IEC 62279 요구사항 충족을 위한 열차제어시스템의 소프트웨어 품질보증 활동에 관한 연구

Software Quality Assurance Activities of Automatic Train Control System to meet Requirements of the IEC 62279 Standard

심규돈† 이종우* 박채영** 김재남*** 서영준***

Shim, Kyudon Lee, Jong-Woo Park, Chae-Young Kim, Jae-Nam Seo, Young-Jun

ABSTRACT

This paper presents the methods to acquire the Safety Certificate from Independent Safety Assessment based on the IEC standard62279 which is commonly applied to railway system for Automatic Train Control(ATC) system in accordance with Urban Maglev project.

This also shows approach methods and relative activities for project life-cycle to accomplish and ensure the system requirements of ATC system, RAMS and S/W quality activities. Furthermore, the key tasks conducted with ISA are noted in detail.

These kind of activities for software quality of ATC system to obtain Safety Certificate could be a CASE model to improve the quality of domestic railway system and products, and also contribute to the growth of railway business and toward the achievement of overseas' railway signaling markets.

1. 서 론

본 논문에서는 최근 들어 철도신호시스템분야에서 중요한 이슈로 부각되고 있는 소프트웨어 측면에서의 신뢰성과 안전성 수준을 국제규격(IEC 62279)에 부합할 수 있도록 하기 위한 접근방법을 모색하며, 실제 적용사례(국토해양부 및 한국건설교통기술평가원이 주관하는 국가 대형연구개발 실용화 사업인 “도시형 자기부상열차 실용화사업 시범노선건설 열차제어시스템 구매/설치”)를 통하여 현실적이고 접근 가능한 구체적인 활동 사항들을 프로젝트 수행과 연관하여 기술한다.

또한 열차제어시스템의 안전성 인증 획득을 위한 소프트웨어를 포함한 시스템 보증활동 및 시스템 보증을 위한 조직체계를 확립하고, 요구사항 관리 및 프로젝트 공정에 따른 절차적 시스템 보증 활동과 안전성평가 활동과의 연관관계, 시스템 전반에 걸친 RAMS 및 소프트웨어 품질보증 활동과 안전성 평가를 통한 인증활동에 대한 부분을 상세 제시하고자 한다.

본 활동을 통하여 지금까지 국제규격에 따른 활동기준에 대해서 모호하거나, 명확하게 정의되지 않은 사항들이 체계적으로 정리될 수 있을 것으로 사료되며, 타 사업 및 국내 철도신호시스템 적용을 위한 소프트웨어 품질 및 안전 무결성 수준 확보에 따른 안전성 확보방안의 구체적인 케이스 모델이 될 것으로 기대된다.

기본적으로 소프트웨어 측면에서의 신뢰성과 안전성 수준을 국제규격(IEC 62279)에 부합하기 위해서는 Hazard와 Risk를 철저히 인식하고 Risk를 분류하며, Risk 분류상에서 리스크 감소의 필요성이 요구된다.

† 정회원, (주)대우엔지니어링, 철도시스템사업그룹, 부장
E-mail : shim@dweng.co.kr
TEL : (031)738-0340 FAX : (031)738-0274
* 정회원, 서울산업대학교, 철도전문대학원/철도전기신호공학, 교수
** 정회원, (주)대우엔지니어링, 철도시스템사업그룹, 팀장
*** 비회원, (주)대우엔지니어링, 철도시스템사업그룹, 대리

위험 감소 요구를 만족하기 위해서는 시스템 안전 요구사항 명세화, 형상관리를 위한 계획 및 감시/제어하는 기술과 감독 활동이 필요하다. 안전 관련 소프트웨어 개발에 있어 적용원리는 기본적으로 Top-Down 설계방식, 각 작업의 모듈화, 개발 생명주기에 따른 각 작업의 검증, 검증된 모듈과 모듈 라이브러리의 사용, 확실한 검증을 위한 문서화 및 검증 가능한 문서들과 검증 시험을 요구한다.

1.1 IEC62279의 소프트웨어 품질요구사항 적용

IEC62279에서 요구하는 품질요구사항의 부합성을 품질계획 수립시 결정하여 프로젝트 진행함에 따라 적용하도록 한다.

