論 文
53B-2-6

경량전철 열차제어시스템의 위험요인 분석

A Hazard Identification and Analysis for the Train Control System of Light Rail Transit

丁 義 鎭* · 金 良 模**
(Eui-Jin Joung · Yang-Mo Kim)

Abstract - Train control system in LRT (Light Rail Transit) is developed as a part of "Light Rail Transit System Development Project". But there was no specific requirement representing the system safety. Because system safety must be ensured before the customization, we applied the system to a officially recognized specific procedure, such as "A Guideline to Ensure the Safety of Train Control System in Korea" that was officially announced by KNR (Korea National Railroad) in 2001. We should draw system safety requirement to guarantee system safety for the first time. In this paper, the hazard identification and analysis to derive the safety requirement on LRT train control system are carried out following the KNR guideline. To analyze hazard, we have to deduce system functions, identify related hazards, derive the effects of the hazards, analyze current risk, define the target risk of the system, and deduce the alternative plans to reduce the effects of the hazards. After the hazard analysis following the upper procedure, 30 hazards are identified and analysed. Especially detailed analysis on train collision that is a main hazard of the train control system is specially carried out.

Key Words : Light rail transit(LRT), Hazard identification, Hazard analysis, Safety Integrity Level(SIL)

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 야기한다. systematic fault는 설계 시 또는 제조공정 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. 이 요구사양에는 시스템의 안전성 확보를 위해서 제조자들이 도달해야하는 기준을 제시할 필요가 있으며, 철도분야에서 특히 열차제어시스템에 대하여는 철도청 고시 "열차제어시스템 안전성확보 기술 권고안 (2001. 7. 20)"을 마련하여 시스템의 요구사항을 등급화하여 SIL(Safety Integrity Level)로서 제시하도록 하고 있다. SIL은 안전무결도를 나타내며, 시스템이 규정된 안전특성을 만족시키기 위해 요구되는 신뢰도를 표시하는 수치이다. SIL은 단계가 높으면 높을수록 시스템 안전 확보에 요구되는 정도가 높게 된다. 즉, SIL 4가 가장 높으며, 반면에 SIL 1은 가장 낮은 요구사양을 가진다. 또한 SIL 1에도 들지 않는 사항에 대하여는 SIL 0으로 둔다.

현재 유럽에서는 철도규격인 CENELEC의 EN50126, 50128, 50129에서 유럽철도의 안전성을 입증하는 절차 및 방법을 정의하고 있으며, 이를 국제 규격인 IEC화함으로써 유럽 실정에 맞춘 안전성 절차 및 규정을 국제화하려고 하고 있다. 국내에서도 철도청 고시인 "열차제어시스템 안전성확보 기술 권고 안"을 마련하여 철도시스템의 안전성 확보에 노력하고 있다.

따라서 본 논문에서는 "열차제어시스템 안전성 확보 기술 권고 안"의 안전성 인증체계에 대하여 살펴보고, 경량전철 열차제어시스템을 대상으로 위험요인 및 위험도 분석을 하였다. 특히 경량전철 열차제어시스템의 중요 기능 중 자동열차제어기능의 고장으로 인한 차량충돌 사건의 경우를 일례로 들어 서술하고자 한다. [1]-[4]

2. 열차제어시스템 안전성 확보 기술 권고 안의 안전성 인증 체계

철도시스템의 안전성을 확보하기 위하여 철도 선진국에서는 자국내 실정에 맞추어 안전성 인증 체계를 마련하여 운영하고 있다. 국내에서도 이에 발맞추어 철도시스템의 안전

* 正 會 員 : 韓國鐵道技術研究院 主任研究員
** 正 會 員 : 忠南大學校 電氣情報通信工學部 電氣工學專攻 敎授
接受日字 : 2003年 7月 18日
最終完了 : 2003年 11月 24日

성을 확보하기 위하여 안전성 인증 체계에 대한 연구가 이루어지고 있는 중이며, 그림 1은 현재 시행중인 열차제어시스템의 안전성 인증 체계를 나타낸 것이다. 그림 1에서 SRP(Safety Review Panel), SRG(Safety Review Group)는 사업주관부처로 철도청이나 건교부가 이에 해당한다. 기업체는 사양에 따라 제품을 개발하는 주체이며, ISA (Independent Safety Assessment)는 SRP, SRG의 요구사양에 따라 기업체의 안전성 업무가 제대로 수행하였는지를 독립적으로 평가하는 기관이다. [7]

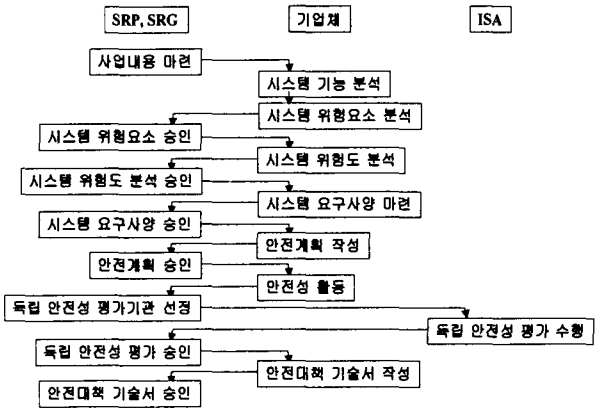

그림 1 철도시스템의 안전성 인증체계
Fig. 1 Safety certification process of railway system

다음은 본 논문에서 수행한 시스템 위험도 분석까지의 절차에 대하여 각 단계별로 수행하여야 할 업무를 부연하여 설명한 것이다.

