한국철도학회논문집
제8권 제2호 2005년 | pp.161-169

자동열차방호장치와 건널목보안장치간의 인터페이스 안전요구사항에 관한 연구

A Study on Safety Requirement of ATP/LCS Interface

신덕호[1] · 이재훈[2] · 이기서[3]
Ducko SHIN · Jae-Hoon LEE · Key-Seo LEE

Abstract

In this paper, we provide safety requirements and advices to guarantee the safety of an interface in a level crossing system which is an interface between the conventional facilities and the new ATP (Automatic Train Protection) system, as well as we accomplish a safety management for the facilities of a country that has a different standard with already standardized ATP system. The system model has been made based on a safety activity of the international standard, and then a tolerance of a risk by the safety activity through PHA (Preliminary Hazard Analysis) has been analyzed, finally we achieved HIA (Hazard Identification and Analysis) for the assumptions that have been produced from a operating scenario and a functional interface. Thus, the safety requirements for the interface has been provided from the safety plan of HIA, and we showed the safety activity to guarantee the system safety through HIA which was depend on the design.

Keywords : Hazard(위험원), HAZOP(Hazard and Operability) Study, SIL(안전무결성레벨)

1. 서 론

자동열차방호장치(ATP, Automatic Train Protection)는 주행하는 열차가 선로정보 이외에 선행열차의 속도 및 거리정보를 지상으로부터 수신하여, 해당 열차의 가감속특성을 고려한 운행속도 패턴을 실시간으로 변경하여 선로용량의 향상을 꾀하는 설비이다. 국내에 도입되는 ATP는 유럽철도관리시스템/유럽열차제어시스템(ERTMS/ETCS)의 Level 1을 만족하는 시스템이 도입되고 있으며, 기본적인 기능과 안전에 관련된 요구사항들은 ERTMS/ETCS의 기능요구사항 및 안전요구사항이 제공되어 도입시 이러한 요구사항을 적용하고 있다[1]. 하지만 국내철도환경에 종속적인 기존설비와의 인터페이스는 국내에 ATP 도입시에 별도의 엔지니어링 부분으로 새롭게 제시되어야 한다.

따라서 본 논문에서는 국내에 도입되는 ATP와 건널목보안장치의 인터페이스에 대한 안전성활동을 수행하여 인터페이스관련 안전요구사항을 도출하였다.

ATP와 건널목보안장치의 인터페이스 안전요구사항의 제시를 위해 본 논문에서는 안전성활동을 수명주기별로 수행하였다. 개념설계단계에 적합한 예비위험원분석(PHA, Preliminary Hazard Analysis)을 통해 인터페이스로 인해 발생할 수 있는 사고와 위험원을 제시하였으며, 위험원으로 인한 리스크(Risk)가 안전대책 수행으로 인해 감소될 수 있는지를 검토하였다. 또한 ATP와 건널목보안장치의 인터페이스 모델을 제시하고, 모델의 기능 및 운영시나리오를 가정하여, 인터페이스모델에서 발생할 수 있는 위험원을 도출하고 분석(HIA, Hazard Identification and Analysis)하였다. 위험원의 도출은 HAZOP(Hazard and Operability) Study기법을 사용하였으며, 도출된 위험원의 분석은 결함트리분석(FTA, Fault Tree Analysis)기법을 정성적인 범위내에서 사용하였다.

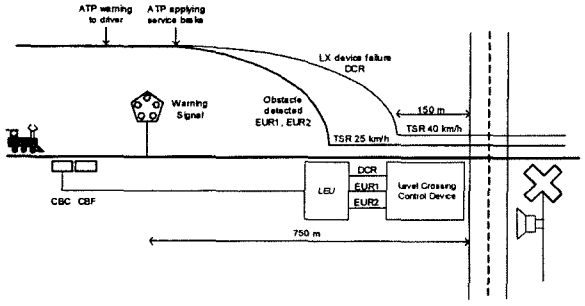
1 정회원 한국철도기술연구원 전기신호연구본부 주임연구원, 광운대학교 제어계측공학과, 박사과정
2 정회원 광운대학교 제어계측공학과, 박사과정
3 정회원 광운대학교 정보제어공학과, 교수

이러한 과정을 거쳐 위험원으로 인한 사고의 크기 및 빈도를 완화시키기 위한 인터페이스 모델에 대한 안전요구사항을 도출하였으며, 안전요구사항을 만족하기 위한 안전성 권고안을 제시하였다.

2. 본 론

2.1 ATP와 건널목보안장치의 인터페이스 모델링

건널목보안장치는 열차의 통행으로부터 건널목 이용자를 보호하기 위한 장치이다. 건널목보안장치의 경보동작은 경보등, 차단기, 경보종, 혼스피커, 방향지시등, 지장물검지장치 등으로 구성되며, 이러한 장치의 고장은 통행열차로부터 건널목이용자의 보호실패와 직결되므로 자체의 고장검지기능이 존재한다.



