공항철도의 기전시스템에 대한 안전성 활동 소개
Introduction of Safety Activities for Electrical and Mechanical System in Airport Railroad

이창환* 임성수** 신석균***
Lee, Chang Hwan Lim, Sung Soo Shin, Seok Kyun

ABSTRACT

In this paper, the results of safety activities for Airport Railroad are introduced according to CENELEC standards. The procedures of safety activity were redefined as 6 phases such as Requirement Analysis phase, Design phase, Manufacture phase, Installation phase, Test & Commissioning phase and Operation phase to ensure the coincidence with 14 phases recommended in CENELEC standard. And the safety activities were implemented in the aspect of the overall E&M system level and in the aspect of each system level for 6 sub-systems consisting of that E&M system to ensure the safety for Airport Railroad using the general methodology such as FMECA.

1. 서론

공항철도는 서울 도심지에서 공항을 이용하는 승객을 위해 서울역에서 인천국제공항역까지 연결되는 철도를 건설 및 운영하게 되며, 일반열차와 직통열차의 2종류로 운영된다. 총 2단계로 수행되는 공사는 2001년 4월에 착공하여, 2006년 3월에 준공되는 1단계(인천국제공항역~김포공항역)구간과 2009년 12월 준공예정인 2단계(김포공항역~서울역)구간으로 나누어 진행되고 있다. 또한, 공항철도는 국내철도 분야에서 최초로 진행된 대규모 민자투자 사업으로써, 민간투자사들이 중심이 되어 설립된 운영회사는 2단계 준공 후 시설물을 정부에 인도하고, 30년간의 운영권을 가지는 BTO(Build-Transfer-Operate) 방식을 채택하고 있다.

공항철도의 특수성을 감안할 때, 가장 중요한 요소는 최종 목적지인 도심에서 인천국제공항역까지 운행되는 열차의 정시성 확보 및 전체 철도시스템의 안전성 확보이다. 정해진 열차운행 다이아에 따라 정확한 시간에 운행되기 위한 열차 정시성의 확보는 전체 철도시스템의 가용성을 극대화함으로써 이루어질 수 있다. 이러한 가용성은 해당 철도시스템의 신뢰성과 유지보수성의 지속적인 관리를 통하여 확보가능하다. 그러나, 철도시스템과 같이 기능고장의 발생으로 인해 대형사고를 초래할 수 있는 시스템의 경우에, 단순히 시스템의 고유 신뢰성 향상만을 고려해서는 안되며, 시스템의 설계 단계에서부터 안전성을 반드시 고려하여야 한다. 이러한 안전성 개념을 체계적으로 도입하기 위해서 1990년대 중반부터 철도의 신호분야를 중심으로 유럽 규격이 제정되었으며, 점차로 철도시스템 전체로 확대 적용되고 있는 실정이다. 최근에는 철도시스템의 안전성과 관련한 유럽 규격이 국제 표준규격으로 확대 적용되고 있으며, 국내에서도 철도안전법을 통해 철도시스템의 구축시 안전성 분석을 실시하도록 권고하고 있다.

* 책임저자, 회원, 공항철도(주) 기술본부 과장
E-mail : leech@arex.or.kr
TEL : (032) 745-7204 FAX : (032) 745-7905
** 회원, 공항철도(주) 기술본부 부장
*** 비회원, 광운대학교 정보제어공학과 박사과정

하지만, 국내에서는 일부 시스템에 한정하여 안전성 분석 활동이 수행되어 왔으며, 철도 기전 시스템의 전반에 대하여 수명 주기 즉, 설계 단계부터 운영 단계에 걸쳐 체계적으로 이루어진 사례가 없다. 따라서, 본 논문에서는 국제 규격인 CENELEC에서 제시하는 안전성 활동을 적용하고 있는 공항철도의 체계적인 안전성 활동 절차 및 결과를 소개하고자 한다. 안전성 활동의 절차는 CENELEC에서 제시하는 14단계의 시스템 수명 주기를 공항철도 사업에 적합하도록 6단계로 재정의하였으며, 공항철도에 도입되는 기전 시스템의 6개 분야 즉 차량, 신호, 통신, 송변전, 전차선, 플랫폼 스크린도어에 대한 안전성 활동을 위하여 고장 유형 및 영향에 따른 치명도 분석 기법을 적용하여 실시하였다.

