HAZOP을 이용한 고속철도시스템의 위험원 식별 및 안전성 분석에 관한 연구
On the Safety Analysis of High Speed Railway Systems using the Hazard and Operability (HAZOP) technique

정 호 전* · 이 재 천*
Ho-Jeon Jung* · Jae-Chon Lee*

Abstract

오늘날 기술의 발전으로 시스템들은 점차 대형화 복잡화 되어가고 있다. 이처럼 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 또한 대형 복합 시스템에서 발생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 있다. 따라서 체계적인 안전관리의 필요성이 점차 커지고 있다. 이에 대응하여 철도, 항공, 해양 등의 산업에서는 각 산업에 적합한 안전관리체계를 수립하려 노력하고 있으며, 표준 및 매뉴얼을 제정하여 보급에 앞장서고 있다. 예로써 가장 활발히 안전관리체계의 도입을 추구하고 있는 항공 분야에서는 국제민강항공기구와 미 연방항공청의 주도로 안전관리체계에 대한 가이드와 매뉴얼을 만들어 각국의 사정에 맞는 안전관리체계를 도입할 수 있는 바탕을 제공 하고 있다. 이처럼 점차 중요해지고 있는 안전관리체계내에서도 위험원 식별 및 분석활동은 그 중요성이 크다. 이를 통해 도출되는 위험원 및 위험원의 영향 및 원인이 시스템 개발 및 운용에서 수행하게 될 안전관리활동의 바탕이 되기 때문이다. 따라서 위험원 식별 및 분석활동에 적용하기 위한 여러 기법에 대한 연구가 활발히 이뤄지고 있다. 본 논문에서는 여러 가지 위험원 식별 기법 중 HAZOP을 이용하여 고속철도시스템의 위험원 식별 및 분석을 수행 했다. 또한 HAZOP의 수행 및 위험원 식별 활동의 프로세스 모델을 제시함으로써 실질적인 위험원 식별 활동의 수행에 도움이 될 것으로 기대한다.

* 아주대학교 시스템공학과

1. 서 론

현대의 안전중시 시스템들은 과거와 비교해서 급격한 운영성능의 발전을 가져 왔고, 동시에 기능적으로도 매우 복잡해지게 되었다. 시스템이 점차 대형화 복잡화됨으로써, 시스템에서 발생할 수 있는 사고나 고장의 위험 또한 증가하고 있다. 특히 이런 안전중시 시스템들은 사고나 고장이 인명 및 재산피해로 직결되기 때문에 체계적인 안전관리가 필요하다. 이에 따라 철도, 항공, 해양, 원자력 등의 산업분야에서는 안전관리체계에 대한 표준 및 매뉴얼을 제정하여 체계적인 안전관리 활동을 수행 할 수 있는 바탕을 제공하고 있다[1]-[4]. 각 산업분야에서 제시하고 있는 안전관리체계는 정책 결정 및 계획단계, 위험관리 단계, 안전보증 단계 등으로 구성되어 있다. 이 중 위험관리 단계는 다시 위험원 식별 및 분석, 위험 평가, 위험통제 등의 활동으로 구성되어 있다. 안전관리 체계의 각 활동 중 위험원 분석활동은 안전관리체계에서 위험을 관리하기 위한 시작점이라 할 수 있다. 위험원 분석 단계에서 적절한 위험원 식별 및 분석이 이뤄져야 이 후 이를 바탕으로 시스템의 위험관리를 수행 할 수 있다. 이처럼 시스템의 위험원을 식별하기 위한 기법에는 What if, FMEA(Failure Mode Effective Analysis), HAZOP(Hazard and Operability)등의 사용되고 있다. What if 기법은 질문지를 이용하여 시스템의 개발 및 운용에 참여하는 기관들의 협의로 통해 시스템내부에서 발생한 임의의 고장으로 인해 사고가 발생할 수 있는 위험원을 도출하는 방식이다. FMEA나 FMECA는 장치의 기능을 중심으로 고장에 대한 영향을 분석하고 이에 더하여 치명도 또한 고려하는 기법이다. 본 논문에서 적용하고자 하는 HAZOP기법의 경우 위험원을 도출하는 방식은 What if 방식이나, FMEA 및 FMECA처럼 시스템의 개발 및 운용관 관련된 사람들의 협의를 통해 위험원을 도출하는 방식이다. 하지만 HAZOP의 경우 고장으로부터 고장의 원인과 결과 및 영향을 모두 고려하여 위험원을 식별하며, 고장에 대응하기 위한 조치까지 식별 함으로써 이후 위험원 식별의 결과를 바탕으로 위험관리를 수행 할 수 있는 바탕을 제공한다.