*LEU 선로변제어유닛 *CBC 가변정보전송용발리스
*CBF 고정정보전송용발리스
*DCR 차단기, 경보등, 경보종에 대한 상태정보
*EUR1, 2 건널목의 상선과 하선에 대한 지장물 검지장치 상태정보
*TSR 임시속도제한 *LX 건널목장치

Fig. 1. Interface Model of ATP and LCS(Level Crossing System)

Table 1. Functional Requirements of the Interface Model

고장 신호검지	열차의 안전확보시나리오
차단기, 경보등, 경보종 상태정보DCR의 고장	1. LEU에서 접근하는 열차에 TSR신호를 인가 2. 건널목진입 150m이전부터 40km/h로 열차가 진입할 수 있도록 속도프로파일 변경 3. 건널목 통과시 기관사가 안전확보에 대한 책임을 짐 4. 열차의후미가 TSR구간 빠져나갈때까지 속도제한 유지
상하행선 지장물검지장치 상태정보 EUR1, EUR2의 검지 및 고장	1. LEU에서 접근하는 열차에 TSR신호를 인가 2. 건널목진입 XXm이전부터 25km/h로 열차가 진입할 수 있도록 속도프로파일 변경 3. 건널목 통과시 기관사가 안전확보에 대한 책임을 짐 4. 열차의 후미가 TSR구간 빠져갈때까지 속도제한 유지

인터페이스 모델링에 적용하는 기능요구사항은 Table 1과 같이 가정하였다.

본 논문에서는 ATP와 건널목보안장치의 인터페이스에 대한 안전성활동을 위해 인터페이스부분을 Fig. 1과 같이 모델링하였다. 또한 인터페이스에 대한 사용자 요구사항은 건널목보안장치의 경보장치(차단기, 경보등, 경보종)의 고장정보와 건널목내에 설치된 지장물검지장치 검지정보를 건널목보안장치가 ATP에게 전송하여, 건널목에 진입하는 열차에게 건널목제어구간에 대한 정보를 전송하는 것이다.

Table 1의 인터페이스 기능요구사항은 안전성활동에 요구되는 시스템상세기능요구사항 및 운영시나리오측면으로 각각 Table 2와 Table 3과 같이 다시정리하였다.

2.2 인터페이스 예비위험원분석(PHA)

본 절의 예비위험원분석은 인터페이스로 인해 발생할 수 있는 위험원을 대상으로 안전대책의 수립으로 인해 사고의 발생빈도 또는 크기를 완화시킬 수 있는지와 안전대책이 인터페이스에 대한 안전권고안으로 써 실행이 될 수 있는지를 검토하기 위한 단계이다.

예비위험원분석에 사용한 위험원은 영국의 철도관리전문기관인 Network Rail의 안전지침서 Yellow Book의 철도분야위험원목록(총 284개, 인접한 시설 및 인명관련 64개, 철도승객관련 101개, 철도종사원관련119개)을 사용하여 건널목보안장치관련 사항에 대하여 예비위험원분석의 기준을 다음과 같이 설정하였다.

철도분야위험원목록에서 건널목의 종류와 관계없이 발생

Table 2. Functional Specific Requirements of IF(Interface)

기능	입력정보	기능요구사항
선로변제어유닛(LEU)	DCR낙하	CBC로 건널목 150m 전방에서 40km/h를 유지하도록 TSR신호출력
	EUR낙하	CBC로 열차가 건널목에 25km/h로 진입하도록 TSR신호출력
	DCR, EUR낙하	EUR낙하와 동일
	DCR복귀	TSR 해제
	EUR복귀	TSR 해제
	DCR, EUR복귀	원상태로 복귀(열차점유시 통과후 복귀)
가변정보정송장치(CBC)	TSR 40km/h 입력	해당 코드 전송(고장정보 없는 경우 정상신호 항시전송으로 가정)
	TSR 25km/h 입력	

Table 3. Operational Requirements of IF

시나리오	세부상황	기능요구사항
열차위치	제어구간에 없음	EUR낙하시에 TSR코드 전송
	CBC로 접근	DCR, EUR낙하시에 TSR코드 전송
	CBC와 건널목사이	DCR, EUR낙하시에 TSR코드 전송
	TSR구간 진출	정상운전 복귀
고장검지	DCR낙하	40km/h로 서행진입하여 기관사에 의한 장애물확인 후 통과
	EUR낙하	25km/h로 서행진입하여 기관사에 의한 장애물확인 후 통과
	DCR, EUR낙하	EUR낙하와 동일
고장검지 해제	DCR복귀	TSR 해제
	EUR복귀	TSR 해제
	DCR, EUR모두복귀	원상태로 복귀(열차점유시 통과후 복귀)
CBC의 설치위치	DCR낙하	건널목 전방 150m에서 40km/h를 유지할 수 있는 위치
	EUR낙하	건널목에 25km/h로 진입할 위치
TSR상태에서 열차의 정지	DCR낙하 (40km/h)	기관사에 의한 정지
	EUR낙하 (25km/h)	기관사에 의한 정지

*Note. DCR 경보등, 경보종, 차단기 고장정보 / EUR-출구측 지장물 검지장치

할 수 있는 위험원은 Table 4와 같다. 위험원의 번호는 고유의 값으로써 'HN'은 철도와 인접한 시설 및 인간과 관련된 위험원이며, 'HP'는 철도이용승객 그리고 'HW'는 철도종사원과 관련된 위험원이다.

