예비위험원분석을 통한 ATP시스템의 위험원 도출에 관한 연구
A Study on the Hazard Identification for the ATP system Using the PHA

이강미* 신덕호** 이재호** 김용규**
Kang-Mi LEE*, Ducko SHIN**, Jaeho LEE**, Yong-Kyu KIM**

ABSTRACT

This study provides a method to identify hazards inherent in the system, relating to the definition of safety actions that verify that any hazard inherent in the system has been controlled to the acceptable level. The hazard can be categorized into two types: representative hazard, which is established at the conceptual level of system design, and system hazard, which is identified at the detailed level of system design according to functional, interface requirements and operational scenario. The system hazard causes the representative hazard, of which result shall be the event defined. The identification of the representative hazard, the beginning of the action to obtain safety, seriously affect the following safety actions and thus it must be objective and reliable. Therefore, to identify the representative hazard this study shall use special format and provide the method which is safe and confirmed by system experts.

---

1. 서론

자동열차방호장치(ATP, Automatic Train Protection)는 주행하는 열차가 선로정보 이외에 선행열차의 속도 및 거리정보를 지상으로부터 수신하여, 해당열차의 가감속 특성을 고려한 운행속도 패턴을 실시간으로 변경하여 선로 용량을 향상시키는 설비이다. 국내에 도입되는 ATP는 유럽철도관리시스템/유럽열차제어시스템(ERTMS/ETCS)의 Level 1을 만족하는 시스템으로, 기본적인 기능과 안전에 관련된 요구사항들은 ERTMS/ETCS의 기능요구사항 및 안전요구사항이 제공되어 도입시 이러한 요구사항을 적용하고 있다.[1][2] 본 논문은 KORAIL 차상신호(ATP)시스템 구축사업의 개념설계 단계에서 프로젝트의 범위를 대상으로 대표위험원의 도출을 양식지를 사용한 예비위험원 분석방법으로 수행하였다. 양식지를 사용한 예비위험원 분석방법은 체계적인 분석을 통해 기존 경험에 의존하던 대표위험원의 도출에서 발생할 수 있는 위험원 누락을 방지한다.[3] 위험원의 누락이 시스템 상세설계 이후 또는 시운전과정에서 발생하면, 많은 설계변경비용이 수반되며, 만약, 시스템의 인수(Demonstration)수명주기 이후까지 주요 위험원이 발생되지 않으면 해당 위험원으로 인한 사고의 발생가능성이 시스템에 지속적으로 남아있게 된다. 따라서 철도신호시스템관련 안전규격인 IEC 62278에서는 개념설계 이전에 시스템의 범위내의 대표위험원을 형식화된 위험

* 책임저자, 회원, 한국철도기술연구원, 전기신호연구본부
E-mail : kmlee246@krri.re.kr
** 공동저자, 회원, 한국철도기술연구원, 전기신호연구본부

원도출 방식을 사용하여 수행하도록 권고하고 있으며, 이러한 형식화된 방법 중 양식지를 사용한 예비위험원분석방법을 본 논문에서 제시하여, ATP프로젝트 전반에 적용할 대표위험원을 도출하였다.

철도시스템관련 위험원은 영국의 Network Rail의 안전지침서 Yellow Book의 철도 분야 위험원목록(총 284개, 인접한 시설 및 인명관련 64개, 철도승객관련 101개, 철도종사원관련 119개) 240여개의 위험원 리스트(Hazard Portfolio)를 제공하고 있으며, Yellow Book Issue 3에서는 위험원의 도출을 위한 체크리스트(Hazard Checklist)를 제공하고 있으며, 영국의 HSE(Health and Safety Executive)에서는 철도관련 위험원을 Hazard Profile로 작성하여 1년에 한번식 위험원으로 인한 손실을 금액으로 환산하여 보고하고 있다. 위험원에 대한 금액의 환산은 영국이 사용하고 있는 경제적 논리에 의한 안전확보 이론인 ALARP(As Low As Reasonably Practicable)을 위한 배려이며, 국내에서도 철도사고에 대한 비용의 계산을 연구 중에 있다.

