DOI: http://dx.doi.org/10.14248/JKOSSE.2014.10.2.043
ISSN 1738-480X (Print)
ISSN 2288-3592 (Online)
Journal of the Korea Society of Systems Engineering

도시철도관제시스템 안전성 확보를 위한 RAMS 활동 및 그 적용사례에 관한 연구

최요철[1)*]

1) LS산전

A Study on the RAMS Activities and Practices for assuring Safety of the Centralized Traffic Control System of Urban Railway

Yo Chul Choi[1)]

1) LSIS Co., Ltd.

Abstract : the Centralized Traffic Control(CTC) System of Urban Railway is an element(subsystem) of the Urban Railway system to aim safety operation and efficient management of rolling stock in accordance with a train scheduling program in train operation ways. That's why the CTC System must be developed considering systematic and safety-guaranteed methods such as RAMS(Reliability, Availability, Maintainability, and Safety) refereed to IEC standards. The CTC System is consists of rolling stock, signaling, power supply, communication, and mechanical equipment and preforms control and remote monitoring functions. The technical activities considering safety process are very important at such an early stage of development in a railway project. This paper introduces RAMS activities and an independent safety assessment by 3rd Party focused on a safety applied to a development of the CTC system of Urban Railway and proposes the experiences as well practices

Key Words : RAMS Process, Reliability, Availability, Maintainability, Safety, Systems Engineering, Railway Project, Urban Railway, Centralized Traffic Control(CTC)

* corresponding author : Yo Chul Choi/LSIS Co., Ltd/ycchoia@lsis.com

1. 서 론

1.1 철도관제시스템의 중요성

본 논문은 도시철도에서 열차의 운영을 담당하는 관제시스템(CTC; Centralized Traffic Control) 개발에 적용한 RAMS 활동에 대한 것이다. 관제시스템은 평상시 고객이 이용하는 시간에는 본선 열차 운행, 신호, 전기, 통신, AFC(Automated Fare Collection), 시설물에 대하여 이상 유무를 24시간 모니터링 하고, 위급사항 발생 시 고객의 안전 확보를 최우선으로 하고 병발 사고를 미연에 방지하여 사고에 대한 피해를 최소화 하도록 현장을 통제, 지시하여 사고의 복구가 빠른 시간 안에 이루어지도록 한다. 영업이 종료되는 시간에는 열차 운행에 대한 준비, 각종 관제 시스템 점검, 각종 유지보수 작업 통제 및 기타 안전 제반 사항을 총괄적으로 관리한다.[1]

이러한 이유에서 도시철도 관제시스템은 철도운영에 있어 열차운영계획에 따라 전동차의 안전운행과 효율적인 관리를 목적으로 하는 철도시스템의 한 요소로서 다양한 시스템이 종합적으로 구성되어 있으므로, 철도운영기관은 체계적이고 안전성이 확보된 개발을 요구한다. 이렇듯이 관제시스템은 전동차뿐만 아니라, 신호, 전력, 통신, 그리고 기계설비 등에 대한 제어, 원격감시, 통제 기능을 수행하므로서 시스템 개발 초기부터 안전에 대한 고려가 반드시 필요하며, 시험 및 시운전 단계에서 최종적으로 안전에 대한 보증활동이 이루어져야 한다.

본 논문은 도시철도관제시스템 개발에 적용된 안전성 중심의 RAMS(Reliability, Availability, Maintainability, and Safety)활동을 소개하고, 그 적용사례를 제시하였으며, 이를 통해 획득한 경험 등을 제시하였다. 본 논문의 구성은 서론부분에서 안전을 고려한 종합관제시스템의 개발 중요성에 대해 제시하였으며, 본론에서는 IEC 62278[2] 및 62279[3] 표준에 따른 안전중심의 종합관제시스템 개발을 위한 절차와 산출물, 그리고 그 적용사례에 대해 기술하였다. 다음의 그림 1은 관제시스템 및 타 시스템의 형상을 나타내고 있다. 이처럼 관제시스템은 철도시스템에 대한 종합적인 제어의 기능과 관리의 기능을 수행하게 된다.

