한국철도학회논문집
제9권 제4호 2006년 ▌pp. 412-418

열차제어시스템의 안전입증에 관한 연구

A Study on the Safety Demonstration of Train Control System

신덕호† · 이재호* · 이강미* · 황종규* · 정의진* · 왕종배** · 박영수***
Ducko SHIN · Jae-Ho LEE · Kang-Mi LEE · Jong-Kyu Hwang · Eui-Jin Joung · Jong-Bae Wang · Young-Soo Park

Abstract

In this paper we deal with the APARP theory which has been applied for UK railway system and risk assessment method which has been using in the domestic railway system for the safety demonstration. Both techniques are applied to the ATP wayside equipment for interface. Also, for the applications of each techniques a analysis of the safety activity and a possibility of the application of ALARP theory are evaluated. Finally, we generate requirements of the safety demonstration for the future domestic railway system by way of the analysis of some assumptions and requirement data which can be applied to the risk assessment of ALARP.

Keywords : TCS(Train Control System), HIA(Hazard Identification and Analysis), ATP(Automatic Train Protection) FMEA(Failure Mode Effect Analysis), HAZOP(Hazard and Operability), FTA(Fault Tree Analysis) Safety Plan, Safety Case, Risk Assessment, Hazard Log, ALARP(As Low As Reasonably Practicable)

1. 서 론

철도운영에서 열차제어시스템의 고장, 결함은 열차충돌, 탈선 등 파국적인 사고를 초래하기 때문에 열차제어시스템에 대한 위험관리와 안전성 인증의 중요성은 국제적으로 강조되어 왔다[1].

이를 위해 국제규격인 IEC 62278은 전기전자프로그래머블제어기로서 열차제어시스템의 RAMS(신뢰성, 가용성, 유지보수성 및 안전성) 요구사항을 IEC 62425(EN 50129)는 제어시스템에 적용되는 전자시스템에 대한 안전요건 그리고 열차방호를 위한 열차제어시스템의 신호통신처리 소프트웨어의 안전요건으로서 IEC 62279(EN 50128) 등이 열차제어시스템의 안전성 관련 국제규격으로 제정되어 있다.

국내 철도도 열차제어시스템 대부분이 컴퓨터화된 전자장비로 구성됨에 따라 특별한 징후없이 발생하는 제어기의 내부고장에 대한 위험측 고장요인을 분석하고, 그 발생빈도와 피해심각도를 일정수준 이하로 관리하기 위한 위험도(Risk)평가를 핵심으로 하는 안전연구를 지속해 왔다[2].

현재 한국철도공사(KORAIL)의 ATP시스템 도입사업은 위험도 평가를 통해 안전요구사항을 도출하고 이를 근거로 시스템 안전성을 판단하고 있으며, 유럽 각국에서도 철도운영환경에 따라 영국 ALARP(As Low As Reasonably Practicable), 프랑스 GAMAB, 독일 MEM 등 위험도 평가에 기반한 적절한 안전관리 원칙을 적용하고 있다.

특히 영국철도는 국제규격과 유럽규격을 준수하여 열차제어시스템의 개념설계부터 폐기까지 전 수명주기 동안 위험원(Hazard)을 도출하고 위험도를 평가하여 허용수준 이하로 관리하는데 필요한 안전활동의 문서화 및 승인절차를 철도시설관리자(Network-Rail)가 Yellow Book이라는 지침으로써 권고하고 있으며, 여기서 안전성을 판단하는 핵심원칙으로서 ALARP을 적용한다[3].

본 논문에서는 현재 국내 열차제어시스템에 대한 안전성 입증활동 사례로서 한국철도공사의 차상신호시스템 도입사업인 ATP시스템 지상장치에 대한 인터페이스 안전성 활동을 분석하고, ALARP이론을 적용하여 안전성 입증이 가능한지를 검토하였다. 그리고 ALARP 원칙에 따른 위험도 평가를 적용하기 위한 가정 및 요구 데이터를 분석하여 향후 국내 철도시스템의 안전입증에 필요한 요구사항을 도출하고자 한다.

† 책임저자 : 회원, 한국철도기술연구원, 전기신호연구본부, 공학박사
E-mail : ducko@krri.re.kr
TEL : (031)460-5442 FAX : (031)460-5449
* 회원, 한국철도기술연구원, 전기신호연구본부, 공학박사
** 회원, 한국철도기술연구원, 철도시스템안전연구본부, 공학박사
*** 회원, 건설교통부, 공학박사