2. 철도시스템 안전성 활동

철도신호시스템에서 안전성 활동이란 대상시스템으로 인해 발생할 수 있는 위험원을 도출하고, 도출된 위험원의 크기와 빈도에 해당하는 리스크(Risk)를 허용할 수 있는 수준이하로 완화시키기 위한 설계변경을 통해 시스템의 안전성을 확보하기 위한 것이다. 따라서 안전성 활동의 단계는 시스템 예비위험원 분석(PHA, Preliminary Hazard Analysis), 위험원 도출 및 분석(HIA, Hazard Identification and Analysis), 사고시나리오예측, 위험측고장정의, 안전대책 수립을 통해 체계적인 리스크의 평가 및 관리를 수행한다. 이러한 안전성활동의 수명주기에서 예비위험원분석은 대표위험원의 도출을 위해 수행된다.

위험원의 도출과 분석에는 각각 여러 가지 기법들이 사용된다.[4] 시스템 내부의 위험원을 도출하기 위한 방법에는 What if, FMEA(Failure Mode Effective Analysis), HAZOP(Hazard and Operability) Study등의 여러 기법이 사용된다. What if 방식은 개발엔지니어, 안전성관리자, 운영기관 종사자가 협의를 거쳐 시스템 내부에서 발생한 임의 고장으로 인해 사고가 발생할 수 있는 위험원을 도출해 보는 접근방식으로써, 기존의 철도신호시스템 개발과정에서 가장 널리 사용되는 방법이다. 장치의 기능을 중심으로 고장에 대한 영향을 분석하는 FMEA 또는 위험원의 치명도를 고려한 FMECA(Failure Mode Effective and Criticality Analysis)는 대상 시스템 관련자의 토론에 의해 위험원을 도출하는 방식이며, HAZOP Study도 거의 같은 방식이다. 이러한 방법들은 수행이 용이하다는 장점이 있으나, 개발엔지니어, 안전성관리자, 운영기관 종사자등의 경험에 종속되어, 위험원 누락 확률이 높아지고, 새로운 시스템으로의 적용이 어렵다는 단점을 가지고 있다. 또한 규격이나 정규화된 문서를 근거로 하지 않으므로, 독립된 제 3기관에 의한 안전 확인을 받을 수 없다. 따라서 위험원 누락 확률을 줄여 시스템의 안전성을 보다 더 확보하기 위해 두가지 작업을 통한 위험원 도출 방안을 다음과 같이 제시한다. 먼저 1차 위험원 도출을 위하여 영국의 철도관련 위험원 리스트를 대상으로 해당 위험원의 안전대책 적용전 리스크를 평가하고, 리스크를 완화하기 위한 안전대책의 수립을 수행하였으며, 각각의 위험원별 안전대책이 프로젝트의 범위를 벗어나는 경우 해당 위험원의 안전확보는 프로젝트의 범위에서는 불가능한 것으로 판단하여 제거하였다. 이렇게 프로젝트 관련 1차 위험원이 도출되면, 2차 위험원 도출을 위해 기존에 법, 규칙, 시행령 및 운영규정 등을 통해 수행되고 있는 안전대책을 위험원별 안전대책과 비교하여, 기존의 운영규정에 포함되는 안전대책을 선별하여 해당 위험원을

삭제하였다. 이와 같이 두 가지 작업을 통해 프로젝트 수명주기의 개념설계 이후 과정인, 상세설계 및 인터페이스설계 그리고 운영시나리오 설계에 고려해야할 시스템단위 대표위험원의 선정이 예비위험원을 도출하였다.

2.1 예비위험원분석(PHA) 양식지

예비위험원분석은 대상시스템의 기능적인 측면을 대상으로 대표적 사고 및 위험원을 정의하여, 정의된 위험원으로 인한 사고의 리스크를 평가하고, 안전대책적용후의 리스크를 평가하여 안전대책으로 인해 리스크를 얼마나 완화시킬수 있는지를 검토하는 단계이다. 예비위험원 분석단계에서는 위에서 기술한 바와 같이 시스템의 개략적인 기능요구사항만을 토대로 하며, 하부시스템의 상세설계단계의 정보를 요구하지 않는다. 따라서 제시되는 안전대책들도 설비보안, 안전대책수립, 교육체계수립 등의 개념적인 대책들만을 제시한다. 따라서 예비위험원분석은 프로젝트의 생성초기에 수행되어야하며, 기본적인 사용자 요구사항(UR, User Requirement)을 토대로 수행하여 하부시스템 기능요구사항 및 안전요구사항 작성시에 참조로 사용해야한다. 예비위험원분석지의 근거는 국제규격에 제시되어 있지 않다. ATP시스템의 예비위험원분석지는 다음과 같이 기존에 수행된 프로젝트에 사용된 양식과의 일관성을 고려하여 작성한다.

