# 통합사령실의 소프트웨어 개발에서 안전성활동과 개발시스템의 관계에 대한 연구

# A study of relation-ship on Safety activites and development systems for Integrated Centralized Traffic Control(CTC) S/W

김원경* 온정근** 창상훈***
Kim, Won-Kyong Ohn, Jung-Ghun Change, Sang-Hoon

**ABSTRACT**

In answer to the increase of demand for the safety in railroad, the safety activities are tried out. According to 'KORAIL Instruction number 2001-49', the project for developing Integrated Centralized Traffic Control Center has been carried out and the safety activities are guaranteed by documents named 'Safety Plan' and 'Safety Requirements' from this project. However the development system is not enough for the full safety activities. Therefore this paper we describes the relationship of safety activities and development systems and proposes the efficient direction of safety activities.

## 1. 서 론

최근 안전성 활동에 대한 요구 증대에 따라 많은 안전성활동이 시도되고 있다. 2001년 철도청장이 고시한 '철도청지시 제2001-49호'에 따라 안전성활동을 실시한 통합CTC소프트웨어 개발은 안전성계획서를 비롯하여 안전성요구사양서 등에 의하여 안전성활동이 보장되었다. 그러나 안전성계획서 및 안전요구사양서에 규정한 안전성활동을 실시하기에는 시스템적인 한계를 가지고 있었다. 안전성평가를 실시하는 과정에서 시스템에 대한 개선을 지시하고 개선이 시행되었다. 이에 이 논문에서는 안전성활동과 개발시스템간의 관계에 대한 고찰을 실시하여 보다 효율성 있고 안전성을 확보할 수 있는 안전성활동의 방향을 제시한다.

### 1.1. 통합사령실 소프트웨어 개발 개요

관제실통합 신호설비 구축 사업은 우리나라의 철도교통망의 통제를 통합하기 위한 사업으로서 열차집중제어시스템을 위한 하드웨어를 비롯하여 소프트웨어, 요원들의 교육을 위한 시설 등을 건설하는 사업이다. 이중 안전성 평가 대상이 되는 것은 계약에 의하여 소프트웨어 개발에 대한 부분만 포함되었다. 안전성 활동 및 평가의 의무 및 권한은 '2001-49호'에 의하여 실시하였다.

* 책임저자, 서울산업대학교 철도전문대학원 철도시스템공학과, 한국철도기술연구원 철도시험인증연구센터, 정회원
wkkim@krri.re.kr
Tel : (031)460-5510 FAX : (031)460-5509
** 서울산업대학교 철도전문대학원 철도전기신호공학과, 한국철도기술연구원 철도시험인증연구센터
*** 한국철도기술연구원 철도시험인증연구센터

## 2. 통합사령실 S/W 개발 체계

통합사령실 S/W의 개발체계는 프로젝트의 안전성보증계획서와 안전 요구 사양서에 명시하고 있다.

### 2.1. 개발 조직

개발조직은 개발팀과 품질보증팀, 안전성보증팀, 시행청, 안전성평가기관으로 구성되어 있다.

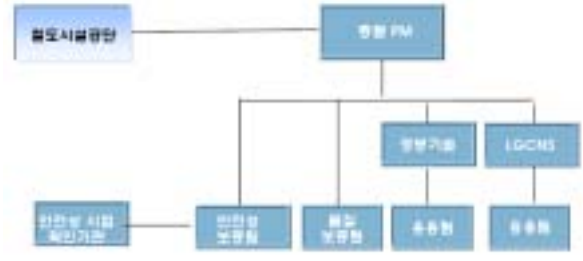

그림 1 통합사령실S/W개발 안전성 조직

개발팀은 소프트웨어의 설계와 제작을 담당하며, 품질보증팀은 결과물에 대한 품질활동을 실

시하였다. 안전성보증팀은 안전성 활동을 계획하고 실시하였으며, 안전성활동에 대한 평가를 한국철도기술연구원에서 실시하였다.