[Figure 1] CTC and other systems configuration[4]

다음의 그림 2는 철도 종합관제시스템의 주요 기능을 나타내고 있다. 종합관제실에는 열차의 운행현황을 종합 제어하는 열차운전관제, 고객안내 정보 및 신호 그리고 통신시스템을 감시 · 제어하는 신호통신관제, 차량 및 역사 내 전력공급 설비를 감시 · 제어하는 전력관제, 그리고 역사 기계 설비를 감시 · 제어하는 기계관제 장치가 있다.

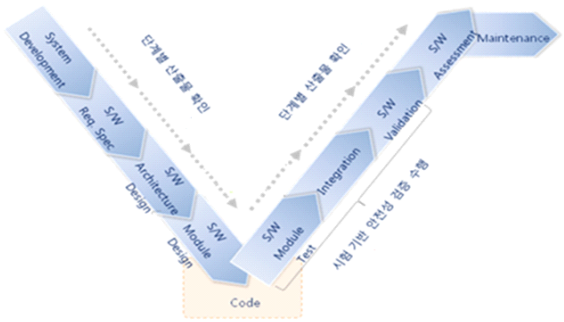
[Figure 2] Main functions of CTC

2. 안전중심의 철도관제시스템 개발

관제시스템은 일반적으로 H/W와 S/W로 구성되며, 그 외에 데이터, 운용자, 프로세스, 절차, 설비, 재료의 제공을 통해서 개발되게 된다. 본 연구는 기존 H/W를 유사한 장비로 교체하기 때문에 별도의 H/W 안전성 활동은 제외하며(RAM활동 제외), 신규로 개발되는 관제 S/W를 대상으로 수행하였다. 특히 신규 관제 S/W(신호 및 전력)를 개발함에 있어 적용한 방법과 그 결과에 대해 제시하였다.

2.1 관제시스템 S/W 안전성 활동 전략

본 논문에서 제시한 관제시스템은 기존 관제시스템의 H/W를 동등 혹은 이상의 성능을 보유한 H/W로 교체, 신규로 건설되는 구간에 대한 관제시스템을 기존 관제시스템과 통합적으로 운용할 수 있는 S/W를 개발하여 구축된다. 다음 그림 3은 관제 SW 개발을 위한 전략을 나타내고 있다.

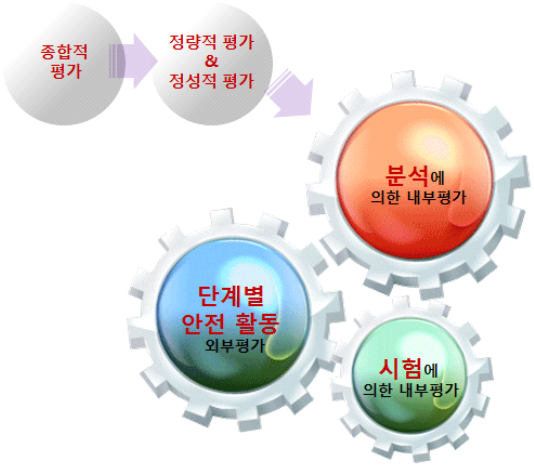


[Figure 3] Strategy of development for CTC SW

2.1.1 SW 안전관리 전략

SW 안전관리는 그림 4와 같이 다음과 같은 세부적인 활동을 통해 소프트웨어 안전성에 대한 종합적인 평가를 실시하였다.

