2004년도 대한전기학회 하계학술대회 논문집 2004.7.14-16

전기적 위험요인에 대한 열차제어시스템의 예비위험요인분석

정의진*°, 김종기*, 신덕호*, 김백현*, 이종우*, 김양모**
*한국철도기술연구원, **충남대학교

Preliminary Hazard Analysis of the ATC System for Electrical Hazards

E. J. Joung*°, J. K. Kim*, D. H. Shin*, B. H. Kim*, J. W. Lee*, Y. M. Kim**
*KRRI(Korea Railroad Research Institute), **Chungnam National University

Abstract - *The system safety must be ensured* before customization. There was no specific requirement representing system safety in Korea until now. So we should draw safety requirements to guarantee system safety for the first time. In this paper, the hazard identification and analysis to derive the safety requirements on the train control system are carried out. To analyze hazard, we have to deduce system functions, identify related hazards, derive the effects of the hazards, analyze current risks, define the target risks of the system, and deduce the alternative plans to reduce the effects of the hazards. For the case study, Preliminary Hazard Analysis(PHA) of the Automatic Train Control(ATC) System for Electrical Hazards are carried out.

1. 서 론

모든 시스템에는 결함이 존재하며, 이러한 결함은 결함양상에 따라 random fault와 systematic fault의 두 가지로 구분할 수 있다. random fault는 예측할 수 없는 방식으로 일어나는 고장상황에 적용되며, 이러한 결함의 대부분은 노후화로 인해 야기된다. systematic fault는 설계 시 또는 제조 공정 중의 잘못으로 인하여 동일한 환경에서 같은 종류의 부품 또는 장치에서 똑같은 고장을 일으키는 형태의 고장상황에 적용된다. 따라서 systematic fault는 주로 동일 원인의 고장형태로 나타나며, 설계 중에 적용되거나 제조 과정 중에 적용된다. 철도시스템에서도 마찬가지로 고장을 분류할 수 있으며, 이러한 시스템의 결함 발생을 줄이고 시스템의 안전성을 관리하기 위해서는 시스템이 갖고 있는 위험요인을 파악하고 이를 정량적으로 분석하여 시스템에 맞는 요구사양을 제시할 필요성이 있다.

본 논문에서는 현재 철도연구원에서 개발 검토 중인 무선을 이용한 열차제어시스템의 위험요인 및 위험도 분석에 대하여 살펴보았다. 특히 전기적 위험요인에 의하여 장치나 인명에 해를 미치는 경우에 대하여 예비위험요인분석(Preliminary Hazard Analysis : PHA)을 실시한 예를 언급하였다. [1]-[4]

2. 열차제어시스템의 위험도 분석

시스템의 안전성을 확보하기 위한 첫 단계로 현 시스템의 위험도 수준을 알 필요가 있다. 즉 인명이나 장치에 손상을 일으킬 위험요인을 찾고 각각의 위험요인의 발생빈도와 심각도를 도출함으로써 현 시스템의 위험도를 알아보는 것이다. 그럼으로써 위험도가 높은 요인에 대해서는 적절한 대책을 제시함으로써 시스템 개발시나 운용시의 위험 상황을 줄여야 한다.

2.1 대상시스템의 구성 및 기능 분석

현재 철도연구원에서 개발 검토 중인 무선을 이용한 열차제어시스템은 자동열차제어기능, 종합운행제어기능, 무선통신기능 등이 있다. ATP/ATO 차상컴퓨터, 간격제어장치는 차상설비 기능인 자동열차제어 기능을 담당하고, 진로제어장치, 사령실 설비, 역설비는 지상설비 기능인 종합운행제어 기능을 수행한다. 또한 열차무선데이터전송장치에서는 지상과 차상간의 무선통신기능을 수행한다. 그림 1은 본 열차제어시스템의 구성을 나타낸 것이며, 표 1에서 각각의 기능에 대한 구성장치 및 내용을 정리하여 나타내었다.