① 사업내용 마련
- 안전성 확보 목적의 설정 단계로 장치의 개발이 목적인지 장비설치가 목적인지를 선정하고, 장치개발을 목적으로 하는 경우 개발하고자 하는 장치를 정의한다.
- 위험상황이 인명손실 또는 열차지연, 장치손상에 해당하는지 위험결과의 범위를 지정한다.

② 시스템 기능 분석
개발시스템의 특성 및 정의 등을 고려하여 기능을 분석한다.

③ 시스템 위험요소 분석
기능구현의 오류로 인한 영향을 분석하는 단계로 장치의 위험 요인을 분석. 이 과정이 PHA (Preliminary Hazard Identification : 예비 위험요인 정의) 이다.

④ 시스템 위험도 분석
기능구현 오류의 심각성 및 발생빈도를 살펴 장치의 위험도를 산정한다.
- ETA(Event Tree Analysis), FMEA(Failure Mode Effect Analysis) 등의 방법을 적용한다.
정량적으로 위험도를 산정하며, 이를 위해 사고데이터 등 체계적인 데이터 확보가 필요하다.
  * ETA : 기능오류로 인해 발생할 수 있는 위험요인 분류 - 위험요인 발생확률 산정에 중요
  * FMEA : 시스템 내의 잠재적 고장을 분석한 뒤 이로부터 발생 가능한 영향을 검토하는 분석방법

3. 개발중인 경량전철 시스템의 개요

경량전철시스템을 개발하기에 앞서 도시철도차량 표준사양을 만들고 설계 제작이 이루어졌으나, 시스템의 안전성과 관련하여서는 원론적인 사항만 언급했을 뿐 구체적인 안전성 분석은 이루어지지 않았다.

다음은 자동안내궤도용 고무차륜형식 대차를 갖는 직류 경량전철의 차량시스템 및 주요 구성품의 기능과 기술규격을 나타낸 표준사양을 정리하여 나타낸 것이다.

차량은 고무차륜형식으로 표준사양에서 차량편성은 동력대차와 부수대차를 포함하여 4량 혹은 6량 1편성으로 구성하도록 하고 있으나, 현재 시험차량으로 2량 고정 1편성으로 하고 있다. [8]-[9]

- 차량편성 : 2량 고정 1편성 (고무차륜 AGT)
- 안내방식 : 측방안내방식
- 분기방식 : 좌우가동분기방식
- 가선공칭전압 : 750V DC (변동범위 500V~900V DC)
- 계통최대전압 : 950V DC
- 제어회로전압 : 100V (변동범위 70V~110V DC)
- 냉난방장치전원 : 380V AC 60Hz (냉방), 220V AC 60Hz (난방)
- 급전방식 : 제3궤조방식
- 최고운행속도 : 60km/h
- 가속도 : 3.5km/h/s
- 감속도 : 3.5km/h/s(상용), 4.5km/h/s(비상)
- 속도제어방식 : 회생브레이크 병용 VVVF 인버터제어에 의한 가·감속 제어
- 브레이크방식 : 회생브레이크 병용 전기 지령식 공기브레이크
- 분기방식 : 좌우가동분기방식
- 편성열차의 1일 평균주행거리 : 400km 이상
- 최소운행시격 : 90초
- 왕복운행시간 : km당 3초의 예비시간
- 정차시간 : 정차역 당 최소 20초
- 운전방식 : 무인자동열차운전(본선), 수동운전(측선)

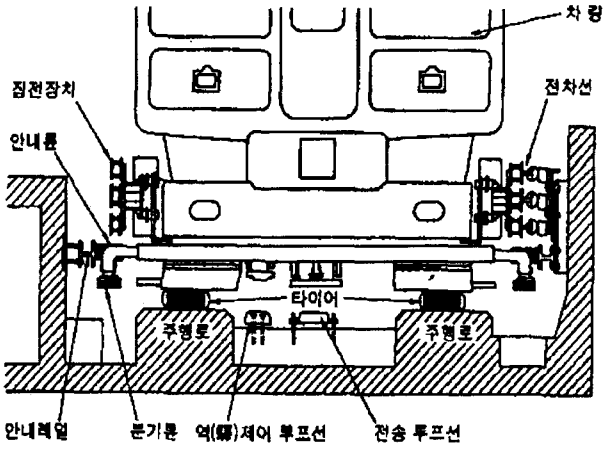

그림 2 경량전철 차량의 구성
Fig. 2 Structure of LRT vehicle system

4. 경량전철 열차제어시스템의 안전성 확보 절차

2장에서 언급한 안전성 인증체계를 적용하여 안전성 분석 예를 제시함으로써 경량전철 시스템의 안전성 확보방안에 대하여 논하고자 한다. 분석대상으로 현재 개발중인 고무차륜을 이용한 경량전철시스템을 대상으로 하였으나, 경량전철 시스템은 차량, 궤도, 전기, 열차제어분야가 함께 어우러져 있는 시스템으로 직접 분석하기에는 매우 큰 시스템이다. 따라서 본 논문에서는 경량전철시스템 중 열차제어시스템을 대상으로 위험요인을 분석하였다.