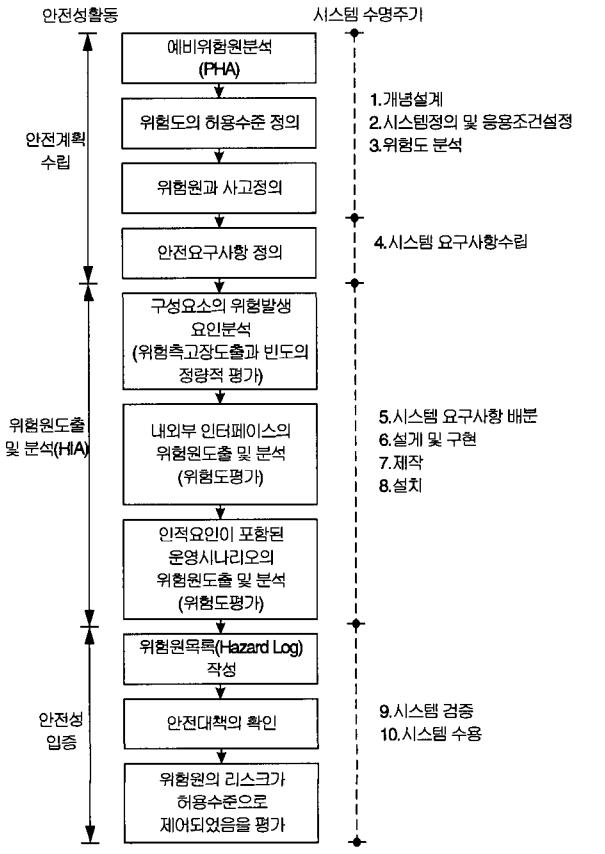
2. 국내 열차제어시스템의 안전입증 절차현황

국내 열차제어시스템에 대한 안전성활동은 2001년 철도청(KNR)의 "철도신호제품에 대한 신뢰성과 안전성 검증기준 제정연구"와 2001년 철도청지시 2001-49호 "열차제어시스템 안전성확보 기술 권고안"을 시작으로 열차제어시스템의 위험원을 도출(Identification)하고 위험도를 평가하여 허용가능한 수준으로 완화하기 위한 체계를 수립하였다. 이후 이러한 안전성 활동은 2002년 KORAIL "통합관제실 CTC 소프트웨어의 안전성연구" 및 2004년 KORAL "차상신호(ATP)시스템 도입사업의 RAMS활동"까지 적용되면서 2005년 철도안전법 제정에도 기여하였다.

이와 같은 위험분석 및 위험도 평가를 기반으로 하는 국내 열차제어시스템 안전성활동체계를 그림 1에 제시한다.

2.1 KORAIL ATP 시스템의 위험도 허용수준 설정

예비위험원분석을 통해 ATP시스템에 내제된 위험원을 도출하고 이들의 위험도를 완화할 수 있는 안전대책을 시스템설계 단계의 안전요구사항으로 활용한다.



PHA : Preliminary Hazard Identification, HIA : Hazard Identification and Analysis

그림 1. 위험도 평가를 통한 안전성 입증의 업무흐름

이때 위험도의 허용수준은 앞에서 제시한 ALARP이론과 같은 이론적 평가기준을 사용할 수 있으나, ATP시스템 안전성활동에서는 표 1과 같은 위험도 허용수준을 안전계획서(Safety Plan)에 설정하여 해당 위험원이 허용할 수 있는 수준으로 제어됨을 입증하는 것으로 수행한다. 따라서 시스템의 모든 위험원에 대해 표 1의 위험도 허용수준을 적용하여 "Intolerable, Undesirable" 영역의 위험원에 대해서는 안전대책을 검토하여 "Tolerable, Negligible"영역으로 위험도가 완화되었음을 입증하는 종합안전대책기술서(Safety Case)를 작성하고 이를 독립안전성평가자(ISA, Independent Safety Assessment)나 최종사용자가 승인하는 것으로서 안전성입증 활동이 종료된다[4,5].

2.2 ATP시스템 지상장치 인터페이스 위험원 도출 및 분석

ATP시스템 지상장치의 내부구성 및 인터페이스는 그림 2와 같다[6].

ATP시스템 지상장치 인터페이스는 ATP지상장치와 기존 KORAIL장치와의 물리적 인터페이스를 범위로 하며, 위험원 도출을 위해 인터페이스별로 Guide Word를 기준으로 이상현상(Deviation)을 예측하여 위험원을 도출하는 HAZOP Study기법을 사용하였다[6]. ATP지상장치의 인터페이스 요