- KTX TCS 예비위험원분석(K690-0-E4220-GL+D-001)
- 철도청 사령실통합 CTC 소프트웨어의 예비위험원분석
- ALCATEL ATCS시스템 Hazard Log

표1은 ATP시스템 예비위험원 도출에 사용된 분석양식지이다.

표1. ATP시스템 예비위험원 분석양식지

시스템 명 :									
시스템번호		작업기간		일		작성날짜			
분석단계		최초 : □				수정 : □	부가 : □		
위험원 번호	위험원 내용	대상	사고심각도	발생빈도	위험도 크기	대책안 : D : 설계변경, E : 안전대책, S : 안전소자, W: 경고체제, P : 절차/교육	대책안 실시 후		
							사고 심각도	발생 빈도	위험도 크기

2.2 시스템범위를 고려한 1차 위험원도출

철도관련 모든 위험원은 안전대책을 통해 리스크를 허용수준 이하로 완화시키는 것이 가능하다. 하지만, 위험원별 안전대책이 프로젝트의 범위를 벗어나는 경우에는 해당 안전대책의 적용이 불가능하므로, 이러한 안전대책만을 포함한 위험원은 표2의 예와 같이 삭제되어야 한다. 이때 예비위험원 분석지에 사용된 위험원 대상의 약어 표기는 다음과 같다.

- N : 철도주변 민간인(Neighbors)
- P : 승객(Passengers)
- W : 철도종사원(Workers)

그리고 대책안은 다음과 같은 체계로 분류한다.

- D (설계변경) : 별도의 추가된 기능과 관련한 부품이 요구되지 않는 설계의 변경
- E (안전대책/교육) : 안전과 관련된 위험의 발생을 미연에 대처하기 위한 방안
- S (안전소자) : 별도의 추가된 기능을 지니는 부품을 필요로 하는 설계의 변경
- W (경고체제) : 인적 위험요소를 감소시키기 위한 주의 환기 방안
- P (절차) : 사고의 후속 처리 절차

표2과 같이 위험원의 안전대책이 시스템범위를 벗어나는 경우는 해당유무를 표시하며, 시스템 범위에 해당되는 경우 시스템개발 수명주기에서 해당 수명주기를 표시한다.

표2. 안전대책과 시스템범위를 고려한 1차 위험원 도출의 예

시스템 명 : 철도공사 차상신호(ATP)시스템 구축사업의 RAMS 활동 및 평가용역								
시스템번호		작업기간		일	작성날짜			
분석단계		최초 : □			수정 : □		부가 : □	
위험원 번호	위험원 내용	대상	사고심각도	발생빈도	위험도크기	대책안 : D : 설계변경, E : 안전대책, S : 안전소자, W: 경고체제, P : 절차/교육	해당유무	적용단계
HN048	두 대의 열차가 동시에 하나의 폐색에 존재	N				S : 열차가 동시에 한 구간에 존재해도 각각에 대하여 추적이 가능하도록 신호설비 구축 W :건널목경보 후 차량통과시 연이어 열차가 진입할 수 있음에 대한 경고표지 설치	O	선행열차와 동일한 폐색에 열차가 들어가지 않도록 방호하는 기능을 설계에 반영
HN052	신호가 아무것도 표시하지 못함	N				S : 전원공급 차단시 시스템이 안전측으로 동작하도록 설계 W :무신호시 위험원에 대한 민간에 대한 경고표지 설치	O	ATP시스템의 전원공급 차단으로 인해 사고가 발생하지 않도록 설계에 반영
HN053	운전자 오류-위험측으로 통과	N				E : 운전자오류에 의한 정지신호통과 방지를 위한 교육 S : 운전자의 정지신호통과시 자동제동 체결	O	ATP시스템의 운전자의 신호무시로 인해 사고가 발생하지 않도록 설계에 반영
HN017	통과열차로부터 사람을 보호하는 건널목의 고장	N				W :건널목 고장을 주변 민간인에게 공지 P : 인명사고 발생에 대한 처리절차 수립	X	ATP시스템 범위를 벗어남
HP089	전력공급 중단	P				S : 전력공급이 중단되어도 시스템은 안전측을 유지하도록 설계 W :전력공급 중단으로 인한 승객동요를 방지하기 위한 안내방송 실시 P : 전력 재공급을 위한 절차 수립	O	ATP시스템 설치 및 시운전과 운영시에 전력공급 중단이 발생 하더라도 안전측으로 유지하도록 설계에 반영
HP057	신호가 아무것도 표시하지 못함	N				E : 신호 미현시에 의한 정차시 대처방안 수립 S : 신호 미현시시 열차는 안전측으로 정차하도록 설계 P : 인명사고(열차의 충추돌)에 대한 처리절차 수립	O	ATP시스템의 전원공급 차단으로 인해 사고가 발생하지 않도록 설계에 반영
HP020	열차정지 중 승객들에 의한 출입문(Slam doors) 개방	P				E : 비상탈출시 승객에 의한 출입문 개방과 탈출절차 홍보 W : 정상상태에서 고의적인 출입문 개방에 대한 법적책임 표지 설치 W : 정지중인 열차에서 출입문 개방시 추락위험 표지 설치	X	ATP시스템 범위를 벗어남
HP024	출입문(Sliding doors)을 닫을 때 승객이나 승객의 의복이 낌	P				W : 미닫이 문 개폐시 안내방송 및 경고문구 부착 P : 인명사고(출입문 관련)에 대한 처리절차 수립	X	ATP시스템 범위를 벗어남