[표-1] IEC62279의 소프트웨어 품질보증 요구사항 적용 상황

No	IEC62279의 소프트웨어 품질보증 요구사항	요구사항 적용	Remarks
1	ISO 9001의 시스템 품질보증에서 요구하는 사항은 반드시 만족해야 한다.	ISO 9001:2008인증서 획득을 통하여 ISO 9000 요구사항에 부합하는 시스템 및 소프트웨어 품질활동을 수행한다.	일반사항
2	ISO 9001에서 소프트웨어 개발에 관련된 사항을 수행해야 하며, 그 방법은 ISO 9000-3을 참조한다.	소프트웨어 품질보증 활동을 수행함에 있어 ISO 90001/ISO 9000-3 요구하는 방법과 절차에 부합하는 활동을 수행한다.	일반사항
3	ISO 9000-3의 전문과 IEC 62279에서 요구하는 실행 사항, 행위, 문서 등은 소프트웨어 품질보증 계획과 세부 개발에 의한 규약을 참조해야 한다. ISO 9000-3에 누락된 사항은 반드시 증명되어야 함을 원칙으로 한다.	ISO 9000-3 과 IEC 62279에서 요구하는 실행사항, 행위, 문서 등은 본 계획서의 단계별 활동 절차 및 문서관리에 포함 시켜 수행하도록 한다.	단계별 품질보증 활동 절차 문서관리
4	수명 주기 모델을 정의	소프트웨어 개발을 수행을 위해, 2가지 개발 방법론으로 접근하고 그에 따른 절차는 폭포수모델을 적용한다.	단계별 품질보증 활동 절차
5	각각에 포함된 단계를 정의	개발 방법론을 정의하고 그에 따른 수명 주기 모델을 정의하고 각각에 포함된 단계를 정의한다	단계별 품질보증 활동 절차
6	활동하는 기본이 되는 업무	개발 방법론을 정의하고 그에 따른 수명 주기 모델을 정의하고 각각에 포함된 단계를 정의하고 활동하는 기본업무를 정의한다	단계별 품질보증 활동 절차
7	진입과 진출점	개발 방법론을 정의하고 그에 따른 수명 주기 모델을 정의 각각의 포함된 정의된 단계에 진입과 진출점을 정의 한다.	단계별 품질보증 활동 절차
8	각 단계의 입력과 출력	개발 방법론을 정의하고 그에 따른 수명 주기 모델을 정의 각각의 포함된 정의된 단계에 입력과 출력을 정의 한다	단계별 품질보증 활동 절차
9	각 단계에서의 중요한 품질 활동	개발 방법론을 정의하고 그에 따른 수명 주기 모델을 정의 각각의 포함된 단계에서 품질활동을 정의한다	단계별 품질보증 활동 절차
10	기본 타스크와 각 활동에 대한 구조 유닛의 책임	개발 방법론을 정의하고 그에 따른 수명 주기 모델을 정의 각각의 포함된 단계에 기본 타스크와 각 활동에 대한 구조 유닛의 책임을 정의 한다.	단계별 품질보증 활동 절차
11	요구사항 추적 용이성	요구사항의 추적 용이성을 위해 요구사항 추적관리표를 작성하여 추적이 용이하도록 적용한다.	계획 및 분석
12	문서 구조의 추적 용이성	문서 구조의 추적 용이성을 위해서 표준화된 서식을 이용한다.	문서관리
13	소프트웨어의 개발, 확인, 검증, 동작 그리고 유지보수와 관련된 문서	소프트웨어 품질보증 활동 동안 산출 될 문서에 대해 정의한다.	소프트웨어 품질보증 산출 문서
14	시스템 통합 절차	시스템 통합 절차를 정의 한다.	통합 및 시험
15	사용된 코딩 표준	코딩기준을 정의한다.	구현