Table 4에의 건널목관련 위험원에 대한 안전대책이 본 논문에서 검토하는 대상인 건널목 인터페이스 외에 건널목 보안장치의 보완 및 자발행위와 테러행위방지를 요구할 수 있다. 따라서 건널목 인터페이스와 관련된 위험원만 정리하기 위해 Table 9, 10, 11과 같이 예비위험원 분석지를 사용하여 Table 4의 위험원에 대하여 모두 수행하였으나, 지면관계상 위험대상에 따라 대표적 예비위험원분석 결과만을 제시하였다. 예비위험원에 사용된 위험원의 사고크기와 발생빈도는 Table 5와 Table 6과 같은 분류방법을 사용하여 접근하였으며, 리스크에 해당하는 위험도크기는 단순 매트릭스 방식으로 구현하며, 예비위험원분석단계에서의 위험도크기는 단순히 개념적인 안전대책 수립후의 내용을 작성한 것이다.

Table 9, 10, 11과 같이 건널목과 관련된 모든 위험원에

Table 4. Hazard Log of LCS

위험원번호	위험원 명세
HN0001	어린이 침입
HN0005	이동중인 열차에서 떨어지는 파편이나 물건
HN0006	열차에서 버리는 물건
HN0008	성인 침입
HN0009	철도시설물상의 안전보호시설 미비
HN0013	부적절한 보호장치가 있는 건널목에서의 자전거
HN0014	건널목의 시야불량
HN0015	허가되지 않은 작업통로의 사용
HN0016	장애인이나 행동부자유자의 건널목 이용
HN0017	통과열차에서 사람을 보호하는 건널목의 고장
HN0018	열차에 의하지 않은 건널목작동
HN0019	건널목 오용
HN0020	본래설계를 벗어난 건널목시설물의 변형운영
HN0021	건널목의 기능을 고의로 변경하는 행위
HN0022	고의적 시작행위(건널목의 허위 작동)
HN0023	SPAD
HN0039	고가선이나 인접선으로부터 충분히 보호되지 않음
HN0044	일반차량이 선로상의 시설물과 충돌
HN0045	건널목상에 정지된 차량
HN0047	열차통과시 보행자 진입
HN0053	기관사오류(정지신호 무시)
HN0064	통과열차와 인근주변의 부적절한 분리
HP0002	부적절/미허가 진로진입 가능성
HP0003	다양한 운영자간의 상호접속관리 부적절
HP0007	역내의 일반통행로에 장애물 존재
HP0009	철도부지 내 인화물질 존재
HP0010	통제시설물에서의 부적절한 업무수행
HP0018	통제시설에 대한 특수상황에서의 비정상적 행동
HP0020	정지중인 열차에서의 승객에 의한 출입문 열림
HP0032	열차내에 인화물질 탑재
HP0041	이동중인 열차에 승하차
HP0056	덜 제한적인 신호의 현시
HP0070	궤도노반의 불안정
HP0098	작업 후 안전하지 않은 상태로 복구된 시설물
HP0100	주행선과 다른선의 부적절한 분리
HW0002	정비작업을 위한 정확한 위치파악 실패
HW0003	안전지대에서 위험지대로 진입한 작업자
HW0048	철도종사원의 격투, 소란
HW0059	불안정한 열차비품/수화물
HW0071	밀폐된 장소에서 작업
HW0075	선로전환기 도중전환
HW0084	접지결함
HW0098	시설물의 보안미비
HW0109	궤도회로고장으로 인한 열차검지실패

대한 예비위험원분석을 실시한 결과, 위험도크기를 사용할 수 있는 수준(III, IV)으로 완화시키기 위한 대책이 건널목 보안장치의 시설물이나 관리체계에 대한 보완, 또는 자발행

Table 5. Quantizer of the Accident Frequency

1	자주(Frequent)	빈번하게 발생되는 것
2	종종(Probable)	일생운용 동안에 여러 회 발생되는 것
3	가끔(Occasional)	일생운용 동안에 가끔 발생할 수 있는 것
4	거의(Remote)	일생운용 동안에 가끔 발생할 가능성이 있는 것
5	없음(Improbable)	발생할 가능성이 전혀 없는 것

Table 6. Quantizer of the Accident Severity

A	치명 (Catastrophic)	생명의 위험, 시스템 손실 : 다수의 사망 혹은 다수의 심각한 부상)
B	심각(Critical)	심각한 상처, 병, 큰 시스템 손상 : 1인 사망, 1인의 심각한 부상
C	상당(Marginal)	가벼운 부상 혹은 병, 작은 시스템 손상 : 손상을 일으킬 수 있는 가능성의 내포
D	무시(Negligible)	가벼운 부상·병, 시스템 손상에 이르지 않는 것

Table 7. Category of the Hazard Log

N	Neighbors	철도와 연관된 시설물이나 인명
P	Passengers	철도를 이용하는 승객
W	Railway Worker	철도종사원

Table 8. Risk Matrix[5]

	A	B	C	D
1	I	I	II	III
2	I	I	II	III
3	I	II	III	IV
4	II	III	III	IV
5	III	III	III	IV

리스크 I) 수용불가(위험도를 반드시 저감해야함)
리스크 II) 부적정(잠재위험도에 대한 문서화된 허용안을 가지고 있어야 함)
리스크 III) 조건부허가(잠재위험도에 대한 문서화된 허용안을 가지고 승인됨)
리스크 IV) 허용가능

위에 의해 발생되는 위험원은 본 논문의 범위인 건널목과 ATP 인터페이스에 적용할 수 없으므로 Table 12와 같이 제외하였다.

