철도 안전필수 소프트웨어를 위한 안전기준 도출

정의진°, 신경호
한국철도기술연구원

Development of Safety Criteria for Railway Safety Critical Software

Eui-Jin Joung°, Kyung-ho Shin
KRRI(Korea Railroad Research Institute)

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. 서 론

철도시스템은 한번에 많은 인원을 수송하기 때문에 여러 특성들 가운데 안전성 확보가 매우 강조되어 왔다. 안전성 확보를 위해서는 소자특성상 fail-safe 특성이 강하게 나타나는 릴레이를 주로 사용하여 왔다. 그러나 안전성 뿐만 아니라 편의성도 중요한 대중 교통수단이란 점 때문에 여러 가지 새로운 기능들이 요구되고 있으며, 릴레이로 구현하기에 비효율적인 부분도 많아지게 되었다. 따라서 안전과 직접적으로 관련없는 설비에 대해서는 소프트웨어로 구현하여 적은 공간에서 빠르게 원하는 기능을 수행하게 하려는 상황이며, 안전과 직접적으로 관련되어 있는 설비에 있어서도 차츰 소프트웨어로 구현해 나가고 있는 추세이다.

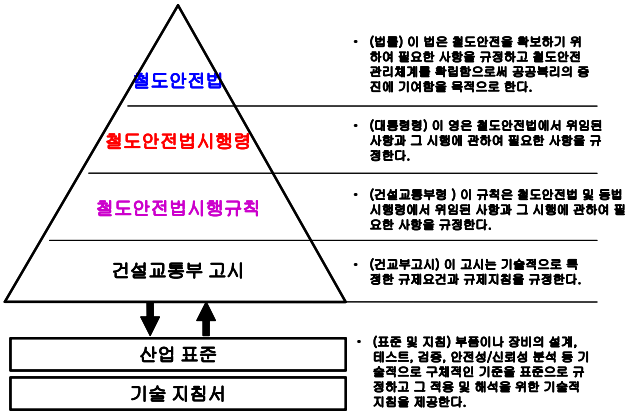
현재까지 개발기간, 비용 등의 이유로 철도분야의 경우 소프트웨어의 기능구현에만 중점을 둔 것이 사실이다. 그러나 소프트웨어의 특성상 불확실성이 존재하며, 이러한 불확실성을 염두에 두지 않고, 안전성 검증없이 소프트웨어를 사용할 경우, 만약의 사태로 인해 사고로 이어진다면 그 피해는 매우 엄청나다고 할 수 있다. 이미 선진국 중에서 안전필수 소프트웨어를 다루는 분야에서는 소프트웨어의 안전을 확보하기 위한 기준을 제시하고, 검증하는 체계를 갖추어 만일의 사태에 대비하고 있다. 철도분야에 있어서도 철도소프트웨어를 위한 안전기준을 제시할 필요가 있으며, 제시된 안전기준에 맞게 철도소프트웨어가 제대로 개발되었는지 검증하고, 인증하는 체계를 구축할 필요가 있다. 본 논문에서는 앞으로 제시될 철도소프트웨어의 안전기준 구성 체계를 살펴보고, 안전기준을 운영할 관리체계에 대하여 논하고자 한다.

2. 철도안전법과 철도안전기준

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 프로세스적 관점이 있다.

건교부 사업인 철도종합안전기술개발사업 중 한국철도기술연구원 주관으로 2004년부터 2008년까지 수행하는 "철도소프트웨어 안전기준 체계구축" 과제의 목적은 철도에 사용되는 컴퓨터 기반 제어기의 소프트웨어 안전성 확보를 위한 안전규제 체계의 개발이다. 즉, 아래 그림에서와 같이 철도안전법, 시행령, 시행규칙의 하위 법령으로 철도소프트웨어에 대한 안전기준을 마련하고, 이에 대한 해석을 뒷받침할 수 있는 지침을 개발하는 것이다. 건설교통부 고시로 제정될 안전기준은 기존의 국제규격(IEC, ISO 등), 국내규격(KS 등), 산업체 표준 (IEEE 표준 등)과 동떨어져 제시되어서는 안되며, 이를 아우르면서 제시되어야 한다.

