2008년도 대한전기학회 하계학술대회 논문집 2008. 7. 16 - 18

철도소프트웨어 발주 및 평가프로세스 제안

정의진*, 신경호*
한국철도기술연구원*

Suggestion of Ordering and Assessment Process for Railway 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, and 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 suggests development process, ordering management and assessment process for railway software with more detail description.

1. 서 론

철도시스템 개발에 있어서 근본적으로 고려해야할 요소를 든다면 안전성 확보를 들 수 있다. 예전에는 전원이 인가되지 않는 조건에서 무조건 낙하하는 릴레이라는 소자를 이용하여 Fail-safe 특성을 구현하였다. 그러나 많은 부피를 차지하는 릴레이를 이용하여 점차 복잡해져가는 철도시스템의 기능을 구현하기에는 많은 어려움이 따랐고, 릴레이 접점불량으로 인한 시스템 고장을 방지하기 위하여 많은 유지보수 비용 또한 들여야 하는 상황이었다. 현재는 이러한 릴레이 구동방식에서 벗어나 안전과 관련하여 원자력, 항공, 국방분야 등 여러 분야에서 소프트웨어를 적용하는 사례가 급증하고 있으며, 철도시스템의 경우도 예외는 아니다.

그러나 소프트웨어의 특성상 불확실성이 존재하며, 이러한 불확실성을 해결하지 않고서 철도시스템과 같이 안전성 확보가 최우선인 시스템에 적용하였을 경우, 만약의 사태로 인하여 사고가 발생한다면 그 결과는 심각하다고 할 수 있다.

이를 위하여 국내뿐만 아니라 국외에서는 철도소프트웨어의 안전성 확보를 위한 연구가 꾸준히 진행되어 오고 있으며, 소프트웨어의 안전성이 확보되었는지를 검증하는 체계 또한 구축 중에 있다. 국내에서는 2004년부터 철도종합안전기술개발사업의 일환으로 철도소프트웨어에 대한 안전기준 및 이에 대한 관리체계를 구축하고자 하는 연구가 진행되고 있으며, 2007년에는 철도소프트웨어의 개발프로세스를 제시한 바 있다. 이는 안전과 관련된 철도소프트웨어를 개발하기 위한 적절한 프로세스를 제시한 것으로 개발업체에서 참고할 프로세스이며, 철도소프트웨어를 발주하고, 발주한 소프트웨어가 개발프로세스에 따라 적절히 수행되고 있는지에 대한 평가프로세스 또한 구축함으로써 전체적인 관리체계를 구축한다고 할 수 있다. 본 논문은 이미 제시한 철도소프트웨어 개발프로세스를 기반으로 발주 및 평가프로세스를 제시한 사례를 논하고자 한다.

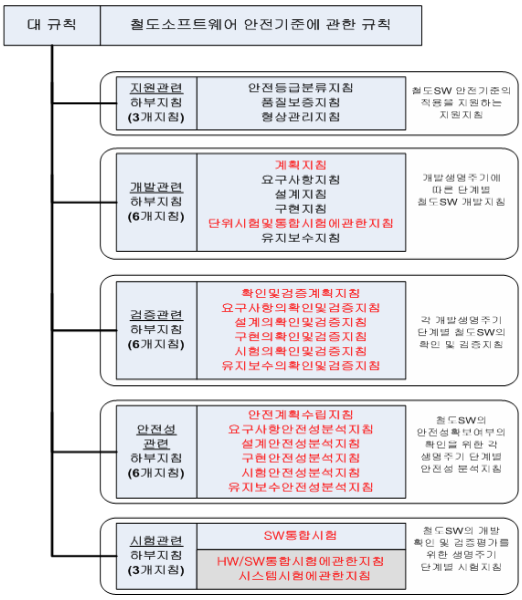
2. 철도소프트웨어 안전기준 및 개발프로세스

2.1 철도소프트웨어 안전기준

좋은 소프트웨어란 품질 좋은 소프트웨어를 말하며, 안전성이라는 것도 소프트웨어 품질의 하나라고 볼 수 있다. 이러한 품질 좋은 소프트웨어를 만들려는 노력으로는 품질 좋은 제품을 만들고, 정확한 시험으로 개발된 제품의 품질이 원하는 수준에 도달했는지를 판단하는 방법이 있을 수 있으며, 이와는 다른 관점으로 품질 좋은 제품은 잘 관리된 조직체계에서 만들어진다는 프로세스 관점을 생각해 볼 수 있다.