표 1. ATP시스템의 위험도 허용수준 매트릭스

설 명	치명적인 위험 (Catastrophic) 3인이상 사망	중대한 위험 (Critical) 1인이상 사망, 3인미만 사망	경미한 위험 (Marginal) 1인이상 중상, 10인미만 중상	사소한 위험 (Insignificant) 1인이상 경상, 20인미만 중상
빈번한 발생 (Frequent) [10^{-3}/h 초과]	Intolerable	Intolerable	Intolerable	Undesirable
가능성 있는 발생 (Probable) [10^{-4}초과, 10^{-3}/h 이하]	Intolerable	Intolerable	Undesirable	Tolerable
종종 발생 가능 (Occasional) [10^{-6}초과, 10^{-4}/h 이하]	Intolerable	Undesirable	Undesirable	Tolerable
발생가능성이 미약함(Remote) [10^{-8}초과, 10^{-6}/h 이하]	Undesirable	Undesirable	Tolerable	Negligible
발생가능성이 거의 없음 (Improbable) [10^{-9}초과, 10^{-8}/h 이하]	Tolerable	Tolerable	Negligible	Negligible
발생가능성이 전혀없음 (Incredible) [10^{-9}이하]	Negligible	Negligible	Negligible	Negligible

인은 선로변전자유닛(LEU, Line-side Electronic Unit)의 아날로그 전원입력, 신호기상태 검지를 위한 비접촉방식 아날로그 입력, 건널목 제어기와의 인터페이스인 지장물검지계전기와 경보장치 고장검지계전기의 접점입력, ATP차상장치와의 텔레파워링 및 텔레그램신호, LEU의 자기검사기능 등으로 구성된다. 표 2는 5현시 구간의 신호기 입력에 대한 HAZOP Study의 예이다.

HAZOP Study 워크시트는 국제규격[7]에서 제시하지만 차상신호(ATP)시스템 도입사업의 위험원 도출에서는 FMECA (Failure Mode Effect and Criticality Analysis)의 장점인 위험원별 위험도평가를 HAZOP Study 워크시트에 포함시켜 동시에 수행하도록 별도의 양식을 표 2와 같이 구성하였다. 따라서 위험원 도출과 함께 사고결과에 따른 위험원의 관리와 안전대책 반영 후의 위험도평가를 통해 안전계획서에 제시된 안전의 허용수준 만족여부를 정량적 기준에 의해 평가할 수 있다.

표 2. ATP지상인터페이스의 HAZOP Study 예(5현시 신호기와 LEU의 인터페이스)

HAZOP Study 대상: LD입력(5현시구간 G)

참조도면번호: 근거3 | 갱신번호: V1.0 | 소요시간: 부록A 참조

참여구성원: ATP시스템 RAMS컨설팅부서, 시스템 검토그룹(SEG), ATP지상장치 설계제작사 엔지니어 | 회의일시: 부록A 참조

기능	Guide Word	이상현상	원인	결과(ATP지상장치의 최종상태)	대책 전Risk F	S	R	안전대책	대책 후Risk F	S	R	세부조치내역	조치 주체
LD입력 (5현시구간 G)	No	신호기의 상태와 관계없이 단일상태로 고정	LEU의 LD보드고장	상용제동 (장애텔레그램전송)	3	D	3D	다중화 설계	6	D	6D	LEU의 LD보드 구성을 사중계방식으로 구현	BT
	More	입력전류의 과다 (허용전류 이상)	LEU-신호기 케이블에 이상신호 유도	상용제동 (장애텔레그램전송)	3	D	3D	실드케이블사용	4	D	4D	LEU-신호기 실드케이블 사용	TJ
								보호회로 내장				과전류방지회로 (내부전원감시 및 차단회로)	BT
	Less	입력전류의 미흡 (5W미만-3W이상)	LD내부 전원불량	상용제동 (장애텔레그램전송)	3	D	3D	전원감시에 의한 안전측 차단	4	D	4D	LD의 전원상태 감시회로 (신호기 상태입력 불안전 텔레그램을 전송)	BT
			단선등에 의한 케이블저항증가										
	As well as	해당 없음											
	Part of	충분한 시간동안 상태입력이 유지되지 않음(20msec 이하)	신호기 점등고장 (ABS or EIS고장)	운행지연 (G신호전송실패)	-	-	-	없음	-	-	-	프로젝트의 범위를 벗어남	-
			LEU의 LD보드고장	정상동작	-	-	-	안전측설계	-	-	-	20ms단위의 실시간 신호기상태 감시(신호기 최종 입력상태를 유지)	BT
	Reverse	신호기 반대상태 입력(점등) (신호기 G점등을 소등으로 인식)	LEU의 LD보드고장	비상제동 (정지텔레그램전송)	3	A	3A	고장진단논리	6	A	6A	모든 신호기 소등시 정지텔레그램 전송되도록 BD의 논리를 구현	BT
		신호기 반대상태 입력(점등) (신호기YG점등을 Y로 인식)	LEU의 LD보드고장	운행지연 (안전측텔레그램 전송)	-	-	R	다중화 설계	-	-	R	LD와 BD를 사중계로 구성하여 고장률을 SIL4수준으로 확보	BT
		신호기 반대상태 입력(소등) (신호기 G소등을 YG으로 인식)	LEU의 LD보드고장	운행지연 (안전측텔레그램 전송)	-	-	R	다중화 설계	-	-	R	LD와 BD를 사중계로 구성하여 고장률을 SIL4수준으로 확보	BT
		신호기 반대상태 입력(소등) (신호기 G소등을 YY1G로 인식)	LEU의 LD보드고장	상용제동 (장애텔레그램전송)	3	D	3D	고장진단논리	6	D	6D	YY1G가 점등되면 고장으로 인식하는 논리를 BD에 적용 (장애텔레그램 전송)	BT
		신호기 반대상태 입력(소등) (신호기 G소등을 RG로 인식)	LEU의 LD보드고장	상용제동 (장애텔레그램전송)	3	D	3D	다중화 설계	6	D	6D	RG가 점등되면 고장으로 인식하는 논리를 BD에 적용 (장애텔레그램 전송)	BT
	Other than	신호현시순서와 상이한 입력	신호기 점등고장 (ABS or EIS고장)	열차충돌 (G신호전송실패)	-	-	-	없음	-	-	-	프로젝트의 범위를 벗어남	-
			LEU의 LD보드고장	열차충돌 (G신호전송실패)	3	D	3D	고장진단논리	6	D	6D	현시순서를 지키지 않고 YG를 현시(LEU의 신호기 상태입력에서 오류가 발생하여 현시순서가 잘못 입력될 확률은 LD보드 사중화로 인해 SIL4수준으로 확보. 따라서, 입력20msec단위로 샘플링하여 최종 신호기상태에 해당하는 텔레그램 전송)	BT
	Early	해당 없음											
	Late	해당 없음											
	Before	해당 없음											
	After	해당 없음											