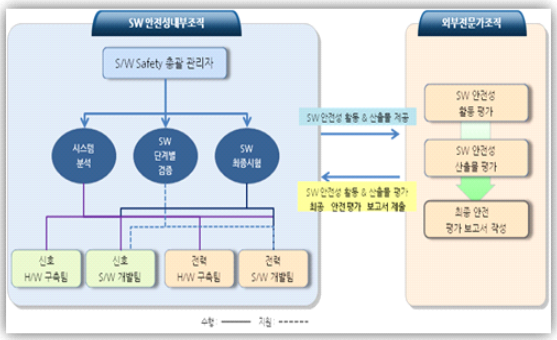
- 생명주기 기반의 SW 개발절차 수립
- 독립 내부조직에 의한 단계별 산출물 확인
- 독립 내부조직에 의한 시험기반 안전성 검증 수행
- 외부 전문가에 의한 SW 안전성 평가 활동 및 산출물 평가



[Figure 4] A comprehensive assessment for CTC SW

2.1.2 SW 안전 조직

올바른 SW 개발 및 안전관리 활동을 위해 그림 5와 같이 전문적이고 독립적인 개발 인원 및 제3의 전문가 조직을 구성하였다.



[Figure 5] Safety activity organization for SW

2.1.3 SW 안전조직의 역할 및 책임

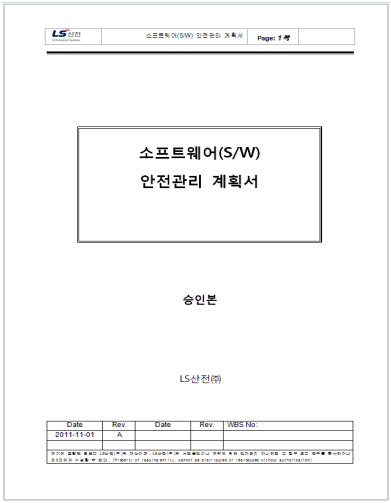
상기에 언급한 SW 개발과 관련된 조직의 역할 및 책임을 표 1과 같이 제시하였다. SW 개발조직(SW 개발과 안전성 조직)은 위험원 식별 및 분석, 설계반영, 시스템 개발 등의 역할 및 책임을 수행하고, 외부 전문가 조직은 SW 안전성 활동에 대한 평가를 수행하고 이에 대한 보고서를 작성하는 역할과 책임을 가진다.

<Table 1> Role & Responsibility of SW Safety Organization

인원	역할	책임
S/W Safety 관리자 및 실무자 (총괄 S/W 분석 및 시험 관리)	시스템 안전 분석 S/W 안전관리 S/W 변경 분석 S/W 안전 시험계획 분석 S/W 시험 안전분석	시스템 안전분석서 S/W 안전관리 계획서 S/W 변경분석서 S/W 안전 시험계획 분석서 S/W 시험 안전분석서
신호 S/W 개발팀	신호 S/W 개발 신호 S/W 변경 관리 신호 S/W 안전 시험계획 작성 신호 S/W 시험 및 결과보고서 작성	신호 S/W 변경보고서 신호 S/W 안전 시험계획서 신호 S/W 시험 결과 보고서
전력 S/W 개발팀	전력 S/W 개발 전력 S/W 변경 관리 전력 S/W 안전 시험계획 작성 전력 S/W 시험 및 결과보고서 작성	전력 S/W 변경보고서 전력 S/W 안전 시험계획서 전력 S/W 시험 결과 보고서
외부전문가조직	안전성 활동 평가 안전성 평가 보고서 작성	최종 안전평가 보고서

2.1.4 SW 안전관리 계획 작성

SW의 체계적인 개발과 객관적 평가를 위한 안전관리 계획서[5]를 되었다. SW 안전관리 계획서는 총체적인 SW 안전활동에 대해 기술하고 있다. 특히 안전활동 전략, 세부적인 안전활동 계획, 안전조직, 안전활동 생명주기, 안전분석과 리스크 평가 방법, SW 안전관리 생명주기 프로세스, 안전활동을 통한 산출물 목록, 그리고 안전활동 일정 을 기술하고 있다.