No	IEC62279의 소프트웨어 품질보증 요구사항	요구사항 적용	Remarks
16	선행된 검증 시험에 대한 평가	감사활동에 따라 선행된 검증 시험에 대한 평가가 이루어진다.	검토 및 감사
17	생산과 절차에서 사용되는 매트릭스(정량적 측정)의 정의. 소프트웨어 생산 매트릭스의 생성 시에는 반드시 품질 특성과 ISO/IEC 9126 시리즈에서 정의된 평가 지침을 참조해야 한다.	매트릭스의 정의와 생성에 관한 사항은 확인 계획서와 검증 계획서에서 정의하도록 한다.	소프트웨어 확인 및 검증 계획서
18	형상관리는 반드시 ISO 9000-3에 기술된 지침에 따라 수행되어야 한다.	소프트웨어 형상관리 계획서를 작성하여 본 사항을 정의하여 형상관리를 수행한다.	소프트웨어 형상관리 계획서
19	소프트웨어 문서는 최초의 승인 버전 출시 이전에 반드시 형상 제어를 수행해야 한다.	소프트웨어 형상관리 계획서에 형상제어에 대하여 정의 하고 절차를 수립하여 형상제어를 수행하도록 한다.	“
20	소프트웨어 소스 코드는 반드시 모듈 시험의 초기 단계 이전에 구조가 제어 되어야 한다.	소프트웨어 구조 사양서 와 소프트웨어 설계 사양서에 모듈 시험의 초기 단계 이전에 구조가 제어 되도록 정의하고 수행한다	소프트웨어 설계 문서
21	형상관리는 모든 수명 주기 동안 사용되는 환경 전반에 적용되어야 한다. 이러한 적용은 개발의 재생산성과 유지 보수 활동을 요구한다.	형상관리 계획에 본 내용을 정의하도록 한다.	소프트웨어 형상관리 계획서
22	소프트웨어 확인 계획의 결과와 적합성은 반드시 시험되어야 한다.	소프트웨어 확인 계획서 결과 및 적합성을 확인 하기 위한 자체 검토 및 감사를 실시한다.	검토 및 감사
23	이전에 개발된 소프트웨어는 반드시 소프트웨어 안전 무결성 수준과 종속성에서 요구하는 완전성을 만족해야 한다. 또한 새로운 소프트웨어는 공급자 또는 공급자들의 정의된 소프트웨어 품질보증 계획과 그 내용에 부합하도록 개발과 유지 보수되어야 한다.	소프트웨어 품질보증 계획서에 정의하고 본 계획과 그 내용에 부합하도록 개발과 유지보수가 되는지 확인 및 검증 활동을 통해 수행할 수 있도록 확인한다.	단계별 품질보증 활동 절차
24	공급자와 개발자는 반드시 문제에 대한 보고와 정정 행위의 절차에 대해서는 작성, 문서화 그리고 유지 보수 절차를 제공해야 한다. 이러한 절차는 품질보증 시스템에 포함되어, ISO 9001의 관련 절차에 따라 수행되어야 한다.	형상관리 계획서 및 유지보스 계획서에 정의되도록 적용한다	소프트웨어 형상관리 계획서 소프트웨어 유지보수 계획서
25	문제점의 보고와 정정 행위, 그리고 관리 책임을 위한 피드백을 목적으로 하는 행위에 필요한 문서의 정의	소프트웨어 관리절차에 정의 하고 자세한 내용을 형상관리 계획서에 정의 하도록 적용한다.	“
26	원인의 분석을 위한 문제점 보고서의 정보에 대한 분석을 정의	형상관리 계획서에 문제점 보고서의 정보에 대한분석을 정의한다.	소프트웨어 형상관리 계획서
27	개발 단계와 소프트웨어 유지보수 단계에서 확인된 문제점의 보고, 추적 그리고 해결에 대한 실행을 정의	소프트웨어의 형상관리 계획서 구체적으로 정의 하여 실행한다.	“
28	소프트웨어 안전 무결성 수준의 요구 사항에 부합하기 위한 문제의 예방 활동에 대한 정의	소프트웨어 안전 무결성 수준의 부합성을 위하여 규격서에서의 요구사항을 각 산출문서에서 예방 활동에 대한 내용을 정의한다.	문서관리
29	개발과 소프트웨어 유지 보수에 대한 책임 한계에 대한 정확한 정의	품질보증 계획서 및 소프트웨어 유지보수 계획서에 소프트웨어조직구성을 정의하고 그에 따른 책임한계를 정의하여 적용한다.	소프트웨어 품질보증 활동 조직 및 역할
30	정정 행위와 그로 인한 영향을 위한 처리 방법의 정의	소프트웨어 형상관리 계획서에 정정행위에 관한 구체적인 절차를 정의하여 적용한다.	소프트웨어 관리 절차
31	사용된 형식에 대한 정의	소프트웨어 형상관리 계획서에 사용된 형식에 대해 정의한다.	소프트웨어 형상관리 계획서
32	재시험, 재확인, 검증 그리고 재평가에 대한 요구사항의 정의	부적합 사항이나 오류의 발생시 시정조치 후 재시험, 재확인, 검증 그리고 재평가하는 것으로 시정조치에 절차에 따라 실행 하도록 한다.	소프트웨어 형상관리 계획서