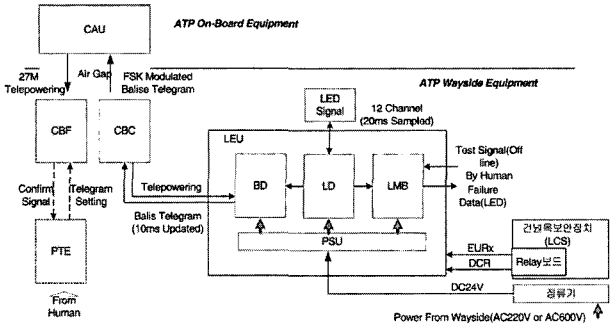
[기타사항]
1.

[변경이력]
1. 2006.03.28 : Guide Word를 포함한 Worksheet 1차 완성(설계엔지니어 및 SEG에 검토의뢰)
2. 2006.04.14 : 11차, 12차 HAZOP 미팅결과 반영(신호기 현시순서에 따른 텔레그램, 신호기 상태입력 오류에 따른 텔레그램, 점등과 소등의 판단정격)

LD : Lamp Detector / BD : Balise Driver / LEU : Line-side Electronic Unit / SIL : Safety Integrity Level / ABS : Automatic Block System / EIS : Electronic Interlocking System

HAZOP Study를 통해 도출된 위험원은 PHA에서 도출된 위험원의 하부 위험원으로써, 위험원을 발생시키는 원인(Casual Effect)에 가까운 형태로 주어진다.

따라서 각각의 하부 위험원 결과의 발생빈도는 그림 3과 같이 결함트리 분석기법을 사용(FTA분석의 이벤트 발생확률 입증자료의 예는 표 3과 같다.)하며, 각각의 위험원에 대한 심각도를 표 4와 같이 가정한 후 위험도를 평가하여 정량적 위험도의 평가결과와 요구사항을 비교한다.



LD : Lamp Detector / BD : Balise Driver / CAU : Compact Antenna Unit
CBF : Compact Balise Fixed / CBC : Compact Balise Controller
PSU : Power Supply Unit / LCS : Level Crossing
LMB : LEU Monitoring Board / LEU : Line-side Electronic Unit
PTE : Programming Test Equipment

