철도소프트웨어 안전기준 및 안전관리체계 연구
A Study on Safety Standard and Safety Management Procedure for Railway Software

정의진* 신경호**
Eui-jin Joung Kyung-ho Shin

ABSTRACT

Safety critical systems are those in which a failure can have serious and irreversible consequences. Nowadays digital technology has been rapidly applied to critical system such as railways, airplanes, nuclear power plants, vehicles. The main difference between analog system and digital system is that the software is the key component of the digital system. The digital system performs more varying and highly complex functions efficiently compared to the existing analog system because software can be flexibly designed and implemented. The flexible design make it difficult to predict the software failures. This paper reviews safety standard and criteria for safety critical system such as railway system and introduces the framework for the software lifecycle. The licensing procedure for the railway software is also reviewed.

1. 서론

철도시스템은 여러 특성들 중에 안전성이 매우 중요한 시스템이다. 요즈음 철도시스템의 기능 구현을 위해 소프트웨어의 사용이 증가하고 있는 것이 사실이다. 소프트웨어의 특성상 불확실성이 존재하며, 현재까지는 기능 구현에만 치중하여 철도소프트웨어를 개발해 왔으나 안전성 검증없이 소프트웨어를 사용할 경우 만약의 사태로 인해 사고로 이어진다면 그 피해는 매우 엄청나다고 할 수 있다. 이를 위해 철도소프트웨어를 위한 안전기준을 제시할 필요가 있으며, 안전기준에 맞게 철도소프트웨어가 개발되었는지 검증하고, 인증하는 체계를 구축할 필요가 있다. 본 논문에서는 철도소프트웨어의 안전기준 구성체계 및 안전기준을 운영할 관리체계에 대하여 논하고자 한다.

2. 철도소프트웨어 안전기준

소프트웨어는 그 복잡성으로 인해서 점점 그 정확성을 확보하기가 어려워지고 있으며, 1990년대 이후부터는 소프트웨어 오류로 인해서 발생한 사고들이 다수 보고되고 있다. 따라서 이들 시스템들의 소프트웨어 안전성을 확보하기 위해서 다수의 국가와 기관들에서 소프트웨어의 안전성 및 신뢰성을 보장할 수 있는 방안들을 제안하고 있다.

소프트웨어 개발과 관련된 일정 지연, 비용 초과, 고객의 불만족 등을 해소하기 위한 방안으로 제품자체의 품질을 향상시키는 방법과 제품을 개발하는 프로세스 관리를 통한 문제해결 방안을 생각할 수 있다. 철도소프트웨어의 신뢰성 및 안전성을 향상시키기 위해서는 제품관점에서 좋은 제품을 만들고, 정확한 시험으로 개발된 제품의 품질이 원하는 수준에 도달했는지를 판단하는 경우가 있으며, 이와는 다른 관점에서 좋은 제품은 좋은 조직 체계에서 만들어진다는 프로세스적인 관점이 있다.

* 한국철도기술연구원 선임연구원, 정회원
** 한국철도기술연구원 주임연구원, 정회원

2.1 철도소프트웨어 안전기준 구성 체계

철도안전법 체계는 철도안전법, 철도안전법시행령, 철도안전법시행규칙, 건설교통부고시 순의 구성체계를 가지고 있다. 철도소프트웨어 안전기준은 건설교통부 고시 레벨에 속하는 기준으로 이러한 법령 또는 기준들은 기존의 산업표준이나 기술지침서들과 상충하지 않아야 한다. 아래 그림은 철도소프트웨어 안전기준을 제시하기 위한 관련 산업표준의 범주를 나타낸 것이다. 여기에서 Reference Standard란 철도시스템의 도메인 특성 및 안전필수 소프트웨어 관련 표준을 나타낸 규격이며, 프로세스 관련 규격, 제품관련 규격으로 구분할 수 있다.

