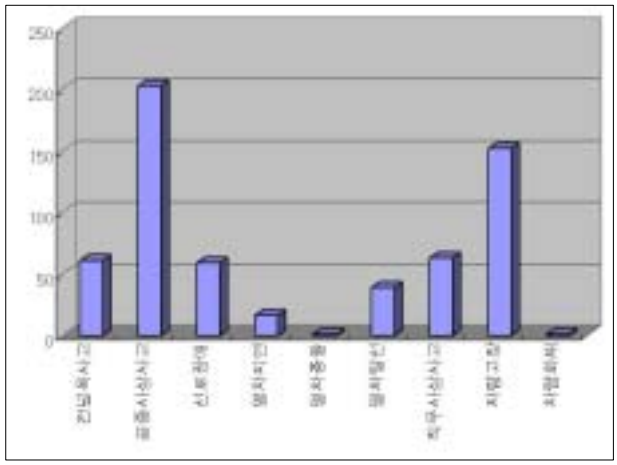
<그림 2 위험원 범위>

위험원도출을 위해 철도 전문가 및 엔지니어에게 범위 없이 위험원을 도출을 위한 회의 결과, 시스템을 보는 견해 차이로 의견 일치가 어려운 사례를 확인하였다.
위험원 도출을 위한 범위는 다음에 기술하게 되는 위험원 도출 각 단계마다 고려되어야 하는 중요한 사항이다. 즉, 범위는 개발하고자 하는 시스템의 발생 가능한 사고에 대한 책임범위라 할 수 있다.

3. 위험원 도출 단계

3.1 위험원 도출 1단계 (최상위 위험원 도출)

위험원 도출의 가장 우선적인 단계는 최상위 위험원을 선정하는 작업이다. 최상위 위험원이라 함은 개발되는 시스템에서 발생할 수 있는 최악의 사고 또는 최종적인 사고의 결과이다.
안전성 관련 국제규격에서 사고 피해 심각도에 대한 정의가 인명에 대한 피해정도와 재산상의 피해정도로 분류되어 있기에 최상위 위험원의 결정도 이와 마찬가지로 시스템이 인명에 대한 피해 정도와 재산상의 피해 정도를 고려하여 결정하여야 한다. 아래 그림은 다년간(1998~2003) 철도사고 발생을 분석한 결과로서 인명피해 사고 건수가 월등히 높게 나타남을 알 수 있다.
예를 들어 개발하고자 하는 시스템이 인적오류나 직·간접적인 인명피해(ex.일반인 선로 침범, 악의적 유발행위 등)와 관련이 깊다면 공중사상사고와 여객사상사고를 최상위 위험원으로 반드시 정의하여야 한다. 그러나 개발하려는 시스템 범위에 따라 공중사상사고와 여객사상사고는 제외될 수 있다.



<그림 3 철도사고 분석 데이터>

위험원 도출 1단계의 최상위 위험원 도출은 전문가 집단에 의해 시스템에서 발생 가능한 사고의 종류를 선별하여 정의하게 된다. 본 논문에서는 A 시스템에 대한 위험원 도출을 예로 설명하였다.

<표 1 최상위 위험원 도출>

시스템	A시스템	
위험원	**설명**	**비고**
열차의 충돌	■ 다른 철도차량과의 충돌 ■ 선로상 차량 이외의 존재와 충돌	
열차의 추돌	■ 같은 선로상의 철도차량과의 추돌	
열차의 탈선	■ 철도시스템의 이상으로 인한 열차탈선 ■ 기타 외적인 요인에 의한 열차 탈선(외란)	
화재	■ 화재로 인한 열차승객, 대기승객의 인명피해	
운행장애	■ 시스템 오류 및 장애로 인한 열차 운행 중단 및 열차 지연	

3.2 위험원 도출 2단계 (위험원 도출)

3.2.1 범주 정의 및 위험원 도출

최상위 위험원을 도출하고 난 후 최상위 위험원을 발생시킬 수 있는 위험원을 도출해야 한다. 위험원이란 용어는 매우 광범위하여 그 범위를 선정하기가 매우 모호함을 지니고 있다. 본 연구에서는 이러한 모호함으로 인한 오류를 줄이기 위해 시스템에 따른 범주를 선정하여 이에 적합한 위험원을 도출하였다.