2. 기전 시스템의 안전성 계약 사항

공항철도에 적용되는 기전 시스템은 알스톰, 유코레일, 로템으로 구성되는 IKFC(Incheon Korean French Consortium)와 2002년 8월에 계약이 체결되었으며, 본 계약사항 중에 기전 시스템의 안전성과 관련된 사항을 발췌하면 다음과 같다.

2.1 정의와 적용 범위

안전성 활동은 기전 시스템이 영업 운행시 제품의 고장으로 인해 야기될 수 있는 상해와 사고를 줄이기 위함이다. 단, 천재지변이나 테러와 같은 자의적인 행위들은 본 고려 대상에서 제외한다.

기전 시스템의 공급자는 기전 시스템의 안전성이 발주자가 허용할 수 있는 수준으로 설계, 시험, 시운전, 운영 및 유지 관리됨을 입증하기 위한 안전성 관련 문서들과 기전시스템 안전성 관리 계획서를 작성하고 관리하여야 한다.

2.2 기전 시스템의 안전성 관리 계획

기전 시스템의 공급자는 기전 시스템의 안전성 관리 계획서를 발주자에게 승인용으로 제출하여야 한다. 기전 시스템의 안전성 관리 계획서는 사업 수행 동안 시스템 안전성의 관리를 위한 원칙들을 상세히 서술하여야 한다. 안전성 관리의 절차와 관련된 최신 규격(예를 들면, EN50126, EN50128, EN50129)의 사항을 고려하여 작성되어야 한다.

본 계획서에는 최소한 다음의 사항들이 포함되어야 한다.

- 안전성 정책의 정의
- 안전성을 이행하고, 평가하기 위한 활동사항
- 안전성 활동의 실행과 입증을 지원하는 조직 구성
- 안전성 활동의 산출물 항목

기전 시스템의 안전성 관리 계획서는 개별적인 하부 시스템 (즉, 차량, 신호, 통신, 전력공급 및 전차선, 스크린 도어)에서 수립되는 기전 하부시스템 안전성 계획서를 요구한다.

기전 시스템의 안전성 관리 계획서는 발주자 안전성 계획에 의거하여 작성되어야 한다. 필요한 경우, 사업 수행 동안 수정되고 갱신되어야 한다.

2.3 기술적 요구사항

승객, 직원과 장비의 안전성은 가장 중요한 사안이다. 완성된 기전 시스템은 운영과 유지관리에 있어서 안전하여야 한다.

예비 위험원 분석은 사업 초기 단계에 수립되어야 한다. 본 분석의 목적은 기전 시스템의 엔지니어링과 더불어 전개되고 이행되는 기술적 요구사항들에 대한 발주자의 승인을 득하기 위함이다.

본 요구사항들은 비교 항목에 대해서 기존의 한국 철도시스템과 동등하거나 보다 향상된 안전성 수준을 갖춘 기전 시스템을 공급하기 위해 기존에 검증된 산업규격 실무에 근거하여야 한다.

안전성 활동은 예비 위험원 분석시 도출되고, 합의된 기술적 요구사항들이 전개되고, 이행됨을 보증하기 위해서 사업 수행과 더불어 상세하게 전개되어야 한다.

안전성 활동의 절차를 추진하는 방법론들이 안전성 계획서에 기술되어야 한다. 분석들은 안전상 가장 치명적인 항목들과 적절하다면 기존 항목들로부터의 적용성에 초점을 두어야 한다.

3. 안전성 활동 사항

3.1 요구사항 단계

기전 시스템에 대한 안전성 분석을 위해서 기전 시스템의 안전성 관리 계획과 각 하부 시스템에 대한 안전성 관리 계획을 수립한다. 수립된 안전성 관리 계획에 포함되는 주요 내용은 다음과 같다.