4.1 경량전철 열차제어시스템의 분석목적 (사업내용 마련)

분석 대상인 경량전철 열차제어시스템의 안전성 분석 목적은 자동열차제어장치, 종합운행제어관리장치, 무선통신장치 등의 장치 개발에 따른 안전성 확보에 있다. 본 개발 제품의 고장으로 인하여 초래될 위험결과로는 인명손실 및 열차손상, 장치손상 등이 해당된다.

4.2 경량전철 열차제어시스템의 구성 및 기능 분석 (시스템 기능 분석)

경량전철 열차제어시스템은 자동열차제어장치, 종합운행제어관리장치, 무선통신장치가 주요 구성장치로 자동열차제어 기능을 담당하는 ATO 차상컴퓨터, 간격제어장치, 진로제어장치와 종합운행제어관리기능을 담당하는 설비로 사령실 설비, 역 설비가 있다. 또한 무선통신기능을 수행하는 장치로 열차무선데이터 전송장치가 있으며, 부가적인 시스템으로 신호검사장치가 있다. 그림 3은 경량전철 열차제어시스템의 구성을 나타낸 것이며, 표 1에 각각의 기능에 대한 구성장치, 내용을 정리하여 나타내었다. [10]

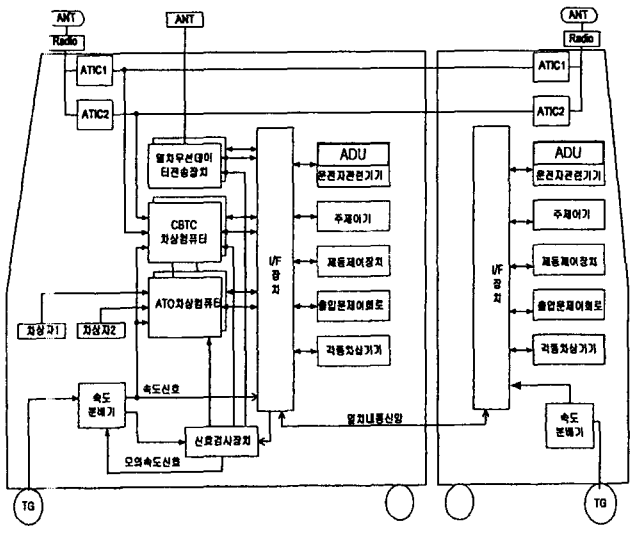

그림 3 경량전철 열차제어시스템의 구성도
Fig. 3 Diagram of LRT train control system

표 1 경량전철 열차제어시스템의 기능
Table 1 The function of train control system of LRT

개발장치기능	구성장치	내 용
자동열차제어 기능	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
	진로제어장치	연동장치에 의한 열차의 운행 진로 제어
종합운행제어 관리기능	사령실 설비	열차운행제어, 열차운전감시 기능 수행
	역 설비	차상컴퓨터로 속도제어 지령 송신
무선통신기능	열차무선데이터 전송장치	무선을 이용한 자동열차제어기능 구축을 위한 데이터 전송 기능 역 설비로부터의 속도제어 지령 등의 정보 수신

4.3 경량전철 열차제어시스템의 위험요인 분석 (시스템 위험요소 분석)

기능 구현의 오류로 인한 영향을 분석하는 단계로 장치의 위험요인을 분석한다. 본 위험요인 분석에서는 위험요인 발생빈도(표 2) 및 위험요인의 심각도(표 3)를 몇 가지 단계로 나누고 서로 조합하여 위험도 단계(표 4)를 만든다.

4.3.1 위험요인의 발생 빈도

표 2 위험요인의 발생 빈도
Table 2 Hazard probability

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	$10^{-6} < X < 10^{-5}$
Improbable (E)	(일어날 것 같지 않은) 발생할 것 같지 않은, 발생 가능성을 예상할 수 없는, 일어날 것 같지 않지만 장치에서 발생 가능한	$X < 10^{-9}$

위험요인 발생 빈도표는 시스템 운용 주체에서 만들게 되며, 기존의 열차제어시스템 관련 규격이나, 유사 시스템의 운행경험이 있는 기관의 사례를 참조하여 구성하거나 시스템 운용 주체가 임의로 정하게 된다. 현재 한국에서는 경량전철의 운행실적이 없으며, 관련 규격의 경우 전체 철도시스템을 대상으로 하기 때문에 다루기에 범위가 넓다. 따라서 실제 운행실적이 있는 기관을 참조하였는데 경량 및 중량

철도시스템의 운행경험이 많은 영국의 Railtrack PLC의 분류 예를 참조하여 표 2에 위험요인의 발생 빈도표로 제시하였다. 위험요인의 발생빈도는 발생 확률에 따라 5개의 단계로 나누었다. [5]

4.3.2 위험요인의 심각도

표 3 위험요인의 심각도
Table 3 Hazard severity

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)	(경제에 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
- 중상 : 팔, 다리, 눈이 하나 또는 둘 다 잃는 부상, 장시간의 입원 및 재활 치료를 필요로 함 - 경상 : 베거나 골절을 당하거나, 긁히거나 상처가 난 부상, 입원은 필요치 않음 - 중대한 시스템 손상 : 30분 이상의 시스템 중단을 일으키거나, 차량이 안전한 운행을 할 수 없거나, 비용 대비 유지보수 값을 넘어서는 고장 - 경미한 시스템 고장 : 30분 이하의 시스템 중단을 일으키거나, 안전 운행은 할 수 있지만 육안으로 찌그러져 보이게 하는 고장		

위험요인의 심각도 또한 운용주체의 결정 및 관련 규격을 참조하여 정하게 된다. 현재 국영 철도의 경우 철도를 이용하는 과정에서 부상 또는 사망한 경우에 보상 금액이 따로 책정되어 있지 않고 국가배상법, 민법 등 관계법률 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 4개 단계로 나누었다.