그리고 1차 도출된 위험원은 안전대책을 제시하도, 표 3,4,5,6을 기준으로 리스크 완화를 계산하여, 표 7과 같이 보여진다.

표 3. 사고 심각도의 등급할당

위험성	등급	설 명	정량적 기준	해당사고
치명적인 위험 (Catastrophic)	A	인명의 사망, 시스템의 손실 또는 심각한 환경상의 피해를 유발하는 위험	3인 이상 사망	열차충돌
중대한 위험 (Critical)	B	심각한 인명의 상해, 직업상의 질병 및 중요한 시스템 또는 환경상의 피해를 초래하는 위험	1인 사망≤x<3인 사망	비상제동 인명사상
중요하지않은 위험 (Marginal)	C	최소한의 상해, 직업상의 질병 및 최소한 시스템 또는 환경상의 피해를 초래하는 위험	1인 중상≤x<1인 사망	-
사소한 위험 (Insignificant)	D	최소한의 상해, 직업상의 질병보다 작고, 최소한의 시스템 및 환경상의 피해보다 작은 영향을 초래하는 위험	1인 이하 중상	상용제동
신뢰성관련 (Reliability Related)	R	인명이나 환경상에 피해를 발생하지 않으나 경제적 손실을 동반하는 위험	-	운행지연

표 4. 사고발생 빈도의 등급할당

발생 빈도	등급	설 명	정량적 기준 (위험측고정률, 단위시간당 발생확률)
빈번한 발생 (Frequent)	1	수명주기 동안 빈번하게 발생할 가능성이 있음	10-3 이상
가능성 있는 발생 (Probable)	2	수명주기 동안 여러 번 발생할 가능성이 있음	10-4 < to ≤ 10-3
종종 발생 가능(Occasional)	3	수명주기 동안 가끔 발생할 가능성이 있음	10-6 < to ≤ 10-4
발생가능성이 미약함(Remote)	4	수명주기 동안 한두 차례 발생할 가능성이 있음	10-8 < to ≤ 10-6
발생 가능성이 거의없음 (Improbable)	5	수명주기 동안 발생 가능성은 있지만, 발생하지 않음	10-9 < to ≤ 10-8
발생 가능성이 전혀없음(Incredible)	6	발생가능성도희박하며, 절대 발생하지 않음	≤ 10-9 이하

표 5. 리스크의 할당

리스크의 등급	치명적인 위험 (Catastrophic)	중대한 위험 (Critical)	경미한 위험 (Marginal)	사소한 위험 (Insignificant)
빈번한 발생 (Frequent)	Intolerable	Intolerable	Intolerable	Undesirable
가능성 있는 발생 (Probable)	Intolerable	Intolerable	Undesirable	Tolerable
종종 발생 가능(Occasional)	Intolerable	Undesirable	Undesirable	Tolerable
발생가능성이 미약함(Remote)	Undesirable	Undesirable	Tolerable	Negligible
발생가능성이 거의없음 (Improbable)	Tolerable	Tolerable	Negligible	Negligible
발생가능성이 전혀없음 (Incredible)	Negligible	Negligible	Negligible	Negligible

표 6. 리스크의 허용기준

리스크 클래스	설 명	각 분류에 적용되는 조치 활동
I	허용 불가능한 위험(Intolerable)	반드시 제거되어야 함
II	부적절한 위험(Undesirable)	리스크 감소가 현실적으로 불가능하고 운영기관이 적절하게 동의를 할 때는 이를 수용해야 함
III	허용 가능한 위험(Tolerable)	적절한 통제 및 운영기관의 동의로 수용할 수 있음
IV	무시 가능한 위험(Negligible)	운영기관의 동의에 상관없이 수용할 수 있음