- 안전성 정책
- 안전성 활동 조직
- 안전성 활동 사항 및 산출물

3.1.1 안전성 정책

기전 시스템에 대한 안전성 정책의 주요내용은 다음과 같다.

- 기전 시스템의 안전성이 허용 수준으로 설계, 시험, 시운전, 운영 및 유지관리 됨을 입증하기 위해, 안전성 관리 계획을 수립하고, 이에 따라 활동하고 문서화 한다.
- 안전성 요구사항은 비교 항목에 대해서 기존의 한국 철도시스템과 동등하거나 보다 향상된 안전성 수준을 갖춘 기전 시스템을 공급하기 위해 기존에 검증된 산업규격 실무에 근거한다.

3.1.2 안전성 활동 조직

기전 시스템에 대한 안전성을 확보하기 위하여, 운영사와 공급사를 중심으로 그림 1과 같이 안전성 활동 조직을 구성하여 안전성 활동을 추진하였다.

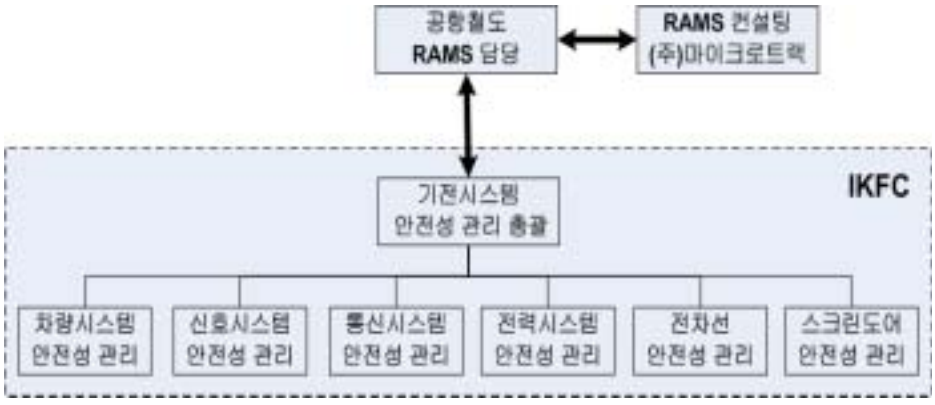

그림 1. 안전성 활동 조직

3.1.3 안전성 활동 사항 및 산출물

안전성 활동은 CENELEC에서 권고하는 14단계의 수명 주기를 공항철도의 사업 공정에 맞게 6단계로 재정의하여 수행하였다. 표 1은 사업 단계별로 수행되는 안전성 활동 사항을 나타내며, 그림 2는 안전성 활동을 통한 산출물의 내용과 흐름을 보여준다.

표 1. 단계별 안전성 활동사항

번 호	수명 주기	주요 활동	상세 내용
1	요구사항 분석 단계	안전성 분석 계획 수립	· 안전성 활동조직 구성 · 안전성 정책 및 목표수립 · 안전성 분석 절차 수립
2	설계 단계	예비 위험원 분석	· 기전 시스템 주요 위험원 규명
		시스템/하부시스템 위험원 분석	· 시스템 위험원 분석 · 하부시스템 위험원 분석
4	제작 단계	인터페이스 위험원 분석	· 시스템간 인터페이스 위험원 분석 · 하부시스템 내 인터페이스 위험원 분석
	설치 단계		
5	시운전 단계	안전성 입증 시험	· 위험원 제거 및 완화 조치 입증 시험 · 안전성 목표 준수 입증 시험
6	영업 운전 단계	안전성 최종 보고	· 안전성 입증 시험 결과 · 안전성 분석 활동 정리