소프트웨어(S/W)
안전관리 계획서

승인본

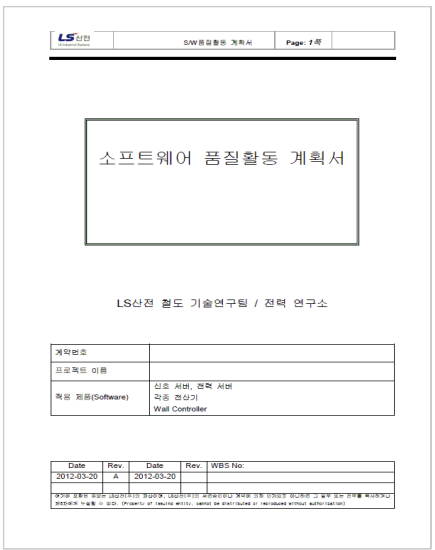
LS산전㈜

Date	Rev.	Date	Rev.	WBS No:
2011-11-01	A			

[Figure 6] SW Safety Management Plan

2.1.5 SW 품질활동 계획 작성

SW 품질활동 계획서는 관제 SW를 체계적으로 개발하는 과정에 수행되는 품질활동에 대해 기술하고 있다.[6] 특히 품질활동 조직 및 인원, 품질활동 전략, 세부적인 품질활동 계획, SW 품질관리 방안, 형상관리, 변경관리 등의 내용을 포함하고 있다.


소프트웨어 품질활동 계획서

LS산전 철도 기술연구팀 / 전력 연구소

계약번호	
프로젝트 이름	
적용 제품(Software)	신호 서버, 전력 서버 각종 전산기 Wall Controller

Date	Rev.	Date	Rev.	WBS No:
2012-03-20	A	2012-03-20		

[Figure 7] SW Quality Activity Plan

2.1.6 관제 SW 개발 생명주기 단계별 활동 및 산출물 목록

아래의 그림 8은 IEC 62278 표준에 따른 관제 시스템 개발과 관련된 생명주기 단계 및 활동, 그리고 산출물을 나타내고 있다.

[Figure 8] Life Cycle and deliveries of CTC SW Development

2.1.7 관제 S/W 리스크 분석 및 안전요구사항

먼저 관제 신호 S/W에 대한 리스크 분석(FHA; Functional Hazard Analysis)을 수행하여 36개의 위험원 중 안전에 영향을 미치는 7개의 위험원(표 2)을 도출하여 설계에 반영하고 시험을 통해 조치하였다.[7] 도출된 36개의 위험원은 개발팀에서 고객의 인터뷰, 기술문서 분석, 기존 시스템의 위험원, 그리고 경험 등을 통해 습득한 위험원을 토대로 작성이 되었으며, 최종적으로 고객의 검토를 통해 안전에 영향을 미치는 핵심 위험원이 분류되었다. 본 연구에서는 관제 S/W의 안전성 수준을 III수준이하로 통제하는 안전 목표를 수립하였다. 표 2는 관제 신호 S/W에 대한 리스크 분석 결과와 안전요구사항을 보여주고 있다.

다음으로 관제 전력 S/W에 대한 리스크 분석을 수행하여 44개의 위험원 중 안전에 영향을 미치는 4개의 위험원(표 3)을 도출하여 설계에 반영하고 시험을 통해 조치한 결과를 나타내고 있다. 중요 관제 신호 및 전력 S/W 위험원은 안전요구사항으로 전환되어 최종단계까지 관리되었으며, 시험을 통해 모든 만족함을 확인하였다. 표 3은 관제 전력 S/W에 대한 리스크 분석 결과와 안전요구사항을 보여주고 있다.