범주는 다음과 같은 사항으로 구분할 수 있다.

- 시스템 기능
- 시스템 인터페이스
- 시스템 특성
- 관련 설비

범주는 위험원에 쉽게 접근할 수 있도록 사용자 또는 전문가 집단에 의해 정의될 수 있다.

위험원 도출 2단계의 적용 Sheet는 다음과 같이 정의하였으며, A시스템에 대한 예를 들었다.

<표 2 위험원 도출>

범주	No.	위험원	설명	원인	최상위 위험원	Lifecycle내 적용단계	비고
1.선로전환기	1.1	선로전환기 오방향 쇄정			열차 충돌 열차 추돌		
	1.2	선로전환기 정보 오류			열차 충돌 열차 추돌		
	1.3	선로전환기 쇄정 오류			열차 탈선		
2.신호기	2.1	신호기 현시 오류			열차 충돌 열차 추돌		
	2.2	신호기 정보 오류			열차 충돌 열차 추돌		
	2.3	신호기 오동작			열차 탈선		
3.열차검지	3.1	열차 궤도점유 검지오류			열차 충돌 열차 추돌		
	3.2	선로작업 시스템 오류			열차 충돌		
4.연동장치	4.1	연동장치 오동작			열차 충돌 열차 추돌		
	4.2	폐색장치 오류			열차 충돌 열차 추돌		
5.열차속도	5.1	허용속도 초과			열차 탈선		
6. ...	n	...					

3.2.2 모호성

위험원을 도출한다는 것은 매우 광범위한 작업이라고 할 수 있다. 개발하려는 시스템이 어떠한 잠재위험원을 내재하고 있는지 예상하기란 쉬운 일이 아니다. 위험원 도출을 위해 그 분야의 전문가 집단이 모여 위험원을 도출한다면 좀 더 명확한 위험원 도출이 이루어질 수 있으나, 최초로 개발되는 시스템에 대한 위험원 도출이나 비전문가 집단에 의한 위험원 도출 작업은 매우 어렵고 위험한 작업이 될

것이다.
모호성이란 위험원의 정답은 없다는 뜻이다. 정답은 없으나 도출된 위험원을 벗어나 발생되는 사고에 대해서는 책임을 져야 하기에 시스템에서 발생 가능한 모든 사고를 만족시키는 위험원을 도출해야 한다. 따라서 위험원 도출 단계에서는 모든 사고를 만족시키는 결과를 얻어야 하지만, 세분화 된 위험원을 무작정 도출한다면 안전성 활동 및 관리대상이 방대해져 안전성 확보가 불확실해질 수 있으며, 미쳐 고려되지 않은 잠재위험원이 존재할 수 있는 오류를 범할 수 있다.
그렇기 때문에 위험원 도출 단계에서는 상위레벨의 위험원을 도출하고 이 위험원을 발생시키는 세부적인 발생요인은 3단계에서 도출하도록 한다.

3.2.3 관련성
최상위 위험원과 그에 따른 위험원을 도출하게 되면 상호 관련성을 분석하여 시스템 개발 시 중점적으로 관리되어야 한다. 아래의 표는 A시스템의 위험원 결과를 예로 분석한 결과이다.

<표 3 최상위 위험원과 위험원의 관계 분석>

위험원 \ 최상위	충돌	추돌	탈선	화재	운행 장애
선로전환기 오방향 쇄정	☑	☑	☐	☐	☑
선로전환기 쇄정 오류	☐	☐	☑	☐	☑
신호기 현시 오류	☑	☑	☐	☐	☑
전원설비 과부하	☐	☐	☐	☑	☐
ATS장치 오류	☐	☑	☐	☐	☑
인터페이스 장애	☐	☐	☐	☐	☑
계	2	3	1	1	5

관련성을 분석한 결과는 PHA 및 FMEA등 위험원 분석으로 리스크 산출시 가중치를 고려할 수 있는 데이터로 적용되며, 이는 곧 전체 시스템의 SIL 결정에도 영향을 미치게 된다.