철도소프트웨어 안전기준을 마련하기 위해서는 기존의 국제규격 및 규정들과 부합하여야 하며, 국내 상황 또한 고려하지 않으면 안된다. 따라서 위에서 제시한 두 가지 관점에 관하여 여러 관련 규격들을 검토하여 안전기준을 제시하고자 하였다. 먼저 철도분야의 안전관련 표준으로는 전기전자 규격인 IEC 61508과 철도관련 규격인 IEC 62278, IEC 62279 규격을 대표적으로 검토하였다. 이중 IEC 62279는 유럽전기전자 표준규격인 CENELEC의 EN 50128에서 국제규격으로 전환된 규격으로 철도분야 소프트웨어에 대해 다루고 있다. 프로세스 관점으로는 미국 SEI (Software Engineering Institute)의 CMMI (Capability Maturity Model Integration)와 ISO/IEC 15504 (SPICE: Software Process Improvement and Capability dEtermination)를 소프트웨어 프로세스 성숙도 측면에서 주요 프로세스 모델로 검토하였으며, 제품 관점으로는 소프트웨어 품질특성을 정의한 ISO/IEC 9126과 소프트웨어 제품의 품질특성 평가를 다루고 있는 ISO/IEC 14598을 주요 검토대상규격으로 검토하였다. [1]-[7]

본 과제에서 제시하는 안전기준은 철도안전법, 시행령, 시행규칙 하부의 국토해양부 고시수준으로 "철도소프트웨어 안전기준에 관한 규칙"과 이에 대한 상세기술지침으로 구성되어 있다. 그림 1은 제안한 철도소프트웨어 안전기준(안)을 규칙과 해당 상세기술지침 목록으로 정리하여 나타낸 것이다. 기술지침에서는 지원, 개발, 검증, 안전성분석, 시험의 5가지 분야로 나누어 기술되어 있으며, 각 기술지침은 조항 및 해설, 근거기준으로 구성되어 있다. 그림에서 모든 상세기술지침은 개발업체에서 참조해야 할 사항이며, 적색으로 표시한 항목은 평가기관에서 고려할 사항이다.



〈그림 1〉 철도소프트웨어 안전기준(안) 구성

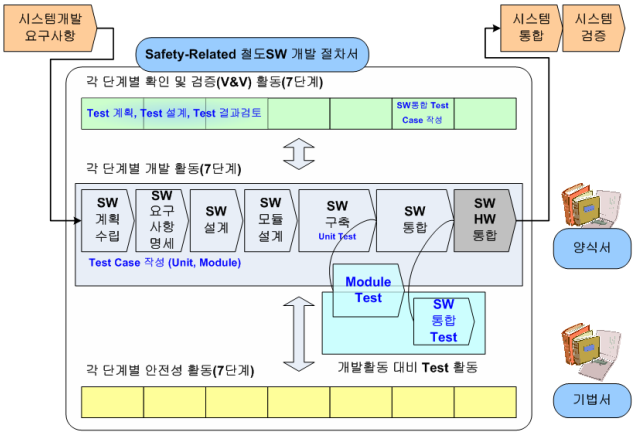
2.2 철도소프트웨어 개발프로세스

제시하는 철도소프트웨어 안전기준은 법적인 성격을 갖추다 보니 구체적으로 수행하여야 할 절차가 언급되어 있지 않아 실제로 개발업체나 평가기관에서 안전기준을 적용할 경우에 많은 혼선이 야기될 수 있다. 따라서 개발, 검증, 시험, 안전성 분석을 하는 Lifecycle 각 단계에서 철도소프트웨어의 개발을 위하여 수행하여야 하는 업무를 체계적으로 규정한 것이 철도소프트웨어 개발프로세스라고 할 수 있다.

