통합사령실의 소프트웨어 개발에서 안전성 라이프사이클 개선에 대한 연구

A Study of Safety Life-cycle for Integrated Centralized Traffic Control(CTC)

온정근* 이종우**
Ohn, Jung-Ghun Lee, Jong-Woo

ABSTRACT

After the year of 2000, the need of safety increases in field of railroad. The project for developing Integrated Centralized Traffic Control(CTC) center started at 2002 to control the full domestic railroad network. A traffic control software was required the safety activity and assessment, according to 'KORAIL Instruction number 2001-49'. There were many trials and errors to perform safety activity because the technology and recognition of safety activity is in primary stage. However the safety activities are gradually stabilized. This paper describes the safety life-cycle and development life-cycle of Integrated CTC S/W and a suitable life-cycle of safety to develop S/W of Integrated CTC.

1. 서 론

최근 2000년 이후부터 철도분야의 안전성에 대한 요구가 증대되어가고 있으며, 우리나라 전국의 철도제어망을 통합하는 사업인 관제실 통합 사업이 2002년부터 시작됨에 따라 2001년 철도청장이 고시한 '철도청지시 제2001-49호'(이후 '2001-49호'로 함)에 의거 안전성활동 대상이 되었다. 이에 동 고시에 의거하여 통합CTC 소프트웨어에 대한 안전성활동과 안전성평가가 실시되었다. 그러나 국내에서 안전성에 대한 인식과 기술이 초기단계로서 안전성활동의 시행에 많은 시행착오를 거쳐 안정화되고 있다. 이에 이 논문에서는 통합CTC소프트웨어에 대한 안전성활동 라이프사이클에 대하여 언급하고 소프트웨어 개발에 적합한 개발 및 안전성 라이프사이클에 대하여 고찰하여 본다.

2. 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.

3. 안전성 라이프사이클

안전성에 대한 규정은 전반적으로 국제규격에 준하여 실행되고 있다. 국내에서는 국제적인 추세를 따라가고자 철도분야 중 열차제어시스템에 대한 안전성 확보 기술권고안을 최초로 규정하였으며, 이에 따라 통합사령실의 소프트웨어 개발 프로젝트가 그 권고안에 의하여 실시되었다.

국제적으로 안전성과 소프트웨어 개발을 규정하는 규격들은 다음과 같다.

3.1. IEC 61508 라이프사이클

IEC61508은 전기/전자/프로그램이 제어에 많이 사용됨에 따라 시스템 개발에 필요한 안전주기활동에 대한 지침을 제공하는 규격이다. 이 규격에서는 안전성활동에 필요한 요건들을 기술하고 있으며 개발되는 시스템의 무결성을 확보할 수 있는 상세한 지침을 제공하고 있다.

* 책임저자, 서울산업대학교 철도전문대학원 철도전기신호공학과, 한국철도기술연구원 철도시험인증연구센터, 정회원
jgohn@krri.re.kr
Tel : (031)460-5516 FAX : (031)460-5509
** 서울산업대학교 철도전문대학원 철도전기신호공학과

IEC61508에서의 라이프사이클은 다음 그림과 같은 주기를 기술하고 있으며, 개발의 개념구상에서부터 안전요건 수립, 배분과 실현, 확인 등의 단계를 가진다.

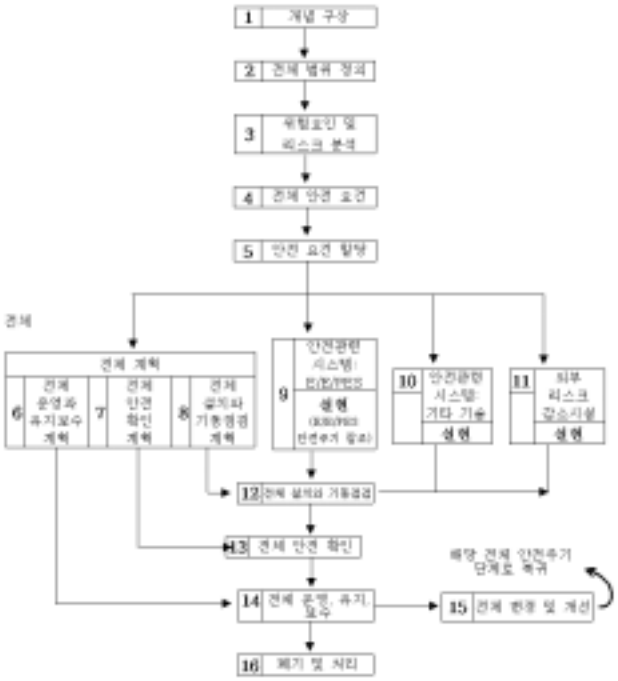

그림 1 IEC61508 안전주기

3.2. IEC 62278 라이프사이클

IEC62278은 IEC61508에서 기술한 안전성활동에 대한 내용을 철도제어시스템의 RAMS활동에 대한 구체적인 요건들로 기술한 규격이다.