2. 본 론

2.1 소프트웨어 품질보증 활동

2.1.1 품질보증 활동 개요

본 품질보증 활동의 목적은 소프트웨어 개발 전 과정에 걸쳐 소프트웨어의 품질 목표를 충족하며, 정의된 프로세스 및 방법을 준수하고 요구사항에 맞게 개발하고 있는지 확인하는 품질보증 활동을 체계적으로 계획하고 이행하는데 있다. 본 활동의 적용 범위는 소프트웨어 수명주기에 따른 개발 프로세스 전 과정이며, 개발체계와 개발 활동 및 각 단계에서의 산출물, 일정 등이 대상이다. 소프트웨어 품질보증 활동은 IEC 62279를 기반으로 하며, 수명주기에 따른 단계별 소프트웨어 품질 보증 활동을 다음과 같이 구성한다.

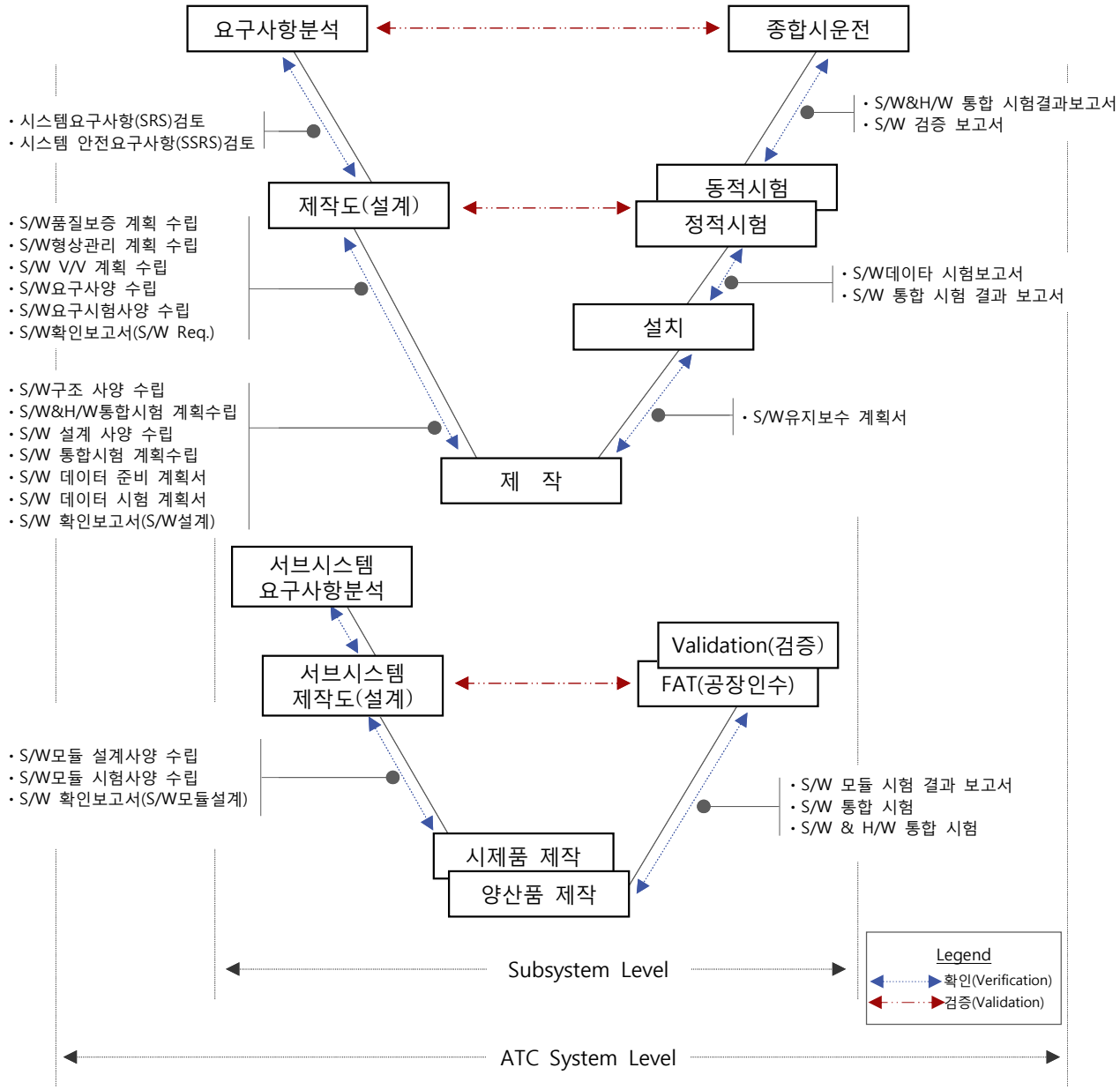


그림 1. 시스템 수명주기 단계별 소프트웨어 품질보증 활동

2.1.2 소프트웨어 품질보증의 구체적 실현방안

소프트웨어 품질보증 계획의 실시에 앞서 소프트웨어 품질보증의 인원은 무슨 문제가 생기고, 왜 그것이 진행되었으며, 어떻게 그것이 조직에 영향을 끼치고, 또한 품질보증 활동의 기대 효과가 무엇인지를 정확히 이해하고 있어야 한다. 품질보증 활동의 주요 업무는 다음과 같다.

- 소프트웨어 품질보증 프로그램의 작성
- 소프트웨어 품질보증의 정책, 절차 및 기준의 개발
- 소프트웨어의 개발활동에 따른 단계별 확인 및 검증
- 다음 사항들에 대한 소프트웨어 품질보증 감사
  (설계, 시험, 확인 및 검증, 형상관리, 문제보고 및 수정조치 사항)

2.2 소프트웨어 품질보증 활동 조직 및 역할

소프트웨어 품질보증 조직은 소프트웨어의 개발조직과 독립적으로 분리되어 존재한다. 단계별 활동 과정에서 발생하는 문제점을 도출하고 대책방안 제시 및 설계반영을 통한 시험단계에서 검증을 할 수 있도록 조직상의 독립성을 유지한다.

2.2.1 소프트웨어 품질보증 조직

“도시형 자기부상열차 실용화 사업 시범노선건설 열차제어시스템 구매·설치” 프로젝트 관련 품질보증 조직은 다음과 같이 구성한다. 프로젝트팀과 RAMS 및 품질보증팀은 상호간 독립성을 가지며, 업무보고와 기술정보 흐름을 독립적으로 운영한다.