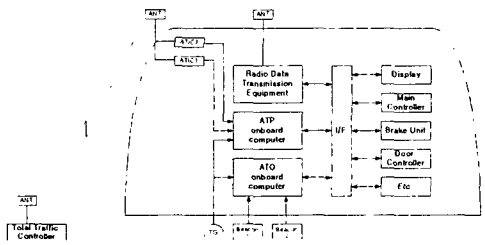

그림 1. 열차제어시스템의 구성도

표 1. 열차제어시스템의 기능

개발장치기능	구성장치	내 용
자동열차 제어기능 (차상설비기능)	ATP/ATO 차상컴퓨터	역 설비로부터 전송된 속도 지령과 속도 센서 정보 비교 지령속도 초과 운행시 브레이크 제어 지령을 브레이크에 전달
	간격제어장치	선행열차, 후속열차의 간격제어, 열차 안전운행 확보
종합운행 제어기능 (지상설비기능)	진로제어장치	연동장치에 의한 열차의 운행 진로 제어
	사령실 설비	열차운행제어, 열차운전감시 가능 수행
	역 설비	차상컴퓨터로 속도제어 지령 송신
무선통신기능	열차무선데이터 전송장치	무선을 이용한 자동열차제어기능 구축을 위한 데이터 전송 역 설비로부터의 속도제어 지령 등의 정보 수신

2.2 대상시스템의 위험요인 분석

시스템에 영향을 미쳐 인명이나 장치에 손상을 일으킬 수 있는 위험요인을 찾아 분석하는 단계로, 본 위험요인 분석에서는 위험요인의 발생빈도(표 2) 및 심각도(표 3)를 몇 단계로 나누고 이를 서로 조합하여 위험도 등급(표 4)을 만든다.

2.2.1 위험요인의 발생 빈도

위험요인 발생 빈도표는 철도신호시스템의 RAMS 관련 규격이나, 안전성 평가를 수행한 유사기관의 사례를 참조하게 되는데 이미 경량 및 중량 철도시스템의 안전성 평가 활동을 수행한 경험이 많은 영국의 Railtrack PLC의 분류 예를 참조하여 표 2에 위험요인 발생 빈도표를 제시하였다. 위험요인의 발생빈도는 발생 확률에

따라 5개의 단계로 나누었다. [5]

표 2. 위험요인의 발생 빈도

발생빈도	설 명	값
Frequent (A)	(자주 일어나는) 자주 발생하거나, 연속적으로 발생하는	$10^{-3} < X$
Probable (B)	(발생 가능성 있는) 장치의 수명기간동안 몇 차례 일어나는, 장치에서 자주 일어나는	$10^{-5} < X < 10^{-3}$
Occasional (C)	(우발적인) 장치 수명기간 중에 몇 차례 일어날 것 같은, 장치에서 몇 번 일어나는	$10^{-6} < X < 10^{-5}$
Remote (D)	(있을법하지 않은) 발생할 것 같지 않지만 장치 수명기간 중에 일어날 가능성이 있는, 장치에서 일어날 것 같지 않지만 일어날 것으로 예상할 수 있는	$10^{-9} < X < 10^{-6}$
Improbable (E)	(일어날 것 같지 않은) 발생할 것 같지 않은, 발생 가능성을 예상할 수 없는, 일어날 것 같지 않지만 장치에서 발생 가능한	$X < 10^{-9}$

2.2.2 위험요인의 심각도

현재 국영 철도의 경우, 철도를 이용하는 과정에서 부상 또는 사망한 경우에 보상 금액이 따로 책정되어 있지 않고 국가배상법, 민법 등 관계 법률 및 대법원 판례 등을 기준으로 배상금액을 개별적으로 산정하고 있다. 따라서 관련 법률 및 보험지급 기준 등을 참조하여 위험요인의 심각도를 표 3과 같이 정리하였다. 위험요인의 심각도는 4 단계로 나누었다.