<Table 2> Safety critical hazards of CTC Signal S/W

구분	No.	세부기능	리스크 분석			관련 프로세스	영향	위험발생 원인 (위험원)	제거/경감 대책 (안전요구사항)	관련 H/W
			심각도	발생 빈도	안전성 수준					
제어 직접 관련 기능 GR	FuHA. 1	열차운행 스케줄에 의한 자동진로 제어	H	L	II	ART	오방향 진로 설정	DB오류	1.철저한 테스트 수행 2.테스트 기간중 모든 DB 검증	서버
	FuHA. 2	제어 정보(수동 제어)	H	L	II	DSP	제어기능 제한	DB오류	1.철저한 테스트 수행 2.테스트 기간중 모든 DB 검증	서버
현장 표시, 열차 추적 관련 GR	FuHA. 3	열차운행 상황 감시	M	M	II	IND	감시기능 제한	DB오류	1.철저한 테스트 수행 2.테스트 기간중 모든 DB 검증	서버
	FuHA. 4	열차번호 관리 및 추적	M	M	II	TRK	1.감시기능 제한	DB오류	1.철저한 테스트 수행	서버

구분	No.	세부기능	리스크 분석			관련 프로세스	영향	위험발생 원인 (위험원)	제거/경감 대책 (안전요구사항)	관련 H/W
			심각도	발생 빈도	안전성 수준					
현장 표시, 열차 추적 관련 GR							2.제어기능 제한		2. 테스트 기간중 모든 DB 검증	
	FuHA. 5	대형표시반과의 인터페이스	M	M	Ⅱ	COMM	감시기능 제한	1.DB오류 2.MAP오류	1.철저한 테스트 수행 2.테스트 기간중 모든 DB 검증 3.MAP VERSION 관리 철저	서버
	FuHA. 8	열차운행 제어 및 표시	M	L	Ⅱ	L/S	1.감시기능 제한 2.제어기능 제한	1.통신장애 2.관제사 취급오류	1.철저한 테스트 수행 2.관제사 교육	전산기 (S/O)
	FuHA. 9	대형표시반 화면 표출정보 제공(열차 운행상황 감시)	M	M	Ⅱ	L/S	감시기능 제한	1.DB오류 2.MAP오류	1.철저한 테스트 수행 2.테스트 기간중 모든 DB 검증 3.MAP VERSION 관리 철저	대형 표시반

<Table 3> Safety critical hazards of CTC Power S/W

구분	No.	세부기능	리스크 분석			관련 프로세스	영향	위험발생 원인 (위험원)	제거/경감 대책 (안전요구사항)	관련H/W
			심각도	발생 빈도	안전성 수준					
제어 직접 관련 기능	FuHA. 1	자동 급단전	H	L	Ⅱ	spxAutoCtrl spxCtrlCmdMng spxIOCommDrv	제어 부동작 및 오동작	기능오류 자동제어식 작성시 실수	자동 제어식 작성교육 자동 제어식 검증 테스트 수행	서버
	FuHA. 2	정류기 교호운전	H	L	Ⅱ	spxSched spxDBCom spxCtrlCmdMng spxIOCommDrv	제어 부동작 및 오동작	기능오류, 교호스케쥴 입력실수	교호 운전 스케줄러 사용 교육 테스트 수행	전산기 (수퍼바이저) (운용자)
	FuHA. 3	자동제어 금지/해지	H	M	I	spxAutoInhibit	제어 부동작	기능오류	테스트 수행	서버
	FuHA. 4	사용자 포인트 제어	H	L	Ⅱ	spxGRun_d.exe spxDBCom spxIOCommDrv	제어 부동작 및 오동작	사용자 오조작	테스트 수행	전산기 (수퍼바이저) (운용자)

2.1.8 관제 S/W 평가를 위한 독립 안전성 평가

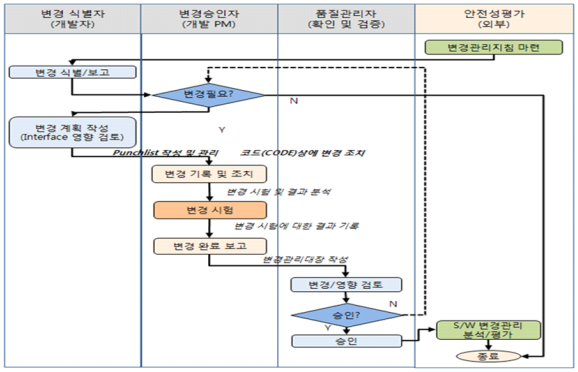
외부 전문가(조직)의 의한 S/W 독립 안전성 평가 활동은 S/W 안전관리 계획서에 정의된 안전성 활동 절차 및 산출물을 중심으로 이를 분석 및 평가하는 업무를 의미하며, 요구사항 명세 단계, 설계, 개발, 시험 및 시운전, 그리고 최종 안전평가 보고서 제출 활동까지 각 진행단계에서 전체적이며, 지속적으로 S/W 개발팀과 협력하여 자료를 입수 및 분석, 그리

