# 철도소프트웨어 안전성 관리체계 제시방안 연구

정의진* 신경호
한국철도기술연구원

# A Study on Derivation of Railway Software Safety Management Procedure

Joung, Eui-jin* Shin, Kyung-ho
KRRI (Korea Railroad Research Institute)

**Abstract** - Softwares in railway system are being used in the area of railway control system, directly associated to safety. Because the instinct characteristic of Software is uncertainty, Software development without safety insurance is very hazardous situation. In order to derive safety certification process in the railway system, certification and approval processes in the nuclear, aviation, and military area are studied. Software quality should be improved by two aspects : one is product aspect, another is process aspect. GS(Good Software) and ES(Excellent Software) certification can be exemplified in a product aspect approach. In those process certification, CMMI (Capability Maturity Model Integration) or SPICE (Software Process Improvement and Capability dEtermination : ISO/IEC15504) is being used as models for assessing process maturity of organization. Following the studies, safety management procedure in the railway system is suggested.

## 1. 서 론

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 품질 관점에서 원자력, 항공, 국방분야의 품질관리절차에 대해 살펴봄으로써 철도소프트웨어에 적절한 안전성 관리 체계에 대하여 검토하고자 한다.

## 2. 타 산업분야 품질관리절차

### 2.1 원자력 분야

한국원자력안전기술원(검토자)에서 수행하는 안전심사의 일반적인 검토절차는 그림 1과 같다. 국내 원자력법에 따른 인허가 사항들은 크게 신규원전의 건설/운영허가, 허가된 사항에 대한 변경허가, 그리고 특정기술주제보고서의 승인으로 구분된다.

검토자는 신청자가 어떤 원자력시설의 허가신청서를 제출하면 그 신청서의 유형을 먼저 결정한다. 그 신청서의 유형을 결정하면, 검토자는 그 신청 서류의 적합성 여부를 검토한다. 신청 서류의 적합성이 결정되면, 검토자는 신청서의 유형에 따라 적합한 검토범위를 결정하고 신청서에 맞는 검토계획을 수립한다. 검토계획의 목적은 계획된 활동과 일정을 상위 관리자에게 보고하고, 검토자가 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.

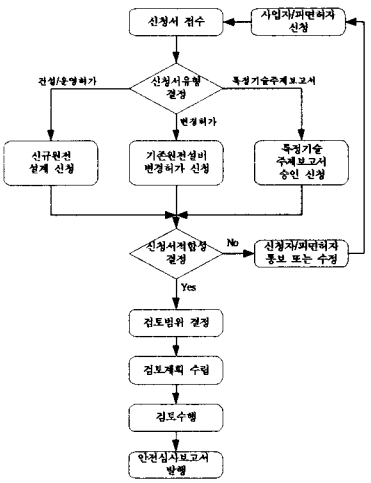


그림 1. 원자력 안전심사 검토절차[1]

### 2.2 항공분야

항공기는 3차원의 공간을 운행하는 비행체로서 임무수행을 위한 성능요구 뿐만 아니라 고도의 신뢰성과 안전성이 요구되므로 항공기의 설계 및 생산 그리고 운용에는 반드시 적합한 증명절차를 거쳐 인증을 받아야 한다. 항공기 품질인증은 감항기준에 대한 합치성의 평가라는 절차로 수행되며, 항공기의 인증은 형식증명, 생산증명, 감항증명의 3가지 개념으로 대별할 수 있다. 형식증명은 항공기 설계의 감항기준에 대한 적합성을 입증하는 것이며, 생산증명은 승인된 설계형식에 적합한 항공기 및 부품을 대량으로 생산하기 위한 생산시설, 생산방법 및 품질관리체제를 승인하는 것이다. 감항증명은 제작된 항공기가 승인된 형식설계와 합치하고 안전한 작동상태에 있음을 증명하는 것으로서 개별 항공기 마다 감항증명을 소지해야 하며 항공기 운항에 필수적이다.