이에 IEC62278의 라이프사이클은 IEC61508의 안전주기를 따르고 있으며, IEC61508의 안전주기를 철도제어시스템에 보다 구체적으로 기술하고 있다.

3.3. IEC 62279 라이프사이클

IEC62279는 IEC61508에서 기술한 안전성활동에서 소프트웨어 무결성(5단계)에 대한 활동을 기술하고 있다. 이에 IEC62279의 라이프사이클은 소프트웨어 개발에 대한 계획단계 이후의 개발 및 실현단계에서의 활동에 대한 V 라이프사이클을 보여주고 있다. 이 라이프사이클은 같은 프로젝트에서 각 별개의 부분으로 개발되는 소프트웨어나 하나의 프로젝트로 개발되는 소프트웨어의 개발라이프사이클에 적합한 방법이다.

3.4. Yellow Book 라이프사이클

YellowBook은 철도를 엔지니어링하거나 유지보수하는 활동을 지원하기 위한 지침으로 작성되었다. 철도를 운영하기 위한 안전성 근거와 활동을 확보하기 위한 목적으로서 각 절차 및 요건들은 철도의 운영을 목표로 기술되어 있으며, 이 규정에서는 각 역할을 담당하는 부분간의 상호작용도를 보이고 있으며, 철도운영에서 수행되는 각 활동들의 안전성 관련 라이프사이클로 판단할 수 있다.