또한 HAZOP은 안내어(Guideword)를 이용하여 위험원으로부터 발생 할 수 있는 고장의 경우의 수를 다양하게 만듦으로써 최대한 누락이 없는 위험원의 식별을 가능하게 한다. 따라서 대표적인 복합시스템 중 하나인 고속철도시스템에 대해서 HAZOP을 이용하여 위험원 식별을 수행하고자 한다. 이를 위해 먼전 각 산업분야에서 제시하고 있는 안전관리체계는 어떻게 이뤄져 있으며, 위험원 분석은 안전관리체계 내에서 어떠한 역할을 하는지에 대해 파악한다. 그리고 위험원 분석활동 및 입출력물 들을 전산지원도구를 이용해 프로세스 모델로 나타냈다. 이를 통해 위험원 분석을 어떻게 수행해야 하는지에 대해 정의하고 위험원 분석을 수행하는데 HAZOP기법을 적용하여 위험원 식별을 수행한다.

2. 본 론

2.1 안전관리체계 분석

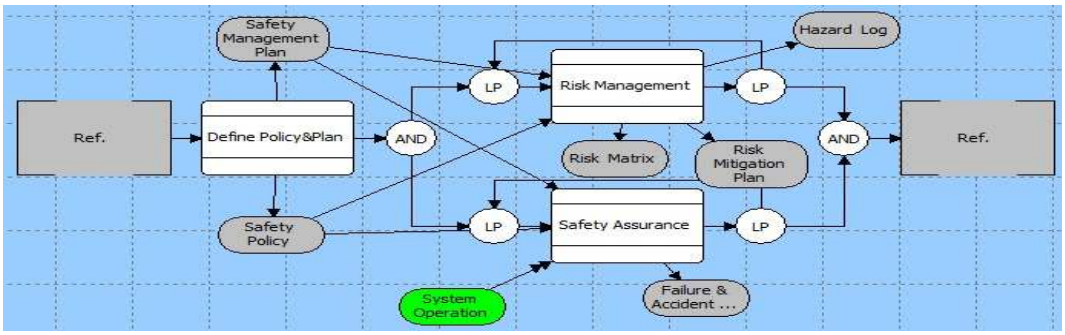
안전관리체계에 대해서 이해하기 위해선 먼저 안전관리가 무엇인지 정의해야 한다. 안전관리는 복잡하고 높은 안전성, 신뢰성이 요구 되어지는 시스템에 대해서 해당 국제규격에 따른 안전성 확보를 위해 수명주기에 따라 정의된 여러 활동들을 수행하는 것을 의미한다. 여러 가지 국제 및 산업 표준이나 지침에 따라 약간의 차이는 있지만 안전관리는 위험원식별, 리스크평가, 위험원 및 리스크 분석/평가 결과를 바탕으로 위험원 및 사고위험성 제거/감축 단계 등을 포함하고 있다.

안전관리체계는 앞서 말한 안전관리활동을 통해 안전이 달성 가능한 적절한 수준으로 유지되도록 하는 시스템을 말한다. 안전관리체계는 안전관리를 위한 조직구조, 책임사항, 절차, 단계 및 예방을 포함하는 안전관리 시스템을 말한다. 또한 안전관리체계에는 안전과 질서에 관한 통제, 사용 및 운영과 관련된 기타 부분들 또한 포함이 된다.

안전관리체계의 구성단계 및 활동을 살펴보면 <Table 1>과 같이 안전관리체계는 크게 세단계로 구성된다. 정책 결정 및 계획 단계, 위험관리 단계, 안전 보증단계 세 단계로 구성되며, 각 단계별 세부 활동을 정의하고 있다. 정책 결정 및 계획 단계에서는 안전관리를 수행하기 위한 정책의 결정, 안전관리를 수행할 조직의 구성 및 책임과 권한의 부여, 수행하게 될 안전관리 활동의 계획을 수립하는 활동을 포함한다. 위험관리 단계에서는 시스템에서 발생할 수 있는 위험의 근원인 위험원을 식별하고, 위험원으로부터 발생할 수 있는 위험을 분석하고 평가하며, 식별된 위험을 허용 가능한 수준에서 통제하는 위험통제 활동 등을 포함한다. 마지막으로 안전보증 단계에서는 시스템이 운영이 된 이후 성능을 모니터링 하며 데이터를 수집하고, 사고 및 고장에 대한 보고 및 조사활동, 안전관리를 수행하는 인력에 대한 안전관리교육 활동 등을 포함한다. <Figure 1>은 <Table 1>에서 제시하는 안전관리체계 단계 및 활동들을 바탕으로 해서 각 단계에서의 입출력 데이터 및 산출물을 정의하여 안전관리프로세스 모델을 생성한 것이다.

