한국철도학회논문집
제9권 제3호 2006년 ▌pp. 264-270

열차제어시스템의 안전계획 수립에 관한 연구

A Study on the Safety Plan for a Train Control System

김종기† · 신덕호* · 이기서**
Jong-Ki Kim · Ducko Shin · Key-Seo Lee

Abstract

In this paper we present a safety plan to be applied to the development of the TCS(Train Control System). The safety plan that can be applied to the life cycle of a system, from the conceptual design to the dismantlement, shows the whole process of the paper work in detail through the establishment of a goal, analysis and assessment, the verification. In this paper we study about the making a plan, the preliminary hazard analysis, the hazard identification and analysis to guarantee the safety of the TCS. The process for the verification of the system safety is divided into several steps based on the target system and the approaching method. The guarantee of the system safety and the improvement of the system reliability is followed by the recommendation of the international standards.

Keywords : TCS(Train Control System), RAMS(Reliability, Availability, Maintainability and Safety), FMEA(Failure Mode Effect Analysis), HAZOP(Hazard and Operability), FTA(Fault Tree Analysis), ETA(Event Tree Analysis), Risk Assessment, Hazard Log, SIL(Safety Integrity Level)

1. 서 론

본 논문은 열차제어시스템 개발과정에 적용하기 위한 안전계획을 수립한다. 시스템의 개념설계부터 폐기까지의 수명주기에 적용하는 안전계획은 신뢰성, 가용성, 유지보수성, 안전성(RAMS)목표설정부터 예측 및 평가를 통한 입증까지의 업무를 구체적으로 제시한다.

한 예로 3-4인승으로 제작된 차량을 무선통신기반으로 제어하는 소형궤도차량 운영제어 시스템의 경우[1], 역에서 승차한 승객을 목적지까지 이동시키는 과정에서 중간의 역을 무정차로 통과하는 특성을 갖는 시스템이다. 따라서 공공의 수송을 목적으로 하는 응용분야의 특성에 의해 서비스 중지 시간의 증가는 많은 사회적 손실을 초래하므로 시스템의 신뢰도와 유지보수도를 바탕으로 가용 서비스 시간인 가용도를 관리하여야 하며, 운전시격이 짧은 열차의 속도프로파일을 생성하여 가속 및 감속을 제어하는 열차제어시스템의 위험측 고장은 인명과 재산의 손실을 발생한다.

열차제어시스템이 해당되는 기술분야인 철도신호와 관련해서는 국제규격 IEC(International Engineering Consortium)에서 기준을 제시하며, 열차제어시스템의 핵심인 전기전자 제어기와 관련해서는 미국방부규격 MIL(Military Specifications and Standards)에서 시스템 RAMS의 목표설정, 예측, 평가를 포함하는 관리방안을 제시하고 있다[2,3]. 또한, 열차제어시스템의 대부분을 차지하는 전자화된 안전관련 제어기에 대하여는 원자력, 항공, 국방, 플랜트 등에 널리 사용되고 있는 국제규격이 제시되고 있다[4].

신뢰성, 가용성, 유지보수성은 정량적인 분야로써, 목표수립 이후에는 수명주기에 따라 시스템의 고장률과 유지보수도를 예측 및 평가한다.

안전성활동은 시스템으로 인한 위험원을 도출하여 허용할 수 있는 수준의 리스크레벨을 설정한 후 위험원으로 인한 리스크가 모두 허용할 수 있는 수준으로 제어되었음을 입증하는 활동이다[5].

따라서, 본 논문에서는 국제규격을 근거로 신뢰성, 가용성, 유지보수성의 목표수립 및 관리방안을 구체적으로 연구하였으며, 안전성에 대해서는 현재 국내에서 수행되었거나

† 책임저자 : 정회원, 한국철도기술연구원, 전기신호연구본부
E-mail : jkkim@krri.re.kr
TEL : (031)460-5430 FAX : (031)460-5449
* 정회원, 한국철도기술연구원, 전기신호연구본부
** 정회원, 광운대학교, 정보제어공학과, 교수

수행중인 열차제어시스템의 안전성확보입증의 문서화를 위해 영국의 Yellow book을 참조하여 세부방안을 제시하며, 프로젝트단위로 할당되는 리스크의 허용수준 설정에 관하여 연구하였다[6].