증명의 과정으로 수행되는 합치성의 평가는 비행성능 및 안정성, 기체구조 안전성, 설계 제작, 동력장치, 계기 및 전기전자 시스템 등의 분야에 대하여 계산, 시험, 검증 그리고 경험의 방법으로 수행하며, 생산에 대한 합치성은 생산자의 품질보증체제 및 절차 검증, 공정 검증, 생산 기술상의 기준 평가 및 감사를 통하여 판단하고, 필요한 경우 공인시험을 거쳐야 한다. 따라서 항공기의 품질인증은 설계, 생산되는 개별 항공기가 감항성을 확보하고 있음을 시스템적으로 입증하는 것이다.

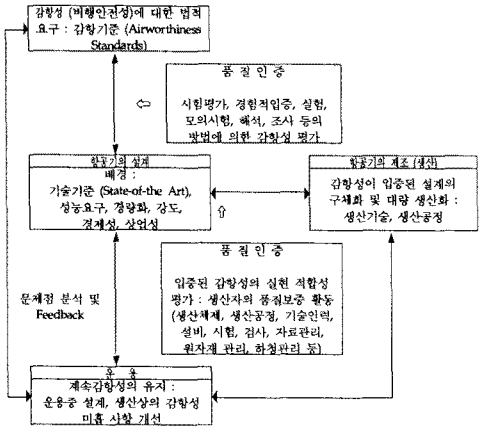


그림 2. 항공기 감항증명의 개요[2]

### 2.3 국방분야

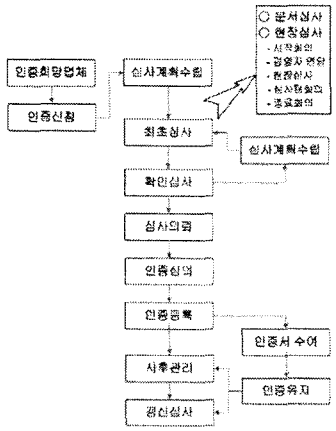


그림 3. 국방시스템 품질관리 절차도[3]

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 다음의 업무를 수행한다.

1) 문서심사

현장심사를 위한 준비단계로 해당 품질시스템 규격의 요구사항에 대한 품질매뉴얼 및 절차서의 적합성을 심사한다.

2) 현장심사

- 시작회의

심사시작 첫날, 첫 시간에 신청업체의 경영자(또는 품질경영 대리인)와 관련부서장, 심사원 전원이 참석하여 상호 인사 소개, 심사계획 및 진행방법에 관하여 설명한 후 질의응답을 한다. 신청업체는 심사원을 현장에 안내하거나, 심사 중 부적합 사항을 입회 확인하는 임무를 수행하는 심사 안내자를 임명하여 현장심사를 지원한다.

- 경영자면담

심사팀장이 신청업체의 경영자(또는 품질경영 대리인)와 면담을 통하여 최고경영자의 품질방침 및 의지, 품질시스템 현황 파악과 개선 여부를 확인한다.

- 현장심사

심사원이 신청품목의 생산공장에서 품질시스템의 이행실태를 확인한다.

- 심사팀회의

심사기간중 일과 마지막시간에 심사원이 한자리에 모여 심사중 발견된 부적합사항 및 심사진행에 관하여 정보교환을 한다.

- 종료회의

심사 종결후 신청업체 경영자(또는 품질경영 대리인)와 관련부서장, 심사원 전원이 참석하여, 심사결과에 대하여 강평하고 의견을 교환한다.

## 3. 철도분야 품질관리 절차

### 3.1 철도분야 안전관리절차

철도시스템의 안전성을 입증하기 위해서는 다음 그림에서 나타난 절차에 따라서 수행한다. 프로젝트관리자, 시스템검토위원회 및 안전성검토그룹간의 행정절차를 그림 4에 나타내었다.

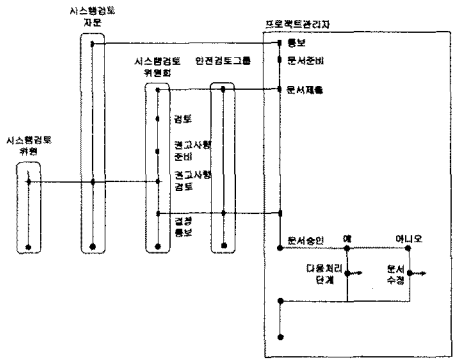


그림 4. 안전관리조직간의 행정절차[4]

프로젝트관리자는 관련된 문서를 준비하여, 시스템검토위원회나, 안전검토그룹에 보내어 안전성 인증처리를 한다.