고 협의 평가하는 활동이 단계적으로 진행하였다. 또한 프로젝트의 종료 단계에서 외부 전문가에 의한 평가 일정을 전체 개발일정 및 S/W 안전성 활동 일정이 종합적으로 완료될 수 있도록 수행하였다. 아래 그림 9는 그림 8의 생명주기(IEC 62278 기준)를 프로젝트 단계로 표현하였으며, 이러한 단계별 외부 독립안전성 평가 활동에 대한 내용을 서술하였다.

[Figure 9] Independent Safety Assessment for CTC S/W

2.1.9 형상관리 절차 및 형상관리 수행

문서나 코드에 대한 형상 변경이 발생할 경우 아래 그림 10과 같은 절차를 준용하여 변경을 수행하였다. 이는 S/W 형상의 무결성을 보장하고 변경의 적합성을 보장하기 위해 실시되었다.



[Figure 10] Procedure for Configuration Management

다음의 그림 11은 형상관리 수행 결과를 기록한 형상관리대장(Configuration Management Register)이다. 형상변경 이력과 문제발생 시 기준이 된다.

구분	장비	목록	버전	변경내역	설치일자
실행파일	서버	BOOT	1.1	프로세스 증설	2012.11.13
		ARC	1.1	알람실적 MSC로 수동 전송 기능 추가	2012.10.24
		ARM	1.0	종합시운전 환경의 설치	2012.09.11
		ART	1.6	1. Fleeting설정 상태 진로 제어 2. 출발 진로(열차) 제어시 조건체크 기준 변경 3. 온수 하선 트리거 포인터 추가(791T) 4. 온수하선 시각제어 (795T)	2012.12.06
		ATO	1.3	차량 회복모드 지정	2012.12.06
		CLS	1.0	종합시운전 환경의 설치	2012.09.11
		COMM	1.3	중계PC(GMIS) I/F 통신 프 로그램 추가	2012.10.24
		CONF	1.0	종합시운전 환경의 설치	2012.09.11
		CVT	1.1	수락산 PSD정보 링크Index 조정	2012.11.13
		DBMS	1.5	1. 온수 역 궤도 데이터 베이스 수정 2. 온수 하선 겐트리업 3. 시스템 데이터베이스 변경	2012.12.06
		DSP	1.1	임시열차 스케줄관리 화면 기능추가	2012.12.06

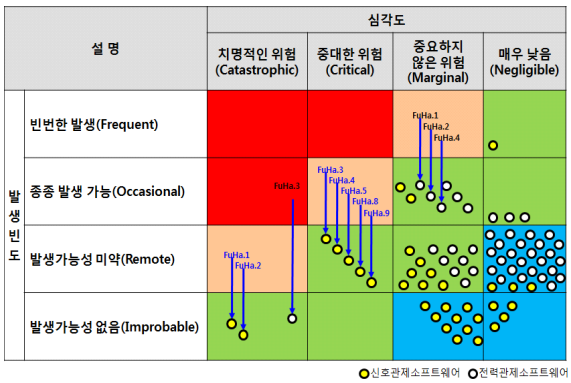
[Figure 11] Configuration Management Register Sample

<Table 4> An action results of Final Hazards(an omission)