그림 2. ATP시스템 지상장치 구성도

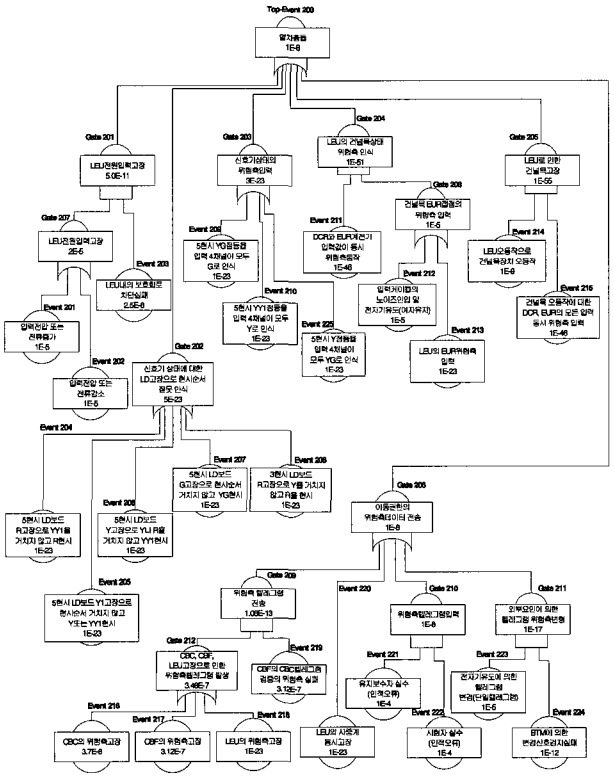


그림 3. 위험원분석을 위한 FTA 예(ATP시스템 지상장치 IF)

HAZOP Study를 통해 도출된 위험원은 안전대책이 적용된 최종시스템의 위험도 평가를 위해 그림 3의 FTA분석에서와 같이 PHA에서 도출된 위험원을 최상위 위험원으로 선정하여 인적오류가 포함된 최종위험원의 발생빈도를 평가한다. 물론 이러한 정량적 발생확률의 표현이 용이하지 않은 이상현상에 대해서는 표 5와 같은 가정이 추가되며, 표 4의 심각도 분류 가정과 마찬가지로 안전계획서 또는 해당 보고서를 통해 최종사용자 또는 독립안전성평가조직의 승인을 받는다.

2.3 KORAIL ATP시스템 지상장치의 안전성 입증

도출된 위험원의 위험도 평가결과는 안전요구사항의 허용 위험도 만족여부를 확인하기 위한 위험원 목록(Hazard Log)을 표 6과 같이 문서화함으로써 안전대책을 반영한 시스템의 위험도가 허용 수준으로 제어될 수 있음을 그림 4를 통해 입증할 수 있다.

표 3. FTA이벤트의 산출근거 예

이벤트 번호	산출근거	적용빈도 [h]
Event 203	LEU의 기능고장 2.5E-6 Reference : 구성요소 기능의 HIA보고서 (CP04011-ETC-0169)	2.5E-6
Event 204	LEU의 위험측고장(LEU기능고장률 2.5E-6의 4배) Reference : 구성요소 기능의 HIA보고서 (CP04011-ETC-0169)	1E-23

표 4. ATP시스템의 심각도 분류에 따른 해당사고의 가정

심각도	등급	설 명	해당사고
치명적인 위험 (Catastrophic)	A	인명의 사상, 시스템의 손실 또는 심각한 환경상의 피해를 유발하는 위험	열차충돌
중대한 위험 (Critical)	B	심각한 인명의 상해, 직업상의 질병 및 중요한 시스템 또는 환경상의 피해를 초래하는 위험	인명사상
중요하지 않은 위험 (Marginal)	C	최소한의 상해, 직업상의 질병 및 최소한 시스템 또는 환경상의 피해를 초래하는 위험	비상제동
사소한 위험 (Insignificant)	D	최소한의 상해, 직업상의 질병보다는 작고, 최소한의 시스템 및 환경상의 피해보다 작은 영향을 초래하는 위험	상용제동
신뢰성관련 (Reliability Related)	R	인명이나 환경상에 피해를 발생하지 않으나 경제적 손실을 동반하는 위험	운행지연

표 5. 발생빈도 정량화를 위한 가정

이상요인	산출근거	적용빈도[h]
전원 및 신호이상	ATP시스템에 공급되는 전원이나 신호의 이상확률로써, 프로젝트의 범위를 벗어나는 사항에 대하여 일괄 적용한다.	1E-5
인적오류	사용자의 인적오류에 대한 발생빈도를 일괄 적용한다.	1E-4

표 6. ATP 지상장치 인터페이스 위험원 목록 사례

위험원 ID	위험원 설명	최종Risk F	S	R	사고 결과 (영향분석)	원 인	관련 장치	관련 구성 요소	안전대책	기타사항 (조치주체)	상태
HIF-WS002	유지보수 인력 보호실패	4	B	4B	인명 사상	1. 유지보수작업오류 2. 유지보수관리절차 실패	ATP 지상장치	지상 장치 유지 보수	1. 운영기관 관련규정 준수 2. 유지보수시 열차방호 및 작업구간 관리에 대한 절차구축	1.KR 2.KR	완료
HIF-WS003	장애 텔레그램 전송에 의한 열차 상용제동 발생	3	D	3D	상용 제동	1. 전원계통이상 2. 3현시에 대한 LD보드 고장 3. 5현시에 대한 LD보드 고장	ATP 지상장치	LEU의 신호기 상태 입력 (LD 보드)	1. LEU내부의 LD전원감시기능 포함 2. 신호기 비가용상태 안전측 현시시에 장애텔레그램 전송 3. 신호기 상태를 실시간 검지하여 고장시 장애 텔레그램 송신	1.BT 2.BT 3.BT	완료