4.3.3 위험도 단계

위에서 제시한 위험요인의 빈도, 심각도를 조합하여 위험도 단계를 구성하였다. 표 4에서 왼쪽 상단으로 갈수록 위험도가 높은 상황을 나타내며, 오른쪽 하단으로 갈수록 위험하지 않음을 나타낸다.

여기에서는 위험도 구간을 명암을 주어 구분하였는데 명암이 가장 낮은 것부터 순서대로 Unacceptable(1, 2, 3, 4, 5, 7), Undesirable(6, 8, 9), Tolerable(10~16), Acceptable(17~20)의 4가지 영역으로 할당한다. 가장 명암이 낮은 Unacceptable은 현재 위험요인이 존재한다는 것으로 최소한 두 번째 명암이 밝은 영역 Tolerable로 위험도를 줄이도록 대책을 강구하여야 한다.

표 4 심각도 빈도 및 위험도
Table 4 Hazard probability, severity, and risk

발생 빈도		심각도			
		Catastrophic	Critical	Marginal	Negligible
		1	2	3	4
Frequent	A	1A (1)	2A (3)	3A (5)	4A (13)
Probable	B	1B (2)	2B (5)	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)

4.3.4. 경량전철 열차제어시스템의 위험요인 분석

위험도 분석 형식은 먼저 위험요인을 각 분야별로 분류하고, 각각의 위험요인에 대하여 위험요인 정의, 위험요인의 발생 원인 및 고장모드 도출, 위험상황 발생시의 영향 추정, 현재의 위험도와 도달해야만 하는 목표 위험도 값의 도출, 목표값에 도달하기 위한 방안 및 그 결과의 순으로 되어 있다. [5]-[6]

본 논문에서는 시스템의 안전성에 영향을 미칠 위험요인(Hazard)을 표 5와 같이 전기, 전자파 방사, 기계, 화학, 기타의 5가지로 분류하였고 이를 또한 운영, 유지보수, 시험별로 위험요인을 분류하였다. 또한 경량전철 열차제어시스템의 위험요인 및 위험도를 표 6에 총괄 정리하여 나타내었고, 앞에서 언급한 위험도 분석 형식을 표 7과 같이 작성하여 위험요인을 분석하였다.

표 5 경량전철 열차제어시스템의 위험요인 및 고장모드
Table 5 Hazard identification and failure mode of LRT train control system

- 전기적 요인

위험요인	위험요인 설명	원인/고장모드
500V 이상 고압	고압으로 장치에 심각한 손상을 일으킬 수 있음	단락, 아크, 접촉사고
70V~500V 고압	전원장치로부터 전기적 쇼크에 노출될 수 있음	낙뢰로 인한 막대한 전기 에너지의 흐름 전기회로의 단락 혹은 개방
대전류	전기회로에 25A를 초과하는 전류의 흐름이나 장치가 견딜 수 있는 한도를 초과하는 전류가 흐름	25A를 초과하는 전류에 접촉하거나 장치가 견딜 수 있는 한도를 초과하는 전류에 노출될 수 있다.
접지	접지 불량	접지가 구성되어 있지 않음
정전기	잘못된 조작이나 이송중의 잘못으로 정전기에 민감한 장치를 손상시킴	정전기에 민감한 장치를 접지하지 않고 만져 장치에 전기적 쇼크를 줄 수 있다.

- 전자파적 요인

위험요인	위험요인 설명	원인/고장모드
RF방사/ 고주파 노출	고주파 노출로 인해 사람에게 화상을 일으킴	위치검지용 마커 등 차량에서 방사되는 고주파 에너지가 설계치를 초과하여 주변 사람에 화상을 일으킬 수 있음
Laser/ LED 방사	레이저/LED의 끝단 접촉으로 인한 화상	에너지가 설계 값을 초과하여 눈이나 다른 신체부위에 화상을 입힐 수 있음

- 기계적 요인

위험요인	위험요인 설명	원인/고장모드
구동부	구동부에 의해 사람이 철과상을 입음	냉방용 팬 등
	출입문 동작 중에 사람이 다친다.	문이 닫힐 때 목이 끼이거나 문이 잘못 열려 승객이나 보수원이 다칠 수 있다.
조작시	한사람이 들고 다닐 수 있는 중량(15kg)보다 무거운 물체에 의한 사고	중량 초과 물체
접근시	유지보수하기에 너무 좁아 이로 인해 발생하는 사고위험	낙하하여 손상을 주는 장치이거나 장치에 쇼트를 일으키는 장치
날카로운 물체	작업중 또는 차량 주위를 순회할 때 긁히거나 다침	차량이나 장치의 날카로운 모서리나 코너
접속시	잘못 연결하여 전압이 초과하여 장치나 사람이 손상을 입을 수 있다.	잘못된 접속부에 전원라인이나 데이터 라인을 연결