표7. 위험원별 안전대책수립 및 리스크평가의 예

시스템 명 : 철도공사 차상신호(ATP)시스템 구축사업의 RAMS 활동 및 평가용역									
시스템 번호		작업 기간	일		작성날짜				
분석단계		최초 : □			수정 : □	부가 : □			
위험원 번호	위험원 내용	대상	사고심각도	발생빈도	위험도 크기	대책안 : D : 설계변경, E : 안전대책, S : 안전소자, W: 경고체제, P : 절차/교육	대책안 실시 후		
							사고심각도	발생빈도	위험도 크기
HN048	두 대의 열차가 동시에 하나의 폐색에 존재	N	B	3	Ⅱ	S : 열차가 동시에 한 구간에 존재해도 각각에 대하여 추적이 가능하도록 신호설비 구축(철도시설물 보완) W : 건널목경보 후 차량통과시 연이어 열차가 진입할 수 있음에 대한 경고표지 설치(철도시설물 보완)	B	5	Ⅲ
HN052	신호가 아무것도 표시하지 못함	N	B	2	Ⅰ	S : 전원공급 차단시 시스템이 안전측으로 동작하도록 설계(철도시설물 보완) W : 무신호시 위험원에 대한 민간에 대한 경고표지 설치(철도시설물 보완)	B	5	Ⅲ
HN053	운전자 오류-위험측으로 통과	N	B	3	Ⅱ	E : 운전자오류에 의한 정지신호통과 방지를 위한 교육(철도운전규정) S : 운전자의 정지신호통과시 자동제동 체결(철도시설물 보완)	C	4	Ⅲ
HP089	전력공급 중단	P	C	1	Ⅰ	S : 전력공급이 중단되어도 시스템은 안전측을 유지하도록 설계(철도시설물 보완) W : 전력공급 중단으로 인한 승객동요를 방지하기 위한 안내방송 실시(철도운영규정) P : 전력 재공급을 위한 절차 수립(철도유지보수규정)	C	4	Ⅲ
HP057	신호가 아무것도 표시하지 못함	P	A	2	Ⅰ	E : 신호 미현시에 의한 정차시 대처방안 수립(철도운전규정) S : 신호 미현시시 열차는 안전측으로 정차하도록 설계(철도시설물 보완) P : 인명사고(열차의 충추돌)에 대한 처리절차 수립(철도안전규정)	A	5	Ⅲ

2.3 시스템범위를 고려한 2차 위험원도출

1차 위험원 도출을 통해 정리된 위험원의 목록은 ATP시스템에 대한 대표위험원이라 할 수 있다. 따라서 2차 위험원 도출과정에서는 ATP시스템관련 운영규정에 포함되는 안전대책의 위험원을 삭제한다. 2차 위험원의 정리를 모든 철도시스템의 운영이 규정을 준수하여 수행된다는 가정에서 출발하며, 테러를 제외한 규정위반에서 발생되는 위험원에 대한 고려는 대표위험원의 경계를 과다해석하게 되어, 이후의 활동인 시스템 위험원도출 및 분석에서의 분석대상의 발산을 초래한다.

만약 1차 위험원도출 과정인 시스템범위를 고려한 분류와 2차 위험원도출 과정인 해당 운영규정을 고려한 분류의 순서를 바꾸는 경우 모든 철도시스템관련 운영규정을 기준으로 해야 하므로, 본 논문에서는 ATP시스템의 범위를 고려하여 1차 위험원도출을 실시하고, 2차 위험원도출은 열차제어시스템 및 열차운행과 관련된 운영 및 운전규정을 기준으로 하였다.

열차제어시스템 운영규정 및 열차운전규정을 기준으로 2차 위험원도출을 실시한 결과의 예는 표4와 같다.

