

한국형 틸팅열차 ATP장치 예비위험원분석에 관한 연구

A Study on the PHA of ATP Equipment for the Korean Tilting Train

신덕호†
Shin, Ducko

백종현*
Baek, Jong-Hyen

이강미**
Lee, Kang-Mi

김용규***
Kim, Yong-Kyu

ABSTRACT

In this paper, we derive the hazard which is a criterion of safety assurance by PHA for the ATP equipped in Korea Tilting Train. The ATP onboard equipment in Korea Tilting Train was introduced as ETCS Level 1(which is ETCS specification). Also, the ATP trackside equipment was introduced as a ETCS SRS(System Requirement Specification) 2.2.2 and it has a target for commercial operation in 2009 late. In IEC 62278(EN50126), it recommend of PHA to derive a hazard of target system in concept establishment step and estimate if it can control as a tolerable level and then derive safety case to control the hazard by lifecycle. Therefore, we indicate the hazard using criterion of safety assurance by PHA using FRS(Functional Requirement Specification) 5.0. which is a upper criterion than SRS. The hazard of ATP onboard equipment derived in Korea Tilting Train will be able to use as ATP functional hazards of unified onboard equipment in G7 which is a multiple unit and preliminary hazards of ATP onboard equipment in NEL driven by Korail.

1. 서 론

본 논문은 한국형 틸팅열차에 설치된 자동열차방호(ATP, Automatic Train Protection)장치를 대상으로 예비위험원분석(PHA, Preliminary Hazard Analysis)을 실시하여 안전확보의 기준이되는 대표위험원을 도출한다.

한국형 틸팅열차의 ATP차상장치는 유럽철도열차제어시스템 규격인 ETCS Level 1을 기준으로 도입되었다. 또한 국내의 ATP지상장치는 ETCS(European Train Control System) 시스템요구사항서(SRS, System Requirement Specification) 버전 2.2.2를 기준으로 도입되고 있으며, 2009년 말 영업운전을 목표로 하고 있다.

PHA는 개념수립단계에서 대상시스템의 위험원을 도출하고, 도출된 위험원의 위험도가 허용수준으로의 제어가능여부를 판단하며, 위험도 억제를 위한 수명주기별 안전요구사항 도출을 목적으로 IEC 62278(EN 50126)에서 실시를 권고하고 있다.

따라서, 본 논문은 한국형 틸팅열차의 ATP차상장치의 위험원을 도출하기 위해 SRS의 상위기준인 기능요구사항(FRS, Functional Requirement Specification) 버전 5.0을 기준으로 기능별 예비위험원분석을 실시하여 안전확보의 기준으로 사용될 위험원을 제시한다.

2. 한국형 틸팅열차 ATP장치

† 책임저자 : 정회원, 한국철도기술연구원, 열차제어통신연구실, 선임연구원
E-mail : ducko@krti.re.kr
TEL : (031)460-5442 FAX : (031)460-5449
* (정)비회원, 한국철도기술연구원, 열차제어통신연구실, 선임연구원
** (정)비회원, 한국철도기술연구원, 열차제어통신연구실, 주임연구원
*** (정)비회원, 한국철도기술연구원, 열차제어통신연구실, 책임연구원

한국형 틸팅열차는 기존선을 약 200km/h의 고속으로 운영하기 위해 곡선구간에서 열차를 곡선의 중심방향으로 최대 8°가량 기울여 곡선구간을 고속으로 운행하는 열차이다. 이러한 한국형 틸팅열차에는 기존선의 신호방식인 자동열차정지(ATS)장치와 ATP장치가 설치되었으며, 특히 ATP장치는 코레일 ATP구간 지상장치에 적용된 ETCS SRS v2.2.2와 인터페이스하여 열차의 안전을 확보하도록 도입되었다.

ATP장치는 지상신호를 기관사에게 현시하며, ATP지상장치로부터 수신된 구배, 곡선, 속도제한 등의 고정정보를 바탕으로 정적속도프로파일을 생성하고, 마찬가지로 ATP지상장치로부터 수신된 선행열차 위치에 따른 이동권한을 바탕으로 동적속도프로파일을 생성한 후 정적속도프로파일과, 동적속도프로파일을 정합하여, 열차의 상용 및 비상제동패턴을 생성하며, 이러한 제동패턴을 기준으로 열차를 과속으로부터 방호한다.