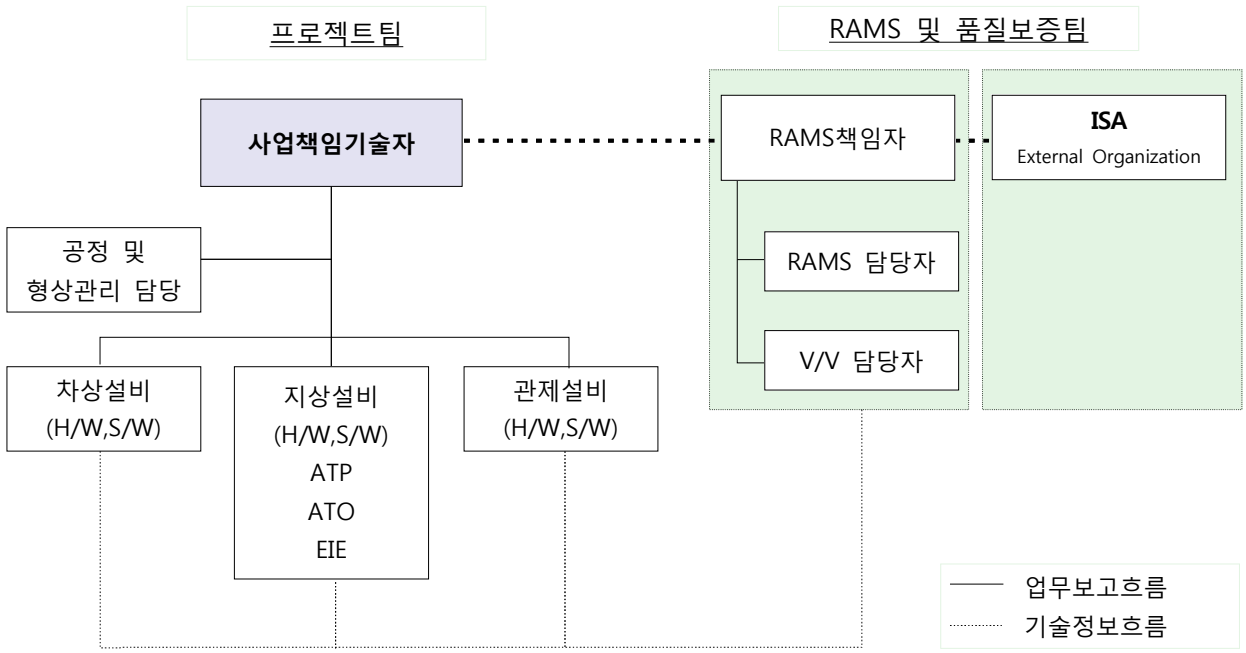


그림 2. 열차제어시스템의 소프트웨어 품질보증 조직도

2.2.2 소프트웨어 품질보증 조직 구성에 따른 책임 및 역할

소프트웨어 안전 보증 활동에 있어서 품질보증 조직 구성에 따른 책임 및 역할을 사전에 정의하여 프로젝트 진행 동안에 적용하도록 한다.

[표-2] 열차제어시스템 품질보증 조직구성에 따른 책임 및 역할

조 직	담당자	책임 및 역할 설명
사업책임	사업책임 기술자	• 사업 제반 계약사항의 이행과 업무 수행을 위한 대외협력업무 추진 • 사업의 적기 완공과 고객만족 업무 유대관계 강화 • 사업총괄 대행 (사업총괄 부재 시) • 내부 소프트웨어 품질 감사에 대한 감독 책임
사업관리 담당	공정관리	• 공정계획수립 • 상세일정계획 수립 • 성과 측정 및 보고 • 공정 및 일정 조정관리
	형상관리	• 형상관리 계획 수립 및 배포 • 형상요소 상태 기록
시스템 설계	지상설비 설계	• 설계계획 수립, 설계수행 및 설계변경관리 • 구매사양 작성 및 외주업체관리 • 하드웨어 제작 관리 및 소프트웨어 제작 • 시험, 검사 및 종합시운전 • RAMS 활동관련 업무수행(H/W, S/W)
	차상설비 설계	• 설계계획 수립, 설계수행 및 설계변경관리 • 구매사양 작성 및 외주업체관리 • 하드웨어 제작 관리 및 소프트웨어 제작 • 시험, 검사 및 종합시운전 • RAMS 활동관련 업무수행(H/W, S/W)
	관제설비 설계	• 설계계획 수립, 설계수행 및 설계변경관리 • 구매사양 작성 및 외주업체관리 • 하드웨어 제작 관리 및 소프트웨어 제작 • 시험, 검사 및 종합시운전 • RAMS 활동관련 업무수행(H/W, S/W)
H/W, S/W 확인 및 검증		• 각 프로젝트 단계별 RAMS 및 소프트웨어 품질 활동에 대한 확인 활동 • 시험 단계에서 초기 요구사항에 대한 충족여부에 따른 검증 활동
RAMS 책임		• 시스템 RAMS 및 S/W 활동에 대한 총괄 책임 • RAMS 분석 및 기술문서 생성 • 시스템 RAMS 요구사항 도출, 설계/제작 담당자에게 통보 • 시스템 RAMS 요구사항 반영여부 확인
RAMS 담당		• RAMS 분석 및 기술문서 생성 • 소프트웨어 산출 문서 검토 및 통합, 개발담당자에게 요구사항 통보
품질보증		• ISO 9001에 부합하는 품질활동 절차 프로젝트에 도입 • 현 프로젝트 수행에 따른 품질활동절차 준수여부 내부감사 시행 • 현 프로젝트 수행에 따른 품질보증 관련 기술문서 생성

2.3 단계별 품질보증 활동 절차

소프트웨어 개발방법론에 따라 소프트웨어 개발 수명주기를 정립한다. 본 사업의 개발 방법론은 각 장치에 사용되는 소프트웨어의 특성상 아래 같이 장치별로 분류하여 진행한다.