위험원 No.	(안전대책 적용 전) 안전성수준	상세 안전 대책	시험 점검표	(안전대책 적용 후) 안전성수준
FuHA.1	II	열차 운행 스케줄에 의한 자동진로 제어 1)역제어 모드 체크 1. 진로구간 궤도점유 체크 2. 선로전환기 상태 체크 3. 대향진로 체크선행열차 체크	합격	III
FuHA.2	II	제어정보(수동제어) 1)역제어 모드 체크 4. 제어권한 체크 5. 제어한 이름(심볼) 체크	합격	III

2.1.10 최종 위험원 조치 결과

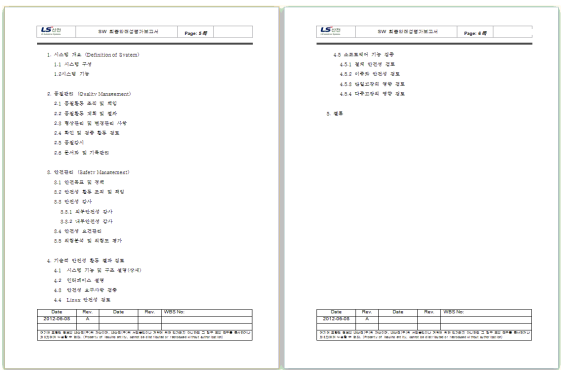
중요 관제 신호 및 전력 S/W 위험원에 대한 경감대책(설계, 시험, 운영 및 유지보수 등)을 수립하여 위험원이 안전에 영향을 미치지 않도록 조치하였다. 위험원은 주로 발생빈도를 낮추는 방향으로 조치하였다.



[Figure 11] Final action results for critical 11 hazards

2.1.11 최종 안전성 평가 보고서 작성

관제 신호 및 전력 S/W에 대한 안전성을 보장하기 위해 최종적으로 아래와 같은 목차로 외부 전문가에 의해서 최종 안전성 평가보고서가 작성되고 평가되었다. 이는 고객에게 전달되어 최종 승인 되었다.



[Figure 12] Contents of Final Assessment Report

3. 결 론

본 논문을 통해서 도시철도 관제시스템 개발에 포함된 S/W에 대한 안전성 중심의 Safety 활동을 소개하고, 적용사례를 제시하였다. 안전성 중심의 Safety 활동은 IEC 62278 및 IEC 62279 표준을 참고하여 정의하였다. 적합한 S/W 안전성 활동을 위해서는 S/W 생명주기에 따른 적절한 개발활동이 선행되어야 하며, 안전성을 보증하기 위해서는 반드시 다양한 위험원 분석이 필요하다. 또한 위험원 분석을 통해 도출된 안전 요구사항을 최종 시험 및 시운전 단계까지 추적하여 해결하는 노력의 중요성도 인식하게 되었다. 안전성 중심의 Safety 활동은 관제시스템과 관련된 위험원 식별/대책수립/설계상 조치/위험원경감/운영상 추가조치 대책 수립 등으로 추진되고 완료되었다. 실제적인 경험을 통해서 종합적인 S/W 안전성 활동을 수행될 경우 안전한 관제시스템을 개발할 수 있다는 확신을 갖게 되었으며, 향후 국제 표준 기반의 체계적인 접근이 수행될 경우 안전하고 국제 수준에 부합하는 관제 S/W 개발이 가능할 것으로 판단된다.

References

1. https://www.ulrt.co.kr/safety/safety_04.do
2. IEC 62278, “Railway applications –Specification and demonstration of reliability, availability, maintainability and safety(RAMS)” 2002. The International Electrotechnics Commission(IEC)
3. IEC 62279, “Railway applications –Communications, signaling and processing systems–Software for railway control and protections systems”, 2002, The International Electrotechnical Commission(IEC)
4. http://www.lsis.com/product/product.aspx?d1=A05&c=P00173
5. S/W Safety Management Plan, 7Line CTC project, SMRT, 2011
6. S/W Quality Activity Plan, 7Line CTC project, SMRT, 2011
7. S/W Functional Hazard Analysis Report, 7Line CTC project, SMRT, 2011