표 3. 위험요인의 심각도

심각도	심각도의 정의	
	사람	장치
Catastrophic (1)	(파국적인) 치명상	현장이 손실되었거나 3억원 이상의 손실을 입는 경우
Critical (2)	(심각한) 중상, 직업병	7천만원에서 3억원 사이의 손실, 비용, 보수를 필요로 하는 중대한 시스템 손상
Marginal (3)	(경계에 있는) 경상 (응급조치만이 필요한 경미한 부상), 경미한 직업병	50만원에서 7천만원 사이의 손실, 비용, 보수를 필요로 하는 경미한 시스템 손상
Negligible (4)	(심각하지 않은) 경상보다 경미한 부상이나 직업병	50만원 이하의 최소한의 시스템 손상 보다 작은 사고일 경우

2.2.3 위험도 단계

위에서 제시한 위험요인의 발생빈도, 심각도를 조합하여 위험도 단계를 구성하는데 표 4에서는 위험도 구간을 명암을 주어 구분하였다. 명암이 가장 낮은 것부터 순서대로 Unacceptable (1, 2, 3, 4, 5, 7), Undesirable (6, 8, 9), Tolerable (10~16), Acceptable (17~20)의 4영역으로 할당하였다.

Unacceptable은 현재 위험요인이 존재한다는 것으로 최소한 Tolerable한 영역으로 위험도를 줄이도록 대책을 강구하여야 한다.

표 4. 심각도 빈도 및 위험도

발생 빈도		심각도			
		Catastrophic	Critical	Marginal	Negligible
		1	2	3	4
Frequent	A	1A (1)	2A (2)	3A (7)	4A (13)
Probable	B	1B (5)	2B (6)	3B (9)	4B (16)
Occational	C	1C (4)	2C (6)	3C (11)	4C (18)
Remote	D	1D (8)	2D (10)	3D (14)	4D (19)
Improbable	E	1E (12)	2E (15)	3E (17)	4E (20)

■ Unacceptable(받아들일 수 없는)
□ Undesirable(의도하지 않은): 영향력 있는 안전성 평가기관으로부터의 동의를 구함
□ Tolerable(허용 가능한): 영향력 있는 안전성 평가기관의 지침에 따라 받아들일 수 있음
□ Acceptable(받아들일 수 있는)

3. 대상시스템의 예비위험요인분석

3.1 대상시스템의 위험요인 분류

예비위험요인분석은 먼저 위험요인을 각 분야별로 분류하고, 각각의 위험요인에 대하여 위험요인 정의, 위험요인의 발생 원인 및 고장모드 도출, 위험상황 발생시의 영향 추정, 현재의 위험도와 도달해야만 하는 위험도 목표값의 도출, 목표값에 도달하기 위한 방안 및 그 결과의 순으로 구성되어 있다.

본 논문에서는 시스템의 안전성에 영향을 미칠 위험요인을 표 5와 같이 전기, 전자파 방사, 기계, 화학, 기타의 5가지로 분류하였다.

표 5. 열차제어시스템의 위험요인 분류

전기	전자파 방사	기계	화학	기타
500V 이상 고압	RF방사/고주파노	구동부	폭발성 물질	예기치 못한 동작
70V~500V고압	Laser/LED 방사	조작시	독성 물질	차량 충돌
대전류		접근시	자극성 물질	출입문 이상 작동
접지		날카로운 물체	화재	
정전기		접속시		

3.2 전기적 위험요인에 대한 대상시스템의 예비위험요인분석

전체 위험요인 중에서 전기적인 위험요인에 대하여 분석하여 보았다. 외국 DB중 "Virgin Operating Safety Records"의 1997년 5월 31일부터 2000년 1월 6일까지의 분석 데이터를 살펴보았다. 본 데이터에는 60 mph의 평균속도로 약 30,493,605 train mile의 운행시간 중 총 7건의 열차제어시스템의 고장이 발생하였는데 이를 참조하여 열차운행시간 당 약 1.38×10^{-5}의 고장발생확률이 있음을 알 수 있다. [6]

$$\text{운행시간} = \frac{30,463,605\text{mile}}{60\text{mile/hour}} = 5.08\times10^{5}\ \text{hour}$$

$$\text{고장 발생 확률} = \frac{\text{발생횟수}}{\text{열차 운행 시간}} = \frac{7\text{건}}{5.08\times10^{5}\ \text{hour}} = 1.38\times10^{-5}$$

위 결과로부터 전기적 위험요인에 의한 고장 발생 확률이 표 2의 B단계인 Probable(발생 가능성 있는)에 속함을 알 수 있다. 또한 전기적 위험요인에 의해 사람에게는 장시간의 입원 및 재활이 필요한 중상을 입힐 수 있으며, 유지보수를 필요로 하는 중대한 시스템 손상을 가져올 수 있기 때문에 심각도는 표 3의 2단계인 Critical(심각한)로 하였다. 표 6은 전기적인 위험요인으로 인명 및 장치에 영향을 줄 수 있는 상황에 대한 예비위험요인분석을 수행한 예를 나타낸 것이다.