□ 차상설비, 지상설비, 관제설비(서버)

• 구조적 개발방법론을 기반으로 하는 자체 개발 방법론을 본사업에 적용하여 사용한다.

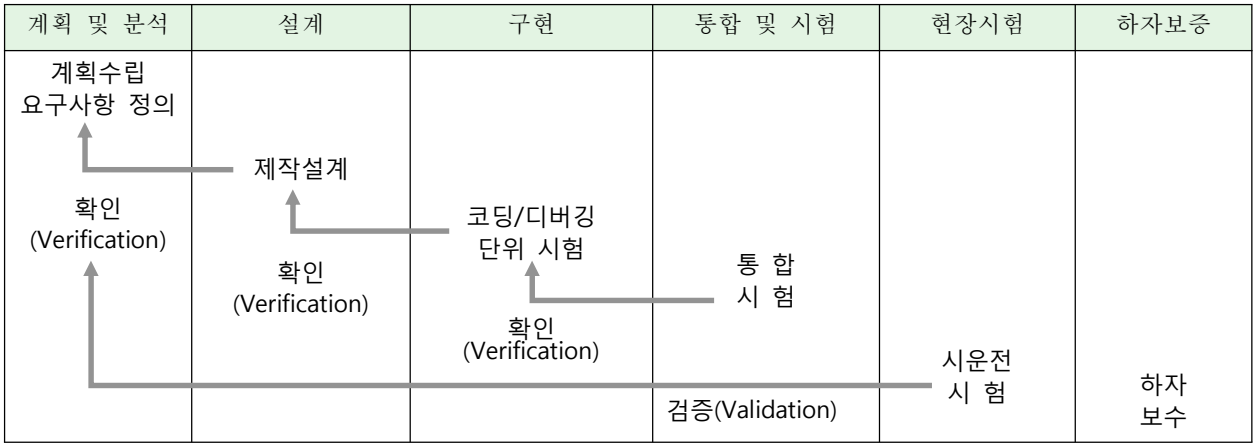
□ 관제설비(콘솔)

• 컴포넌트 기반의 개발방법론을 기반으로 하는 자체 개발방법론을 본 사업에 적용하여 사용한다.

개발방법론에 따라 본 사업의 소프트웨어 개발 모형은 폭포수 모델에 따른 절차를 기반으로 한다. 폭포수 모델을 기반으로 하여 계획 및 분석, 설계 구현, 통합 및 시험, 현장시험 순으로 나누어 각 공정 단계별을 순차적으로 접근하여 개발활동을 수행한다. 또한, IEC 62279에서 언급된 각 단계별 소프트웨어 확인활동을 통하여 단계별 요구사항 충족여부를 확인하는 점진적인 개발방식을 도입하여 소프트웨어 개발을 진행한다.

소프트웨어 개발 절차에 따른 단계별 활동은 다음과 같다.

[표-3] 소프트웨어 개발 수명주기에 따른 절차



또한 개발방법론의 절차에 따른 소프트웨어 개발 전 수명주기 동한 이루어지는 수행활동 및 소프트웨어 산출물은 다음과 같이 규정한다.