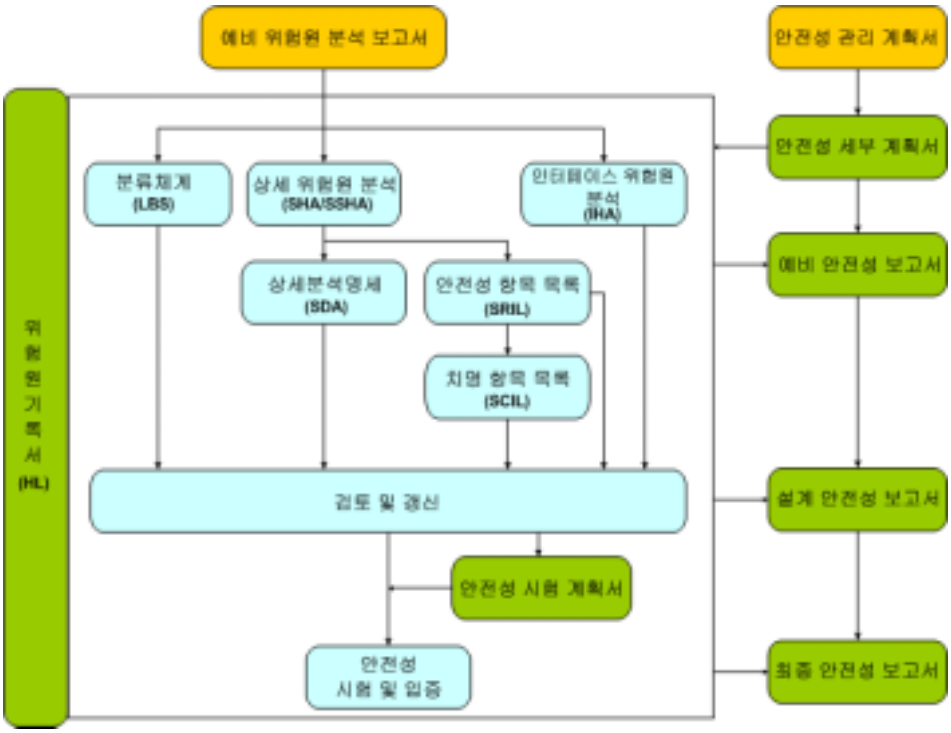

그림 2. 안전성 활동 산출물

3.2 설계 단계

1) 예비 위험원 분석

시스템의 안전성은 위험원의 심각도(Severity) 수준과 발생빈도(Frequency)의 조합에 의해 위험도(Risk) 수준이 결정되며, 안전성 분석에 적용된 심각도와 발생빈도는 표 2와 표 3과 같이 정의하였다.

표 2. 심각도 수준 정의

심각도 수준	등급	인명 및 환경 피해 정도
재난 수준	I	· 다수의 사망자 또는 중상자 · 심각한 환경 훼손 · 집단적 사고 형태
위급 수준	II	· 단일 사망자 또는 중상자 · 주요한 환경 훼손 · 개별적 사고 형태
보통 수준	III	· 부상자 · 주요한 환경 훼손
경미 수준	IV	· 경미한 인명 및 환경 피해

표 3. 발생빈도 수준 정의

발생빈도 수준	등급	정 의
상시 발생	A	일일 기준으로 연속적인 발생
자주 발생	B	한달 기준으로 수차례 발생
가끔 발생	C	년간 기준으로 수차례 발생
드문 발생	D	수명 주기 동안 수차례 발생
거의 없는 발생	E	낮은 확률의 이례적인 발생
지극히 발생 안함	F	발생하지 않는 것으로 가정

정의된 심각도 수준과 발생빈도 수준을 조합하여, 기전 시스템의 위험도 수준을 표 4와 같이 정의하였다. 위험도 수준은 안전성 분석을 위해 정량적인 지표로 사용되며, 시스템 설계 및 구현에서 도출되는 위험원의 허용 수준을 결정하기 위해 표 5와 같이 기준을 정의하였다.