2. RAMS목표수립

RAMS목표수립은 최종사용자가 요구하는 운영조건을 기준으로 수립한다. 열차제어시스템에 요구되는 서비스제공 불능시간 및 복구시간을 토대로 각각의 신뢰성, 가용성, 유지보수성의 목표가 수립되며, 안전성목표는 열차제어시스템에 존재하는 위험원의 허용할 수 있는 수준을 최종사용자와 협의하여 결정한다. 본 연구에서 제시하는 열차제어시스템의 RAMS 목표는 표 1과 같다.

안전은 IEC에서 정의한 "받아들일 수 없는 리스크로 부터의 해방"을 기본 개념으로 출발하였다[2]. 또한 본 연구는 일반적인 열차제어시스템을 대상으로 하므로, 운영환경에 따라 요구사항은 유동적이라 할 수 있다. 따라서, 본 논문에서는 열차제어시스템으로 인한 "위험측고장에 대한 발생빈도 10^{-8}이하"로 안전성목표를 제시한다. 이는 IEC 61508(전기/전자/프로그래머블 제어기의 안전성)과 IEC 62278(철도신호시스템의 안전성요구사항)에서 제시된 위험측고장의 발생을 억제하기 위한 안전대책의 수준인 안전무결성레벨(SIL) 4의 정량적 기준을 근거로 한다[2,4].

신뢰성목표인 평균고장시간(MTBF) 100,000시간은 안전성목표의 근거와 동일한 IEC 61508과 IEC 62278에서 제시하는 SIL4수준의 시스템 기능상실에 대한 정량적 기준인 단위시간에 대한 고장률 10^{-5}이하를 근거로 한다. 고장률(λ, Failure Rate)에 따른 MTBF의 계산은 열차제어시스템이 기능을 상실하는 평균고장수명(MTTF, Mean Time To Failure) 시간에 대하여 식 (1)과 같이 수리를 통한 기능복구까지의 시간이므로 MTBF는 식 (2)와 같이 시스템고장률의 역수가 된다[7].

$$MTBF = MTTF + MTTR \quad (1)$$

$$MTBF = \frac{1}{\lambda} \quad (2)$$

유지보수활동은 예방유지보수(PM, Preventive Maintenance)와 교정유지보수(CM, Corrective Maintenance)로 분류할 수 있다. PM은 시스템의 기능상실 이전에 현장교체가능장치(LRU, Line Replaceable Unit)별 점검 및 교체주기이며, CM은 LRU의 기능상실에서부터 교체를 통한 전체시스템 기능복구까지의 시간이다. PM에 대한 목표는 상세설계 이후의 수명주기에서 할당되며, 잔존수명의 비율에 대한 교체주기 등의 최종사용자 지침을 제외하면 별도의 기준을 요구하지 않는다. 따라서, 본 연구에서는 유지보수목표를 CM에 대해서만 2시간 이내로 설정하였다. 설정된 CM MTTR 2시간 이내는 미국방규격 MIL-STD-472에서 정의한 바와 같이 고장이 발생한 LRU의 예비품 및 교체에 필요한 도구를 준비한 유지보수자의 현장도착을 시점으로, 교체 및 점검을 마치고 시스템이 정상상태로 복구되기까지의 시간이다.[8] 2시간의 근거는 열차제어시스템의 대표적 사례인 KORAIL의 "차상신호(ATP)시스템 구축사업"의 CM MTTR 목표를 활용하였다[9].

마지막으로 가용도 목표인 정상상태 가용도(Ass)는 식 (3)과 같이 MTBF 목표와 MTTR 목표가 설정되면 연동되어 계산된다[7].

$$Ass = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF} \quad (3)$$

따라서, MTBF 100,000시간, MTTR 2시간, MTTF 99,998시간을 대입하면 Ass는 99.998%가 되며, 1년(24시간×365일)을 기준으로 하면 약10분이 된다.

