한국철도학회논문집
제8권 제6호 2005년 | pp. 533-538

HAZOP Study를 사용한 ATSRX의 위험원도출 및 리스크완화에 관한 연구

A Study on the Hazard Identification and Risk Mitigation for ATSRX Using Hazard and Operability Study

신덕호† · 이준호* · 이강미* · 김용규*
Ducko SHIN · Jun-Ho LEE · Kang-Mi LEE · Yong-Kyu KIM

Abstract

In this paper we identify the hazard using HAZOP study for ATSRX which is a subsystem of the ATP system, and we study a safety management method for the mitigation of the risk to the acceptable level. ATSRX is a device that make a train which has a ATP system operate in ATS line. For this ATSRX send a induction signal with ATS system to vehicle controller. Thus ATSRX can be said as a safety equipment that makes a train operate safely. In order to identify the hazard for the internal faults in ATSRX system, we employ HAZOP study method which is recommended as hazard identification in IEC 62278, RAMS requirements in railway signal, and also it provide the detail activity in IEC 61882. Thus, in this paper we perform HAZOP study based on ATSRX related standards and using the assessment of the identified hazard we study a method to guarantee the system safety through the change of the design to mitigate the risk to the acceptable level.

Keywords : *RAMS*(Reliablity, Availability, Maintainability and Safety), *ATP*(Automatic Train Protection), *ATS*(Automatic Train Stop), *HAZOP Study*(Hazard and Operability Study)

1. 서 론

국내 열차제어시스템 분야에서는 2007년 호남선을 시작으로 차상신호시스템인 자동열차방호장치(ATP, Automatic Train Protection)의 사용을 위한 도입사업이 진행되고 있다[1]. ATP시스템의 차상제어장치는 유럽철도관리시스템사양 및 열차제어 사양인 ERTMS/ETCS를 만족하는 분산제어개념의 제어기로 구성되어 있다[2]. 또한 ATP시스템을 장착한 열차가 기존신호구간을 병행운전하기 위해 ERTMS/ETCS에서는 특정전송모듈(STM, Specific Transmission Module)을 제공하고 있으며, 국내의 경우 자동열차정지장치 (ATS, Automatic Train Stop)가 설치된 기존선구간의 열차운행을 위한 ATSRX모듈을 포함한 장치가 STM에 해당한다. 본 논문은 ATP시스템의 하부구성요소인ATSRX를 대상으로 HAZOP Study기법 [3]을 사용하여 위험원을 도출하고, 도출된 위험원으로 인한 리스크를 허용할 수 있는 수준이하로 감소시키기 위한 안전성활동에 대한 연구이다[4,5].

시스템 내부의 위험원을 도출하기 위한 방법에는 What if, FMEA(Failure Mode Effective Analysis) [6], HAZOP (Hazard and Operability) Study등의 여러 기법이 사용된다. What if 방식은 개발엔지니어, 안전성관리자, 운영기관 종사자가 협의를 거쳐 시스템내부에서 발생한 임의 고장으로 인해 사고가 발생할 수 있는 위험원을 도출해 보는 접근방식으로써, 기존의 철도신호시스템 개발과정에서 가장 널리 사용되는 방법이다.

장치의 기능을 중심으로 고장에 대한 영향을 분석하는 FMEA 또는 위험원의 치명도를 고려한 FMECA(Failure Mode Effective and Criticality Analysis)는 대상시스템관련자의 토론에 의해 위험원을 도출하는 방식이며, HAZOP Study도 대동소이하다. 하지만 본 논문에서 사용한 HAZOP Study기법은 대상시스템의 발생고장으로 인한 결과를 경우의 수를 고려하여 분석하기 위한 Guide Word를 사용하여, FMEA와 기타 다른 기법에 비하여 위험원 누락의 가능성을 상대적으로 감소시킬 수 있다[3]. 본 논문에서는 ATSRX

† 책임저자 : 회원, 한국철도기술연구원, 전기신호연구본부
E-mail : ducko@krri.re.kr
TEL : (031)460-5442 FAX : (031)460-5449
* 회원, 한국철도기술연구원, 전기신호연구본부

시스템 내부에서 발생되는 고장에 대하여 위험원을 도출하기 위한 방법으로 HAZOP Study기법을 사용하였으며[7], HAZOP Study관련 세부활동 지침인 IEC 61882를 근거로 ATSRX의 위험원을 도출하였다. 그리고 도출된 위험원으로 인한 리스크를 허용할 수 있는 수준이하로 완화시키기 위한 설계변경을 통해 시스템의 안전성확보를 위한 활동방안을 연구하였다.