<Table 1> 안전관리체계의 구성단계 및 단계별 수행 활동

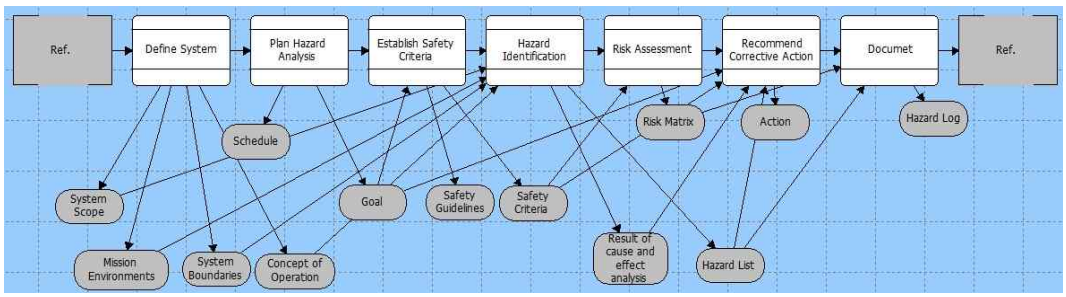
안전관리체계 구성단계	각 단계별 활동
정책 결정 및 계획	정책결정
	안전관리활동 수행조직 구성
	위험관리 및 안전보장 활동에 대한 계획 수립
위험 관리	시스템 정의
	위험원 식별
	위험 분석
	위험 통제
안전 보장	성능 모니터링
	사고 및 고장 보고 및 조사
	안전관리 교육



[Figure 1] 안전관리체계 프로세스 모델

이와 같이 체계적인 안전관리 활동을 위한 시스템인 안전관리체계는 안전성이 중시되는 여러 산업분야에서 표준 및 매뉴얼이 제정되어 안전관리체계를 도입하도록 촉진하고 있다. 항공분야에서는 국제민간항공기구(ICAO)의 주도로 각 국가의 항공당국은 안전관리체계 구조를 제시하도록 추천하고 있으며 이를 위해 ICAO Safety Management Manual을 개발하여 배포하고 있다[1]. 또한 미 연방항공청(FAA)는 ICAO에서 제시하는 안전관리체계와 미국의 자국 규정을 비교하여 부족한 부분을 보충한 Aviation Safety Management System을 구축하여 체계적인 안전관리 활동을 수행하고 있다[2]. 해양산업분야에서는 UN산하의 국제해사기구(International Maritime Organization)이 안전관리체계의 도입을 위해 노력하고 있으며, 이를 위해 모든 국제여객선, 유조선, 가스운반선 및 500톤 이상의 화물선에 대해서는 안전관리체계를 도입하여 안전관리를 수행하도록 권고하고 있다. 철도산업 분야에서는 캐나다 교통국(Transport Canada)에서 철도산업에 대한 안전관리체계를 구축했다[3]. 또한 안전관리체계의 구축을 위해 Railway Safety Management System Regulations을 제정하여 철도분야의 안전관리체계에 대한 요구사항을 제시하고 있다. 이처럼 안전이 중요시 되는 산업분야에서는 체계적인 안전관리를 위해 안전관리체계를 구축하고 표준 및 매뉴얼을 제정하여 실제적인 안전관리 활동의 수행에 도움이 되도록 하고 있다[5]-[6].