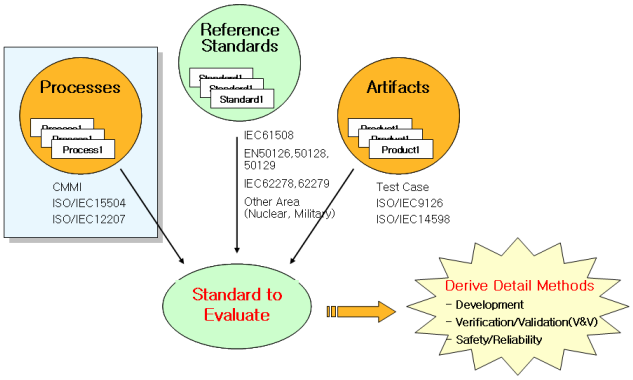


<그림 1> 철도안전법과 표준과의 관계

3. 철도소프트웨어 안전기준

3.1 철도안전기준 도출을 위한 표준

철도소프트웨어 안전기준은 그림 1에서 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, 조직체계를 다룬 프로세스 관련 규격들과, 제품 품질과 관련된 규격들로 구분할 수 있다.

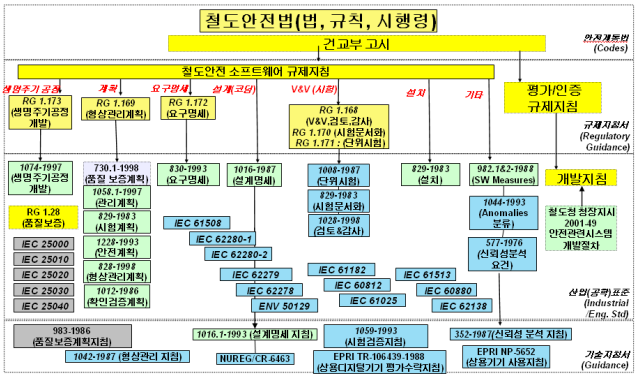


<그림 2> 철도소프트웨어 안전기준 관련 표준의 범주

Reference Standard로는 전기전자 규격인 IEC 61508과 철도관련 규격인 IEC 62278, IEC 62279 규격들을 대표적으로 들 수 있다. 소프트웨어 프로세스와 관련하여서는 미국 SEI (Software Engineering Institute)의 CMMI(Capability Maturity Model Integration)와 ISO/IEC 15504

(SPICE: Software Process Improvement and Capability dEtermination)를 들 수 있으며, 소프트웨어 제품과 관련하여서는 소프트웨어 품질특성을 정의한 ISO/IEC 9126과 소프트웨어 제품의 품질특성 평가를 다루고 있는 ISO/IEC 14598이 있다.

아래 그림에서 철도소프트웨어 안전기준을 작성하는데 있어서 생명주기 공정, 계획, 요구명세, 설계, 시험, 설치 등으로 구분하여 참조하여야 하는 규격 및 기준과의 관계를 도식화하여 나타내었다. [1]-[4]