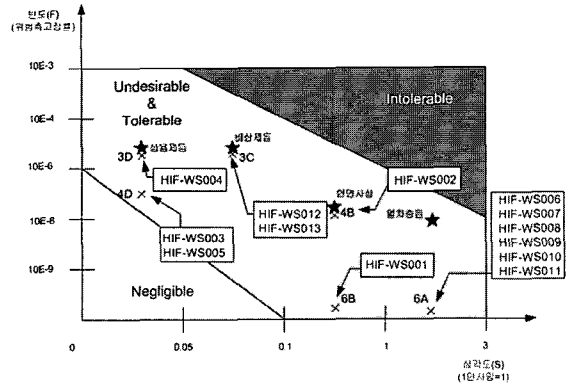


그림 4. ATP 차상신호시스템 지상인터페이스 안전성 입증

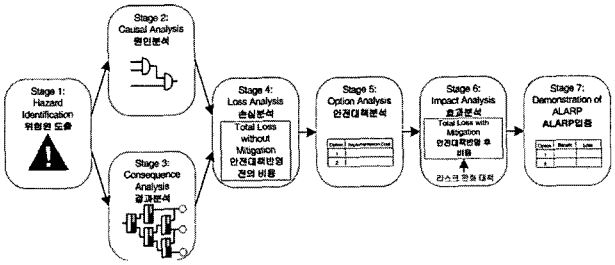


그림 5. ALARP이론을 적용한 영국철도 안전활동 7단계

3. ALARP이론을 적용한 안전입증 요구사항 검토

영국철도는 ALARP이론으로 안전성을 입증하기 위해 Yellow Book에서 그림 5와 같은 7단계의 안전성활동 절차를 제시하고 있다[8].

7단계 안전성활동 중 1단계와 2단계인 위험원도출 및 분석은 본 논문 2장의 국내 열차제어분야 위험도평가방식 안전활동의 HIA(Hazard Identification and Analysis)와 동일하게 수행되지만, 3단계의 결과분석과 4단계의 손실분석은 위험도 평가방식의 빈도분석과 약간의 차이점을 가지고 있다. 국내 위험도 평가방식에서는 위험도의 정량화를 위해 위험원의 발생빈도계산을 안전대책이 모두 반영된 시스템의 최종상태와 인적오류의 발생빈도에 대한 가정을 통해 시스템의 최종상태에 대한 위험도를 평가하는 반면, Yellow Book에서는 안전대책과 인적오류를 빈도분석과 별도로 이벤트트리(ETA, Event Tree Analysis)형태의 결과분석으로 분류하여 수행한다. 이러한 방식은 기존 철도사고의 손실비용을 기반으로 위험원으로 인한 사고의 손실분석을 수행한다.

3.1 Yellow Book활동체계에 따른 위험원 원인과 결과분석

ATP시스템 지상장치 인터페이스에 대한 안전성활동을

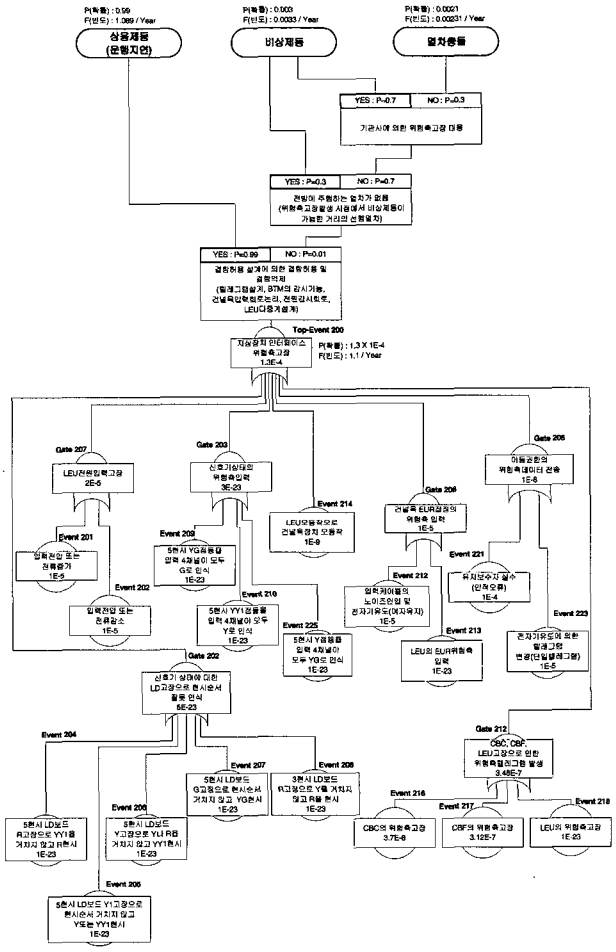


그림 6. 위험원의 원인과 결과분석 예(ATP 지상장치 IF)

Yellow Book에서 제시하는 7단계 활동으로 수행하면 그림 3의 결함트리분석결과는 안전활동의 3단계와 4단계에서 그림 6과 같이 변경된다. ALARP이론은 안전대책의 적용 전과 적용 후의 손실비용을 별도로 산출해야 한다. 그림 6은 FTA와 ETA를 통한 위험원의 원인 및 결과분석을 안전대책의 적용 전 시스템을 대상으로 계산한 결과이다.