### 2.2. 개발과 안전성 라이프사이클

통합사령실의 개발은 그림2와 같은 소프트웨어 개발 라이프사이클과 그림3과 같은 안전성 라이프사이클을 적용하였다.

그림 2 통합사령실 S/W 개발 라이프사이클

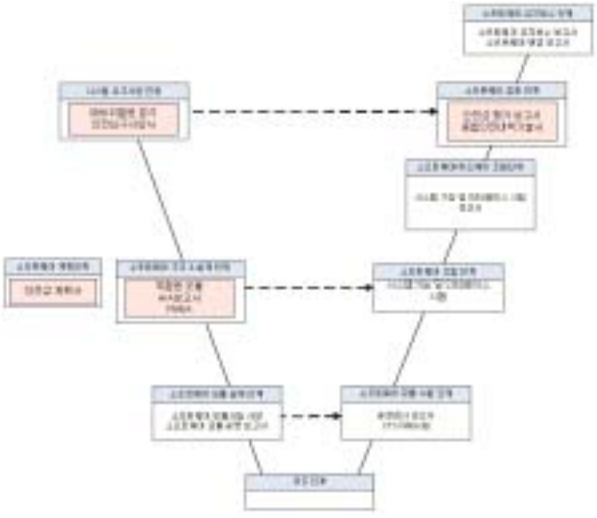

그림 3 통합사령실 S/W 개발 안전라이프사이클

개발라이프사이클과 안전성라이프사이클은 동일한 라이프사이클로서 각 분야의 성과물을 분리하여 표현하기 위하여 별도로 분리한 것이다. 결국 동일한 라이프사이클을 안전성조직과 개발조직 간의 업무분리를 위하여 별도의 라이프사이클로 표현한 것이다.

### 2.3. 품질 시스템

통합사령실 S/W 개발사인 경봉기술(주)의 품질시스템은 ISO9000에 의한 품질시스템을 유지하고 있다. 소프트웨어의 개발 및 품질보증을 위한 활동은 품질시스템메뉴얼에 의하여 운영되고 있다.

## 3. 통합사령실 안전성활동

통합사령실 프로젝트에서 개발사는 품질보증계획서를 제출하여 시행청으로 부터 승인을 받아 수행하였다. 품질보증계획서는 개발사가 유지하고 있는 ISO900에 의한 품질시스템에 의하여 수립된 계획서이다. 품질계획서는 품질보증활동을 위한 조직 및 절차, 성과물, 품질보증팀의 활동 등에 대하여 명시하고 있다. 각 팀과 각 담당자의 권한과 의무가 포함되어 있어, 개발시에 필요한 활동과 이에 대한 검토, 승인, 평가 등의 절차가 명확히 구분되어 있어 활동의 주체를 분명히 하고 있다.

그러나 안전성 계획서에서는 품질조직과 더불어 안전성활동 조직을 명시하고 있으나 안전성활동을 위한 체계가 구체적으로 수립되어 있지 않았다. 또한 ISO9000에 의한 품질시스템 매뉴얼에도 안전성활동 및 부서에 대한 체계가 수립되어 있지 않았다. 이는 안전성 부서와 활동이 임시적으로 구성되었으며, 활동에 대한 권한이 명확하지 않음을 의미하고 있었다. 결과적으로 안전성 활동은 안전성부서의 국한된 업무가 되었으며, 실제로 설계와 제작을 담당하는 부서에서는 안전성 활동의 내용과 방법, 결과 등에 대한 인식이 미비한 상태였다.

IEC62279와 다른 안전성 관련 규격에서 이에 대한 사항을 명시하고 있다. IEC62279의 6절에서는 소프트웨어 개발 프로젝트의 책임을 지는 인원에 대한 훈련 및 경험 등에 관한 자격의 책임 및 의무를 강조하고 있으며, 이에 대한 절차는 ISO 9001의 관련부분에 근거하여 활동하도록 요구하고 있다.