### 3.2 각 조직별 역할

프로젝트관리자는 안전에 관련된 모든 사항을 수행하며, 안전에 관련된 사항은 시스템검토위원회의 승인을 받는다. 시스템 검토위원회는 철도 안전에 관련된 모든 사항을 담당하여 처리한다. 시스템검토위원회에서 위임

된 사항은 안전검토그룹에서 취급한다. 독립적 안전성검토위원회는 프로젝트관리자가 안전계획에 따라 안전 활동을 제대로 수행하였는지를 확인한다.

#### 3.2.1 시스템검토위원회

시스템검토위원회는 안전과 관련하여 개념구상과 개발단계에서부터 적용, 유지보수, 폐기단계까지의 과정에서 안전에 영향을 미칠 수 있는 장비와 시스템의 생애에 걸친 공식적인 안전평가를 하며, 지도한다. 프로젝트의 안전기록을 검토함으로써 프로젝트의 안전관리를 감독한다. 시스템검토위원회가 검토할 문서는 안전계획과 안전대책기술서가 포함되며, 안전평가 일정, 위험원 분석기록, 위험평가기록, 안전요건명세, 안전평가보고서, 안전감사 보고서 등을 검토한다. 시스템위원회의 주요 수행내용은 다음과 같다.

- 안전대책기술서의 검토
- 안전과 관계있는 문서 여부를 표시하고 공인
- 합리적 근거에 의해 부적절, 부정확, 부적합하다고 생각되는 제출물 거부
- 안전을 위한 제도를 권고하고, 이에 대한 승인을 위해 관련조직에 제공
- 시스템, 장비, 부속품, 서비스 수준 협의, 운영과정에 대한 형식승인
- 검토안 제출 조직에게 권고내용을 공식 기록한 증명서를 발급

#### 3.2.2 안전검토그룹

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. 안전검토그룹의 주요 내용은 다음과 같다.

- 제출물의 검토
- 제출물의 승인
- 안전과 관계있는 문서의 존재를 표시하고 공인
- 합리적 근거에 의해 부적절, 부정확, 부적합하다고 생각되는 제출물의 거부

안전검토그룹의 업무분야는 다음과 같다.

- 차량한계 및 궤간의 변경
- 궤도의 지지형태 변경
- 새로운 열차 정지패턴의 도입
- 새로운 역사도입
- 신호시야에 영향을 미칠 때

#### 3.2.3 독립적 안전성검토위원회

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.

안전감사는 프로젝트의 안전성확보 관리활동이 적합하고 안전 계획에 준하여 실행되고 있는지 확인하기 위한 목적으로 행해진다. 만일 안전계획이 없다면, 안전감사가 실행되기 전에 이를 설정해야 한다. 안전계획에 준하는 프로젝트의 범위에 대한 결정, 안전계획의 적합성에 대한 결정, 계획에 따른 작업의 권장 또는 이의 개선을 권고한다.

- 기존 감사 이래로 행해진 작업(첫 감사일 경우는 지금까지 행해진 모든 작업)
- 다음 단계를 위한 계획

안전성 평가는 개발되고 있는 시스템에 관련한 위험이 적절한 수준으로 감소되었는지의 여부를 결정하는 과정이다. 시스템 안전성 요구사양을 중심으로 하여 평가자는 안전성 요구사양의 규정이 위험도를 통제하는데 충분한 지를 평가하기 위해 이를 검토하고 이 시스템이 안전성 요구사양의 규정을 충족시키는 지의 여부를 검토한다.

## 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 안전감사 및 안전성 평가 관점이 있음을 알 수 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] 과학기술부, "원자력 안전백서 2005"
[2] 이종희, 항공산업연구소 논문집, "항공기의 품질인증과 미국의 제도분석", 1994. 6
[3] 박윤호, 국방품질관리소, "국방품질시스템 인증", 1999. 12
[4] Railtrack PLC, "Engineering Safety Management(Yellow Book) Issue 3", October 2003
[5] ISO/IEC 15504 "Information Technology-Process Assessment-Part 1-5"
[6] ISO/IEC 9126 "Information Technology-Software Quality Characteristics and Metrics-Part 1,2,3"