4. 결론

본 논문은 현재 개발 검토 중인 무선을 이용한 열차제어시스템의 안전 요구사양을 작성하기 위한 위험요인 분석 및 위험도 분석 절차에 대하여 언급한 것으로 열차제어시스템의 발생 가능한 위험요인을 전기, 전자파 방사, 기계, 화학, 기타의 5개 부문으로 분류하고, 특히 전기적 위험요인에 대하여 예비위험요인분석을 수행한 예를 나타내었다. 본 분석은 시스템 설계 전에 수행하며, 제시된 안전대책 및 권고된 안전기법을 고려하여 시스템을 제작한 후 시험 및 검증 작업을 통하여 실제 위험도 목

표값에 도달했는지를 파악함으로써 안전성을 입증하게 된다. 본 논문은 안전 관리 활동의 기초 단계로 앞으로 많은 연구가 진행되어야 할 것이다.

[참 고 문 헌]

[1] IEC61508 parts 1-6, Functional safety of electrical /electronic/ programmable electronic safety-related system, March 1998.

[2] CENELEC EN50126, Railway application The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS) : March 2000.

[3] CENELEC prEN 50128, Railway Applications Software for Railway Control and Protection Systems : June 1997.

[4] CENELEC EN50129, Railway application Safety related electronic systems for signalling : April 2000

[5] Railtrack PLC, Engineering Safety Management issue 3, Vol. 1~2, 2000.

[6] Lloyd's Register, "Korea National Rail Safety Committee 19 to 23 May 2003 Safety Advisory Service Final Report", June 2003.

표 6. 전기적 위험요인에 대한 예비위험요인분석 예

1위험요인	500V 이상의 고압			
원인/고장모드	단락, 아크, 접촉사고			
영향	장치	장치에 큰 손상을 일으킴		
	사람	감전으로 인해 심각한 부상 발생		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 고압 접점부에 보호설비를 갖춘다. 2. 전기사고의 위험이 있는 모든 곳에 경고라벨을 붙인다. 3. 매뉴얼 및 유지보수 지침서에 경고 및 지시사항을 기재한다. 4. 경고 라벨에는 750V DC의 고압이 집전되어, 추진제어장치에 급전 증임을 나타내어야 하며, 경고 라벨은 전원 분배기함에 부착하고, 전원 분배기함으로의 접근은 제한한다. 또한 외함은 내부전압을 방전하기에 충분한 시간을 가지도록 구성하여야 한다. 5. 현장 직원에게 안전 교육을 실시하고, 유지보수 요원에게는 구두로 명령을 전한다.			
대책예상 결과	고압이 존재함을 유지보수원에게 경고하고, 보호설비와 연동함으로써 접촉사고를 방지한다.			

2위험요인	70V~500V의 고압			
원인/고장모드	낙뢰로 인한 막대한 전기 에너지의 흐름 전기회로의 단락 혹은 개방			
영향	장치	장치에 큰 손상을 일으킴		
	사람	감전으로 인해 심각한 부상 발생		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 가이드부에 적정 접지 및 본딩 처리를 한다. 2. 전기접점부에 보호장치를 둔다. 3. 전기적 위험이 있는 모든 곳에 경고 라벨을 붙인다. 4. 매뉴얼 및 유지보수 지침서에 경고 및 지시사항을 기재한다. 5. 추가로 접지 경로를 두기 위해 각각의 차량에 접지 슈를 둔다. 고장전류 검지장치가 시스템 견인 전원의 급전을 자동적으로 차단하도록 한다. 70V~500V 사이의 전압을 사용하는 기기를 최소화한다. 차량에서 100V DC를 사용하는 출입문제어장치 및 380V AC를 사용하는 냉방장치 및 220V AC를 사용하는 난방장치로의 접근을 제한한다. 출입문제어장치 및 냉난방장치로의 승객 접근을 통제하고, 장치에는 라벨을 붙여 운영요원들이 알 수 있도록 한다. 지상 신호설비도 220V AC 전원을 제외하고는 본 영역의 전압 범위 내 전원을 사용하여서는 안된다. 현장의 모든 장치는 사람의 임의 조작이 불가능하여야 한다. 6. 모든 도체부에는 덮개를 두며, 전원 분배기함에도 덮개를 두어 운영자의 예기치 않은 접촉을 막는다. 7. 현장 직원에게 안전 교육을 실시하고, 유지보수 요원에게는 구두로 명령을 전한다.			
대책예상 결과	전기장치로부터 감전에 노출될 위험을 최소화한다.			