Table 4의 건널목관련 위험원목록에서 Table 12의 건널목보안장치관련 위험원 및 자발행위에 의한 위험원을 제외하면 Table 13과 같다.

2.3 인터페이스 위험원도출(HAZOP)

위험원의 도출은 설계사양을 바탕으로 발생할 수 있는 위험원을 확인하는 과정이다. 전체 시스템에 대한 위험원도출은 기능사양, 인터페이스사양, 운영시나리오의 3가지 측면으로 실시하지만, 본 논문의 범위인 인터페이스사양을 기능측면과 운영측면으로 분류하여 HAZOP Study를 통해 위험원을 도출하였다[2-4].

Table 9. PHA Using PHA Sheet(Neighbours)

시스템 번호		작업기간		2일		작성날짜	2004.12.30 2005.01		
분 석 단 계		:				수정 : □	부가 : □		
위험원 번호	위험원 내용	위험원 대상	사고 심각도	발생 빈도	위험도 크기	대책안 : D: 설계변경 E: 안전대책 S: 안전소자 W: 경고체제 P: 절차/교육	대책안 실시 후		
							심각도	확률	위험도 크기
HN0001	어린이 침입	N	B	3	3B (II)	E: 건널목제어구간에 어린이의 침입을 방지하는 시설물 보완 W: 어린이 관점에서의 경고문 보완	C	4	4C (III)
HN0005	이동중인 열차에서 떨어지는 파편이나 물건	N	B	4	4B (III	E: 통과열차에서 떨어지는 물체에 의한 피해를 최소화하기 위한 건널목이용자 대기거리 확보 W: 통과열차에서 물체가 떨어질 수 있음을 경고	D	4	4D (IV)
HN0006	열차에서 버리는 물건	N	C	4	4C (III	E: 통과열차에서 떨어지는 물체에 의한 피해를 최소화하기 위한 건널목이용자 대기거리 확보 W: 통과열차에서 물체가 떨어질 수 있음을 경고	D	4	4D (IV)

Table 10. PHA Using PHA Sheet(Passengers)

시스템 번호		작업기간		2일		작성날짜	2004.12.30 2005.01		
분 석 단 계		:				수정 : □	부가 : □		
위험원 번호	위험원 내용	위험원 대상	사고 심각도	발생 빈도	위험도 크기	대책안 : D: 설계변경 E: 안전대책 S: 안전소자 W: 경고체제 P: 절차/교육	대책안 실시 후		
							심각도	확률	위험도 크기
HP0002	부적절/미허가 진로진입 가능성	P	A	4	4A (II)	D: 복선구간에서 반대방향 열차진입시 검지할 수 있는 방안 구축	B	5	5B (III)
HP0003	다양한 운영자간의 상호접속 관리 부적절	P	A	4	4A (II)	P: 건널목 종별 및 보안장치별 취급교육 강화, 작업결과에 대한 보고체계 구축	C	5	5C (IV)
HP0007	역내의 일반통행로에 장애물 존재	P	A	4	4A (II)	D: 역구내 건널목 주변의 장애물검지 시설확충	D	4	4D (IV)

Table 11. PHA Using PHA Sheet(Rail Workers)

시스템번호		작업기간		2일		작성날짜	2004.12.30 2005.01			
분석단계		:				수정 : □	부가 : □			
위험원번호	위험원내용	위험원대상	사고심각도	발생빈도	위험도크기	대책안 : D: 설계변경 E: 안전대책 S: 안전소자 W: 경고체제 P : 절차/교육	대책안 실시 후			
							사고심각도	발생확률	위험도크기
HW0002	정비작업을 위한 정확한 위치파악 실패	W	B	4	4B (III)	P: 작업결과에 대한 보고체계 구축 W: 작업중 또는 임시 변경사항으로 인한 경보동작의 표시 P: 건널목 기능관련 작업에 대한 보고체계 구축	D	4	4D (IV)	
HW0003	안전지대에서 위험지대로 진입한 작업자	W	B	4	4B (III)	S: 건널목관련 시설물 보완시 차량에 통지 P: 지정된 작업장소 이탈금지 교육강화	C	4	4C (III)	
HW0048	철도종사원의 격투, 소란	W	A	4	4A (II)	E: 건널목 고장정보에 대한 자동적인 운전모드변경 및 재동체결, 시스템 구축	D	4	4D (IV)	
HW0059	불안정한 열차비품/수화물	W	B	4	4B (III)	P: 위험물 취급 및 관리에 대한 체계구축	D	4	4D (IV)	

Table 12. Hazard log that requires the safety plan for out of the interface in the level crossing system

분 류	위험원번호	제외사유
건널목 보안장치관련 위험원	HN0005, 0006, 0009, 0013, 0016, 0019, 0020, 0021,0 039,0 044,0 064 HP0002, 0003, 0007, 0009, 0010, 0018, 0070,0 098,0 100 HW0002, 0059, 0071, 0075	안전대책을 위한 건널목시설물 보완이 본 논문의 결과로 부적절함.
자발행위에 의한 위험(테러 포함)	HN0001, 0008,0 015,0022 HP0020, 0032,0041 HW0003, 0048	자발행위 및 테러에 의한 사고는 ALARP수준을 만족한다고 가정(이후 활동에서 제외)

2.3.1 기능측면 위험원도출

기능측면의 HAZOP Study는 건널목 인터페이스를 구성하는 기능요소에 대하여 각각의 성질에 부합하는 Guide Word에 따라 수행한다. 건널목 인터페이스의 구성요소는 다음과 같다.