3.2 ALARP이론 적용을 위한 손실분석 및 가정

ALARP이론을 만족하기 위한 손실분석을 위해서는 발생된 사고의 사회적 손실비용을 계산해야 한다. 현재 국내에는 위험원의 결과분석으로 도출된 운행지연(상용제동), 비상제동, 열차충돌에 대한 운영환경별 사회적 비용이 제시되어있지 않으므로, 영국의 손실비용을 가정으로 활용한다[9].

영국 철도에서는 그림 6과 같이 치명적 사상(Fatalities), 심각한 사상(Major Injurers), 경미한 사상(Minor injuries)에 대하여 각각의 비율을 식 (1)과 같이 정의하고 있다.

$$1\ \text{Fatality} = 10\ \text{Major Injury} = 200\ \text{Minor Injury} \quad (1)$$

따라서, 그림 6의 위험원 결과분석에 따른 상용제동, 비상제동, 열차충돌에 대하여 각각의 인명손실의 크기와 경제적 손실비용을 표 7과 같이 가정해야 한다.

각각의 사고결과는 가정에 의해 산출된 손실을 정량적인 경제적 가치로 환산하기 위해 그림 6에서 도출된 발생확률을 곱하여 연간손실비용을 표 8과 같이 산출한다[9].

표 7. 사고결과의 인명손실과 경제적손실의 가정 예[9]

사고결과	인명손실	경제적 손실
열차충돌	30 치명적 사상 50 심각한 사상 200 경미한 사상 **합계 36 치명적 사상**	720억원
비상제동	2 심각한 사상 6 경미한 사상 **합계 0.23 치명적 사상**	4.6억원
상용제동 (운행지연)	2 경미한 사상 **합계 0.01 치명적 사상**	0.2억원

*치명적사상 1건의 경제적 손실은 20억원(1백만 파운드)으로 가정

표 8. ATP지상장치 인터페이스관련 사고의 손실분석

사고결과	손실분석	연간손실비용
열차충돌	720억원 × 0.00231	1.663억원
비상제동	4.6억원 × 0.0033	0.015억원
상용제동 (운행지연)	0.2억원 × 1.089	0.217억원
	합 계	1.895억원

*그림 6의 발생빈도(F)는 ETA분석결과에 위험원 발생확률인 시간당고장률을 지상장치가 24시간 동작하므로, 년간 발생빈도로 변환하기 위해 8760배 하여 산출.

3.3 ALARP이론을 적용한 안전확보 입증

위험원으로 인한 사고의 손실분석까지 완료되면 그림 5의 5단계인 안전대책의 비용분석을 수행한다. 안전대책에 소요되는 비용은 설계비용 및 시스템변경비용 그리고 변경된 설계가 반영된 시스템의 유지보수비용을 모두 연간소요비용으로 산출하며, 이를 표 8의 안전대책반영 전 연간손실비용과 비교하면 표 9와 같다.

표 9의 안전대책 A를 적용한 후 년간 사고의 손실비용 0.11억원과, 안전대책이 적용된 시스템의 안전대책을 위한 연간 추가 유지보수비용 1억은 모두 본 논문의 가정으로써, 실제 안전대책이 수립된 이후에 소요비용이 정량적으로 산출되어야 한다.

따라서 표 9의 비교결과 대책A는 안전대책 적용 전후 사고손실비용의 차가 안전대책을 위한 투자비용보다 크므로 대책A는 반영되어야 하며, 대책B는 안전대책 적용 전후 사고손실비용의 차가 안전대책을 위한 투자비용보다 작으므로 반영하지 않는다[9]. ALARP이론은 표 9와 같이 예측할 수 있는 안전대책에 대하여 모두 손익을 계산하여 위험원목록과 함께 안전승인기관의 승인을 받아야 하며, 이때 모든 안전대책이 고려되었는가의 보장은 종합안전대책기술서의 절차를 토대로 승인기관이 활동의 건전성을 정성적으로 평가하여 시스템의 안전성확보를 승인한다.