3.4 위험원 도출 3단계
위험원 도출 3단계는 도출된 위험원의 원인(요인)을 찾아내는 단계이다. 이미 도출된 하나의 위험원에는 여러 가지의 발생원인을 가지고 있다.
도출된 원인은 예비 위험원 분석(PHA)에서 명확한 대책을 수립할 수 있도록 가이드라인을 제시하게 된다. 위험원에 대한 원인까지 도출이 마무리 되면 최종적으로 아래와 같은 위험원도출문서를 작성하여 위험원에 대한 관리가 이루어지도록 해야 한다.

<표 3 위험원 도출 Sheet>

위험원	선로전환기 오방향 쇄정			
설명	선로전환기에 전달된 명령과 달리 오방향으로 쇄정된 경우 선로전환기의 방향과 제어부 현시가 다른 경우			
위험원 원인	No.	원인	빈도	결과(최상위위험원)
	1	선로전환기 계전기 고장		
	2	릴레이 고장		
	3	선로전환기 모터 전원 고장		
	4	크로싱의 분기부 장애로 인한 방향전환 불가		
	5	궤도회로 고장		
시스템 관련기능				
주석				

작성된 표는 위험원에 대한 상세 보고서로서 예비위험원 분석(PHA)의 기초자료가 되며, 발생되는 원인과 시스템 기능과의 연계성을 확인하여 설계문서에 이를 반영하여야 한다.

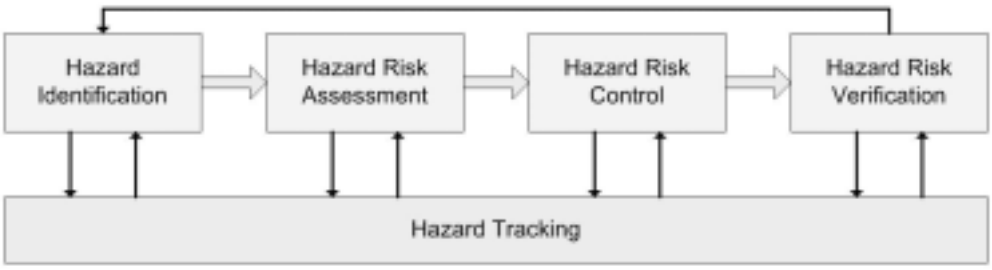
3.5 결과

위험원 도출 단계는 가장 우선적으로 수행되는 활동으로 예비위험원 분석(PHA) 및 기타 다양한 분석에 필요한 정보를 제공해야 한다. 이 단계에서 산출되는 문서는 다음과 같다.

■ 위험원 도출 Sheet

■ 위험원 도출 보고서

위험원은 설계 및 개발 단계에서 새롭게 발생되거나 예상되는 위험원에 대해 지속적으로 추가 및 수정이 이루어져야 하며, 정기적인 회의를 통해 관리되어야 한다.

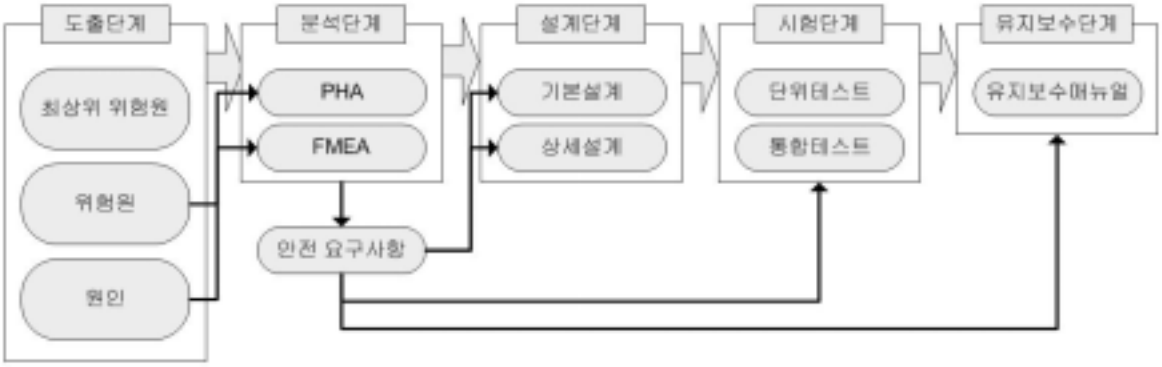


<그림 4 위험원 관리 프로세스>

4. 추적성

시스템의 설계 및 개발 생명주기동안 도출된 위험원의 관리는 지속적으로 이루어져야 한다. 관련된 산출문서는 이에 대한 증빙자료로서 추적성이 유지될 수 있어야 한다.