[표-4] 소프트웨어 개발 수명주기에 따른 세부절차 및 산출물

개발단계	소프트웨어 산출물	수행활동(검토 및 감사)
계획 및 분석 단계	• 소프트웨어 형상 관리 계획서(SwCMP) • 소프트웨어 품질보증 계획서(SwQAP) • 소프트웨어 확인 계획서 • 소프트웨어 검증 계획서 • 소프트웨어 요구 사양서 • 소프트웨어 요구사항 시험 사양서 • 소프트웨어 확인 보고서(요구사항)	• 계획, 표준, 절차의 수립 및 검토 • 계획서 검토 • 산출물 검토(요구사항 검토) • 프로세스 감사
설계단계	• 소프트웨어 통합 시험 계획서 • 소프트웨어 및 하드웨어 통합 시험 계획서 • 소프트웨어 구조 사양서 • 소프트웨어 설계 사양서(SwDS) • 소프트웨어 데이터 준비 계획서 • 소프트에어 데이터 시험 계획서 • 소프트웨어 확인 보고서(설계)	• 산출물 검토 (설계 검토) • 프로세스 감사
구현단계	• 소프트웨어 모듈 설계 사양서 • 소프트웨어 모듈 시험 사양서 • 소프트웨어 확인 보고서(모듈 설계) • 소프트웨어 유지보수 계획서 • 소프트웨어 모듈시험 보고서	• 산출물 검토 • 프로세스 감사
통합 및 시험단계 현장 시험	• 소프트웨어 통합시험 보고서 • 소프트웨어 및 하드웨어 통합시험 보고서 • 소프트웨어 데이터 시험 보고서 • 소프트웨어 검증 보고서	• 프로젝트 산출물 검토(시험 결과 검토) • 프로세스 감사 • 기능적 형상 감사 • 초기 요구사항에 대한 부합성 여부 검증
하자 보증	• 하자보증 처리 보고서	• 하자에 대한 보수

3. 결 론

본 논문은 국토해양부 및 한국건설교통기술평가원이 주관하는 국가 대형연구개발 실용화 사업인 "도시형 자기부상열차 실용화 사업 시범노선건설 열차제어시스템 구매 · 설치" 프로젝트 관련하여 열차제어시스템에 대하여 시스템에 탑재되는 소프트웨어 및 소프트웨어 개발절차에 대한 품질보증 활동에 대한 사항으로서, 일반적인 품질보증 규격(ISO 9001), 소프트웨어 품질시스템 규격(ISO 90003)과 IEC 62279 및 EN 50129에 준한 소프트웨어의 품질보증 활동을 수행함으로써 소프트웨어의 품질보증 활동에 대한 내용을 구체적으로 제시하였다.

또한 소프트웨어 안전성 분류에 따른 활동은 별도의 독립적인 활동을 통하여 보증업무를 수행하도록 계획하였고, 지금까지 국제규격에 따른 활동기준에 대해서 모호하거나, 명확하게 정의되지 않은 사항들이 체계적으로 정리될 수 있을 것으로 사료되며, 타 사업 및 국내 철도신호시스템 적용을 위한 소프트웨어 품질 및 안전 무결성 수준에 따른 소프트웨어 안전성 확보방안의 구체적인 케이스 모델이 될 것으로 기대된다.

감사의 글

본 연구는 국토해양부 및 한국건설교통기술평가원이 주관하는 국가 대형연구개발 실용화 사업인 "도시형 자기부상열차 실용화 사업 시범노선건설 열차제어시스템 구매 · 설치" 프로젝트 일환으로 수행되었습니다.

참고문헌

1. IEC 62278, 철도 적용 - 신뢰성, 가용성, 유지보수성 및 안전성(RAMS)의 사양과 증명, 2002
2. IEC 62279, 철도 적용 - 통신, 신호 처리 시스템-철도제어 및 보호 시스템을 위한 소프트웨어, 2002
3. EN 50129 : Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
4. 김종기, 신덕호, 이기서(2006), “열차제어시스템의 안전계획 수립에 관한 연구” 한국철도학회논문집. 제9권, 제3호, pp.264-270
5. "도시형자기부상열차실용화사업 시범노선 건설 기본 및 실시설계 보고서(신호분야)", 2009, 한국철도시설공단
6. "도시형 자기부상열차 실용화 사업 시범노선건설 열차제어시스템 구매 · 설치", 사업의 제안서
7. "도시형 자기부상열차 실용화 사업 시범노선건설 열차제어시스템 구매 · 설치", 사업의 안전성 및 품질관리 계획서
8. 윤학선, 이기서, 이종우, 박재영(2008), '도시형자기부상열차 열차제어시스템 RAMS 적용에 관한 연구', 추계철도학회논문집, pp.1113-1125
9. "전자연동장치 안전성 평가체계 구축 연구" 보고서, 철도기술연구원, 2001
10. "전자연동장치의 안전성 관리방안 적용을 위한 연구" 보고서, 철도기술연구원, 2002
11. ISO 9001:2000, 품질관리체계 - 요구사항
12. ISO IEC90003: 2004, 소프트웨어 엔지니어링 - 컴퓨터 소프트웨어에 적용