표 4. 위험도 수준 정의

수 준		심각도 수준			
		I	II	III	IV
발생빈도 수준	A	I	I	I	T
	B	I	U	U	T
	C	I	U	T	N
	D	U	T	N	N
	E	U	T	N	N
	F	T	N	N	N

표 5. 위험도 허용 수준 정의

위험도 분류	정 의
I (허용 불가)	해당 위험도 수준에서 반드시 완화되어야 함.
U (바람직못함)	해당 위험도 수준에서 안전성 정책과 부합하다면 허용이 가능하지만, 반드시 위험도 완화 과정의 검토가 요구됨.
T (허용 가능)	해당 위험도 수준에서 안전성 정책과 부합하다면 허용이 가능하며, 경우에 따라 위험도 완화 과정의 검토가 필요함.
N (무시할만함)	해당 위험도 수준에서 허용이 가능함.

또한, 기전 시스템에 대한 전반적인 안전성의 기준을 수립하기 위하여, 표 6과 같이 발생 가능한 주요 위험원을 분류하고, 해당 심각도 수준을 정의하였다.

표 7은 예비 위험원 분석 결과의 예를 보여준다.

표 6. 주요 위험원 정의

고유번호	잠재사고 분류	심각도 수준
00	모든 사고	I
01	열차 충돌	I
02	열차 탈선	I
03	화재 및 질식	I
04	승객 대피	I
05	범람	I
06	환경 침해	II
07	승객 추락	II
08	승객이 물체에 끼임	II
09	고정물체 또는 이동물체와 충돌	II
10	화상 및 감전	II
11	기타 침해	III

표 7. 예비 위험원 분석 예

번호	안전성 요구사항	분야	기입증시스템 및 참조규격	잠재사고 No.	치명도
1	비상제동시스템은 정상운전에서 점착조건과 모든 구배에서 설계최고속도의 범위에서도 안전 운전을 확보하도록 설계되어야 한다.	차량	KNR#1, SMSC #2,3,4 SMRT #5,6,7,8	01	I
2	스크린도어는 운영조건에서 발생되는 최대압력을 견딜 수 있도록 설계되어야 한다.	스크린 도어	강도계산서	07	II
3	일반 전원의 정전시에 주요 통신장비에 대하여 백업 전원 공급이 이루어져야 한다.	통신	부산2호선	04	I

2) 분류 체계(LBS: Logistic Breakdown Structure) 수립

기전 시스템을 구성하는 하위 기능품에 대한 안전성 분석을 위하여 체계적으로 분류되었으며, 표 8은 통신 시스템의 분류 체계에 대한 예를 보여준다.

표 8. 통신시스템 분류체계 예

ID-SS	하부시스템	ID-E	장 치	ID-LRU	구성품
1	DTS	1.1	Main ADM	1.1.1	STM-1 O/E Converter
				1.1.2	STM-1 ADM
				1.1.3	Control Part
				1.1.4	Power Supply Unit

3) 시스템 및 하부 시스템 위험원 분석

시스템 및 하부 시스템 수준에 대한 위험원 분석은 고장 유형 및 영향에 따른 치명도 분석(FMECA: Failure Modes, Effects and Criticality Analsysis)기법을 적용하여 실시하였다. 상향 전개식 분석을 위해, 분류 체계의 하위 기능품부터 분석을 실시하였고, 해당 기능품의 고장 발생시 예측되는 고장 특성을 분석하였다. 또한, 예비 위험원 분석에서 정의된 위험도 등급을 적용하여, 허용 가능한 수준으로의 위험 완화 대책을 설계 및 운영 규정에 반영하도록 권고하였다. 표 9는 차량 시스템에 대한 위험원 분석 결과 예를 나타낸다.