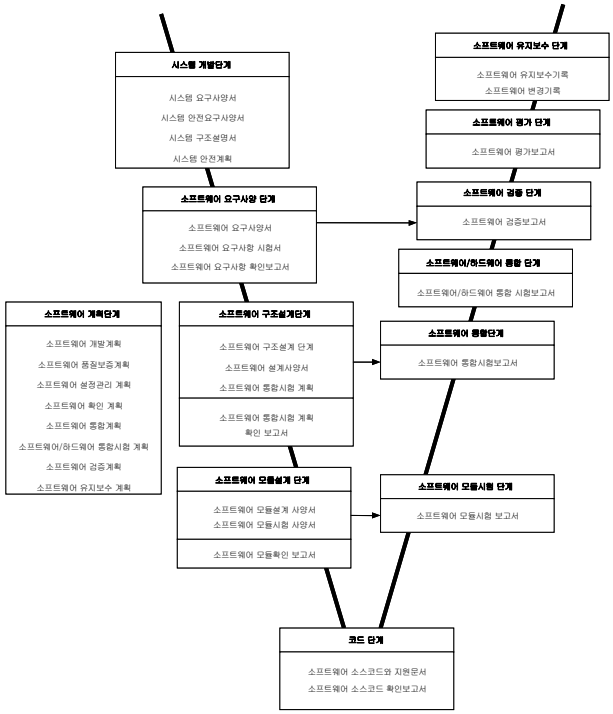

그림 2 IEC62279 라이프사이클

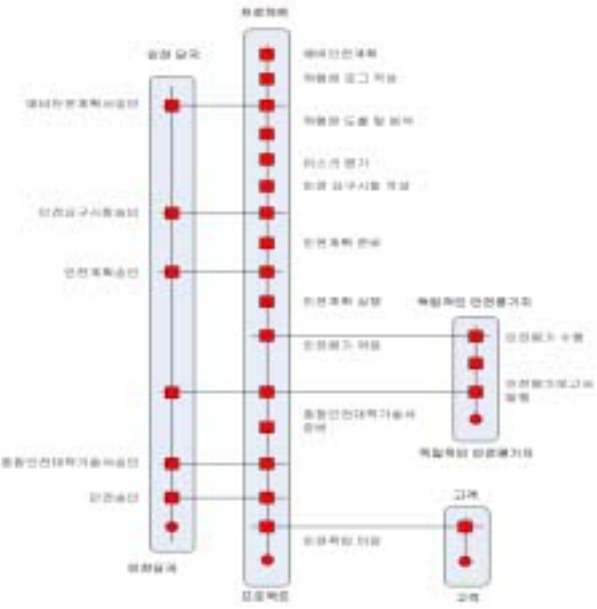

그림 3 Yellow Book 상호작용도

3.5. 철도청지시 제2001-49호

'2001-49호'는 컴퓨터를 사용하는 열차제어시스템에 대한 설계/제조/운용에 필요한 안전성활동

을 제시한 것이다. 2001-49호에서는 개념설계, 사전안전성해석, 설계, 제조, 운용, 보수, 개수 등의 과정을 안전성라이프사이클로 제시하고 있으며, 이는 IEC61508의 라이프사이클을 기본 모델로 적용하고 있다.

4. 통합사령실 안전성활동 계획

통합사령실 프로젝트는 안전성활동 계획으로 안전성보증계획서와 안전요구사양서를 수립하였다.

4.1. 안전성 보증 계획서

안전성보증계획서에서는 안전성활동의 목표, 안전성조직, 안전성활동의 내용, 생산물의 종류 등을 기술하여 안전성활동의 기초를 수립하였다.

안전성보증계획서에서는 안전성활동을 통하여 안전무결성레벨(SIL)을 만족하는 소프트웨어를 개발하는 것을 목표로 수립하였다

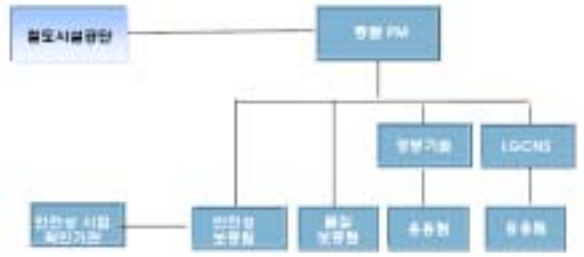

그림 4 통합사령실S/W개발 안전성 조직

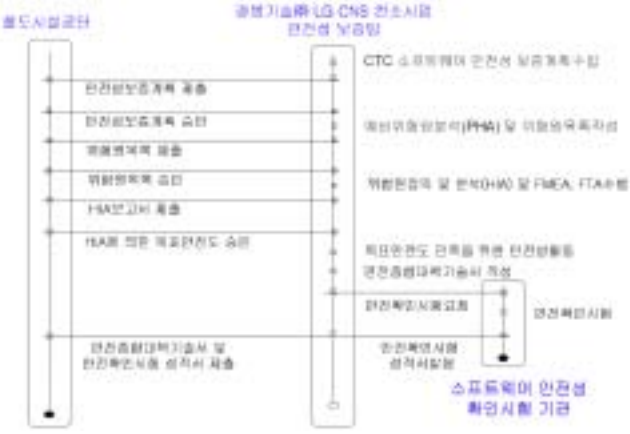

그림 5 프로젝트 추진체계

안전성보증계획서에 포함된 안전성조직은 시행청을 포함한 안전성위원회를 설치하여 운영하도록 하였으며, 그림4는 프로젝트의 개발을 위한 안전성조직을 보인다. 특히 안전성확인기관을 독립적으로 유지하도록 하였다.

4.2. 안전 요구 사양서

안전요구사양서에서는 통합사령실S/W를 개발하는 것에 필요한 안전요건, 라이프사이클, 상세 조직 구성과 역할, 단계별 업무체계, 소프트웨어의 레벨분류 등으로 안전성활동의 수행에 필요한 사양을 규정하였다. 이 규정은 설계/제작부서와 안전성부서에서 업무에 지침으로 사용한다.

안전요구사양서에서는 그림2와 같은 IEC 62279를 만족하는 V 라이프사이클을 제시하고 있으며, 별도의 수행체계를 그림5와 같이 제시하고 있다.

5. 소프트웨어 개발 라이프사이클

5.1. 각 라이프사이클의 특성

각각의 라이프사이클은 해당하는 시스템이나 절차의 특성을 반영하고 있다.