- 화학적 요인

위험요인	위험요인 설명	원인/고장모드
폭발성 물질	밧데리의 폭발	밧데리 과충전
독성 물질	밧데리에서 독성 기체가 만들어진다.	밧데리 내부에서의 화학 반응
부극성 물질	밧데리가 차체에 부식을 일으킨다.	밧데리 내에서의 화학반응
화재	차량 내에서 발생한 화재위험	전기시스템과 관련된 화재 승객의 발화성 물질 소지에 따른 화재
	차량 내의 유독가스	전기시스템과 관련된 화재 승객의 발화성 물질 소지에 따른 화재

- 기타 요인

위험요인	위험요인 설명	원인/고장모드
예기치 못한 동작	승객이 차량 옆이나 내부시설에 부딪혀 부상을 입는다.	승객이 승하차하는 동안 차량의 이상 움직임이나 역에서의 오출발로 인해 승객이 차량 내의 출입문이나 벽면에 부딪히거나 선로상의 역이나 차량 바닥에 넘어진다.
	승객이 차량 내부설비에 부딪쳐서 부상을 입는다.	예기치 않은 급가속이나 갑작스러운 차량의 작동으로 승객이 차내에서 넘어지거나 머리나 목을 다친다.
차량 충돌	차량이 다른 차량과 충돌	차량 위치를 모르는 상태에서, 차량에 전원이 투입되어 움직임으로써 서로 충돌 발생 : 차량 충돌
	차량과 차량간의 충돌	자동제어 하에서 다른 열차와 충돌
		수동제어상태에서 다른 열차와 충돌
		부주의하게 운행 중에 다른 차량과 충돌
		규정속도로 운행하지 않아 다른 열차와 충돌
		선로변 제어장치와 통신하지 못하여 다른 열차와 충돌
		차량이 잘못된 진로로 진입하여 운행
		차량이 잘못하여 분리되었을 경우
출입문 이상 작동	승객이 차량 밖으로 떨어져 선로 집전선로에 감전된다.	출입문이 잘못 열려 승객이 잘못 하차함으로써 선로 상에 떨어진다. 차량이 운행중 출입문이 열린 경우 차량이 선로 상에 일시 정차하고 있는 중에 출입문을 열 경우
	승객이 차량내에 갇힌다.	선로 상에 차량이 멈추어 있으면서 전원공급이 두절된 경우, 출입문이 안 열림

4.4 경량전철 열차제어시스템의 위험도 분석 결과 (시스템 위험도 분석)

표 6에서 ☑ 표식은 잠재적 위험요인이 존재한다는 의미이며, □는 위험요인이 존재하지 않음을 의미한다. 그 외 심각도, 빈도, 초기값, 목표값에서 나오는 알파벳 및 숫자는 표 2, 3, 4의 해당 위험요인의 발생빈도, 심각도, 위험도를 나타낸 것이다.

표 6 경량전철 열차제어시스템의 위험요인 및 위험도

Table 6 Hazard identification and risk of LRT train control system

세부분야	운영	심각도	빈도	초기값	목표값	유지보수	심각도	빈도	초기값	목표값	시험	심각도	빈도	초기값	목표값
전기적 요인															
500V 초과						V	1	B	2	12	V	1	B	2	12
70 ~ 500V						V	1	B	2	12	V	1	B	2	12
30 ~ 70V															
시험부 300V 초과															
대전류						V	1	B	2	12	V	1	B	2	12
접지	V	1	B	2	12	V	1	B	2	12	V	1	B	2	12
정전기						V	2	B	5	15	V	2	B	5	15
전자파적 요인															
X선															
RF방사	V	3	A	7	17	V	3	A	7	17	V	3	A	7	17
방사능 물질															
Laser/LED	V	3	A	7	17	V	3	A	7	17	V	3	A	7	17

세부분야 (계속)	위험	심각도	빈도	초기값	목표값	유지 보수	심각도	빈도	초기값	목표값	시험	심각도	빈도	초기값	목표값
기계적 요인															
구동부	V	2	B	5	15	V	2	B	5	15	V	2	B	5	15
조작시						V	3	B	9	17					
접근시						V	3	B	9	17	V	3	B	9	17
날카로운 물체	V	3	A	7	17	V	3	A	7	17	V	3	A	7	17
접속시						V	2	A	3	15	V	2	A	3	15
CRT 파열															
열															
기압															
유체															
스팀															
화학적 요인															
폭발성 물질	V	2	A	3	15	V	2	A	3	15	V	2	A	3	15
독성 물질						V	3	A	7	17					
자극성 물질						V	3	A	7	17					
화재	V	2	A	3	15	V	2	A	3	15	V	2	A	3	15
발암물질															
오존 파괴 물질															
기타 요인															
예상치 못한 동작	V	3	B	9	17	V	3	B	9	17	V	3	B	9	17
차량 충돌	V	2	B	5	15	V	2	B	5	15	V	2	B	5	15
출입문 이상 작동	V	2	B	5	15	V	2	B	5	15	V	2	B	5	15
구조적인 상태															

5. 열차 충돌을 고려한 위험요인 분석

전체 위험요인 중에서 경량전철 열차제어시스템의 가장 중요한 기능인 자동열차제어기능의 고장으로 인한 차량충돌 사건에 대하여 분석하여 보았다.