2. ATSRX의 구조

ATS신호방식을 사용하는 선구에서 지상의 신호기상태에 따른 ATS지상자의 응동주파수를 ATP차상제어장치로 전달하는 ATSRX시스템을 포함한 ATP차상장치의 구성은 그림 1과 같다.

따라서, 그림 1의 ATSRX를 본 논문에서 제시하는 HAZOP Study를 이용한 위험원도출의 범위로 설정하였다.

2.1 ATSRX의 기능요구사항

ATS구간 지상에 설치된 ATS지상자의 위를 열차가 통로하는 순간, 열차가 진입하는 폐색구간의 신호현시상태는 ATS차상안테나를 통해 제한속도에 해당하는 응동주파수로 열차에 수신된다.

ATSRX는 상시 ATS지상자와의 응동을 위한 주파수를 발진하며, ATS지상자를 통과하는 순간 응동된 주파수를 분석하여 제한속도코드를 산출한다. 산출된 제한속도코드는 ATSRX의 상위 장치인 ATSLU와의 통신을 통해 ATP차상제어장치로 전달된다. 이러한 기능요구사항을 구현하기 위해 ATSRX는 그림 2와 같은 내부구성으로 설계되었다.

그림 2에서와 같이 ATSRX는 동작을 위한 전원, ATS차상안테나, 주파수송신을 위한 ATSLU 그리고 전후방운전을 위한 스위치로 인터페이스하여 동작을 수행한다.

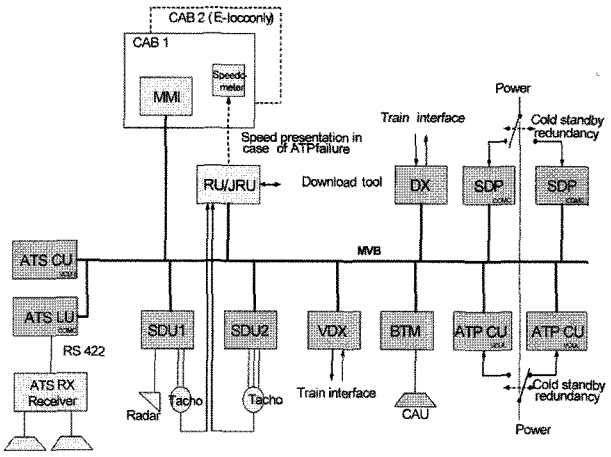

그림 1. ATSRX를 포함한 ATP차상장치의 구성

MMI : Man Machine Interface, **RU/JRU** : Juridical Recording Unit, **ATSCU** : ATS Core Unit, **ATSLU** : ATS Logic Unit, **ATSRX** : ATS Receiver, **SDU** : Speed and Distance Unit, **VDX/DX** : Vital Digital Exchanger, **BTM** : Balise Transmission Module, **CAU** : Compact Antenna Unit, **COMC** : Communication Controller, **VCU** : Vehicle Control Unit, **MVB** : Multifunctional Vehicle Bus.

2.2 ATSRX의 내부구성 및 인터페이스

ATSRX의 내부구성 및 인터페이스는 HAZOP Study를 위한 Guide Word의 선정기준이 된다. HAZOP Study는 하부시스템의 기능단위별로 고장에 대한 시스템의 영향을 판단하기 위한 방법으로써, 본 논문에서 수행한 HAZOP Study는 ATSRX의 인터페이스를 기준으로, 세부구성에서 발생된 고장이 다음 세부구성에 미치는 영향을 통해 위험원을 도출하였다.

따라서 ATSRX의 세부구성을 열차로부터 제공된 전원을 변환하여 ATSRX의 구동전원으로 공급하는 전원모듈, 발진주파수를 발생시키는 OSC모듈, ATSLU와의 통신을 수행하는 COM모듈, 전후방 운전을 선택하는 CHR모듈 그리고 ATSRX의 기능을 수행하는 소프트웨어로 분류하고, ATSRX의 인터페이스를 고려하여 HAZOP Study를 수행하였다[8]. 소프트웨어를 제외한 부분은 ATSRX를 구성하는 PCB(Printed Circuit Board)모듈단위로 선정하여 유지보수도의 예측 및 입증을 위한 LRU(Lineside Replaceable Unit) 분류와 통일시켰다. 표 1은 ATSRX의 하드웨어 및 소프트웨어의 구분과 각각의 입출력이다.