통합사령실 S/W 개발 프로젝트에서는 기존의 품질보증에 대한 절차 및 업무는 구체적으로 명시되어 활동하고 있으나, 안전성활동에서는 미비함을 발견하였다. 이에 안전성활동을 구체적으로 실시할 수 있는 절차의 수립을 요구하였다. 그림4의 진행절차는 안전성 활동을 위한 팀간의 활동 절차를 명시한 것이다.

### 3.1. 안전성을 위한 시스템 수립

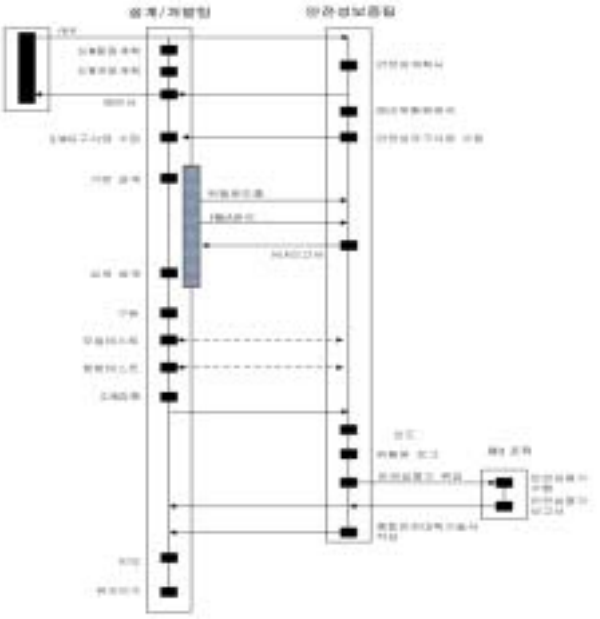

그림 4 안전성활동 진행 절차

안전성보증팀에서는 안전성계획서를 수립한 이후 설계/개발부서에 계획서의 확인을 요구하며, 설계/개발부서는 계획서에 의한 안전성활동을 준비하게 된다. 설계/개발부서는 프로젝트를 위하여 입력되는 문서에 의하여 사양분석을 실시하게 되고 사양 및 환경에 대한 예비위험원을 분석하게 되며 안전부서에서는 이 활동에 대한 결과를 검토하게 된다.

이러한 진행절차는 각 안전성 활동의 주체를 명확히 구분하게 하며, 설계/개발부서에서 실시하여야 하는 안전성활동의 의무를 갖게 한다.

이 진행절차에서 안전성평가는 소프트웨어의 개발 이후에 실시되도록 구성되어 있다. 그러나 이러한 구성은 소프트웨어의 안전성평가에 적합하지 않다. IEC62279, IEC61508 등에서는 안전성평가는 각 부분별로 반복적으로 실시할 수 있도록 규정하고 있다. 이는 개발된 이후에 실시되는 안전성평가에서 위험원이 발견되었을 경우, 이에 대한 후속조치를 위한 시스템의 복구가 커다란 부담이 될 수 있기 때문이다. 때문에 개발시의 안전성평가는 각 단계의 시행이 완료된 시점에 반복적으로 실시되는 것이 합당하다.

### 3.2. 안전성 활동 세부 절차 수립

통합사령실 S/W 개발 프로젝트에서는 안전성활동 진행절차와 더불어 세부 절차를 수립하였다. 세부절차에서는 각 팀의 활동 내역과 산출물, 팀 간 인터페이스 절차 등을 명시하고 있다.

그림 5 요구사양수립 단계 절차

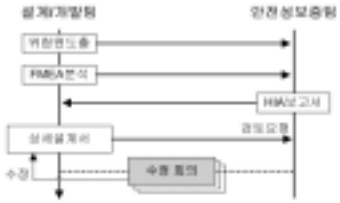

그림 6 상세설계 단계 절차

상세절차로서 각 부서와 담당자의 안전성활동의 권한과 의무가 명확히 되었다.