다음의 그림에서와 같이 위험원과 원인은 분석단계의 PHA와 FMEA에서 적용되어 요구사항을 수립하게 되며, 개발하고자 하는 시스템의 설계에 이를 반영하게 된다. 또한 각종 테스트에서도 이러한 요구사항에 대한 체크리스트가 작성되어 이를 증명하여야 한다.



<그림 5 단계별 추적성>

5. 결론

시스템의 안전성을 확보하기 위해 가장 우선적으로 위험원을 도출하는 작업이 이루어져야 하며, 또한 시스템에서 발생할 수 있는 가장 적합한 위험원을 도출하여야 한다. 그러나 안전성활동에서 가장 난해하게 여겨지는 사항은 도출된 위험원과 시스템의 기능이 어떠한 연계성을 가지고 지속적으로 관리되는가이다. 이러한 현상이 발생하는 이유는 도출된 위험원이 개발 Lifecycle동안 설계와 개발 그리고 테스트에서 배제되는 경우가 발생하기 때문인데, 배제되는 이유는 시스템과 관련성이 적은 위험원을 도출하였거나 위험원의 추가 및 수정이 이루어지지 않은 경우가 대부분이다.

본 연구에서는 시스템에 내재되어 있는 잠재적인 위험원을 도출하기 위한 단계에 대해 제시하였다. 총 3단계로 구분하여 각 단계마다 도출하여야 하는 위험원과 범위에 대해 기술함으로서 누락되는 위험원을 감소시킴과 동시에 시스템에 근접한 위험원을 도출할 수 있도록 하였다.

<표 4 위험원 도출 단계>

단계	단계명	설명
1	최상위 위험원	시스템에서 발생 가능한 최종 사고의 결과 정의
2	위험원	시스템의 기능 장애 및 오류 정의
3	원인	도출된 위험원을 발생시킬 수 있는 에러 및 오류 정의

또한 도출된 위험원이 개발Lifecycle동안 지속적으로 적용되고 관리될 수 있는 추적성에 대해 언급하였으나, 향후 계속되는 안전성활동 연구에서 보다 깊게 다루어져야 할 중요한 사항이기에 본 논문에서는 간략히 흐름에 대해서만 기술하였다. 추적성은 본 논문의 초반에 설명된 바와 같이 시스템과 관련된 사고가 발생하였을 경우 이에 대한 잠재적인 원인을 찾을 수 있도록 모든 단계가 연계되어 관리되어야 한다.

본 연구는 위험원 도출 후 THR을 통한 SIL 결정과 리스크 분석방법에 대해 진행할 예정이며, 초기 안전성활동에 대한 전반적인 체계를 구축할 수 있는 연구를 수행할 것이다.

현재 국내 및 해외에서도 위험원 도출에 대한 다양한 방법과 Sheet가 제시되고 있지만, 이에 따른 산출물을 살펴보면 차이점이 많다는 것을 알 수 있다. 국내에서는 앞으로도 안전성활동 및 각 단계별 활동의 체계화가 확립될 수 있도록 많은 노력과 깊은 연구가 이루어져야 할 것이다.

참고문헌

1. “철도사고 사례집”, 철도공사

2. Clifton A. Ericson, “Hazard Analysis Technipues for System Safety” WILEY.

3. Jeffrey W. Vincoli, CSP, “Basic Guide to System Safety”, WILEY.

4. TUV, “Technical Report-Establishment of a Hazard Log for Railway applications”, 2006.6.

5. Jorn Drewes, Jorg May, “Euro-Interlocking Generic Signalling Hazard List”, iVA