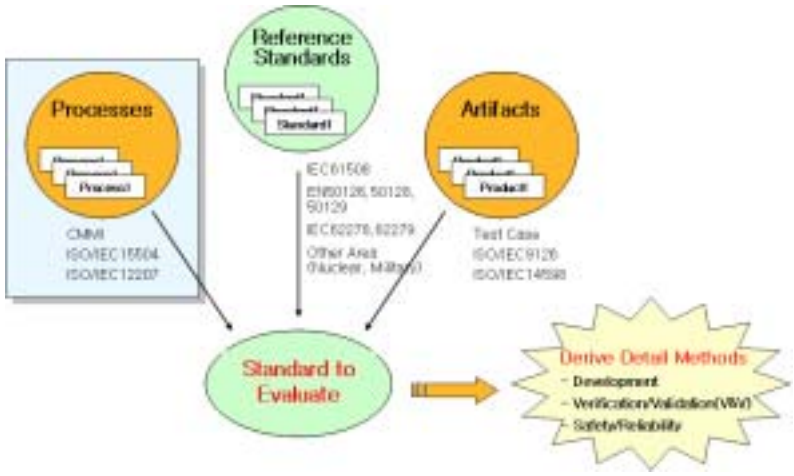

그림 1. 철도소프트웨어 안전기준 관련 표준의 범주

현재 수행중인 건교부 사업인 철도종합안전기술개발사업중 철도소프트웨어 안전기준 및 체계구축 과제에서는 해당 규격들을 참고하여 수명주기별로 안전기준(안)을 제시하고 있다. 여기에서 수명주기는 여러 관점에서 접근하여야 하며, 본 과제에서는 개발, 검증, 시험, 안전성의 4가지 수명주기로 분류하고 각각에 대한 안전기준(안)을 제시하였다. 또한 각각의 수명주기에 대한 세부 지침(안)을 개발 중에 있다.

아래 그림은 안전기준 즉, “철도소프트웨어 안전기준에 관한 규칙” 레벨에서의 4가지 수명주기에 대비한 안전기준과 안전기준을 기술적으로 보완 설명하는 지침레벨에서의 구성을 나타낸 것이다.

그림 2. 철도소프트웨어 안전기준 구성 체계

2.2 철도소프트웨어 안전기준 관리체계

제시한 안전기준이 제대로 집행되고 있는지 아닌지를 검증하기 위해서는 이를 심사하는 조직체계가 구성되어야 한다. 아래 그림은 일반적인 인증제도 관련 국가체계를 나타낸 것이다.

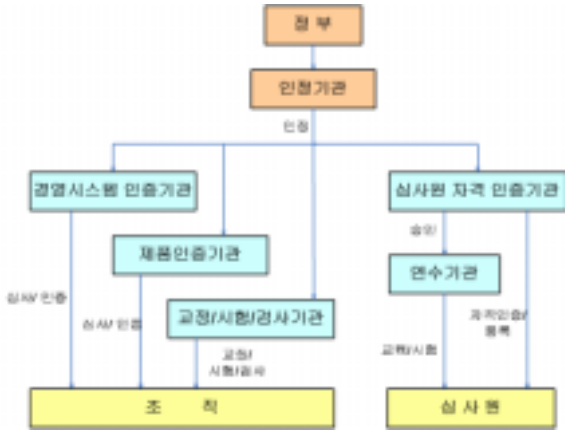

그림 3. 일반적인 인증제도 국가 체계

정부에서는 인정기관을 지정하고 인정기관에서는 여러 인증기관을 관리한다. 일반적인 국가 인증체계는 프로세스 관점의 경영시스템 인증, 제품관점의 제품인증, 시험/검사로 구성되어 있으며, 인증수행 요원을 교육하기 위한 연수기관으로 구성되어 있다.

인증에 있어서는 강제인증과 임의인증이 있는데 기존의 국내 소프트웨어를 관장하고 있는 산업자원부와 정보통신부의 경우 대부분이 임의인증방식을 취하고 있었다. 인증업무에 대한 효력은 법으로 명시하고 있다.