- 건널목에서 LEU로 전송되는 DCR신호(물리적 신호)

Table 13. Hazard Log of ATP/LCS Interface

위험원번호	위험원 명세
HN0014	건널목의 시야불량
HN0017	통과열차에서 사람을 보호하는 건널목의 고장
HN0018	열차에 의하지 않은 건널목작동
HN0023	SPAD(Signal Pass at Danger)
HN0045	건널목상에 정지된 차량
HN0047	열차통과시 보행자 진입
HN0053	기관사오류(정지신호 무시)
HP0056	덜 제한적인 신호의 현시
HW0084	접지결함
HW0098	시설물의 보안미비
HW0109	궤도회로고장으로 인한 열차검지실패

Table 14. Guide Word of IF HAZOP Study

Deviation Type	Guide word	물리적 신호에 대한 의미	연산에 대한 의미	시나리오에 대한 의미
부정	No	접점이 동작하지 않음	접점에 대한 출력을 하지 않음	기대하는 시나리오의 수행을 하지 않음
정량적 변형	More	무여자 상태에서 전원이 비정상으로 높아짐	TSR신호가 비정상적으로 빨리 전송됨(해당없음)	해당 없음
	Less	여자 상태에서 전원이 비정상으로 낮아짐	TSR 신호가 비정상적으로 늦게 전송됨(해당없음)	해당 없음
정성적 변형	As well as	다른 접점으로 입력	TSR외에 다른 전문을 전송	잘못된 시나리오를 수행
	Part of	여자를 유지하지 못하고 접점이 채터링	CBC로 완전한 전문을 송신실패	시나리오를 완료하지 못함
대체	Reverse	접점이 반대로 동작	DCR과 EUR에 대한 반대 TSR을 송신	해당 없음
	Other than	접점의 값을 반대로 읽어옴	다른 정보가 CBC로 전송	해당 없음
시간	Early	접점입력이 예상보다 빨리 들어옴	CBC로의 TSR전송이 예상보다 빨리 전송됨	시나리오를 일찍 수행
	Late	점점입력이 예상보다 늦게 들어옴	CBC로의 TSR전송이 예상보다 늦게 전송됨	시나리오를 늦게 수행
명령 또는 흐름	Before	예상순서보다 빨리들어옴(건널목 인터페이스는 단일 접점으로 동작하므로 해당없음)	고장정보 복귀 이전에 TSR정보가 정상상태로 복귀	해당 없음
	After	예상순서보다 늦게들어옴(건널목 인터페이스는 단일 접점으로 동작하므로 해당없음)	고장정보 복귀 이후에도 TSR정보가 고장상태를 유지	해당 없음

- 건널목에서 LEU로 전송되는 EUR신호(물리적 신호)
- 건널목의 DCR이나 EUR에 의한 TSR신호 산출(연산)
- LEU에서 CBC로 전송하는 TSR신호(물리적 신호)