2.2 HAZOP을 이용한 위험원 분석



[Figure 2] 위험원 분석 프로세스 모델

시스템의 위험원은 인명의 사상, 시스템의 손상 및 손실 등을 유발시킬 수 있는 잠재적인 위험요소들을 의미한다. 즉 위험원은 사고를 발생시킬 수 있는 시스템 내부의 결함 또는 외부적인 요인들을 나타낸 것이다.[6]-[8] 따라서 안전관리체계에서는 위험관리 단계에서 위험원을 식별하고 이를 제거하거나 위험원으로 인한 위험을 허용수준 이하로 통제할 수 있는 조치를 수립하도록 하고 있다. <Figure 2>은 선행연구분석을 통해 도출한 위험원분석 단계에 대한 프로세스 모델이다. 위험원 분석의 각 단계와 각 단계별 주요 산출물들을 제시하고 있다. 프로세스 모델을 통해 위험원 분석의 세부 활동 및 산출물들을 제시함으로써 각 산업표준에 부합하는 안전관리 활동을 수행할 수 있도록 한다.

앞서 제시한 위험원 분석 프로세스 모델에서 Hazard Identification이 바로 위험원 분석 및 위험관리의 가장 기본이 되는 위험원 식별 단계이다. 위험원 식별 단계에서는 시스템의 위험을 초래하는 위험원들을 식별하는 단계로써 여러 가지 기법들의 적용이 이뤄지고 있다. 본 논문에서는 여러 가지 기법들중 HAZOP기법을 이용하여 위험원 식별을 수행한다.

HAZOP 기법은 위험원 도출을 위한 형식화된 시스템적 기법으로서 특정 파라미터가 안내어에 따라 벗어났을 경우에 대한 결과와 원인을 분석한다. 위험원 식별 단계에서 가장 중요한 것은 식별된 위험원에 대한 원인과 결과를 분석하는 것으로써 HAZOP은 이에 가장 부합하는 기법이라 할 수 있다.

HAZOP은 시스템의 위험원 도출을 위해 안내어(Guideword)라는 개념을 사용한다. More, No, Less 등과 같은 안내어들은 위험원을 도출하는 과정에서 시스템의 여러 상태와 결합되어 설계의도에서 벗어난 상태, 즉 이탈(Deviation)을 식별하여 위험원의 발생을 찾는다.

<Table 2> HAZOP 수행 단계 및 단계별 수행 활동

HAZOP 수행단계	각 단계별 수행 활동
Definition	수행범위 설정
	수행대상 설정
	조직 구성
Preparation	수행 계획 수립
	자료 수집
	일정 조절
Examination	시스템 정의
	설계의도 파악
	안내어를 이용한 일탈 식별
	원인과 결과 분석
	적절한 조치 도출
Documentation & Follow Up	조사결과 기록
	보고서 작성
	조치 수행

HAZOP의 수행 단계 및 활동은 <Table 2>와 같다. HAZOP는 크게 Definition, Preparation, Examination, Documentation & Follow-up 로 나눌 수 있다. Definition 단계에서는 HAZOP을 수행할 대상 및 범위를 설정하고 수행할 조직을 구성한다. Preparation 단계에서는 수행계획을 수립하고 일정을 조절하며, HAZOP을 수행하기 위해 필요한 Data를 수집한다. Examination단계에서는 실제 대상 시스템에 대한 HAZOP을 수행하며 식별된 위험원을 안내어를 이용해 나타내며 식별된 위험원으로 인해 발생가능한 위험의 원인과 결과를 분석하는 과정을 거친다. Documentation & Follow-up 단계에서는 Examination단계에서 수행한 HAZOP의 결과를 문서화하고 Examination단계에서 위험의 통제를 위해 수립한 적절한 조치들을 수행한다.

이와 같이 HAZOP은 식별한 위험원이 미칠 영향뿐만 아니라 위험원에 대한 원인을 함께 분석하여 발생 가능한 위험에 대한 조치까지 미리 수립함으로써 적절한 수준으로의 위험통제를 통해 위험관리가 가능하게 한다. 뿐만 아니라 안내어를 이용하여 위험원의 경우의 수를 모두 표현함으로써 미처 식별해내지 못할 수 도 있는 위험원을 최소화 하여 예측하지 못하는 위험의 발생을 최소화 할 수 있다. 따라서 HAZOP을 이용한 위험원 식별은 철도와 같은 사고나 고장이 큰 재산피해 및 인명 피해로 직결 될 수 있는 안전중씨 시스템에 적절한 기법이라 할 수 있다.