시스템의 RAM목표는 정량적이므로 그 적용범위가 매우 중요시된다. 따라서, RAM목표를 적용하는 열차제어시스템의 구성요소를 기준으로 차상제어장치 1대와 지상장치 1세트(기능구성을 위한 최소단위)로 제한하여 수립한 목표이다.

표 1. 열차제어시스템 RAMS목표의 예

항 목	목 표
안전성	열차제어시스템으로 인한 위험원은 허용할 수 있는 수준(위험측고장에 대한 발생빈도 10^{-8}이하)으로 완화된다.
신뢰성	MTBF 100,000 Hour
가용성	Ass = 99.998% (1년간 평균 서비스 상실시간 0.18시간)
유지보수성	CM MTTR < 2 Hour

MTBF : Mean Time Between Failure , MTTR : Mean Time To Repair
Ass : Stady State Availability, CM : Corrective Maintenance

3. 안전활동 계획수립

열차제어시스템 안전성목표인 "허용할 수 있는 수준으로 위험원을 완화"를 만족하기 위해서는 위험원도출 및 분석의 건전성을 입증해야 하며, 허용할 수 있는 수준의 설정에 대한 적합성을 최종사용자가 승인해야 한다. 그림 1은 안전성

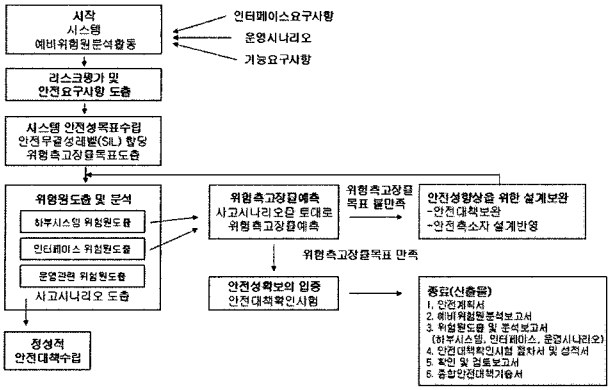

그림 1. 안전성활동의 흐름

표 2. 적용규격 및 문서화 기준

항 목	목 표	적용활동
적용 규격	IEC 61508 전기전자프로그래머블 제어기의 안전성	수명주기 전체
	IEC 62278(EN 50126) 철도신호시스템의 안전성요구사항	수명주기 전체
	IEC 62279(EN 50128) 철도신호시스템 소프트웨어 안전성	소프트웨어 위험원도출 및 안전요구사항 확인
	IEC 62425(EN 50129) 철도신호시스템 안전필수 요구사항	시스템 위험원도출 및 안전요구사항 확인
	IEC 62280(EN 50159) 철도신호시스템통신안전성	통신 위험원도출 및 안전요구사항 확인
	IEC 61882 HAZOP Application	예비위험원분석 및 위험원도출 및 분석
	IEC 60812 고장모드영향분석	예비위험원분석 및 위험원도출 및 분석
	IEC 61025 결함트리분석(FTA)	위험원발생빈도 분석
문서화 기준	Yellow Book Issue 3 & 4 영국 철도안전 문서화 및 승인관련 지침	

FTA : Fault Tree Analysis, EN : European Norm

활동의 흐름의 도식화이다[10].

그림 1의 활동흐름은 모두 국제규격을 근거로 활동되며, 프로젝트기반 안전성활동의 최종목표인 시스템 안전승인을 위해서는 체계적인 문서화가 반드시 요구된다.

본 논문에서는 안전성활동과 문서화의 근거로 표 2와 같은 규격 및 기준을 적용하였다.