ETCS SRS는 버전이 지속적으로 변경되고 있으며, 본 논문에서는 최신 자료인 SRS v3.0.0[1]과 SRS의 상위개념 요구사항인 FRS v5.0[2]을 기준으로 한다. SRS는 총 8장으로 분류되며, 1장 서론, 2장 시스템기본사양, 3장 개념, 4장 모드 및 천이, 5장 절차, 6장 기존시스템버전의 관리, 7장 ERTMS/ETCS 언어(프로토콜), 8장 메시지(텔레그램, 패킷, 변수)으로 구성된다. FRS는 상세사양인 SRS의 상위개념으로써 ETCS의 필수기능에 대한 명세를 포함하고 있다.

본 논문의 범위인 틸팅열차 ATP장치의 예비위험원분석을 위해서는 FRS의 ATP차상관련 Level 1기능만을 대상으로 한다. 표 1은 ETCS FRS v5.0의 차상관련 기능사양이다.

표 1. ETCS FRS v5.0의 차상관련기능[2]

대분류	세부기능
운영시나리오	4.1.1 차상장치 자기검사 4.1.2 기관사 및 열차정보 입력 4.1.3 입환동작 4.1.4 부분감시 4.1.5 완전감시 4.1.6 ETCS차상장치 차단 4.1.7 기존제어 및 방호장치와의 호환성 4.1.8 지상장치 미설치구간 운행
차상장치기능	4.3.1 정적속도프로파일 연산 4.3.2 동적속도프로파일 연산 4.3.3 완해속도 연산 4.3.4 열차위치결정 4.3.5 속도계산 및 현시 4.3.6 MMI현시 4.3.7 이동권한 및 제한속도 감시 4.3.9 구름 및 퇴행방호 4.3.10 ETCS정보기록
특수기능	4.4.1 다중편성(Multiple Units) : 기관사 1명 4.4.2 중련편성(Tandom Units) : 동력차별 기관사 탑승 4.4.7 퇴행운전
사고 또는 ETCS외부 고장에 대한 기능	4.5.2 정지신호 및 이동권한 종단의 통과
방호기능	4.6.4 열차의 비상정지 4.6.12 열차트립
추가기능	4.8.1 판트제어 및 전원공급 4.8.2 기밀제어 4.8.8 명확한 문자수신 4.8.9 고정된 문자수신 4.8.10 특수제동관리
차상장치 고장	5.1.3 전송장애 5.2.1.차상장치 고장

3. 한국형 틸팅열차 ATP장치의 PHA

PHA의 목적은 철도시스템 신뢰성, 가용성, 유지보수성, 안전성의 명세 및 입증에 관한 국제규격인 IEC 62278에서 강제하는 바와 같이 개념수립단계에서 안전확보의 기준이 되는 대표위험원을 선정하고, 대표위험원의 위험도를 허용수준이하로 제어가능한지 판단하며, 대표위험원의 위험도 제어를 위해 사용

된 방법을 수명주기(설계, 제작, 설치, 운영, 유지보수, 폐기)별 안전요구사항으로 도출하는 것이다[3].

본 논문에서는 한국형 틸팅열차 ATP장치의 PHA를 위해 표 1 FRS의 기능별로 표 2와 같이 고장모드 영향 및 심각도 분석(FMECA, Failure Mode Effect and Criticality Analysis)기법을 적용하여 위험원을 도출하였다. 이 과정에서 위험원별 위험도의 안전확보가능성을 위한 위험도평가는 모든 위험원의 위험도를 허용할 수 있는 수준으로 제어해야 하므로 배제하였다.

표 2. FRS의 기능별 PHA실시 예

PHA ID	위험원	원인	결과	안전대책	기타
PHA01	차상장치의 위험측 자기검사실패	1.속도검지관련 결함 2.제동제어관련 결함 3.속도프로파일 생성관련 연산오류 4.자기검사 연산오류	열차충돌 또는 탈선	1.속도검지의 신뢰성확보 및 안전측설계 2.출발전 계동시험 3.속도프로파일 생성관련 기능시험 4.자기검사관련 기능시험	
PHA02	자기검사기능고장으로 정상인 차상장치를 고장으로 인식	1.자기검사 연산오류	운행지연	1.자기검사관련 기능시험	
[기타사항] 1. 차상장치 자기검사기능관련 FRS의 강제사항은 다음과 같다. 가. 차상장치 기동시 자동적인 자기검사 시행해야 함(4.1.1.3a) 나. 차상장치 자기검사시 기관사의 개입 수행되어야 함(4.1.1.4b) 다. 차상장치 자기검사결과를 MMI에 표시되어야 함(4.1.1.4c)					

표 1의 각 기능별 FMECA를 표 2와 같이 실시한 결과를 표 3에 제시하였다. 따라서 틸팅열차 ATP장치의 안전확보유무는 표 3의 위험원별 발생빈도를 SIL4인 10-8/hour 이하로 제어하는 것으로 정의된다. 원칙적으로는 구매자인 운영기관에서 안전요구사항을 설정해야 하지만, 한국형 틸팅열차와 같이 구매자가 확정되지 않은 시스템의 경우에 안전대책의 적용수준을 가장 높은 수준으로 적용하는 원칙을 적용하였다.