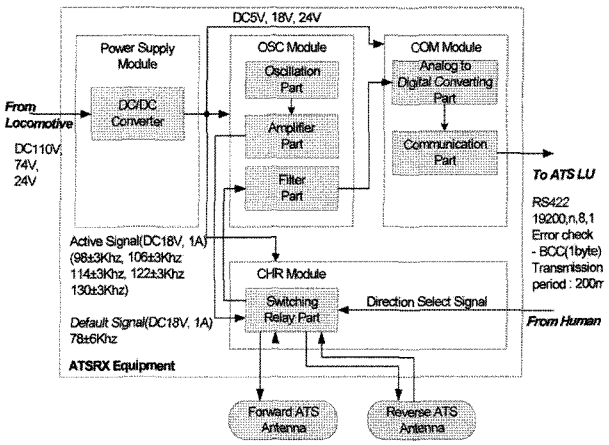

그림 2. ATSRX의 내부구성도

표 1. ATSRX의 세부구성별 입출력

모듈	입력		출력	
	대상	특성	대상	특성
전원모듈	기관차	DC전원	OSC모듈	DC전원
			COM모듈	DC전원
			CHR모듈	DC전원
OSC모듈	전원모듈	DC전원	CHR모듈	ATS발진신호
	CHR모듈	ATS응동신호	COM모듈	ATS응동신호
COM모듈	전원모듈	DC전원	ATSLU	통신전문
	OSC모듈	ATS응동신호		
	ATSLU	통신전문		
CHR모듈	전원모듈	DC전원	OSC모듈	ATS응동신호
	ATS안테나	ATS응동신호		
	절체버튼	방향전환접점	ATS안테나	ATS발진신호
	OSC모듈	ATS발진신호		
소프트웨어	COM모듈	8비트디지털	ATSLU	통신전문
	ATSLU	통신전문		

표 1과 같은 ATSRX의 세부기능과 인터페이스의 분류를 ATSRX의 HAZOP Study를 위한 Guide Word로 선정하였다[3].

3. ATSRX의 위험원도출

위험원도출은 장치 내부에서 발생할 수 있는 결함 또는 오류의 결과인 고장과, 장치로 인해 사고와의 연관관계를 분석하는 활동이다. 하부시스템의 세부기능 또는 인터페이스 그리고 운영시나리오에 따라 실시되는 위험원도출을 위해 본 논문에서는 HAZOP Study기법을 사용하였다. 위험원도출 및 분석(HIA, Hazard Identification and Analysis)활동과 관련된 위험원은 원인에 가까운 위험원의 형태를 보이며, 전체시스템차원에서의 위험원분석인 예비위험원분석(PHA, Preliminary Hazard Analysis)활동의 결과로 제시된 위험원은 사고와 밀접한 관계를 갖는다. 따라서, PHA의 위험원과 HAZOP Study에서 도출된 위험원의 연관관계를 분석하는 것이 위험원분석이며, 본 논문에서는 ATP도입사업에서 PHA 활동결과로 제시된 위험원목록과 위험원으로 인해 발생되는 사고의 크기와 빈도의 조합인 리스크의 평가결과를 활용하였다.

3.1 Guide Word

Guide Word는 위험원도출을 목적으로 사용하는 HAZOP Study기법의 사전활동으로써, 대상 세부구성의 내부에서 결함 또는 오류가 발생하여 다른 세부구성에 영향을 주었을 때의 결과를 예측하기 위한 기준이다. 따라서 대상 세부구성의 입출력특성에 따른 Guide Word의 선정이 매우 중요하며, 세부구성 내부에서 발생할 수 있는 결함의 결과를 비교적 체계적으로 검토하여 HAZOP Study를 사용한 위험원도출의 완성도를 향상시킬 수 있다는 점에서 FMEA나 FMECA보다 장점을 갖는다. ATSRX의 세부구성이 갖는 인터페이스는 표 1에서와 같이 인터페이스 특성에 따라 DC전원, ATS발진 및 응동, 통신전문의 전기적신호, 통신전문의 데이터, ADC(Analog to Digital Converter)신호로 정리할 수 있으며, 표 2는 본 논문에서 ATSRX관련 HAZOP Study를 수행하여 극복할 수 없는 위험원을 도출한 DC전원의 Guide Word이다.