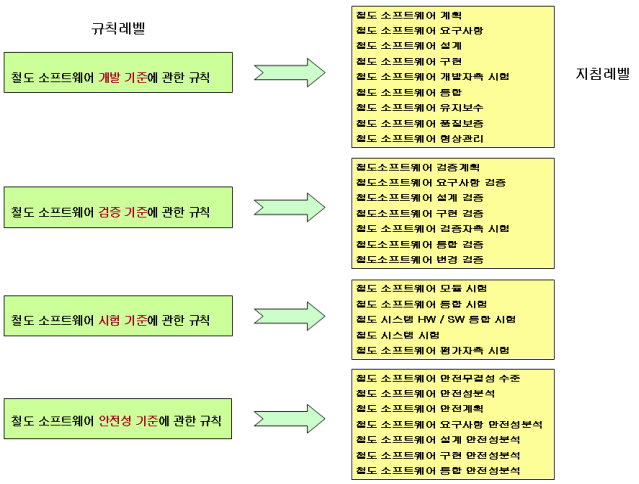


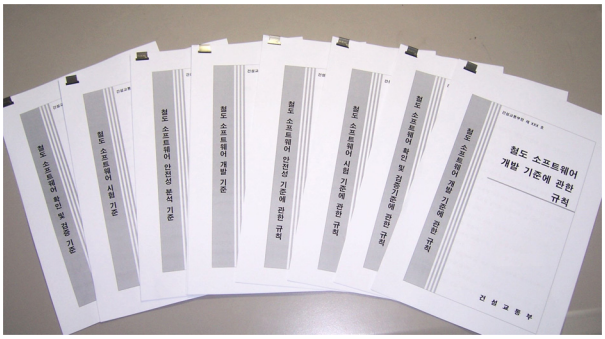
<그림 3> 철도S/W안전기준과 표준과의 관계

3.2 철도소프트웨어 안전기준 구성 체계

현재 수행중인 "철도소프트웨어 안전기준 및 체계구축" 과제에서는 해당 규격들을 참고하여 건교부 고시 수준에 해당하는 규칙레벨로 수명주기별로 안전기준(안)을 제시하고 있다. 여기에서 수명주기는 관점에 따라 여러 수명주기가 있을 수 있는데 본 과제에서는 개발, 검증, 시험, 안전성의 4가지 수명주기로 분류하고 각각에 대하여 수명주기별 안전기준(안)을 제시하였다. 또한 지침레벨로 각각의 수명주기에 대한 세부 지침(안)을 개발 중에 있다.

아래 그림에서는 안전기준 즉, "철도소프트웨어 안전기준에 관한 규칙" 레벨에서의 4가지 수명주기에 대비하여 안전기준을 기술적으로 보완 설명하는 지침레벨의 구성을 나타내었다.

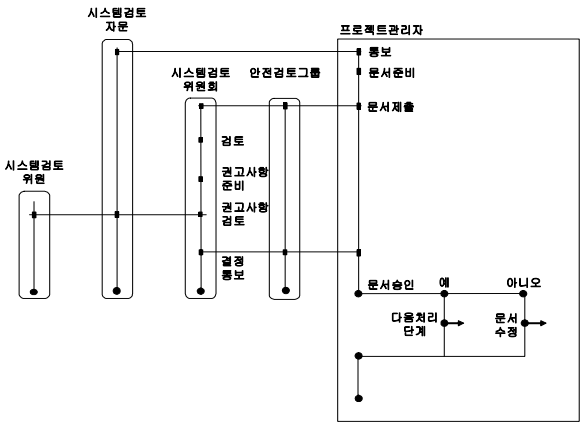




<그림 4> 철도소프트웨어 안전기준 구성 체계

3.3 철도소프트웨어 안전관리절차

철도시스템의 안전성 입증과 관련하여서는 다음 그림에서 나타난 절차에 따라서 수행하도록 제시하고 있다. 프로젝트관리자, 시스템검토위원회 및 안전성검토그룹간의 행정절차를 아래 그림에 나타내었다. [5]



<그림 5> 안전관리조직간의 행정절차

프로젝트관리자는 안전관련 문서를 준비하여, 시스템검토위원회나, 안전검토그룹에 보내어 안전성 인증을 요청한다.

프로젝트관리자는 안전에 관련된 모든 사항을 수행하며, 안전에 관련된 사항은 시스템검토위원회의 승인을 받는다. 시스템 검토위원회는 철도 안전에 관련된 모든 사항을 담당하여 처리하며 시스템검토위원회에서 위임된 사항은 안전검토그룹에서 취급한다. 기술적인 내용에 대하여 안전검토그룹으로부터 검토 위임을 받은 독립적 안전성검토위원회는 프로젝트관리자가 안전계획에 따라 안전 활동을 제대로 수행하였는지를 확인한다. 위 절차는 위험요인 도출 및 분석, 위험도 평가, 안전요구사항 도출, 안전계획 수립, 안전성 평가보고서 작성의 각각의 단계에서 반복 수행된다.

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 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. 철도소프트웨어의 안전기준은 철도 도메인과 프로세스 측면, 제품 측면에서의 관련 규격들과 호환되도록 작성되었다. 앞으로 세부 지침 제시에 있어서 개발자 및 평가자가 직접 적용할 수 있도록 현장 적용성을 확보하는 것 또한 중요하다고 하겠다.

[참 고 문 헌]

[1] ISO/IEC 15504 "Information Technology-Process Assessment-Part 1~5"

[2] ISO/IEC 12207 "Information Technology- Software lifecycle processes"

[3] ISO/IEC 9126 "Information Technology-Software Quality Characteristics and Metrics-Part 1,2,3"

[4] ISO/IEC 14598 "Information Technology-Software Product Evaluation-Part 1~6"

[5] Railtrack PLC, "Engineering Safety Management(Yellow Book) Issue 3", October 2003