Yellow Book은 철도의 운영을 목적으로하는 안전지침으로서, Yellow Book에서 제시하는 그림3의 절차는 철도의 운영에 필요한 안전성 라이프사이클을 보여주고 있다. Yellow Book의 라이프사이클은 해당 활동을 규명하고 활동 중에 발생할 수 있는 위험원에 대하여 계획을 수립하고 위험원에 대한 조치 등을 시행하기 위하여 수립된 절차이다. 활동에 대한 계획과 결과는 안전당국의 승인을 받아야 하며, 이에 대한 평가는 별도의 독립적 평가기관에서 받도록 하였다. 이 라이프사이클에서 위험원은 초기에 활동에 대하여 명시를 실시하고 예비 위험원 도출과 평가를 통하여 안전계획을 수립하고 승인받으며, 안전계획 이후에 위험원에 대한 리스크평가를 실시하여 안전요구사양을 수립하도록 하였다. 이후 운영을 통하여 안전요구사양을 준수하고 안전계획상의 안전목표의 달성 여부를 지속적으로 감시하게 된다. 이에 대하여 독립기관으로부터 정기적인 평가를 받음으로 수행결과에 대한 보고를 실시한다.

이와 같이 Yellow Book에서 제시된 라이프사이클은 철도운영에서 필요한 안전계획과 요건을 수립하고 운영자가 지속적으로 감시해야하는 안전요구사양을 수립함으로 운영상에 발생할 수 있는 위험원을 제거하고 줄이는 것을 목적으로 하고 있다.

반면 그림1과 같은 IEC61508의 안전주기는 제품의 개발에서 발생할 수 있는 안전성에 대하여 기술되어 있다. 운영과 달리 개발주기는 개발목표에 대한 사양을 수립하고 사양에 대한 분석과 설계, 제작, 시험 및 검사, 납품에 해당하는 절차를 일반적으로 가진다. 이에 대하여 최근에는 납품 이후의 운영단계에까지 제작자의 안전주기를 확대하고 있다. 이와 같이 IEC61508은 개발주기에 맞추어진 안전주기를 제시하고 있으며, 개발절차를 제시하고 있지는 않다. 다만 제품에서 요구된 기본 사양이 내포한 위험원과 설계 및 제작 중에 발생할 수 있는 위험원들을 찾아내 제어하는 목적의 지침인 것이다. 제품사양에서 발생할 수 있는 위험원은 리스크분석을 통하여 방지할 수 있는 안전사양을 수립하고 안전사양을 설계(시스템 설계)과정을 통하여 각 해당 모듈에 분배하도록 요구하고 있다. 제작 상에 발생할 수 있는 위험원은 무결성 활동을 통하여 제거하도록 요구하고 있다.

IEC6228은 IEC61508의 안전성활동 및 요건을 철도제어시스템에 적용할 수 있도록 명시하고 있으며, IEC62279는 소프트웨어의 개발에서 실시하는 무결성활동에 대한 지침을 보여준다.

5.2. 소프트웨어 개발 라이프사이클

소프트웨어의 개발에서는 IEC62279의 라이프사이클을 적용하는 것이 합당하다. IEC62279에서는 시스템의 설계에서 필요한 각 요건이나 사양을 검토하고 사양의 분석에 따라서 모듈에 각 성능이나 기능을 분배하고 분배에 따른 독립적 특성들을 유지하도록 하는 개발 라이프사이클을 갖고 있다. 또한 각 부분에 대한 검증 사이클을 포함하여 V형 라이프사이클을 가진다.

5.3. 통합사령실 소프트웨어 개발 라이프사이클

통합사령실의 개발은 IEC62279의 라이프사이클과 Yellow Book의 시행절차를 동시에 인용하고 있다. 개발에서는 IEC62279의 수행절차와 수행결과물으로서 안전무결성활동을 실시하고, 안전성활동의 승인과 수행, 책임을 위하여 Yellow Book과 같은 수행체계를 인용하였다.

일면 이러한 라이프사이클은 합당하게도 보이나 소프트웨어 개발을 위한 절차에 중복이 발생한다. IEC62279의 라이프사이클에서도 설계 이전에 개발 요구사양에 대한 분석을 실시하고 사양분석 이후에 예비설계를 거쳐 실제의 설계와 제작 과정을 가지고 있다. 안전성활동에서도 이와 동일한 사이클을 가질 수 있다. 먼저 기본 안전요건을 수립하는 예비안전성계획을 수립하고 예비위험원의 도출을 통하여 안전사양에 대한 분석을 실시하고 예비위험원의 리스크분석을 통하여 안전사양과 안전성계획을 수립하고 설계와 제작과정에서 위험원에 대한 배분과 무결성 활동을 실시해야 한다. 이를 위하여 IEC62279의 무결성 활동에 안전성 활동을 위한 일부 절차의 명시가 필요하다.