### 3.3. 안전성 시스템 수립

상기에서 언급하였던 통합사령실 S/W 개발프로젝트에서의 시스템 및 절차는 안전성보증계획서와 안전요구사양서의 수정으로 보완하도록 요구되었다. 이는 프로젝트를 담당하는 인원이 자신의 활동 의무와 목표에 대한 정확한 인식이 필요하기 때문이다. 안전요구사양서의 안전조직 항목에 안전시스템의 진행절차 및 상세절차와 권한, 의무, 성과물 등을 명시함으로 각 부서의 안전성활동을 의무화 하였다.

그러나 안전성보증계획서와 안전요구사양서에 절차가 보완되었음에도 제작사의 품질시스템과는 맞지 않는 오류는 여전히 남아 있었다. 이는 추후 발생되는 프로젝트에서는 의무적인 안전성활동을 보장하지 못하고 있는 것이다.

때문에 추후 지속적인 안전성활동을 위해서는 제작사의 품질시스템에 안전성 시스템을 포함시키는 품질시스템의 수정이 요구된다.

## 4. 결 론

안전성활동은 하나의 프로젝트에서 일시적으로 수행되는 임시적인 활동이 아니다. 제작사에서는 제작품의 사용에서 발생할 수 있는 위험원을 비롯하여 제작 시에 내재될 수 있는 위험원을 파악하고 위험원을 제어할 수 있는 시스템을 갖춰야 한다. 제작사에서 수립된 안전성시스템은 각 구성원에 대한 안전성활동의 의무를 명시하게 되고 구체적인 활동을 요구할 수 있는 근거가 될 것이다.

통합사령실 S/W 개발 프로젝트에서는 안전성활동을 위한 시스템 구축이 미비하여 안전성활동이 해당 부서의 역할을 벗어나지 못하고 있었다. 이에 안정성평가에서 시스템에 대한 시정을 요구하였으며, 제작사는 안전성활동을 위한 시스템과 절차가 수립하였다. 수립된 안전성시스템에 의하여 위험원 도출 및 분석 활동이 실시되었으며, 위험원의 감소와 제거로 통합사령실 S/W에 대한 무결성 및 안전성의 향상을 보였다. 이와 같은 안전성 활동은 안전대책기술서로 보고되었다.

이와 같이 안전성활동에서 개발시스템과의 관계를 정립하는 것은 안전성활동의 실행을 위하여 매우 중요하다. 이 관계를 정립한 것이 안전성 시스템이다. 안전성 시스템은 각 제작사나 운영기관에서 수행되어온 품질시스템에 안전성활동을 접목시킨 것으로서 각 담당자에게 권한과 의무를 규정하는 역할을 한다.

국내에서 철도안전법이 시행됨에 따라 운영기관에서는 지속적으로 위험원을 감시하고 위험원의 제거 및 안전성의 향상을 체계적으로 실시할 것을 요구받고 있으며, 위험원을 감시하고 제어하는 안전성활동을 의무화하고 있다. 또한 안전성활동의 계획과 시행 결과에 대한 평가를 받도록 요구받고 있다. 그러나 아직 운영기관의 품질시스템에는 안전시스템이 포함되지 않고 있어 일상적인 활동이 아니라 일시적인 활동으로 인식되는 문제를 안고 있을 뿐 아니라 안전성활동의 주체가 되어야 할 담당자는 안전성활동에 대한 인식이 미비한 상태이다. 그러므로 앞으로 운영기관에서는 안전성활동에 대한 적합한 안전성활동 모델을 수립하고 이를 품질시스템에 반영하는 등의 안전성시스템을 수립하려는 노력이 필요할 것이다.

## 참고문헌


1. 경봉기술(주)(2004년), “통합CTC S/W개발 안전요구사양서”
2. 경봉기술(주)(2004년), “통합CTC S/W개발 안전성 보증 계획서”
3. 경봉기술(주)(2006년), “통합CTC S/W개발 종합안전대책 기술서”
4. 한국철도기술연구원(2006년), “통합CTC S/W개발 안전성평가보고서”, 보고서
5. 대우엔지니어링(2001년), “전자연동장치 안전성 평가체계 구축 연구”, 보고서
6. 한국철도기술연구원(2001년), “철도신호제품에 대한 신뢰성과 안전성 검증기준 제정 연구”, 보고서