3.1 안전계획서(Safety Plan) 작성

안전성활동의 시작은 계획의 수립이다. 안전계획서에서는 적용대상의 범위, 리스크의 허용수준(안전성 목표), 관련

표 3. YB3의 안전계획서 권고목차

목차	세부목차
1. 서론	세부목차 없음
2. 배경과 요구사항	세부목차 없음
3. 안전관리 엔지니어링의 활동(ESM)	1. 안전성의 임무 및 책임 2. 안전성 수명주기 3. 안전성 분석 4. 안전성의 실행가능성 5. 안전관련 규격들 6. 안전성 평가 7. 안전성 감사 8. 종합안전대책기술서와 안전승인 9. 공급자의 관리 10. 구성관리 11. 프로젝트의 안전성 훈련 12. 시스템 운용, 변경 그리고 유지보수 13. 사용중지 및 해체
4. 안전성 제어	세부목차 없음
5. 안전성 문서화	세부목차 없음
6. 안전성 엔지니어링	세부목차 없음
7. 외부요인에 대한 확인	1. 안전관련 관점에서 도출되는 요인에 대한 판단의 범위 2. 외부항목의 모든 문서의 적합성을 포함 3. 문서의 평가 4. 외부요인들에 대한 프로젝트 요구사항을 기준으로 성능과 제한사항을 명시 5. 외부요인에 대한 안전관련 특성의 시험과 새로운 시스템과의 독립성 6. 외부요인 사용에 대한 리스크평가 수행 7. 외부요인의 공급자에 대한 안전성 평가 수행

YB3 : Yellow Book Issue 3
ESM : Engineering Safety Management

기관의 책임 및 역할, 안전성활동인력의 경력 및 이력, 적용규격 및 기준, 프로젝트 일정, 안전성활동을 위한 수명주기별 적용기술, 최종산출물 목록 등이 기술되어야 하며, 예비위험원분석에서 종합안전대책기술서 작성까지의 활동단계별 사용 양식도 제시되어야 한다. 또한 안전계획서는 최종사용자 또는 최종사용자가 안전승인을 위임한 기관으로부터의 승인을 취득해야 하며, 영국의 경우 안전계획서와 종합안전대책기술서에 대해서는 국제규격을 근거로 활동한 산출물의 검토시간을 최소화하기 위해 Yellow Book이라는 문서화 기준을 제시하여 문서의 목차 및 목차에 해당하는 내용의 요구사항을 제시하고 있다.

본 논문의 계획수립의 대상인 운영제어시스템의 안전성활동 문서화는 Yellow Book을 바탕으로 이루어지며, 안전계획에 해당하는 Yellow Book의 권고내용은 표 3과 같다.

열차제어시스템의 위험원을 허용할 수 있는 수준으로 완화하기 위해서는 허용할 수 있는 수준에 대한 정의가 요구

표 4. 위험원으로 인한 사고심각도의 분류[2,4,11]

심각도	정성적 기준	정량적 기준
치명적인 위험 (Catastrophic)	인명의 사망, 시스템의 손실 또는 심각한 환경상의 피해를 유발하는 위험	3인 이상 사망
중대한 위험 (Critical)	심각한 인명의 상해, 직업상의 질병 및 중요한 시스템 또는 환경상의 피해를 초래하는 위험	1인 이상 사망, 3인 미만 사망
중요하지 않은 위험 (Marginal)	최소한의 상해, 직업상의 질병 및 최소한 시스템 또는 환경상의 피해를 초래하는 위험	1인 이상 중상, 10인 미만 중상
사소한 위험 (Insignificant)	최소한의 상해, 직업상의 질병보다 작고, 최소한의 시스템 및 환경상의 피해보다 작은 영향을 초래하는 위험	1인 이상 경상, 20인 미만 경상

* 1인 사망 = 10인 중상, *1인 중상 = 20인 경상

표 5. 위험원 발생빈도의 분류[2,4]

발생빈도	정성적 기준	정량적 기준
빈번한 발생 (Frequent)	수명주기 동안 빈번하게 발생할 가능성이 있음	10^{-3}이상
가능성 있는 발생 (Probable)	수명주기 동안 여러 번 발생할 가능성이 있음	10^{-4} < to ≤ 10^{-3}
종종 발생 가능 (Occasional)	수명주기 동안 가끔 발생할 가능성이 있음	10^{-6} < to ≤ 10^{-4}
발생가능성이 미약 (Remote)	수명주기 동안 한두 차례 발생할 가능성이 있음	10^{-8} < to ≤ 10^{-6}
발생 가능성이 거의 없음 (Improbable)	수명주기 동안 발생 가능성은 있지만, 발생하지 않음	10^{-9} < to ≤ 10^{-8}
발생 가능성이 전혀 없음 (Incredible)	발생가능성도 희박하며, 절대 발생하지 않음	≤ 10^{-9}