프로세스 관점에서의 인증은 ISO9000, ISO14000 등의 프로세스 분야와 관련하여 인정기관인 한국인정원에서 인증기관을 인정하고, 해당 인증기관에서 인증업무를 수행하고 있으며, 다음 분야를 담당한다.

- 품질경영시스템 (ISO 9001)
- 환경경영시스템 (ISO 14001)
- 자동차분야 품질경영시스템 (QS 9000)
- 정보통신 품질경영시스템 (TL 9000)
- 안전보건 경영시스템 (K-OHSMS)

소프트웨어의 경우 소프트웨어 프로세스 성숙도를 판가름하기 위하여 CMMI(Capability Maturity Model Integration)와 SPICE(Software Process Improvement Capability dEtermination : ISO/IEC15504) 모델을 이용하여 체크하고 있다.

제품관점에서의 인증은 제품에 따라 안전과 관련된 분야와 일반 산업분야로 나눌 수 있으며, 적용 분야에 따라 H/W 또는 S/W로 나눌 수 있다. H/W에서 일반 산업분야의 경우, 한국교정시험기관인정기구(KOLAS : Korea Laboratory Accreditation Scheme) 등의 시험업무를 인정기관인 기술표준원에서 인증기관을 인정하고, 해당 인증기관에서 인증업무를 수행하고 있으나 안전필수 시스템에 대한 안전성 분석은 다루고 있지 않다. 철도시스템의 경우, 안전성 분석 등에 대하여 외국의 전문 인증기관인 (Lloyd, TUV)에서 위험요인 도출, 분석, 위험도 분석 등의 안전성 분석 업무를 수행하고 있는데 원자력 분야의 경우 규제기관인 한국원자력안전기술원(KINS : Korea Institute of Nuclear Safety)에서 업무를 수행하고 있어서 철도 분야와는 대비되는 것을 알 수 있다. S/W에서 일반 산업용 소프트웨어 제품은 산자부 소속 기술표준원의 ES (Excellent Software)마크에 의한 인증과 정통부 협회인 한국정보통신기술협회 (TTA : Telecommunication Technology Association)의 GS(Good Software)마크에 의한 인증이 있다. ES인증 및 GS인증 모두 ISO/IEC 9126 및 ISO/IEC 14598의 내부, 외부 메트릭 및 평가기준을 토대로 해당시스

템에 맞춘 메트릭을 마련한 후 제품인증업무를 수행하고 있는데 ES인증 및 GS인증의 경우 일반 소프트웨어를 대상으로 하며 안전필수 소프트웨어에 대해서는 다루지 않고 있다. 안전필수 소프트웨어의 경우 원자력, 국방 분야에서는 별도로 관리하고 있다.

3. 품질확보 차원의 관리절차

3.1 원자력 분야 품질관리 절차

한국원자력안전기술원에서 수행하는 안전심사의 일반적인 검토절차는 그림 4와 같다.[4] 국내 원자력법에 따른 인허가 사항들은 크게 신규원전의 건설/운영허가, 허가된 사항에 대한 변경허가, 그리고 특정기술주제보고서의 승인으로 구분된다.

한국원자력안전기술원은 신청자가 어떤 원자력시설의 허가신청서를 제출하면 그 신청서의 유형을 먼저 결정한다. 그 신청서의 유형을 결정하면, 그 신청 서류의 적합성 여부를 검토한다. 신청 서류의 적합성이 결정되면, 신청서의 유형에 따라 적합한 검토범위를 결정하고 신청서에 맞는 검토계획을 수립한다. 검토계획의 목적은 계획된 활동과 일정을 상위 관리자에게 보고하고, 한국원자력안전기술원이 검토에 따른 재원들을 검토 초기에 파악하고, 검토 참여자들이 검토기준과 각 검토자의 역할을 모두가 알 수 있도록 하기 위한 것이다. 검토는 허용기준과 관련 검토절차를 이용하여 신청서에 맞는 검토계획에 따라 수행한다. 검토결과는 안전심사보고서에 수록한다.