3위험요인	대전류			
원인/고장모드	25A를 초과하는 전류에 접촉하거나 장치가 견딜 수 있는 한도를 초과하는 전류에 노출되는 경우			
영향	장치	차량에 큰 손상을 일으킴		
	사람	감전으로 인해 심각한 부상 발생		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 예기치 않은 접촉으로부터 보호하기 위해 보호장치를 구비한다. 2. 고압 접점부에 보호장치를 둔다. 3. 전기적 위험이 있는 곳에 경고 라벨을 붙인다. 4 매뉴얼 및 유지보수 지침서에 경고 및 지시사항을 기재한다. 5. 추진제어장치 및 전원 분배기 등 단락 전류가 흐를 위험이 있다고 생각되는 모든 곳에 퓨즈를 단다. 6. 추진제어장치 출력단에는 암 소켓을 사용하여 의도치 않은 감전 사고를 막는다. 대전류 전원부에는 퓨즈를 설치하고 추진제어장치 및 전원 분배기 등은 실드를 한다. 7. 추진제어장치를 구동시키기 위해 대전류를 사용한다는 경고 라벨을 유지보수 요원이 볼 수 있도록 하여야 한다. 8. 현장 직원에게 안전 교육을 실시하고, 유지보수 요원에게는 구두로 명령을 전한다.			
대책예상 결과	대전류에 접촉할 가능성을 줄인다.			

4위험요인	접지			
원인/고장모드	접지가 구성되어 있지 않은 경우			
영향	장치	단락으로 인해 장치에 큰 손상을 일으킴		
	사람	감전으로 인해 심각한 부상 발생		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 모든 도체에 적정 접지설비를 갖춘다. 2. 매뉴얼 및 유지보수 지침서에 경고 및 지시사항을 기재한다. 3. 추진제어기는 접지를 하여야 하며, 특히 누설 전류 귀환 경로 중에 의도치 않은 순환 전류를 억제하기 위하여 추진제어기 내부에 저항을 둔 접지 설비를 갖춘다. 선로변 제어기 또한 접지한다. 4. 현장 직원에게 안전 교육을 실시하고, 유지보수 요원에게는 구두로 명령을 전한다.			
대책예상 결과	적정 접지를 하여 잠재적인 단락위험 및 감전위험을 줄인다.			

5위험요인	정전기			
원인/고장모드	정전기에 민감한 장치를 접지를 하지 않고 만져 장치에 전기적 쇼크를 주는 경우			
영향	장치	차량에 고장을 발생시킴		
	사람	-		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 정전기에 민감한 부품이거나 장치라는 것을 표시한다. 2. 차량설비, 역설비, 유지보수장비의 적정 조작을 위해 접지부를 둔다. 3. 경고레벨이나 표식 등을 붙인다. 4. 매뉴얼 및 유지보수 지침서에 경고 및 지시사항을 기재한다. 5. 새로이 개발된 제품에 대하여 정전기 주의 마킹을 한다. 6. 정전기 접지 밴드를 추진제어장치에 설치하여 VME보드의 교체에 이용한다. 주기적으로 정전기 도체 매트 설치장소를 보수한다. 정전기에 민감한 H/W의 사용을 위해 기술자를 교육시킨다. 7. 정전기에 민감한 모든 하드웨어에 정전기 주의 마킹을 한다. 8. 현장 직원에게 안전 교육을 실시하고, 유지보수 요원에게는 구두로 명령을 전한다.			
대책예상 결과	정전기에 민감한 장치로의 예상치 않은 접촉의 가능성을 줄인다.			