표 6. 열차제어시스템의 리스크 매트릭스[2,4]

설 명	치명적인위험 (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

되며, 리스크가 위험원의 발생빈도와 사고심각도의 조합이므로 국내 철도안전법에서 제시하는 사고의 기준인 3인 이상 사망을 근거로 표 4와 같이 위험원의 심각도 분류 및 표 5와 같이 사고의 발생빈도를 정성적 및 정량적으로 분류하였다[11]. 또한, 심각도분류와 발생빈도분류에 의해 리스크를 허용할 수 있는 수준을 표 6과 같이 IEC 62278을 근거로 매트릭스 형태로 제시하였다. 표 6의 매트릭스는 리스크를 정성적으로 판단하는 경우에 사용되며, 정량적인 기준으로 변환하면 그림 2와 같이 표현할 수 있다.

그림 2에서 사고의 심각도를 완화시키기 위해서는 별도의 시설(예를 들어 승강장의 승객추락으로 인한 심각도를 완화시키기 위한 승강장 부분 선로의 완충물 설치)이 추가되거나, 프로젝트의 범위를 벗어나는 경우가 발생하므로, 대부분의 리스크의 감소는 발생빈도를 감소시켜 리스크를 허용할 수 있는 수준으로 완화시키는 활동을 수행한다.

3.2 안전승인을 위한 계획

열차제어시스템 안전성활동의 최종목표는 안전승인이다. 따라서 본 논문에서는 그림 3과 같이 열차제어시스템의 안

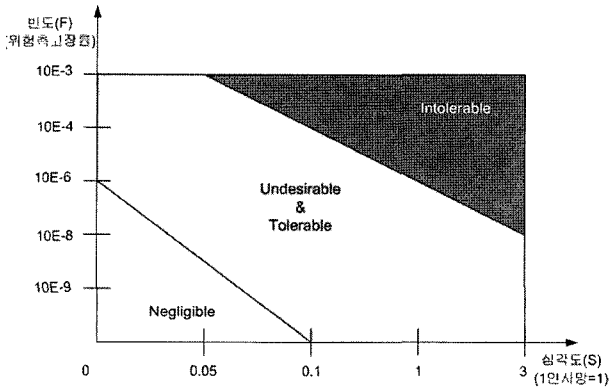

그림 2. 열차제어시스템의 리스크허용기준

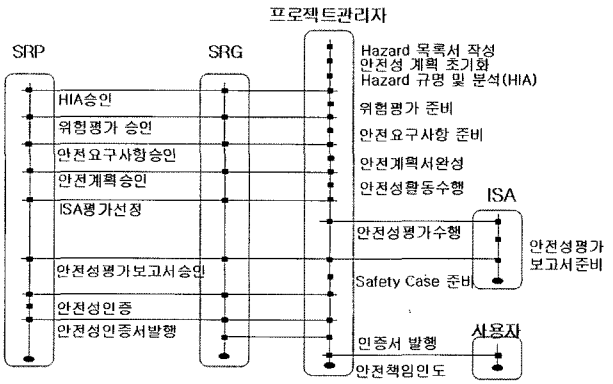

그림 3. 열차제어시스템의 안전승인관련기관

전성확보에 대한 프로젝트관리자, 안전성검토위원회(SRP, Safety Review Panel), 안전성검토조직(SRG, Safety Reveiw Group), 독립안전평가기관(ISA, Independant Safety Assessment) 및 사용자로 관련기관 및 업무의 흐름을 영국의 승인관련 지침(Yellow Book)을 근거로 제시한다[6].

3.3 예비위험원분석(PHA)

예비위험원분석의 목적은 열차제어시스템의 안전성활동에 적용할 최상위 위험원을 도출하기 위한 과정이다. 안전성활동의 결론부분에서 정리되는 위험원목록에서는 예비위험원분석에서 도출된 최상위 위험원을 대상으로 위험원별 리스크가 허용할 수 있는 수준으로 제어되었는지의 유무를 기준으로 작성된 위험원목록을 근거로 안전성확보를 판단하므로, 최상위 위험원도출을 위한 과정의 건전성이 중요시된다.