표 3. 한국형 틸팅열차 ATP차상장치의 대표위험원

구분	위험원	관련 PHA결과
PHA_H01	차상장치 위험측 결함발생에 대한 안전확보 실패	PHA01, PHA65
PHA_H02	열차정보의 위험측 오류발생	PHA03
PHA_H03	운행중 연산오류에 의한 방호실패(다음 모드는 필수 개별검토) - 입환모드 - 부분감시모드 - 안전감시모드 - 비상착모드 - 퇴행운전모드 - 기관사책임모드 - 트립모드(트립 후 모드 포함) - STM모드	PHA07, PHA11, PHA15 PHA19, PHA20, PHA24 PHA37, PHA39, PHA44 PHA46
PHA_H04	속도프로파일 및 완해속도 프로파일의 위험측 생성	PHA25, PHA27, PHA29
PHA_H05	열차위치 및 속도관련 위험측 검지 및 현시	PHA31, PHA33
PHA_H06	SPAD에 대한 안전확보 실패	PHA51, PHA53
PHA_H07	지상으로부터 수신된 정상정보의 오류수신에 대한 안전확보 실패	PHA58, PHA63

PHA의 목적인 대표위험원 도출과정에서 각각의 위험원별 위험도를 억제하기 위한 방안들이 제시되었다. 이러한 위험원별 위험도억제를 위한 방법들은 PHA가 수행되는 개념설계 이후 단계인 설계, 제작, 시험, 설치, 운영, 성능감시, 유지보수, 폐기 단계별로 표 4와 같은 안전요구사항으로 적용되어야 한다.

표 4. 한국형 틸팅열차 ATP차상장치의 수명주기별 안전요구사항

해당수명주기	안전요구사항
설계단계	다음 기능관련 구성요소의 신뢰성확보 및 안전측설계 - 속도검지 - 제동제어 - MMI현시 - 발리스수신 - 회전속도계입력 - 기록장치에 기록
시운전단계	다음 기능의 기능시험을 각각 실시 - 제동제어 - 속도프로파일 생성 - 자기검사 - MMI현시 - 모드전환 - 차단 - 회전속도계입력 - 기록장치에 기록 - 운전모드시험(입환, 부분감시, 완전감시, 비상착, 퇴행운전, 기관사책임, 트립, STM, 비활성) - 판토크어 및 전원공급관련 - 문자수신

4. 결 론

본 논문은 한국형 틸팅열차 ATP장치에 적용된 대표위험원의 도출과정인 PHA에 대한 절차 및 근거를 제시하였다. 열차의 충돌 및 탈선과 관련된 철도위험원은 본 논문에서 제시하는 바와 같이 PHA를 통해 대표위험원을 도출하고, 도출된 위험원별 위험도가 허용할 수 있는 수준으로 제어되어 안전이 확보되었음을 신뢰도, 가용도, 유지보수도의 예측 및 검증과, 하부장치, 인터페이스, 운영 및 유지보수에 대한 위험원도출 및 분석을 통해 증거자료를 바탕으로 검증되어야 한다.

도출된 ATP차상장치 위험원은 한국형 틸팅열차뿐 아니라 현재 정부가 개발하고 있는 차세대고속철도 동력분산식 통합차상장치의 ATP기능에 대한 위험원으로도 활용이 가능하며, 코레일이 추진하고 있는 신형전기기관차 ATP차상장치의 예비위험원으로도 활용될 예정이다.

본 논문은 국토해양부 “한국형 틸팅열차 신뢰성 평가 및 운용기술개발” 연구과제로 수행되었음.

참고문헌

1. ERTMS/ETCS(2008.12), "System Requirements Specification", Issue 3.0.0
2. ERTMS/ETCS(2007.06), "Functional Requirements Specification", Version 5.00
3. IEC 62278(2002.09), "Railway applications –Specification and demonstration of RAMS", pp.85