표 9. 차량시스템 위험원 분석 예

분석 항목		고장유형	고장원인	고장 영향		심각도	빈도	위험도	위험 완화 대책
기능품	주요기능			차량시스템	기전시스템				
대차 답면 제동장치	답면 제동을 통하여 제동력을 공급해주는 기계적 인터페이스 제공	요구제동력 제공 실패	제동 패드의 과도한 마모	충돌	중대사고	I	F	T	1. 대차별 다중 제동패드 설계 2. 적합한 예방정비 설정 3. 비상제동시 기술사양에 부합하는 최소 제동거리 확보 설계
TCMS	열차 주요장치의 감시 및 제어 수행	감시 기능 상실	중앙처리 장치 고장	기타 침해	기타 침해	Ⅲ	F	N	1. 정기적인 예방정비 실시 2. 이중계 설계

3.3 제작 및 설치 단계

설계 단계에서 수행된 시스템 및 하부시스템 위험원 분석을 근거로 하여, 시스템을 구성하는 하부시스템간의 인터페이스상에서 발생 가능한 위험원을 도출하였다. 위험원 분석 방법은 고장유형 및 영향에 따른 치명도 분석(FMECA)방법을 적용하였다. 표 10은 신호 하부시스템간의 인터페이스상에서 발생 가능한 위험원 분석 예를 나타낸다.

표 10. 신호시스템 인터페이스 위험원 분석 예

항목	기능	고장 유형	직접 영향	위험상황	잠재사고	안전성 요구사항	심각도	빈도	위험도
궤도회로 & 연동장치 & 지상ATC	열차점유검지 및 열차동작감시	열차점유 상태가 전송되지 않음	궤도회로 불량으로 이전 궤도회로 비점유상태로 유지	열차동작을 검지하지 못함	충돌	1. 연동장치와 지상ATC는 각 메시지의 수신상태에 대한 허가를 확인해야함. 2. 운행 허용가능상태에서 어떠한 데이터도 송신되어서는 안됨.	I	F	T
		궤도회로 상태의 반응이 느림	열차점유임에도 불구하고 비점유로 판단	열차동작을 검지하지 못함	충돌	연동장치와 지상ATC는 각 메시지의 임시적인 허가를 보장해야 함. 만약 허가가 완료되었다면, 지상ATC는 제한된 상태에서 입력값을 확인해야 함	I	F	T
		궤도회로 상태가 부적합한 시점에서 비점유상태라고 전송	열차점유임에도 불구하고 부적합한 시점에서 비점유로 판단	열차동작이 연속적으로 검지되지 못함	충돌	연동장치와 지상ATC는 각 메시지의 수신상태에 대한 허가를 확인해야 함. 운행 허용가능상태에서 어떠한 데이터도 송신되어서는 안됨.	I	F	T

3.4 시운전 단계

시운전 단계에서 실시되는 안전성 입증 시험은 요구사항 분석 단계, 설계 단계 그리고 제작 및 설치 단계에서 수행된 안전성 분석 결과를 바탕으로, 초기에 수립된 안전성 목표에 부합되었는지를 검증하는 활동이다. 단계별로 수행된 안전성 분석 결과에 따라 규명된 위험원들이 설계 변경을 통하여 안전성 목표를 달성하였는지 또는 설계 변경을 통해서도 위험도 완화가 이루어지지 않은 위험원들에 대해서는 운영 규정에 반영하여 허용 가능 수준으로 완화가 되었는지를 검증한다.
표 11은 스크린도어 시스템에 대한 안전성 입증 항목의 예를 보여준다.

표 11. 스크린 도어 시스템 안전성 입증 항목 예

Ref	대상	도출원	안전성 요구사항	입증 방법
1	도어 모듈	SHA	스크린 도어는 승객의 끼임이나 부상이 발생되지 않도록 닫혀야 한다. (장애물 감지 장치와 2단 닫힘 구조)	현장 시험 실시
		SHA	정기적인 유지보수가 요구된다.	운영 및 유지관리 매뉴얼 반영
		SHA	다음의 하중 조건을 지탱할 수 있어야 한다. -풍압 : 270kgf/m^2 -승객혼잡하중 : 980 N/m	강도 보증 계산서 작성

3.5 위험원 기록서 관리

설계 단계에서부터 제작 및 설치 단계에 이르기까지 안전성 분석 활동을 통해 도출된 모든 위험원들은 위험원 기록서(Hazard Log)를 통해 관리하였다. 도출된 위험원들은 설계 변경이나 운영 규정으로의 반영을 통하여, 영업 운행이 시작되기 전에 위험원을 제거하거나 허용 가능 수준으로 완화 조치한다. 또한, 모든 위험원들은 고유번호를 부여하여 안전성 입증 활동시에 추적성이 용이하도록 하였다.