2.3.2 운영측면 위험원도출

운영측면의 HAZOP Study는 건널목 인터페이스를 구성하는 운영요소에 대하여 각각의 성질에 부합하는 Guide

Table 15. HAZOP Study of IF Function

HAZOP Study 대상: 건널목 인터페이스 기능측면 해석								
참여구성원: ATP RAMS컨설팅부서, 시스템 검토그룹(SRG)							회의일시:	
기능	GW	이상현상	원인	결과	안전대책	기타사항	세부조치 내역	조치의 주체
건널목에서 LEU로 전송되는 DCR신호(물리적 신호)	No	DCR의 여자정보가 전달되지 않음(차단기, 경보등, 경보종 정상시)	DCR과 LEU사이의 케이블 절손	LEU에서 CBC로TSR 40km/h정보 전송	안전측고장이므로 고려 않함	운영효율저하	-	-
		DCR의 무여자 정보가 전달되지 않음	DCR과 LEU사이의 케이블에 노이즈 인입	경보등,경보종, 또는 차단기가 정상으로 동작하지 않은 상태에서 열차진입	케이블 포설 및 노이즈에 대한 실드처리	지장물과 충추돌	안전대책 수행	시공자
			LEU의 입력소자 고장		LEU의 DCR입력소자를 안전하게 구성		안전대책 수행	설계자
	More	DCR무여자 상태에서 입력되는 전원이 비정상 상승	DCR과 LEU사이의 케이블 노이즈 인입	경보등,경보종, 또는 차단기가 정상으로 동작하지 않은 상태에서 열차진입	케이블 포설 및 노이즈에 대한 실드처리	지장물과 충추돌	안전대책 수행	시공자
			DCR계전기 입력을 위한 LEU의 전압 상승		DCR계전기 입력을 위한 LEU전원의 안전구성			설계자
	Less	DCR여자 상태에서 입력되는 전원이 비정상 상승	DCR과 LEU사이의 케이블 노이즈 인입	LEU에서 CBC로 TSR 40km/h정보 전송 (운영효율저하)	안전측고장이므로 고려 않함	-	-	-
			DCR계전기 입력을 위한 LEU의 전원 하강					
	As well as	DCR계전기 정보를 EUR계전기 정보로 입력	결선 오류	경보등,경보종 또는 차단기고장시 열차가 건널목에 25km/h로 진입	DCR,EUR계전기 입력이 바뀌면 결선이 않되도록 커넥터를 구조화	안전측 고장으로 고려 않함	-	
				지장물 검지장치 고장시 열차가 건널목에 40km/h로 진입		기관사의 육안을 통한 지장물 검지후 정지에 필요한 제동거리 필요	안전대책 수행	설계자
	Part of	DCR이 여자 또는 무여자를 유지하지 못하고 채터링	DCR과 LEU사이의 케이블 노이즈 인입	LEU의 오동작 유발	케이블 포설 및 노이즈에 대한 실드처리	지장물과 충추돌	안전대책 수행	시공자
			DCR계전기 입력을 위한 LEU의 전원 고장		계전기 입력을 위한 LEU의 전원을 안전하게 구성		안전대책 수행	설계자
					LEUIO입력에서 채터링이 발생해도 안전측입력설계		안전대책 수행	설계자
	Reverse	DCR, EUR계전기 정보가 반대로 입력	결선 오류	DCR,EUR계전기 입력값이 반대동작	건널목 인터페이스 설치후 시험	-	안전대책 수행	시공자
	Other than	DCR, EUR계전기 정보를 반대로 읽어옴	LEU IO Map오류	DCR,EUR계전기 입력값이 반대로 읽힘	건널목 인터페이스 설치후 시험	-	안전대책 수행	설계자
	Late	DCR계전기 입력속도가 예상보다 늦음	DCR입력에 대한 연산처리가 늦어짐	경보등,경보종 또는 차단기의 고장이나 지장물이 있는 상태에서 열차진입	DCR, EUR상태에 대하여 실시간(200ms)으로 TSR정보 송신	지장물과 충추돌	안전대책 수행	설계자

Table 16. HAZOP Study of IF Operating Scenario

HAZOP Study 대상: 건널목 인터페이스 운영측면 해석								
참여구성원: ATP RAMS컨설팅부서, 시스템 검토그룹(SRG)							회의일시:	
기능	GW	이상현상	원인	결과	안전대책	기타사항	세부조치 내역	조치의 주체
기관사의 수동열차 정지	No	기관사 수동열차 정지의 실패	시스템구조상 제동거리 미확보	지장물과 충돌을 피할 수 없는 속도로 진입	통과열차의 제동거리를 고려한 CBC의 설치	지장물과 충추돌	안전대책 수행	설계자
			기관사의 실수		인적 오류억제		안전대책 수행	교육자
	Part of	기관사의 완전한 수동열차 정지 실패	기관사 가시거리 미확보 (곡선, 안개)	지장물과 충돌을 피할 수 없는 속도로 진입	가시거리 미확보구간에서는 발견즉시 제공이 가능한 운전시나리오 개발	지장물과 충추돌	안전대책 수행	설계자 시공자
	Early	지장물 발견후 조기정지	안전측 정지	지장물과 충돌 회피	-	운영효율 저하	-	-
	Late	지장물 발견후 정지조치의 시간지연	인적오류에 의한 제동거리 미확보	지장물과 충돌을 피할 수 없는 속도로 진입	인전오류 억제	지장물과 충추돌	안전대책 수행	교육자

Word에 따라 수행한다. 건널목 인터페이스의 구성요소는 다음과 같다.

- 기관사의 수동열차정지
- TSR 40km/h 운영시나리오
- TSR 25km/h 운영시나리오
- 고장신호의 복귀

위 기능요소는 계전기 접점과 프로세서의 연산이며, 기능요소의 HAZOP Study를 위해 사용되는 Guide word및 운영시나리오관련 위험원도출을 위한 Guide Word는 Table 14와 같다[2].

Table 14를 이용하여 ATP와 건널목보안장치 인터페이스에 대한 HAZOP Study를 Table 15-16과 같이 수행하였다.

2.4 인터페이스 위험분석(FTA) 및 사고시나리오

도출된 위험원을 결함트리분석(FTA)기법을 사용하여 분석하였으며, 분석된 자료는 안전요구사항의 작성에 활용한다. 앞 절의 HAZOP Study의 기능별 이상현상을 위험원으로 설정하여, 위험원이 발생되는 원인을 분석하는 FTA는 시스템의 하드웨어 및 소프트웨어에 대한 정확한 사양을 토대로 수행해야 하지만 본 논문의 인터페이스 모델은 정확한 하드웨어 사양을 고려하지 않았으므로, FTA를 통한 위험발생확률의 정량화는 제외한다.