예비위험원분석의 수행은 철도에서 발생할 수 있는 위험원을 대상으로 리스크를 완화할 수 있는 안전대책이 운영제어시스템의 범위에 포함되는 위험원만을 선별한다. 따라서, 철도에서 발생할 수 있는 위험원들은 영국의 철도분야 위험원관련 보고서인 "Hazard Portfolio", "Hazard Checklist", "Risk Profile Bulletin" 등의 자료를 근거로 사용하여 건전성을 확보하며, 위험원별 안전대책수립 및 최상위 위험원도출을 위한 활동은 안전계획서에 명시된 참여연구원의 경력 및 자격으로 건전성을 확보해야 한다.

예비위험원분석의 결과인 최상위 위험원은 예를 들어 "소형궤도차량의 진로설정과 분기병합장치의 상태가 서로 상이함(일반철도신호에서의 연동장치 선로전환기 불일치)"과 같이 매우 정성적이므로, 이러한 위험원이 발생되는 원인을 추적하여, 발생빈도와 위험원으로 인한 심각도가 리스크의 허용수준 이하로 완화되었음을 정량적으로 입증하기 위해 위험원도출 및 분석(HIA, Hazard Identification and Analysis) 활동을 수행한다. 또한 예비위험원분석 단계에서 위험원별 안전대책이 설계를 위한 안전요구사항으로 적용된다.

3.4 위험원도출 및 분석(HIA)

위험원도출 및 분석은 시스템 수명주기의 설계이후에 수행되는 과정으로써, 운영시스템 설계사양에서 그림 4와 같이 구성요소별 기능사양서, 인터페이스 사양서, 운영시나리오를 대상으로 각각 수행된다. HIA활동의 목표는 전체시스템 운영시나리오와 구성요소의 기능사항 그리고 인터페이스 요인에 대한 위험원을 도출하고 분석하는 단계이다.

위험원의 도출을 위한 방법은 고장모드영향분석(FMEA, Failure Mode Effect Analysis)와 HAZOP(Hazard and Operability) Study기법이 사용된다. 두 가지 기법 모두 위험원도출이라는 동일한 목표를 가지지만, 위험원도출을 위한 이상현상의 분석기준을 FMEA에서는 고장모드(Failure Mode)[12], HAZOP에서는 Guide Word를 사용한다[13]는 점에서 차이가 있다. 전자부품과 같이 고장의 일반적인 패턴이 존재하는 경우에는 고장모드의 사용이 용이하며, 인터페이스사양과 운영시나리오와 같이 경우의 수에 대한 누락을 최소화하기 위한 대상에는 Guide Word의 적용이 용이하다.

FMEA와 HAZOP의 차이점은 고장모드와 Guide Word에 대한 사항 외에도 고장원인으로 인한 이상현상의 리스크 평가 및 안전대책 보완주체와 세부안전대책에 대한 내용이 차이를 갖는다. FMEA는 리스크의 평가를 수행하는 반면 보완주체 및 세부안전대책에 대한 추적성이 용이하지 않으며, HAZOP은 안전대책의 적용유무에 대한 추적성 용이하지만 반대로 리스크 평가를 이상현상 별로 수행하지 않아 위험원목록 작성이 용이하지 않다. 따라서 FMEA와 HAZOP의 장점을 반영한 표 7과 같은 위험원도출 워크시트를 제안한다.

표 7을 통해 도출된 위험원은 PHA에서 제시된 최상위 위험원과의 연관관계를 분석하여 발생빈도를 계산해야 한다.