표 2. DC전원의 Guide Word

일탈 유형	Guide Word	의미	전원관련 결과
부정	No	명령이 실행되지 않음	전원출력 차단
정량적 변형	More	수량의 비정상증가	출력전압 또는 전류의 증가
	Less	수량의 비정상감소	출력전압 또는 전류의 감소
정성적 변형	As well As	기대하지 않은 동작	해당없음
	Part of	완전한 수행을 실패	해당없음
대체	Reverse	목적과 반대되는 결과	해당없음
	Other than	목적과 다른 결과	해당없음
시간	Early	예상시간보다 일찍 발생	해당없음
	Late	예상시간보다 늦게 발생	초기가동시 전원출력의 공급지연(200ms이상)
명령 또는 흐름	Before	예상순서보다 일찍 발생	해당없음
	After	예상순서보다 늦게 발생	해당없음

3.2 HAZOP Study의 결과

표 1에서 분류한 ATSRX의 세부구성 중 DC전원을 대상으로 표 2에서 제시한 Guide Word를 기준으로 HAZOP Study를 수행하였다.

HAZOP Study의 수행결과 도출된 위험원의 원인과 결과 그리고 안전대책을 점검한 결과, PHA활동에 의한 ATP시스템 위험원목록과 관련된 위험원들이 도출되고 검토되었다. 해당 HAZOP Study를 통해 도출된 위험원과 관련 PHA에 의한 위험원과의 관계를 분석하여 위험원별 리스크에 따른 SIL(Safety Integrity Level)[9,10]을 만족하는 안전대책수준을 부품의 고장률을 토대로한 정량적 기준으로 검토하였으

표 3. 전원모듈(DC24V)의 HAZOP Study

HAZOP Study대상 : ATSRX의 전원모듈(DC24V)								
참조도면번호 : 유경제어 ATSRX 사양서				갱신번호 : 1		소요시간 : 6		
참여구성원 : ATP시스템 RAMS컨설팅부서, 시스템검토그룹, ATSRX제작사 엔지니어				회의일시 : 2005.07.27				
기능	Guide Word	이상현상	원인	결과	안전대책	기타사항	세부조치내역	조치의 주체
전원모듈 DC24V	No	전원공급 중단	DC/DC 고장	보호회로고장, 방향전환불가(후방고정)	-	HN051 / HP056	설계보완	제작사
	More	전압 또는 전류의 증가(정격의 20%이상)	DC/DC 고장	방향계전기 고장, 방향전환불가(후방고정)	-	HN051 / HP056	설계보완	제작사
	Less	전압 또는 전류의 감소(정격의 20%이하)	DC/DC 고장	방향계전기 오동작 방향전환불가(후방고정)	-	HN051 / HP056	설계보완	제작사
	Late	초기 가동시 전원공급지연(200ms 이상)	DC/DC 고장	정상공급까지 후방진행고정	-	HN051 / HP056	설계보완	제작사

며, 검토결과 표 4와 같이 안전대책수준의 수립이 불가능한 DC24V전원 및 CHR모듈관련 위험원이 도출되었다.

표 3의 기타사항에 해당하는 HN051과 HP056은 PHA에 의한 ATP시스템의 위험원으로써, "신호현시가 규제측면으로 충분히 현시되지 않음"을 의미하는 위험원 분류체계이며, 위험원에 대한 안전대책과 리스크의 평가는 다음과 같다.

4. ATSRX의 리스크평가

ATSRX의 HAZOP Study에 의해 도출된 위험으로 인한 리스크 평가는 ATP시스템의 안전확보를 위한 활동의 기준과 활동결과의 입증을 위해 반드시 요구된다. 따라서 본 논문에서는 도출된 위험원의 분석을 통해 PHA에서 제시된 ATP시스템 위험원목록과 HAZOP Study에 의해 도출된 위험원의 인과관계를 분석하여 표 3의 기타사항에 ATP시스템 위험원목록의 색인을 추가하였다.