Fig. 2의 사고시나리오는 "건널목 지장물과 열차의 충추돌"을 최상위 이벤트로 설정하여 예비위험원분석에서 도출된 위험원과 HAZOP Study활동에 의해 도출된 위험원의 연관관계를 분석한 것이다.

따라서 사고시나리오분석에서 도출된 결함트리분석은 건널목인터페이스에 사용된 구체적인 하드웨어 및 소프트웨어를 적용하지 않고, 기능단위별 위험원 연관관계를 분석한 것이므로, Minimal Cut Set방법의 사용이 의미를 갖지는 않는다[6]. 다만, 분석결과를 통해 LEU에서 DCR과 EUR계전기 값을 읽어들이기 위한 전원과, 건널목 보안장치와 LEU 및 CBC와의 연결케이블 고장이 공통모드고장(Common Mode Failure)임을 알 수 있다.

2.5 인터페이스 리스크평가

예비위험원분석에서 도출된 위험원 리스트와 위험원도출 및 분석을 통해 구체화된 위험원목록을 결함트리분석을 통해 분석한 결과 건널목 인터페이스관련 최종 위험원 목록을 다음과 같이 정의하고 안전무결성레벨을 할당하였다.

위험원에 연관관계에 따라 할당된 리스크를 기준으로 안전무결성레벨을 할당하였다. 본 논문에서의 안전무결성레벨 할당은 리스크레벨과의 1:1대응을 전제로 한다.

건널목 인터페이스의 위험원정의와 분석결과로써 발생할 수 있는 사고는 "건널목 지장물과 열차의 충추돌"이다. 따라서 건널목의 인명 또는 일반차량과 통과열차가 충추돌 했을 경우, 철도원, 승객, 공공의 인명피해 및 재산상 피해가 모두 치명적임을 알 수 있다. 따라서 건널목 인터페이스는 다음과 같은 안전무결성레벨에 따른 고장률을 가져야 하며, 예측과 시험을 통해 시스템이 안전무결성레벨에서 제안하는 고장률 사이에 존재함을 입증해야 한다.

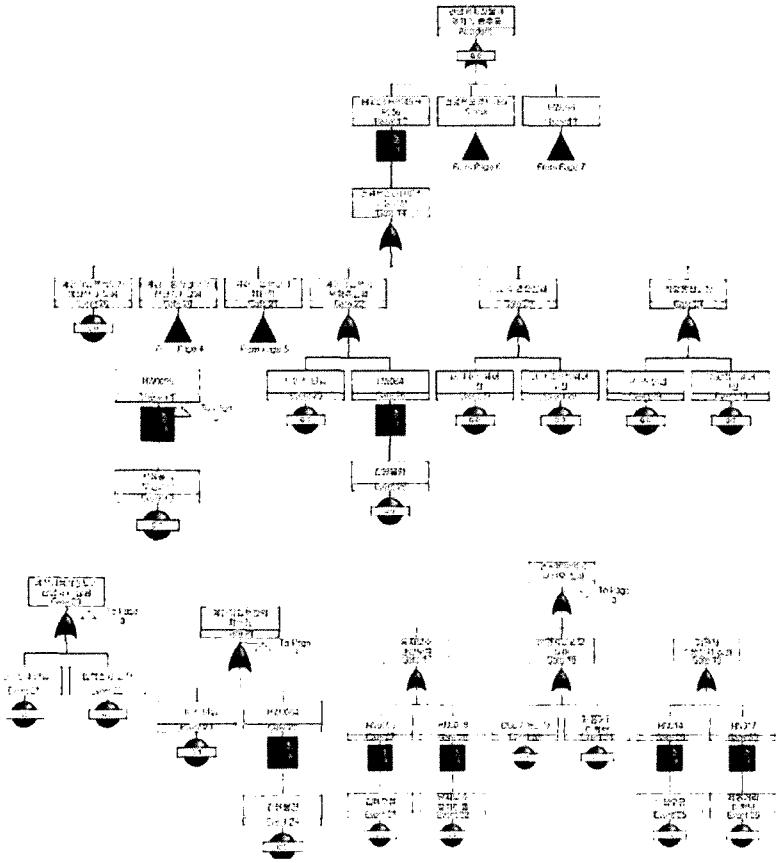


Fig. 2. Accident Scenario of IF

2.6 인터페이스 안전요구사항

본 절에서는 건널목으로 진입하는 열차가 건널목을 안전하게 통과하기 위한 안전관련 요구사항을 예비위험원분석(PHA)단계에서 도출된 안전대책을 정리하여 제공한다.

가. 건널목 고장시 지장물과의 충돌을 방지할 수 있는 가시거리와 제동거리를 확보해야 한다.

Table 17. Hazard Log of IF

위험원번호	위험원 명세	리스크 등급	안전무결성등급
HN0014	건널목의 시야불량	II	SIL4
HN0017	통과열차에서 사람을 보호하는 건널목의 고장	III	
HN0018	열차에 의하지 않은 건널목작동	II	
HN0023	SPAD	II	
HN0045	건널목상에 정지된 차량	II	
HN0053	기관사오류(정지신호 무시)	II	
HP0056	덜 제한적인 신호의 현시	II	
HW0084	접지결함	II	
HW0098	시설물의 보안미비	II	

나. 유지보수에 의해 건널목 인터페이스 기능이 영향을 받지 않아야 한다.