그림 3은 위험원 기록서에 수록되는 단계별 분석 결과의 흐름을 나타내며, 표 12는 차량시스템의 위험원 기록서의 작성 예를 보여준다.

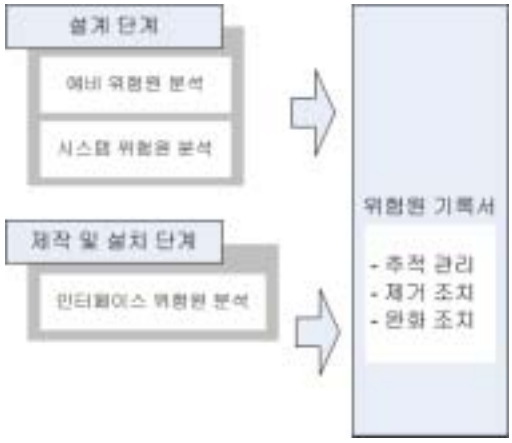

그림 3. 위험원 기록서 관리

표 12. 차량 시스템 위험원 기록서 예

관리 번호	등록일	근거	안전성 요구사항	단계	심각도	잠재 위험	안전성 완화대책	완화 근거	안전성 입증 여부
1	2006. 3.16	PHA	대차 프레임은 충분한 강도를 견딜 수 있도록 설계되어야 한다.	설계	I	탈선/ 전복	1. 피로시험 실시 2. 주행시험 실시	1. 강도계산서 2. 시험보고서	완료

4. 결 론

본 논문에서는 공항철도의 기전시스템에 적용되는 안전성 활동을 소개하였다. 본 활동은 국제 규격인 CENELEC을 근거로 하여 실시되었으며, 시스템 수명 주기는 공항철도 사업에 적합하도록 6단계로 재정의하여 수행하였다. 수명 주기 동안에 개별 시스템 자체에서 예측되는 위험원 뿐만 아니라, 시스템 간의

인터페이스 측면에서 예측되는 위험원도 도출하였다. 또한, 각 단계에서 도출된 위험원들에 대하여 요구사항 분석 단계에서 정의된 안전성 목표에 부합하도록 위험원 제거 및 완화 조치를 수행하였으며, 위험원 기록서를 통해 영업운행 전까지 안전성 입증 과정을 추적 관리할 수 있도록 하였다.

현재 공항철도는 기전 시스템에 대한 시운전을 수행 중에 있으며, 이전 단계에서 도출된 모든 위험원들에 대한 안전성 입증 시험을 실시할 계획이다. 그러나, 복잡한 철도시스템의 특성상 설계 및 제작 단계에서 예측하지 못한 위험원들이 운영 단계에서 유발할 수도 있다.

이를 보완코자 공항철도에서는 자체적으로 고장 보고, 분석 및 조치 체계(FRACAS: Failure Reporting, Analysis & Corrective Action System)를 적용하여, 운영 단계에서 발생될 수 있는 기전시스템의 고장 및 위험원들을 지속적으로 관리함으써 신뢰성과 안전성을 확보할 계획이다.

참고문헌

1. Incheon International Airport Railroad Co. Ltd and Incheon Korean French Consortium- INCHEON INTERNATIONAL AIRPORT RAILROAD FACILITIES-Exhibits A, B, C and D.
2. EN50126, Railways applications- The specification and demonstration of Reliability, Availability, Maintainablility and Safety (RAMS), 1999.
3. EN50128, Railway applications- Software for railway control and protection systems, 2001.
4. EN50129, Railway applications- Safety related systems for signalling, 2002.