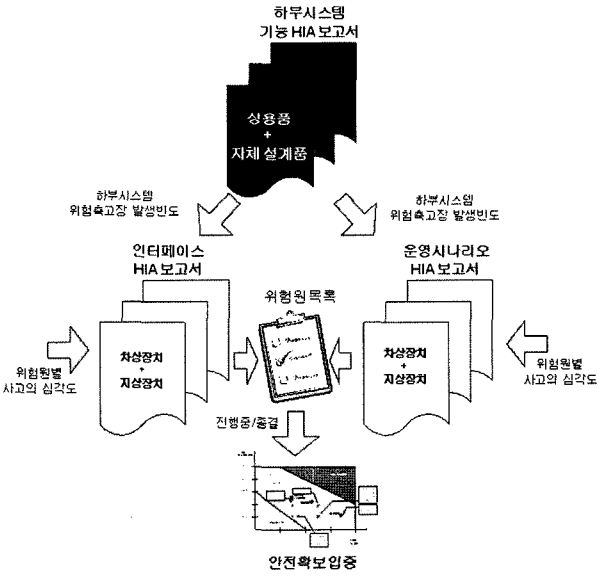

그림 4. 열차제어시스템의 위험원도출 및 분석의 구조

표 7. 열차제어시스템의 위험원도출 워크시트

HAZOP Study 대상:											
참조도면번호:					갱신번호:			소요시간:			
참여구성원:								회의일시:			
기능	Guide Word	이상현상	원인	결과	대책 전Risk			안전대책	대책 후Risk			세부조치내역	조치주체
					F	S	R		F	S	R		

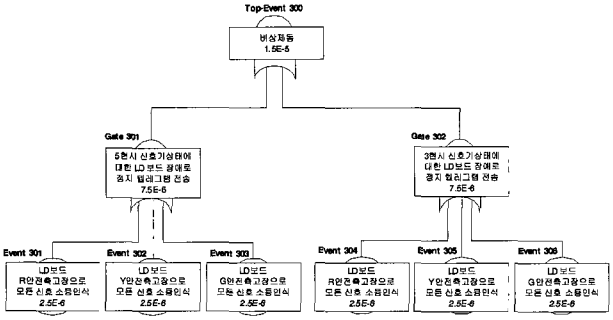

그림 5. FTA분석의 예(차상신호시스템 비상제동이벤트)

표 8. 열차제어시스템의 위험원목록 양식 예

위험원 ID	위험원 설명	최종리스크 F	S	R	사고결과 (영향분석)	원 인	관련 장치	관련구성 요소	안전대책	기타 사항 (참고 문서, 조치 주체)	상 태
HIF-WS001											

위험원 도출과 마찬가지로 위험원분석방법에서도 결함트리분석(FTA)과 이벤트트리분석(ETA)방법이 주로 사용된다. FTA는 상향식분석방법으로써, 위험원도출 워크시트의 이상현상 및 원인을 최하위 이벤트로 설정하여 최상위 이벤트의 발생빈도를 그림 5와 같이 분석할 수 있다.

FTA의 최하위 이벤트에는 주로 기능고장, 인적오류에 대한 발생빈도가 정량적으로 입력되어야 한다. 따라서, 기능고장의 경우 신뢰성분석에서 사용된 구성요소의 고장률데이터가 입력되며, 인적오류와 같이 정량적 접근이 용이하지 않은 사항에 대해서는 PHA단계에서와 같이 안전성과 시스템에 대한 전문가 집단이 ETA를 통해 정량적 수치를 할당한다.

또한, 모든 이벤트의 발생빈도의 근거자료는 HIA보고서의 중요한 요구사항 중 하나로써, 제3자 확인이 가능한 설계사양서, 도면, 회의록 등이 포함된다.

3.5 위험원목록(Hazard Log) 작성

위험원목록에 대한 작성기준은 별도로 규격화 되어있지 않으며, 제작사 및 운영기관별로 자체 양식을 정하여 활용하고 있다. 따라서 운영제어시스템 위험원목록은 표 8과 같은 형태로 제시하였다. 위험원목록의 목적은 운영제어시스템의 위험원이 모두 허용할 수 있는 수준으로 완화되었는지의 여부를 판단하기 위한 것으로써, 진행 중인 사항과 완료된 사항을 구분하여 관리하며, 위험원의 처리가 완료된 사항에 대해서는 안전대책을 확인할 수 있는 입증자료를 FTA 이벤트 근거문서와 동일하게 포함시킨다.