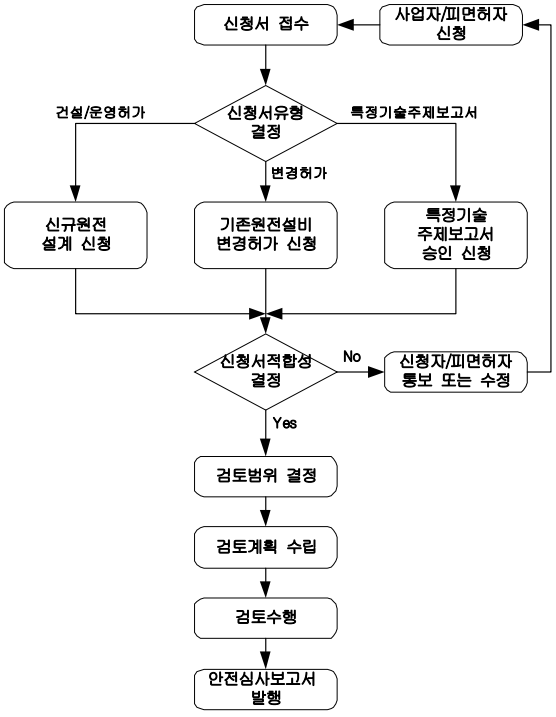

그림 4. 원자력 안전심사 검토절차

3.2 국방분야 품질관리 절차

국방분야일 경우, 인증을 위한 최초심사 절차는 신청업체에 대하여 품질평가센터 품질인증팀의 심사원에 의해 문서심사와 현장심사가 수행되며, 인증여부를 결정하기 위한 목적으로 실시된다. 최초심사는 신청업체의 생산공장에서 이루어지며, 심사범위는 신청업체의 품질경영시스템 전반에 걸쳐 수행된다. 최초심사의 경우, 심사원이 신청업체의 공장에서 문서심사, 현장심사의 작업을 수행하며, 현장심사절차로는 시작회의, 경영자면담, 현장심사, 심사팀회의, 종료회의 순으로 심사가 이루어진다.[5]

그림 5. 국방시스템 품질관리 절차도

3.3 철도분야 안전관리 절차

철도시스템의 안전성을 입증하기 위해서는 아래 그림에서 나타난 절차에 따라서 수행한다. 프로젝트관리자, 시스템검토위원회 및 안전성검토그룹간의 행정절차를 그림 6에 나타내었다.[6]

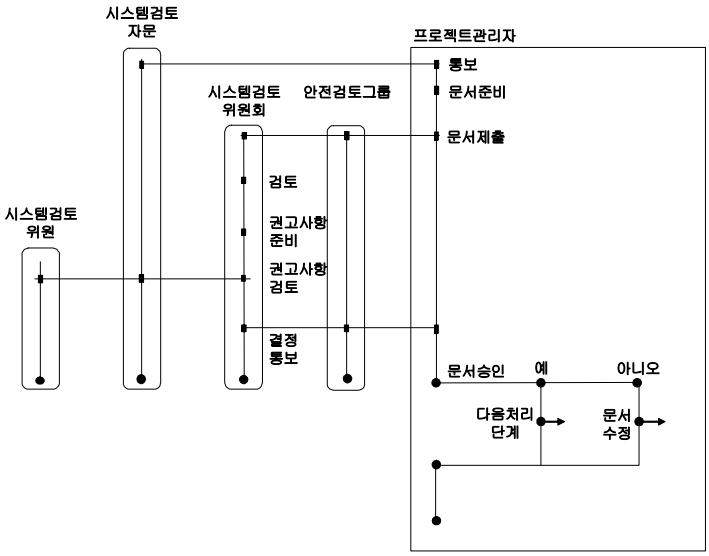

그림 6. 안전관리조직간의 행정절차

프로젝트관리자는 관련된 문서를 준비하여, 시스템검토위원회나, 안전검토그룹에 보내어 안전성 인증처리를 한다. 프로젝트관리자는 안전에 관련된 모든 사항을 수행하며, 안전에 관련된 사항은 시스템검토위원회의 승인을 받는다. 시스템 검토위원회는 철도 안전에 관련된 모든 사항을 담당하여 처리한다. 시스템검토위원회에서 위임된 사항은 안전검토그룹에서 취급한다. 독립적 안전성검토위원회는 프로젝트관리자가 안전계획에 따라 안전 활동을 제대로 수행하였는지를 확인한다.