국내에는 경량전철의 운행경험이 없기 때문에 사고와 관련된 데이터가 축적되어 있지 않다. 따라서 외국의 사고 사례를 살펴보았는데 본 논문에서는 "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 운행 시간 중 총 8건의 열차제어시스템의 고장이 발생하였는데 이를 참조하여 열차 운행시간 당 약 1.57×10^{-5}의 고장발생확률이 있음을 알 수 있다. [11]

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

$$\text{고장 발생 확률} = \frac{\text{발생횟수}}{\text{열차 운행 시간}} = \frac{8\text{건}}{5.08\times10^{5}\ \text{hour}} = 1.57\times10^{-5}$$

위 결과로부터 열차제어시스템의 고장 발생 확률은 표 2의 B단계인 Probable(발생 가능성 있는)에 속함을 알 수 있다. 또한 열차 충돌이 발생할 경우 장시간의 입원 및 재활이 필요한 중상을 입을 수 있으며, 30분 이상 시스템 중단을 일으키거나 차량이 안전한 운행을 할 수 없기 때문에 심각도는 표 3의 2단계인 Critical(심각한)로 하였다. 표 7은 경량전철 열차제어시스템의 자동열차제어기능의 고장으로 인한 차량충돌 사건에 대한 분석 내용을 나타낸 것이다.

표 7 차량이 충돌할 경우의 경량전철 열차제어시스템 위험요인 분석

Table 7 *Hazard identification of LRT train control system in the condition of train collision*

1. 위험요인	차량이 다른 차량과 충돌			
원인/고장모드	차량 위치를 모르는 상태에서, 차량에 전원이 투입되어 움직임으로써 서로 충돌 발생 : 차량 충돌			
영향	장치	차량 및 선로에 심한 손상을 일으킴		
	사람	승객에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 시스템상의 모든 차량 위치가 확인될 때까지 열차를 정지시킨다. 일단 ATC가 모든 차량 위치를 인식하면 ATC를 구동한다. 2. 모든 차량이 선로 상에 있을 때에는 ATP 제어 하에서 움직이도록 한다. 3. 승객을 태우기 전에 모든 차량의 제동시스템, 견인시스템, 연동장치, ATP시스템이 완전하게 기능을 수행하고 있는지를 점검한다. 4. 현장 직원에게 안전 교육을 하고 현장 유지보수 요원에게는 구두로 명령을 하달하며 공식적으로 기술 매뉴얼에 기입한다.			
대책예상 결과	차량이 충돌한 가능성을 최소화한다.			

2. 위험요인	차량과 차량간의 충돌			
원인/고장모드	부주의하게 운행 중에 다른 차량과 충돌			
영향	장치	차량에 심각한 손상을 일으킴		
	사람	사람에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. ATC가 ATP의 고장을 확인하고 이중계 시스템으로 제어권을 넘기도록 설계한다. 2. 단순조작으로 차량이 잘못 운행할 가능성을 막도록 설계한다. 3. 부주의 운행에서도 연동장치가 여전히 동작하도록 설계한다.			
대책예상 결과	부주의 운행의 가능성을 가능성을 최소화한다.			

3. 위험요인	차량과 차량간의 충돌			
원인/고장모드	자동제어 하에서 다른 열차와 충돌			
영향	장치	차량에 심각한 손상을 일으킴		
	사람	승객에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. ATP의 고장이 발생하면 소프트웨어의 실행을 중지한다. Watchdog 프로세서로 시스템의 움직임을 체크하고 이상시 비상제동을 걸어 시스템을 안전한 상태로 둔다. 이중계 시스템은 시스템 가용도를 높일 뿐 안전성에는 관여하지 않는다. 2. ATC 시스템이 고장을 검출하자마자 차량을 목적지로 이동시키고, 승객을 하차시키고, 차량을 운행시키지 않도록 한다. 3. 차량 위치를 감시하고, 선로변 제어기에 각각의 열차 위치를 기록한다. 만약 차량의 위치를 확인하지 못할 경우 후속 열차를 정지시킨다. 4. 차량 센서의 고장은 중앙사령실에 알린다. 중앙사령실은 역으로 차량을 견인하기 위해서 차량의 목적지를 바꿀 수 있다. 5. 모든 차량의 위치 기록을 잃게 되는 경우 후속열차를 정지시킨다. 6. 현장 직원에게 안전 교육을 하고 현장 유지보수 요원에게는 구두로 명령을 하달하며 공식적으로 기술 매뉴얼에 기입한다.			
대책예상 결과	차량을 손상을 최소화하거나, ATC 장치의 고장으로 인한 영향을 최소화한다.			