표4. 안전대책과 관련규정을 고려한 위험원제거의 예

시스템 명 : 철도공사 차상신호(ATP)시스템 구축사업의 RAMS 활동 및 평가용역								
시스템 번호		작업 기간		일	작성날짜			
분석단계		최초 : □			수정 : □	부가 : □		
위험원 번호	위험원 내용	대상	사고심각도	발생빈도	위험도크기	대책안 : D : 설계변경, E : 안전대책, S : 안전소자, W: 경고체제, P : 절차/교육	규정확보유무	적용근거
HN048	두 대의 열차가 동시에 하나의 폐색에 존재	N	B	3	Ⅱ	S : 열차가 동시에 한 구간에 존재해도 각각에 대하여 추적이 가능하도록 신호설비 구축(철도시설물 보완) W : 건널목경보 후 차량통과시 연이어 열차가 진입할 수 있음에 대한 경고표지 설치(철도시설물 보완)	X	선행열차와 동일한 폐색에 열차가 들어가지 않도록 방호하는 기능을 설계에 반영
HN052	신호가 아무것도 표시하지 못함	N	B	2	Ⅰ	S : 전원공급 차단시 시스템이 안전측으로 동작하도록 설계(철도시설물 보완) W : 무신호시 위험원에 대한 민간에 대한 경고표지 설치(철도시설물 보완)	X	ATP시스템의 전원공급 차단으로 인해 사고가 발생하지 않도록 설계에 반영
HN053	운전자오류-위험측으로 통과	N	B	3	Ⅱ	E : 운전자오류에 의한 정지신호통과 방지를 위한 교육(철도운전규정) S : 운전자의 정지신호통과시 자동제동 체결(철도시설물 보완)	X	ATP시스템의 운전자의 신호무시로 인해 사고가 발생하지 않도록 설계에 반영
HP089	전력공급 중단	P	C	1	Ⅰ	S : 전력공급이 중단되어도 시스템은 안전측을 유지하도록 설계(철도시설물 보완) W : 전력공급 중단으로 인한 승객동요를 방지하기 위한 안내방송 실시(철도운영규정) P : 전력 재공급을 위한 절차 수립(철도유지보수규정)	X	ATP시스템 설치 및 시운전과 운영시에 전력공급 중단이 발생 하더라도 안전측으로 유지하도록 설계에 반영
HP057	신호가 아무것도 표시하지 못함	P	A	2	Ⅰ	E : 신호 미현시에 의한 정차시 대처방안 수립(철도운전규정) S : 신호 미현시시 열차는 안전측으로 정차하도록 설계(철도시설물 보완) P : 인명사고(열차의 충추돌)에 대한 처리절차 수립(철도안전규정)	X	ATP시스템의 전원공급 차단으로 인해 사고가 발생하지 않도록 설계에 반영

2.3 ATP시스템의 위험원

1차, 2차 작업을 통해 프로젝트 수명주기의 개념설계 이후 과정인, 상세설계 및 인터페이스설계 그리고 운영시나리오 설계에 고려해야할 시스템단위 대표위험원이 다음과 같이 선정되었다. 단, 해당 위험원의 안전대책이 모두 안전규정에 제시되지 않은 위험원에 대해서는 대표위험원으로 선정하여 규정에 제시되지 않은 안전대책이 적용되도록 관리해야 한다.

■ATP-TH001 : 두 대의 열차가 동시에 하나의 폐색에 존재

■ATP-TH002 : 신호가 아무것도 표시하지 못함

■ATP-TH003 : 운전자 오류-위험측으로 통과

■ATP-TH004 : 전력공급 중단

■ATP-TH005 : 신호가 아무것도 표시하지 못함

3. 결 론

본 논문에서는 안전성활동을 위해 기준이 되는 시스템의 위험원 중 개발수명주기의 초기단계에 수립하여 관리해야할 대표위험원을 도출하기 위한 방법으로 양식지를 사용한 예비위험원분석방식을 제안하였으며, 위험원의 도출을 위한 구체적인 방법으로 시스템 범위를 고려한 위험원 정리와, 관련 규정을 근거로 한 위험원 정리의 2단계 가정을 제안하였다. 이러한 시스템 대표위험원은 시스템기본설계와 상세설계과정에서 각각의 시스템레벨 위험원의 연관관계에 따라 인과관계가 성립되어 통합 또는 분리될 수 있으며, 이는 영국의 안전성활동 문서화 지침 Yellow Book에서 표현한 "Hazard Log is Alive"와 같이 수명주기 전반에 대하여 지속적으로 갱신과 검토가 진행되어야 한다.

[참고문헌]

1. 철도청(2003), “차상신호(ATP)시스템 도입을 위한 제안요청서”
2. UIC((2000), "ETRMS/ETCS-Class1 System Requirements Specification"
3. “HAZOP Study를 사용한 ATSRX의 위험원도출 및 리스크완화에 관한 연구” 한국철도학회논문지, 신덕호 외 3인
4. IEC 60812(1985), "Failure Mode Effect analysis"
5. 김영태 저, 2003 “신호제어시스템”