시스템검토위원회는 안전과 관련하여 개념구상과 개발 단계에서부터 적용, 유지보수, 폐기단계까지의 과정에서 안전에 영향을 미칠 수 있는 장비와 시스템의 생애에 걸친 공식적인 안전평가를 하며, 지도한

다. 프로젝트의 안전기록을 검토함으로써 프로젝트의 안전관리를 감독한다. 시스템검토위원회가 검토할 문서는 안전계획과 안전대책기술서가 포함되며, 안전평가 일정, 위험원 분석기록, 위험평가기록, 안전요건 명세, 안전평가보고서, 안전감사 보고서 등을 검토한다.

안전검토그룹은 안전과 관련된 업무에 대해서 시스템검토위원회가 이양한 범위에 대해서 안전업무를 수행한다. 수행하는 프로젝트의 안전에 영향을 미치거나, 잠재적으로 영향을 미칠 수 있는 것에 대해서 검토한다. 안전검토그룹이 검토할 문서는 안전계획과 안전대책기술서가 포함되며, 안전평가일정, 위험원 분석기록, 위험평가기록, 안전요건명세, 안전평가보고서, 안전감사보고서 등을 검토한다.

독립적 안전성검토위원회는 안전감사와 안전성 평가를 수행한다. 안전감사에서는 사용되고 있는 안전성확보 관리활동 절차에 초점을 두고 이들이 적합하게 잘 수행되는지를 확인한다. 안전성 평가에서는 프로젝트의 제품에 초점을 맞추어 개발되고 있는 시스템과 관련되어 있는 위험도가 적당한 수준까지 감소되었는지를 확인한다.

4. 결　　론

본래 불확실성이 존재하는 소프트웨어를 철도와 같이 안전성이 중요한 시스템에 적용하기 위해서는 철저한 안전성 검증이 필요하다. 원자력, 항공, 국방분야의 경우에서도 각기 시스템에 맞추어 품질보증 체계를 구축하고 있음을 알 수 있다. 철도소프트웨어의 경우 프로세스 성숙도 향상으로 관리 관점에서 소프트웨어의 품질을 확보하고자 하는 방법이 있으며, 정형기법에 의한 개발 및 검증이나, 적절히 도출한 Test Case에 따라 시험을 수행하여 소프트웨어 자체의 오류를 줄이고자 하는 제품관점의 접근법이 있다. 또한 안전성 입증과 관련하여 안전 감사 및 안전성 평가가 있다. 안전감사의 경우, 안전성 입증 프로세스에 정확히 따르는지를 보는 프로세스 측면이 강하며, 안전성 평가의 경우 안전성 분석의 수행내용을 검토하는 제품관점의 성격이 강하다. 따라서 향후 철도소프트웨어의 안전성 확보를 위해서는 절차측면의 안전감사 뿐만 아니라 제품 품질 확보 측면의 안전성 평가 기술의 확보가 중요하다고 하겠다.

[참 고 문 헌]

[1] ISO/IEC 15504 "Information Technology-Process Assessment-Part 1~5"
[2] ISO/IEC 9126 "Information Technology-Software Quality Characteristics and Metrics-Part 1,2,3"
[3] ISO/IEC 14598 "Information Technology-Software Product Evaluation-Part 1~6"
[4] 과학기술부, "원자력 안전백서 2005"
[5] 박윤호, 국방품질관리소, “국방품질시스템 인증”, 1999. 12
[6] Railtrack PLC, "Engineering Safety Management(Yellow Book) Issue 3", October 2003