3. 구현

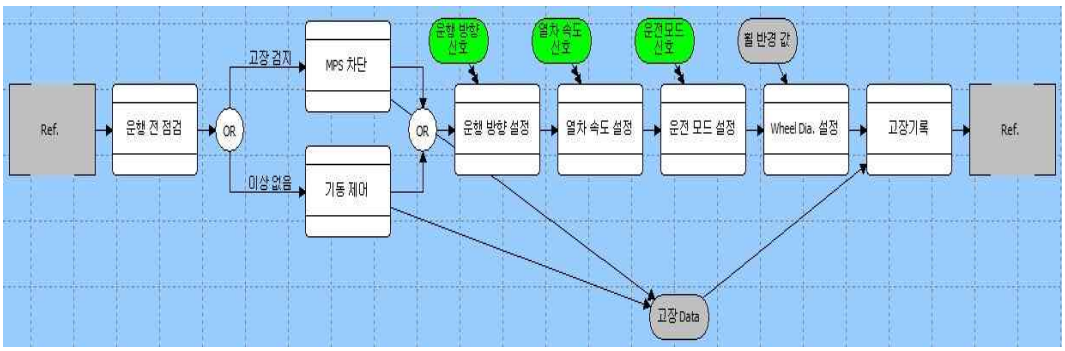
3.1 HAZOP을 이용한 고속철도 시스템의 위험원 식별

<Table 2>에서 제시되는 HAZOP 수행 단계 및 단계별 활동을 바탕으로 고속철도 시스템 중 주회로 차단기와 관련한 위험원 식별을 수행하였다. HAZOP수행은 다음과 같이 수행하였다.

(1) HAZOP 수행 대상 및 범위 설정 : 고속철도 시스템의 하부 컴포넌트 중 하나인 주회로 차단기에 대한 위험원 식별 수행
(2) HAZOP 수행 계획 수립 및 자료 수집 : 고속철도차량에 대한 기술문서들 중 하나인 차량제어 설명서를 바탕으로 해서 차량 제어와 관련된 본래의 설계의도를 파악할 수 있으므로, 차량 제어 설명서를 바탕으로 차량제어에 대한 정보 수집
(3) HAZOP 수행 : 철도차량의 하부 시스템중 하나인 MPS에 대하여 차량제어설명서를 바탕으로 하여 본래 설계의도에 따른 MPS운용의 모델을 구현. 이를 바탕으로 해서 본래의 설계의도에 벗어나는 이탈, 즉 위험원의 경우의 수를 수집. 수집한 위험원의 원인과 결과 분석 및 조치 수립
(4) 문서화 : 이전단계에서 수행한 결과를 바탕으로 하여 위험원 분석단계의 산출물 중 하나인 Hazard Log 작성

3.2 고속철도 시스템의 MPS에 대한 HAZOP 수행 결과

먼저 <Figure 3>과 같이 고속철도 시스템의 하부 시스템중 하나인 MPS의 정상상태에서의 운용에 대한 모델을 제시했다. 이는 HAZOP을 수행하기 위해 대상시스템의 본래의 설계의도를 알아내기 위함이다. 이 모델을 통해 정상상태일 때 MPS는 어떤 순서로 운용되어야 하는지 그때 필요한 신호나 입출력 데이터들을 정의했다. 이를 바탕으로 MPS운용 과정에서 발생할 수 있는 고장의 경우의 수를 수집했다. 경우의 수를 바탕으로 하여 MPS에 대한 위험원을 식별 했으며 위험원에 대한 원인과 결과의 분석 및 위험통제를 위한 조치들을 정의했다. 그 결과로써 위험원 분석단계의 최종 산출물 중 하나인 Hazad Log를 <Figure 4>와 같이 도출 할 수 있었다. Hazard Log에는 위험원 식별 대상 Parameter, Guideword, Deviation, 원인과 결과, 조치까지 모두 포함하여 작성하였다. 최종 작성된 Hazard Log는 차후에 시스템을 개발하면서 새로운 위험원의 식별이나 고장 발생 시에 계속하여 업데이트 되어야 하며, Hazard Log는 시스템 개발 전주기에 걸쳐 위험관리를 하는 가장 기초적인 자료가 된다.