4 위험요인	차량과 차량간의 충돌			
원 I/고장모드	수동제어상태에서 다른 열차와 충돌			
영향	장치	차량에 심각한 손상을 일으킴		
	사람	사람에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. ATC가 ATP의 고장을 확인하고 이중계 시스템으로 제어권을 넘기도록 설계한다. 2. ATP 제어로 수동운전 중의 차량을 이동하는 절차를 마련한다. 3. 수동운전 중에는 최대 속도를 제한한다. 4. 적정 매뉴얼 및 유지보수 지침서에 관련 경고 및 지시사항을 기재한다.			
대 예상 결과	수동제어의 영향을 최소화한다.			

5. 위험요인	차량과 차량간의 충돌			
원 I/고장모드	규정속도로 운행하지 않아 다른 열차와 충돌			
영향	장치	차량에 심각한 손상을 일으킴		
	사람	사람에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. ATP의 고장이 검지되면 운행을 중지한다. Watchdog 프로세서에 의해 비상제동을 걸어서 시스템은 안전한 상태로 된다. 이중계 시스템은 시스템의 가용도를 높일 뿐 안전성이 요구되지 않는다. 2. 단일차량 혹은 모든 차량이 구간 최고 허용속도를 초과하여 운행할 때, 인간의 개입없이 즉시 열차를 멈추게 하기 위해서 fail-safe한 과속 방지장치를 설계한다. 3. 차량이 운행하고 있는 실제 속도를 검지하여, 제어 속도와 비교하고 적절한 제어를 가하거나 열차를 멈추게 할 수 있도록 하기 위해 최대 속도를 시스템 맵에서 설정하고, ATP가 과속인지를 교차 비교하여 차량이 과속으로 주행할 때 ATP가 비상 제동을 건다. 4. ATP는 차량의 실제 속도를 검지하기 위해서 바퀴에 엔코더를 이용한다. 이 속도는 ATC에 전해지며, ATC는 실제 속도와 시스템 맵에 있는 선로 제한 속도를 비교하여 차량 속도를 제어한다. 만약 ATC가 차량 제어에 실패한다면 (즉 차량이 과속할 경우) ATP는 차량에 비상제동을 건다. 5. 차량 속도를 감시하고 선로변 제어기 및 중앙 사령실로부터 차량을 서행하거나 정지하라는 명령을 받을 수 있도록 한다. 6. 중앙 사령실로는 차량 속도가 제공되며, 만약 필요하다면 중앙 사령실이 차량을 비상제동 시킬 수 있어야 한다.			
대책 예상 결과	과속으로 인한 영향을 최소화한다.			

6. 위험요인	차량과 차량간의 충돌			
원인 고장모드	차량이 잘못하여 분리되었을 경우			
영향	장치	차량에 심각한 손상을 일으킴		
	사람	사람에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 지속적으로 차량 분리 여부를 검지할 수 있도록 한다. 2. 15m/h까지 지속적인 속도 제어를 한다. 3. 안전설비를 사용한다. 4. 열차가 분리되었다는 것이 검지되는 즉시 두 차량 모두 자동적으로 비상제동을 체결한다.			
대책 예상 결과	고장이 발생할 경우 비상제동을 인가함으로써 차량분리로 인한 영향을 최소화한다.			

7. 위험요인	차량과 차량간의 충돌			
원인/고장모드	선로변 제어장치와 통신하지 못하여 다른 열차와 충돌			
영향	장치	차량에 심각한 손상을 일으킴		
	사람	사람에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 통신시스템의 고장을 상쇄토록 하기 위해 선로변장치 및 자동열차제어장치를 이중계로 한다. 2. ATC는 ATP의 고장을 확인하고 이중계 시스템으로 제어권을 넘기도록 설계한다. 이중계 시스템은 시스템 가용도를 높일 뿐 안전성이 요구되지는 않는다. 3. ATP는 선로변 및 차량 설비를 이용하여 통신 고장을 검지한다. 만약 많은 통신 에러가 발생할 경우, 데이터 통신이 실패한 것으로 간주한다. 4. 선로변 장치와의 통신 고장을 검지할 수 있도록 한다. 5. 데이터 통신이 실패하면 ATP가 자동적으로 차량을 정지시키도록 한다.			
대책예상 결과	통신 고장의 영향을 최소화한다.			

8 위험요인	차량과 차량간의 충돌			
원인/고장모드	차량이 잘못된 진로로 진입하여 운행			
영향	장치	차량에 심각한 손상을 일으킴		
	사람	사람에게 심각한 부상을 일으킴		
위험도	초기값	2B (5)	목표값	2E (15)
대책	1. 모든 차량은 운행 방향을 검지할 수 있도록 한다. 2. 차량이 잘못 진입한 구간의 모든 열차를 자동적으로 멈추게 하여야 한다. 3. ATP는 연속적으로 위치를 검지하고 시스템내의 모든 차량의 이동을 검지한다. 만약 차량이 예상치 않은 방향으로 50cm 이상 움직일 경우 ATP는 위험 상황으로 보고 차량에 비상제동을 체결한다. 4. ATP의 안전거리 유지 규칙을 지키지 못한 차량에 대하여 비상제동을 건다. ATC가 잘못 운행하고 있는 차량의 후속 차량에 대하여 안전하게 정차하도록 한다. 또한 중앙사령실에서는 선로 상의 전원을 차단함으로써 모든 차량을 정지시키며, 모든 열차에 정지 명령이 표시된다. 5. ATP가 잘못된 진로로의 운행 검지 등 위험 상황을 중앙사령실로 알려 경고를 보내면, 이 경우 중앙사령실에서는 위험상황발생 경고를 발하고 적절한 조치를 취한다.			
대책예상 결과	충돌 영향뿐만 아니라 차량이 잘못 진입할 가능성을 최소화 한다.			