IEC62279의 라이프사이클을 그림6과 같이 수정하여 통합사령실의 S/W 개발에 적용하였으며, 별도의 안전성 라이프사이클을 다음 그림7과 같이 제시하였다.

그림 6 통합사령실 S/W 개발 라이프사이클

그림5의 추진체계는 철도의 운영 및 개발 프로젝트를 위한 추진체계로 적합하다. 철도의 운영은 주기적으로 반복하게 되며 계획과 사양에 대한 수행, 평가를 통하여 다음 주기의 운영에서 보완을 실시할 수 있는 체계인 것이다. 그러나 개발의 주체가 기업이 되는 개발 프로젝트에서는 이러한 체계는 적용하기 어렵다. 시행청의 안전성활동에 대한 개입은 기업에게 안전성활동의 주체에 대한 모호함을 주기에 충분하다. 개발에서 안전성 활동의 주체는 개발사가 되어야 한다. 예비위험원 분석은 개발사의 시스템 분석 및 입출력, 기능, 성능에 대한 분석 및 배분을 통하여 예비위험원 활동을 실시하기에 충분할 것으로 판단된다. 다만

안전계획 및 중요 안전요건의 승인, 안전대책기술서의 승인 등은 시행청의 활동으로 적합하며, 안전에 대한 요구사항은 제작사양에 추가하는 것으로 충분하다.

그림 7 통합사령실 S/W 개발 안전라이프사이클

추진체계는 라이프사이클의 추진을 위한 설계/개발부서와 안전성팀, 평가팀 간의 관계 및 절차를 명시하는데 이용하는 것이 합당하다.

5.4. 안전성 평가

‘2001-49호’와 통합사령실 S/W ‘안전성 보증계획서’와 ‘안전 요구 사양서’에 의하여 독립 기관으로부터 평가를 실시하였다. 평가는 그림5의 프로젝트 추진체계에 의하여 개발이 완료되는 시점에서 의뢰되었다.

그러나 IEC62279, IEC61508 등에서는 무결성의 확인을 위하여 각 단계별로 반복하여 평가를 실시할 수 있도록 명시하고 있다. 이는 안전성 평가 결과를 사양, 설계, 제작, 유지보수 등의 안전요건에 반영할 수 있도록 요구하는 것이다. 그림5와 같이 최종 단계에서 실시되는 안전성 평가는 사양에서부터 설계, 제작까지 대규모의 변경이 요구될 수 있으므로 시스템의 개발에서 수행되는 안전성활동은 각 단계별로 반복적으로 수행되는 것이 합당하다.

6. 결 론

안전성 활동을 규정하는 많은 규격에서는 라이프사이클을 정의하고 있다. 정의된 라이프사이클은 각 규격에서 요구하는 목적에 적합하도록 활동을 규정하고 있다. 이러한 라이프사이클은 각 프로젝트의 크기 및 목적에 따라서 조정될 필요가 있다.

IEC61508과 IEC62278, IEC62279등에서는 개발을 위한 라이프사이클 및 안전성 라이프사이클을 제시하고 있다. 이 규격에서 제시된 라이프사이클은 제품의 개발과정에서 수행되어야 할 안전성활동과 무결성활동을 명시하고 있다. 반면 Yellow Book에서는 철도운영을 위한 체계를 제시하고 있다.

통합사령실 소프트웨어 개발프로젝트에서는 IEC62279의 라이프사이클과 Yellow Book의 체계를 동시에 적용하였다. 그러나 이러한 혼용은 안전성 활동의 주체를 모호하게 하는 결과를 가져왔다. 이를 수정한 라이프사이클을 적용하여 성공적인 안전성활동을 수행하였고 적합한 안전성 평가가 수행되었다.

추후 안전성활동은 지속적으로 실시될 것으로 예상되는 바, 활동목적에 맞도록 구성되어 있는 각 라이프사이클을 프로젝트나 수행기관의 조직이나 프로세스에 적합하도록 모델링하는 것이 꼭 필요하다.

이후 안정적인 안전성활동을 위하여 국내 철도분야나 제작자, 운영기관에 적합한 라이프사이클 모델을 개발하는 것이 지속적으로 필요할 것으로 판단된다.

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