개발프로세스를 적용함으로써 수요자는 균질한 산출물을 얻을 수 있으며, 체계적인 품질보증을 받을 수 있고, 프로젝트 진행 중에 품질을

확인할 수 있다. 공급자는 프로세스 기반의 개발을 할 수 있어 체계적인 품질보증이 가능하고, 표준을 쉽게 만들 수 있으며, 체계적이고 구체적인 계획을 수립할 수 있어서 불필요한 일을 최소화 할 수 있으며, 개발자의 경우 프로세스에 기반한 개발활동이 가능해져 계획에 따라 개발을 할 수 있으며, 결함유발의 가장 큰 원인인 요구사항을 조기에 확정할 수 있어서 시간과 노력을 줄일 수 있으며, 업무의 중복이나 누락을 최소화 할 수 있는 장점이 있다.

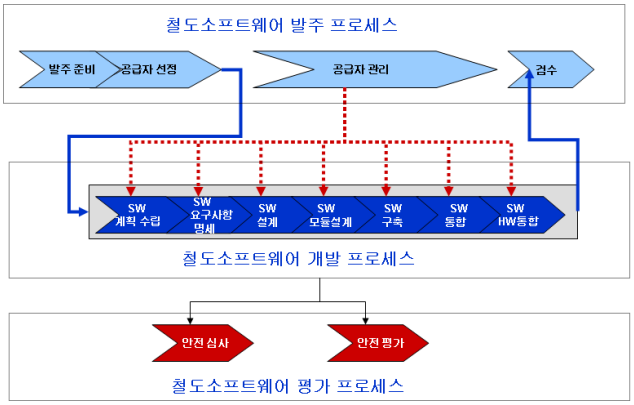
철도소프트웨어 개발프로세스는 철도분야에서 특히 강조되는 안전과 관련된 소프트웨어를 개발할 때 적용할 수 있는 접근방법을 제공하기 위해 개발되었다. 본 프로세스는 절차서, 양식서, 기법서의 세 부분으로 구성되어 있으며, 절차서는 프로세스를 구성하는 각 단계와 각 단계에 포함된 활동을 보여준다. 각 단계는 개발, V&V 및 Safety의 3분야의 활동으로 구성되어 있으며, 각각의 활동들은 주어진 입력을 받아들여 출력을 생성하기 위한 과정을 나타내었다. 그 외 절차서에서 정의된 입·출력물을 작성하기 위한 템플릿으로 양식서를, 보다 기술적인 내용을 담기 위하여 기법서를 작성하였다. 그림 2는 철도소프트웨어 개발프로세스의 구성을 나타낸 그림이다. 총 7단계의 개발프로세스가 있으며 각 개발활동에 대하여 V&V, Safety 활동이 연계되어 개발이 이루어지도록 하고 있다. 일반소프트웨어의 경우 V&V에서 Safety 활동까지 포함하여 전반적으로 검토하고 있으나 안전이 중요한 철도시스템의 특성을 감안하여 Safety를 따로 분리하여 프로세스를 제시하였다. [8]



〈그림 2〉 철도소프트웨어 개발프로세스

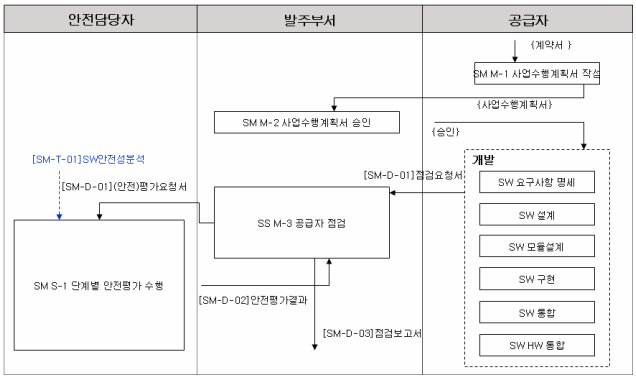
3. 철도소프트웨어 발주 및 평가 프로세스

철도소프트웨어의 발주 및 평가프로세스는 철도 분야에서 특히 강조되는 안전과 관련된 소프트웨어를 발주할 때 적용할 수 있는 접근방법을 제공하기 위해 개발되었다. 본 발주 및 평가프로세스는 철도소프트웨어 개발프로세스와 연계하여 활용될 수 있도록 작성되었다. 따라서 본 발주 및 평가 프로세스는 안전과 관련된 철도소프트웨어를 발주하는 조직에서 활용하고, 선정된 공급자는 제시한 철도소프트웨어 개발프로세스를 적용하여 소프트웨어를 개발할 경우에 효과적으로 적용할 수 있다.