6. 결 론

철도청 고시 "열차제어시스템 안전성확보 기술 권고 안(2001. 7. 20)"의 안전성 기술지침에 대한 소개 및 안전성 확보 절차에 대하여 살펴보았다. 개발 시스템의 안전성을 확보하기 위해서는 개발하려는 시스템 각각의 기능에 대하여 어느 정도 안전성을 확보해야 한다는 안전성 요구사양(Safety Requirement)을 제시하여야 한다. 여기에서 어느 정도라는 기준을 제시하기 위해서는 시스템의 기능 분석을 거쳐 개발하려는 기능의 고장원인 및 그 결과를 제시한 위험요인 분석을 하고 각각의 위험요인의 발생빈도와 심각도를 도출하여 위험도를 제시하여야 한다. 이와 같이 각각의 위험요인에 대하여 위험도를 제시한 안전성 요구사양이 도출되면, 제품 개발 당사자는 각각의 기능을 구현하기 위한 모

듈 구성 및 모듈별로 고장발생 확률을 할당하여 시스템의 안전성을 확보하기 위한 계획을 세운 후(Safety Plan) 제품을 실제로 개발하는 안전성 활동을 수행하여 시스템의 안전성을 확보하게 된다.

본 논문은 현재 개발 진행 중인 경량전철 열차제어시스템을 대상으로 안전성 요구사양을 작성하기 위한 위험요인 분석 및 위험도를 제시하였다. 전체 경량전철 열차제어시스템의 발생 가능한 위험요인 30개를 전기, 전자파 방사, 기계, 화학, 기타의 5개 부문으로 분류하고, 각각의 위험요인에 대하여 위험도를 제시하였다. 위험도를 제시하기 위해서는 사건 발생빈도와 심각도를 먼저 고려하여야 하는데, 발생빈도를 5개 단계로 심각도를 4개 단계로 나누어 관리하였으며, 경량전철 열차제어시스템의 중요 기능 중 자동열차제어기능의 고장으로 인한 차량충돌 사건의 경우를 일례로 들어 자세히 서술하였다.

본래 안전성 확보 기술 권고안에 따르면 안전성 요구사양에 맞추어 장치 설계를 하는 안전계획 단계에서 장치의 위험도를 고려하여 모듈별로 SIL을 할당하여 제작하여야 하는데 "열차제어시스템 안전성확보 기술 권고 안"이 발의되기 이전에 이미 설계가 완료되어 차량은 제작 완료되고 단품시험, 종합시험 및 시운전 시험을 기다리고 있다. 이 경우 안전성을 해치는 설계오류나 미처 생각지 못한 사항이 발견되어 설계변경을 하여야 할 경우, 조치가 어려운 것이 문제라고 할 수 있다. 단, 현재 개발중인 시스템이 상용 시스템이라기 보다는 시험 차량임을 감안이여 정확한 시험으로 안전에 위해를 가할 요인을 더 많이 도출함으로써 경량전철 열차제어시스템의 안전성 확보에 노력하여야 할 것이다.

참 고 문 헌

[1] International Electrotechnical Commission, 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) Issue : March 2000.

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

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

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

[6] Raythyon system company, "Phase II Demonstration PRT Project Safety Compliance Assessment Report for the Personal Rapid Transit System", September 1998.

[7] 철도청, 고시 "열차제어시스템 안전성확보 기술 권고안", 2001. 7. 20

[8] 백남욱 외, 철도기술총서, 골든벨, pp.207-517, 2003. 4.

[9] 건교부, 도시철도법 관련 시행규정 (도시철도차량 표준사양), 건교부, pp.121-159, 2001. 3.

[10] 최규형 외, "신호제어시스템엔지니어링" 경량전철시스템기술개발 사업연구보고서, 4차년도, pp.9-11, 2003. 1.

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

[12] 정의진 외, "철도신호시스템의 정량적 분석 기법을 통한 SIL 도출방안 검토", 대한전기학회 하계학술대회 논문집, pp.1303-1305, 2003. 7

[13] 정의진 외, "안전무결도 도출을 위한 정량적 분석기법 고찰", 한국철도학회 춘계학술대회논문집, pp.511-516, 2003. 5.

저 자 소 개

정 의 진 (丁 義 鎭)

1971년 1월 9일생. 1993년 충남대학교 전기공학과 졸업. 1995년 동 대학원 전기공학과 졸업(석사). 1995년~현재 한국철도기술연구원 주임연구원

Tel : (031) 460-5081, Fax : (031) 460-5459

E-mail : ejjoung@krri.re.kr

김 양 모 (金 良 模)

1950년 3월 29일생. 1973년 서울대학교 전자공학과 졸업. 1986년 동경대학교 대학원 전자공학과 졸업(공박). 1979년~현재 충남대학교 공과대학 전기정보통신공학부 전기공학전공 교수

Tel : (042) 821-5657, Fax : (042) 823-7970

E-mail : ymkim@ee.cnu.ac.kr