표 4. HN051과 HP056의 PHA결과

시스템 명 :											
제품번호		작업기간		60일		작성날짜		2005.07.23 최종갱신			
분석단계		1단계종료				수정 : 유		부가 : 유			
위험원번호	위험원 내용	위험원대상	대책실시전			대책안	대책실시후		
			사고심각도	발생빈도	위험도크기		사고심각도	발생빈도	위험도크기
HN051	신호현시가 규제측면으로 충분히 현시되지 않음	N	B	3	II	D: 설계변경 E: 안전대책 S: 안전소자 W: 경고체제 P: 절차/교육 S:신호현시 고장시 안전측으로 동작하도록 설계 S:단일시스템의 위험측 고장이 사고로 발전되지 않도록 설계	B	5	III
HP056		P	A	3	I	S:단일신호의 위험측동작 실패는 실시간으로 모니터링하여 차단 S:단일 신호의 위험측 동작 실패는 정상신호통과시 복귀되도록 설계 P:인명사고(열차의 충추돌에 대한 처리절차 수립	A	5	III

N : Neighbor, P : Passenger

4.1 사고시나리오 및 리스크평가

HAZOP Study에 의해 도출된 위험원과 관련된 ATP시스템 위험원목록의 해당 위험원은 HN051과 HP056으로써, PHA활동에 의한 리스크평가결과는 표 4와 같다.

따라서, ATSRX의 전원 및 방향전환기능관련 위험원은 위험원목록의 HN051과 HP056와 동일한 리스크레벨을 갖으며, PHA에 의한 리스크평가 결과 HN051과 HP056의 리스크는 각각 II와 I로 평가되었으므로, 리스크레벨 I을 발생시킬 수 있는 위험원으로 등록하였다.

ATP시스템 구축사업의 안전기준으로 적용된 ALARP(As Low As Reasonably Practicable)이론에 의거하여 리스크레벨 I은 반드시 II 또는 III이하로 감소시키기 위한 대책을 수립해야 한다. 특히 방향전환관련 위험원의 발생은 열차의 ATS구간 전방운전시 CHR모듈고장 또는 DC24V전원공급 고장의 위험원이 발생하여 ATS안테나가 후방으로 고정되어도, 상위시스템 또는 운전자에게 경고하기 위한 별도의 대책이 수립되지 않아서 ATS 무응동상황 발생의 원인이 될 수 있다.