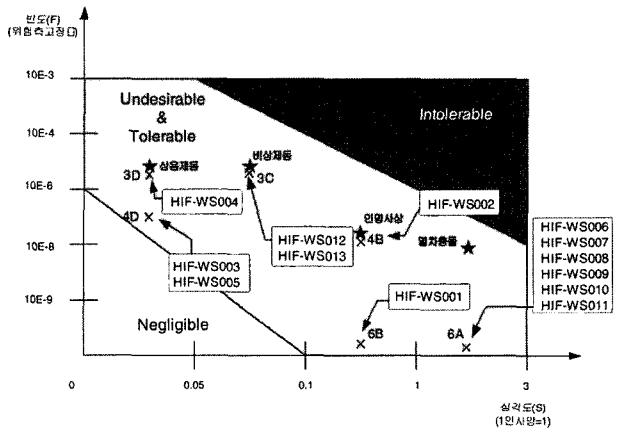

그림 6. 안전확보의 입증 예

3.6 종합안전대책기술서(Safety Case)작성

종합안전대책기술서는 안전계획서와 함께 Yellow Book에서 요구사항을 포함한 목차를 제시하고 있으며, 열차제어시스템 종합안전대책기술서도 위와 같은 목차를 준수하여 작성된다.

종합안전대책기술서의 목적은 안전승인기관이 안전성활동 전반에 대한 건전성과 안전의 확보유무를 판단하기 위한 것으로써, 건전성은 모든 입증서류의 첨부로써 보장해야 하며, 안전의 확보유무는 그림 6과 같이 열차제어시스템의 위험원들이 모두 허용할 수 있는 수준으로 완화되었음을 입증해야 한다. 그림에서 HIF-WSXXX는 위험원 ID이다.

4. 결 론

본 논문에서는 일반적인 열차제어시스템을 대상으로 수행될 RAMS활동에 대한 수명주기 전반의 계획수립을 수행하였다. 또한, 안전성활동 수명주기별 상세 활동계획을 수립하여, 예측하지 못한 상황을 최소화하기 위한 체계적 활동을 수행하였다. 이러한 활동은 안전승인이 요구되는 철도시스템에 중요한 사항으로써, 수립된 안전계획은 최종사용자 또는 최종사용자가 위임한 기관으로 인해 승인을 받아야 한다.

안전계획서는 IEC 62278 및 Yellow Book에서 제시된 바와 같이 프로젝트의 종료까지 지속적으로 변경될 수 있으며, 종합안전대책기술서와 함께 안전확보의 중요한 평가 자료로 활용될 것이다.

감사의 글

이 연구는 2005년 광운대학교 교내연구비 지원에 의하여 이루어 졌습니다.

참 고 문 헌

1. 이준호, 김종기, 김백현, 신경호 (2005), "개인고속 이동 시스템에서 운전시격과 차량의 감속도에 관한 상관관계의 연구", 한국철도학회 추계학술대회논문집, pp.586-591.
2. IEC62278 (2002), "Railway applications-Specification and demonstration of RAMS", pp.59-65.
3. MIL-STD-882C (1993), "System Safety Program Requirements".
4. IEC61508 (1998), "Functional safety of electrical/electronic /programmable electronic safety-related systems".
5. 신덕호, 이준호, 이강미, 김용규 (2005), "HAZOP Study를 사용한 ATSRX의 위험원도출 및 리스크완화에 관한 연구", 한국철도학회논문집, 제8권 제6호.
6. Published by Railway Safety on behalf of the UK rail industry (2000), "Engineering Safety Management Yellow book 3".
7. Barry W. Johnson (1989), "Design and Analysis of Fault-Tolerant Digital systems", pp.169-258.
8. MIL(Militany Specifications and Standards)-HDBK-472 (1966), "Maintainability Prediction".
9. 철도청 (2003), "차상신호(ATP)시스템 도입을 위한 제안요청서".
10. 한국철도기술연구원 (2005), "고속철도 열차제어시스템 안정화 기술개발 3차년도 연구보고서".
11. 한국철도기술연구원 (2005), "철도사고 위험요인(PHA) 분석기술 개발 연구보고서".
12. IEC60812 (2006), "Analysis techniques for system reliability-Procedure for failure mode and effects analysis(FMEA)".
13. IEC61882 (2001), "Hazard and operability studies(HAZOP Studies) - Application guide".