다. 무경보상태에 열차진입이 발생하지 않아야 한다.(열차의 CBC통과 후 발생되는 무경보는 제외)

라. 경보시작 후 건널목에 정차된 일반차량은 검지되어야 한다.

마. 덜 제한적인 신호가 발생하지 않아야 한다.(예. TSR25 km/h상황에서 TSR40km/h명령 발생)

바. 건널목 인터페이스에 사용되는 장비(LEU, CBC는 단순고장으로부터 안전성이 입증되어야 한다.)

사. 건널목 인터페이스에 사용되는 장비는 보안조치가 되어야 한다.

2.7 인터페이스 안전권고안

건널목 인터페이스의 안전성 확보를 위한 안전권고안은 위험원도출 및 분석(HIA)에서 제시된 안전대책을 기반으로, 안전무결성레벨에 따른 신호시스템 국제규격의 권고안을 추가한 것이다.

가. 하드웨어 안전권고안

(1) 건널목 인터페이스에 사용되는 케이블은 외부에서 인입되는 노이즈로부터 차폐되어야 한다.
(2) LEU의 계전기입력 및 통신출력 소자는 안전설계 되어야 한다.
(3) CBC, LEU와 LEU의 전원장치는 안전설계 되어야 한다.
(4) LEU와의 결선은 물리적으로 바뀌지 않도록 커넥터가 설계 되어야 한다.
(5) 신호가 부적절(예. 채터링)하게 입력되어도 설비가 보호되어야 한다.
(6) LEU는 입력에 대하여 실시간(200ms 이내)으로 동작되어야 한다.
(7) LEU와 CBC의 전문은 안전설계되어야 한다.
(8) CBC로 입력되는 정보의 적합성을 LEU로 궤환하도록 설계되어야 한다.

나. 소프트웨어 안전권고안

(1) IEC62279의 수명주기별 소프트웨어 안전무결성레벨(SWSIL) 4에 대한 권고사항을 준수해야 한다.

다. 운영의 안전권고안

(1) 건널목에 진입하는 열차가 CBC고장을 검지하면 서행운전해야 한다.
(2) CBC의 정상상태 유무를 통과열차가 확인할 수 있어야 한다.
(3) 40km/h속도로 건널목에 진입하는 열차는 기관사의 육안판단에 의해 열차통과의 안전성이 확보될 수 있도록 제동거리가 확보되어야 한다.
(4) 건널목 인터페이스의 설치 후 시험계획이 수립되어야 한다.
(5) TSR 40km/h로 건널목 진입 150m이전과 25km/h로 건널목에 진입할 수 있도록 통과열차 속도를 고려한 곳에 CBC가 설치되어야 한다.
(6) 가시거리 미확보구간에서는 지장물의 발견즉시 정지가 가능한 운전시나리오가 제공되어야 한다.
(7) CBC와 건널목 사이에 기관사의 수동정지를 위한 경고등이 설치되어야 한다.
(8) 건널목 및 건널목 인터페이스의 고장 후 복귀는 일정한 절차가 수행되어야 한다.
(9) 건널목 및 건널목 인터페이스의 유지보수 후 복귀는 일정한 절차가 수행되어야 한다.

3. 결 론

본 연구는 국내에 새롭게 도입되는 자동열차방호장치(ATP) 시스템과 기존시설물과의 인터페이스 중 건널목보안장치와의 인터페이스를 대상으로 안전성활동을 수행하여, 안전요구사항 및 안전확보를 위한 권고사항을 제공하기 위한 연구로써, 이미 규격화 되어있는 ATP의 기능과는 달리 적용되는 국가의 고유시설물에 대한 안전관리를 수행하였다.

안전권고안의 제시는 국제규격에서 제시하는 절차에 근거하여 대상시스템을 모델링하였으며, 예비위험원활동을 통한 안전활동으로 인한 리스크의 완화를 검토하고, 인터페이스에 대한 기능 및 운영시나리오를 가정하여 가정에 대한 위험원도출 및 분석을 수행하였다. 따라서 예비위험원활동의 안전대책으로 제시한 개념적인 사항을 정리하여 인터페이스 안전요구사항을 작성하였으며, 설계에 종속적인 위험원도출 및 분석을 통해 시스템안전확보를 위한 안전권고안을 제시하였다.

향후에는 ATP와 국내기존설비와의 인터페이스인 자동폐색장치(ABS) 및 자동열차정지장치(ATS)와의 인터페이스에 대한 안전성활동도 수행되어야 한다.

참 고 문 헌

1. 김영태 저, 2003 "신호제어시스템"
2. Felix Redmill et al. "System Safety : HAZOP and Software HAZOP", John Wiley & Sons, 1999
3. Defence Standard 00-58, "HAZOP Studies on System Containing Programmable Electronics", 2000
4. International Standard IEC61882 "HAZOP Studies - Application guide"
5. International Standard IEC82278 "Railway Applicaiton RAMS"
6. International Handbook NUREG-0492 "Fault Tree Handbook"