[Figure 3] MPS의 정상적인 운용 모델

No.	Parameter	Guide Word	Deviation	Possible Causes	Consequencs	Safeguards	Comments	Actions required
1	Interface	No	신호 미인가로 인한 인터페이스 불가	열차 속도 신호 미인가	운행전 기동제어 불가			운행 전 네트워크 신호 검사
2	Interface	No	신호 미인가로 인한 인터페이스 불가	운행 방향 신호 미인가	운행전 기동제어 불가			운행 전 네트워크 신호 검사
3	Interface	No	신호 미인가로 인한 인터페이스 불가	운전모드 설정신호 미인가	운행전 기동제어 불가			운행 전 네트워크 신호 검사
4	Data	No	Data 없음	고장 Data 전송 불가	고장 Data수집 불가			네트워크 검사 및 각 차량의 랙에 Data 임시 저장
5	Data	Other	비정상적인 Data	고장 Data 전송 오류	고장 Data수집 불가			네트워크 검사 및 각 차량의 랙에 Data 임시 저장
6	Action	Other	비 정상적인 동작	변압기 과전류	과전류로 인한 주회로 차단기 고장			보호 회로 구축
7	Action	No	동작하지 않음	변압기 과열	과열로 인한 주회로 차단기 고장			보호 회로 구축
8	Action	No	동작하지 않음	오일 펌프 고장	오일펌프 미동작으로 인한 냉각 계통 전원 고장			오일 펌프 고장시 MCB차단 기능 추가

Figure 4 고속철도차량의 MPS에 대한 Hazard Log

4. 결론 및 요약

오늘날 점차 대형화 및 복잡화 되고 있는 시스템들은 개발 및 운용단계에서 많은 사고 및 고장의 위험을 내재하게 된다. 이를 극복하기 위해서는 각 산업분야에서 제시하고 있는 안전관리 체계의 도입이 중요하다. 또한 모든 안전관리 활동의 바탕이라 할 수 있는 위험원의 식별 및 분석은 시스템의 안전을 확보하는데 매우 중요하다. 이에 따라 많은 위험원 식별 기법이 연구되고 적용되고 있으나 본 논문에서 제시하고 있는 HAZOP은 대형화 및 복잡화 된 시스템에 가장 적합한 위험원 식별 기법이라 할 수 있다. 또한 위험원을 나타내는데 이용하는 Guideword 및 Parameter를 적용하고자 하는 대상 시스템에 맞게 적절하게 변경하여 사용한다면 수 많은 산업분야에 적용이 가능하다. 따라서 본 논문에서는 고속철도시스템의 안전관리체계에 따른 안전관리 활동 수행의 기본이 되는 위험원 식별단계에 HAZOP을 적용하여 수행하였다. 이를 통해 서브시스템 및 컴포넌트라도 최대한 누락이 없는 위험원의 식별이 가능했다. 또한 위험원의 원인과 결과 및 이후 조치를 미리 수립해 놓음으로써 실지 개발 및 운용단계에서 위험원으로 인한 사고 및 고장이 발생하더라 최소한의 비용 및 일정의 소모 내에서 대응이 가능 할 것이다. 추후에는 HAZOP이 운용과 환경 및 인적요소를 포함 할 수 있다는 특성을 바탕으로 하여, 철도시스템의 하위 시스템이나 컴포넌트 수준이 아닌 전체 철도시스템 수준에서 인터페이스 위험원 식별에 HAZOP을 응용함으로써 대형 복합체계의 완전한 위험원 식별이 가능하게 할 수 있는 연구가 필요 할 것이다.

5. 참 고 문 헌

[1] Safety Management Manual (SMM), International Civil Aviation Organization, 3rd ed., 2012.
[2] System Safety Handbook, Federal Aviation Administration, 2000.
[3] Introduction to SAFETY MANAGEMENT SYSTEMS, Transport Canada, 2001.
[4] Occupational Health and Safety Assessment Series, OHSAS 18001, 1999.
[5] 오세화, "철도시스템에서의 안전성 확보 방안에 관한 연구 (A Study on a Methodology for Safety Ensuring in Railway System)", 학위논문(공학석사), 서울산업대학교, 철도전기-신호공학과, 서울, 2008년 1월.
[6] 이창룡, 정호형, 오세화, 윤학선, 이기서, "철도신호시스템 분석을 위한 위험원 분석 techniques연구," 한국철도학회 춘계학술대회, (주최) 한국철도학회, 2011년, pp. 232-238.
[7] 한찬희, 이영수, 안진, 조우식, "안전성 확보를 위한 위험원 분석 기법간 상관관계에 대한 연구," 한국철도학회 추계학술대회, (주최) 한국철도학회, 2007년 11월, pp. 634-641.
[8] Netta Liin Rossing, Morten Lind, Niels Jensen, and Sten Bay Jorgensen, "A functional HAZOP methodology," Computers and Chemical Engineering, vol. 34, no. 2, pp. 244-253, Fab 2010.