표 4는 안전대책을 적용하여 사고발생빈도의 완화를 통한

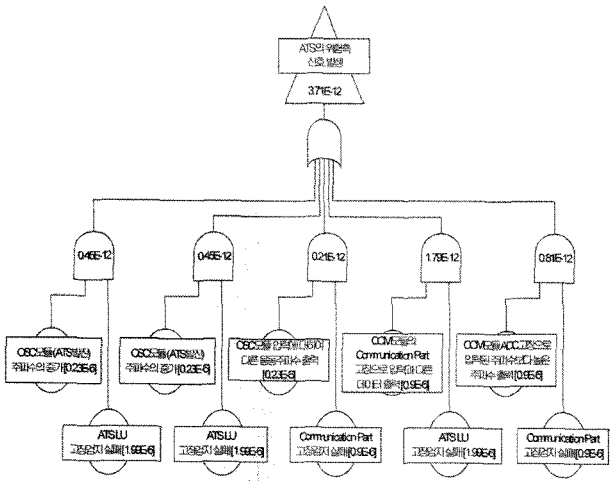

그림 3. 안전대책이 추가된 ATSRX의 위험측고장 FTA

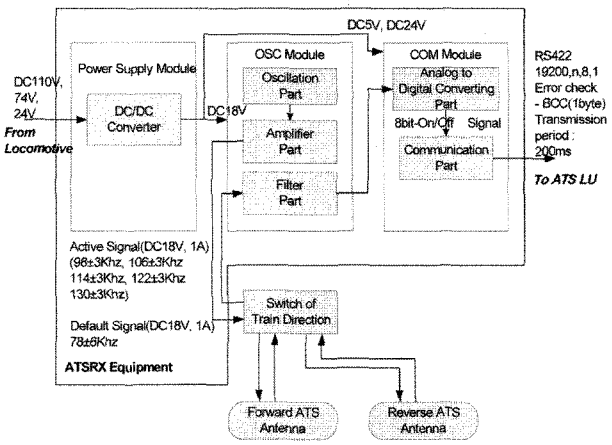

그림 4. 변경된 ATSRX의 내부구성도

리스크의 제어결과이다. 발생빈도의 완화는 안전대책 및 ATSRX의 고유기능 수행을 위한 하드웨어의 정량적인 고장률을 그림 3과 같이 결함트리분석(FTA)기법을 사용하여 철도신호시스템 RAMS관련 국제규격인 IEC 62278[9]과 안전관련 전기전자프로그래머블 제어기의 RAMS규격인 IEC 61508[10]에서 제안하는 리스크 매트릭스의 발생빈도 단계 5인 "Improbable"에 해당하는 평균고장확률 10^{-9}(약 10만년에 1회)이하임을 입증하여 평가하였다.

5. 리스크완화를 위한 설계변경

ATSRX의 HIA결과 제기된 열차의 방향전환을 설정하기 위한 CHR모듈관련 위험원에 대하여 허용할 수 있는 수준으로 안전대책을 수립하기 위하여 제작사의 설계엔지니어 및 ATP시스템 RAMS연구팀이 협의를 수행하였다.

5.1 ATSRX 설계변경

ATS구간의 방향전환관련 위험원의 근본적인 제거를 위해 기존 CHR모듈을 그림 4와 같이 무전원타입의 방향전환 스위치로 대체한 ATSRX의 변경방안을 제작사의 엔지니어가 제안하였다.

그림 4와 같이 변경된 ATSRX의 내부구성에 따라 세부구성요소의 기능 및 인터페이스도 표 1에서 표 5와 같이 변경되었으며, 설계가 변경된 ATSRX의 HAZOP Study를 위해 표 6과 같이 ATSRX의 인터페이스 사양도 변경되었다.

5.2 변경사항에 대한 위험원분석 및 리스크평가

안전성활동의 수명주기에서 안전의 확보를 위해 변경사항이 발생하는 경우, 해당부분 또는 시스템전반에 걸쳐 HIA를 반복수행하도록 IEC 62278에서 권고하고 있다.

표 5. 변경된 ATSRX의 세부구성별 입출력

모듈	입력		출력	
	대상	특성	대상	특성
전원모듈	기관차	DC전원	OSC모듈	DC전원
			COM모듈	DC전원
OSC모듈	전원모듈	DC전원	ATS차상 안테나	ATS발진 신호
	ATS차상 안테나	ATS응동신호	COM모듈	ATS응동신호
COM모듈	전원모듈	DC전원	ATSLU	통신전문
	OSC모듈	ATS응동신호		
	ATSLU	통신전문		
소프트웨어	COM모듈	8비트디지털	ATSLU	통신전문
	ATSLU	통신전문		

따라서, 물리적인 구성이 변경된 ATSRX를 대상으로 표 7과 같이 HAZOP Study를 사용한 위험원의 도출과 분석을 다시 실시하였다. 또한 설계가 완성됨에 따라 ATSRX의 설치, 시운전, 유지보수시 발생할 수 있는 위험원에 대한 도출을 수행하였으며, 시험이 완료되어 영업운전 수행시 사용자로 인해 발생할 수 있는 위험원에 대한 도출도 HAZOP Study를 통해 검토하였다.

ATSRX의 세부기능 및 인터페이스와 관련된 설계 및 제작단계에 대한 HAZOP Study를 통해 ATSRX 내부에서 발생할 수 있는 위험원에 대한 안전대책을 모두 수립하였으며, 설치, 시운전, 유지보수, 운영에 대해서도 위험원분석 및 안전대책을 수립하였다. 설치, 시운전, 유지보수 및 운영과 관련된 안전대책은 보호회로 등의 물리적 또는 정량적 판단기

표 6. 변경된 ATSRX의 인터페이스 사양

인터페이스	세부사양
DC전원	철도차량으로부터 DC110V±30%/500mA, DC74V-20%+30%/500mA, DC24V-20%+30%/500mA를 입력받아 ATSRX내부로DC24V/130mA, 18V/1A, 5V/2A를 공급
ATS 발진신호	78±6kHz, DC18V, 1A
ATS 응동신호	98±3kHz,106±3kHz,114±3kHz,122±3kHz,130±3kHz 68±3kHz(전차선절연구간)사구간예고지상장치
통신전문	RS422(19200,n,8,1)/BCC 1Byte Error Check Transmission period 200ms
COM모듈내 ADC신호	8bit-Digial신호