3.4 ALARP의 적용방안 검토

안전성확보를 입증하기 위한 절대적인 방법은 현재까지 존재하지 않는다. 다만, 안전입증을 승인해야 하는 최종사용자는 안전성활동절차의 합리성과 객관성의 향상을 지향한다는 공통의 목표를 갖는다.

ALARP이론은 영국철도에서 반영되어 많은 수행실적과 검증을 거친 방법으로, 경제적 이득이라는 정량적 가치기준

표 9. ALARP이론을 적용한 안전입증 예(ATP지상장치 인터페이스)

	연간손실 (억원/년)	대책으로 인한 연간이득 (억)	대책을 위한 연간비용 (억원)	대책의 필요성
현재설계	1.895	-	-	-
대책 A	0.11[1)]	1.785[2)]	1.00[3)]	Yes
대책 B	1.55[1)]	0.345	1.00	No

1)은 안전대책을 적용한 후 손실분석에 의한 결과, 2)변경 전 손실비용에서 변경 후 손실비용을 제한 값, 3)변경에 소요되는 비용을 연간비용으로 환산한 값.

표 10. 위험도평가방식과 ALARP이론의 가정요인에 대한 분석

	위험도평가방식	ALARP이론
가정 요인	1. 허용할 수 있는 위험도 수준 2. 인명사상의 심각도에 대한 클래스 화 3. 인적오류에 대한 발생빈도 4. 자연재해의 발생빈도	1. 사고별 손실비용 2. 인적오류 3. 인명사상의 심각도에 대한 클래스 화
가정의 정당화	최종사용자 또는 독립안전 인증기관의 승인취득	과거 사고데이터의 연구로써 손실비용 및 발생빈도의 정량화와 지속적인 관리

을 사용함으로써, 안전성활동의 합리성에는 긍정적인 효과를 주는 것이 자명하다. 하지만 현재 국내철도의 열차제어시스템 안전성분야에 ALARP을 적용하기 위해서는 프로젝트 전주기에 걸쳐서 비용을 예측하고 평가하는 비용기반수명주기관리(LCC, Life Cycle Cost)기법 등이 먼저 전제되어야 한다.

또한, 표 10과 같이 위험도평가방식과 ALARP이론을 적용하기 위한 각각의 가정요인 항목비교에서와 같이 사고에 대한 사회적 손실비용, 인적오류에 대한 정량화기법 그리고 사고의 빈도와 심각도에 대한 기준의 확립이 무엇보다 중요하다. 이러한 가정요인의 최소화는 안전성활동의 객관성과 비례할 것이다.

4. 결 론

본 논문은 현재 국내철도 열차제어시스템분야에서 시스템 안전성입증을 위해 사용되는 위험도평가방법과 영국철도에서 적용하고 있는 ALARP이론을 ATP시스템 지상장치 인터페이스를 대상으로 각각 적용하였다. 동일한 대상에 대한 각각의 적용을 통해 위험도평가방식과 ALARP이론을 적용하기 위한 가정요인들을 도출하였으며, 사용된 가정의 최소화 및 정량화가 안전확보의 객관성과 비례함을 입증하였다. 다행히 도출된 가정요인들을 객관화하기 위해 국내 철도안전분야에서는 2004년 건설교통부 주관으로 철도종합안전기술개발사업을 수행 중에 있으므로[10], 본 논문에서 가정으로 사용된 여러 요인이 정량화 및 객관화될 것으로 판단되며, 특히 사고의 손실비용통계 및 위험도완화의 정량적 기준은 정보의 정확성과 객관성을 위해 영국의 경우와 같이 국가의 주도로 지속적으로 연구 및 관리되어야 한다.

참 고 문 헌

1. IEC62278 (2002), "Railway applications-Specification and demonstration of RAMS", pp.59-65.
2. 한국철도기술연구원 (2001), "철도신호제품에 대한 신뢰성과 안전성 검증기준 제정 연구"보고서.
3. Railtrack (2000), "Engineering safety Management Issue 3, Yellow Book 3", Chapter 8.
4. 한국철도기술연구원 (2005), "차상신호(ATP)시스템 구축사업의 RAMS활동계획서".
5. MIL-STD-882C (1993), "System Safety Program Requirements".
6. 한국철도기술연구원 (2006), "차상신호(ATP)시스템 구축사업의 위험원도출 및 분석보고서(지상장치 인터페이스)".
7. IEC61882 (2001), "Hazard and operability studies(HAZOP Studies) - Application guide".
8. Lloyd's Register Rail Limited/Atkins Rail Limited, "Engineering Safety Management Engineers' Overview, Module 3: Change Fundamentals", pp.11.
9. Lloyd's Register Rail Limited/Atkins Rail Limited, "Engineering Safety Management Engineers' Overview, Module 3: Change Fundamentals", pp.88.
10. 한국철도기술연구원 (2005), "철도사고 위험요인(PHA) 분석기술 개발 연구보고서".