Bit	해당의미	Hex Value
0	98kHz	0xFE
1	106kHz	0xFD
2	114kHz	0xFB
3	122kHz	0xF7
4	130kHz	0xEF
5	78kHz(평상시)	0xDF
6	68kHz(사구간)	0xBF
7	Hear Beat Signal	0x7F

준을 수립하기 보다는 정성적분야에 해당하는 예방 및 대처 절차를 수립하여 위험원의 발생빈도를 줄이기 위한 대책이다. 따라서, ATSRX와 관련해서는 철도안전법, 철도청 안전규정 및 각종 운영규정을 검토하여 적절한 대책이 현재 적용되고 있음을 제시하였으며, ATSRX의 안전한 운영을 위한 요구사항 중 관련규정에 없는 대책에 대해서는 유지보수 메뉴얼 및 운영메뉴얼에 해당 절차를 포함시켰다.

6. 결 론

본 논문은 철도신호시스템 RAMS규격인 IEC 62278의 안전성활동 수행체계에서 시스템단위 위험원도출을 위하여 HAZOP Study 기법을 적용하여 ATSRX장치의 위험원을 도출하였으며, 도출된 위험원으로 인한 리스크를 평가하여 허용할 수 있는 수준으로 위험원에 대한 안전대책수립 및 설계변경을 수행하였다. 이러한 연구는 철도안전법의 공표 이후에 새로이 개발되는 철도신호시스템의 안전성입증을 위한 세부 적용방안으로 제시하기에 충분하며, 특히 ATSRX의 위험원도출을 통해 ATP시스템이 ATS구간을 운행할 때 발생할 수 있는 ATS지상자 무응동현상의 원인을 설계단계에서 도출하여 보완하였으며, 해당위험원을 제거하기 위한

표 7. 변경된 ATSRX의 HAZOP Study 결과

해당 수명주기	HAZOP Study의 대상	결과
설계/제작	전원모듈(DC18V)	안전대책수립
	전원모듈(DC05V)	안전대책수립
	OSC모듈(ATS발진)	안전대책수립
	OSC모듈(ATS응동)	안전대책수립
	COM모듈(ATSLU로 전송-전기적신호)	안전대책수립
	COM모듈(소프트웨어)	안전대책수립
	COM모듈(ADC기능)	안전대책수립
	전원인터페이스	안전대책수립
	ATSLU인터페이스(전기적신호)	안전대책수립
	ATSLU인터페이스(데이터)	안전대책수립
설치/시운전/유지보수	ATSRX의 설치/시운전/유지보수	안전대책수립
운영	ATSRX의 운영	안전대책수립

설계변경으로 ATP시스템의 안전성을 보다 향상시킬 수 있었다.

본 논문의 내용을 포함한 ATP시스템의 안전입증은 안전성활동 전반에 걸쳐 국제규격을 근거로 작성된 문서와 함께, 2007년 개통 전까지 실시되는 시운전을 통한 FRACS데이터에 의해 입증될 것이다.

참 고 문 헌

1. 철도청 (2003), "차상신호(ATP)시스템 도입을 위한 제안요청서"
2. UIC (2000), "ETRMS/ETCS-Class1 System Requirements Specification"
3. IEC61882 (2001), "Hazard and operability studies(HAZOP Studies) - Application guide"
4. RailTrack, UK (2000), "Engineering Safety Management" Issue3, Yellow Book 3
5. 한국철도기술연구원 (2002), "철도신호제품의 안전성검증을 위한 실행체계 구축방안에 관한 연구"
6. IEC 60812 (1985), "Failure Mode Effect analysis"
7. 한국철도기술연구원 (2005), "철도청 차상신호(ATP)시스템 구축사업의 1단계 종합안전대책기술서(Safety Case)"
8. 유경제어 (2004), "Specification of the ATSRX functionality requirements"
9. IEC62278 (2002), "Railway applications-Specification and demonstration of RAMS", pp.59-65
10. IEC61508 (1998), "Functional safety of electrical/electronic /programmable electronic safety-related systems"