〈그림 3〉 안전관련 철도소프트웨어 발주 및 평가 프로세스

본 발주 및 평가프로세스 또한 철도소프트웨어 개발프로세스에서와 마찬가지로 절차서, 양식서, 기법서의 세 부분으로 구성되어 있다. 또한 발주 준비, 공급자 선정, 공급자 관리, 검수의 4단계로 구성된다. 본 발주 및 평가 프로세스의 절차서에서는 각 수행단계에 대한 활동 및 실무부서, 발주부서, 계약부서의 담당자와 안전담당자, 공급자들간의 역할을 제시하고 있다. 또한 구체적으로 해당 단계의 입·출력문서 및 수행내용을 기술하고 있다.



〈그림 4〉 철도소프트웨어 공급자 관리단계의 발주 및 평가 프로세스

그림 4는 철도소프트웨어 발주 및 평가 프로세스 중 공급자 관리단계를 나타낸 것으로 공급자 영역의 개발부문과 관련하여 기존에 제시한 철도소프트웨어 개발 프로세스와의 연계를 나타낸 그림으로 개발단계 각 단계마다 발주부서에서는 공급자 점검과정을 거치고 안전담당자는 단계별 안전평가를 수행하도록 구성하고 있다.

4. 결 론

본래 불확실성이 존재하는 소프트웨어를 철도시스템과 같이 안전성이 중요한 시스템에 적용하기 위해서는 철저한 안전성 검증이 필요하다. 원자력, 항공, 국방분야의 경우에서도 각기 시스템에 맞추어 품질보증 체계를 구축하고 있음을 보아도 알 수 있다. 철도소프트웨어의 경우 안전성을 확보하고 품질 좋은 소프트웨어를 개발하기 위해서 프로세스관점 및 제품관점의 접근이 필요한데 프로세스 성숙도 향상 관점에서는 개발하고자 하는 소프트웨어의 품질을 확보하고자 CMMI나 SPICE(ISO/IEC 15504)에서 제시하는 여러 절차 및 프로세스를 따르도록 함으로써 소프트웨어 개발조직의 성숙도를 향상시키고자 하고 있으며, 제품관점의 접근법으로는 정형기법에 의한 개발 및 검증이나, 개발 초기부터 검토하여 도출한 Test Case에 따라 시험을 수행하여 소프트웨어의 품질을 향상시키는 방법을 고려하고 있다.

본 프로젝트에서는 앞서 언급한 프로세스관점 및 제품관점의 소프트웨어 품질향상 방법을 감안하여, 철도소프트웨어에 대한 안전기준을 제시하였으며, 제시된 안전기준의 현장 적용성을 높이기 위하여 절차서, 양식서, 기법서로 구성된 철도소프트웨어에 대한 개발프로세스를 제시하였다. 또한 철도소프트웨어를 발주하고, 운영하는 기관을 위하여 발주 및 평가프로세스를 제시하였다. 제시한 프로세스가 국내 실정에 맞는지에 대한 여부는 별도 프로젝트로 진행하여 그 결과를 피드백 받음으로써 최종적으로 한국상황에 적합한 개발 및 발주, 평가 프로세스를 제시한다면 아직까지 기반이 취약한 철도소프트웨어 산업의 육성에 크게 기여할 것으로 기대한다..

[참 고 문 헌]

[1] IEC 62278, "Railway application - The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)", March, 2002
[2] IEC 62279, "Railway application - Software for railway control and protection system", June, 2002
[3] CENELEC EN50129, "Railway application - Safety related electronic systems for signaling", April, 2000
[4] ISO/IEC 15504 "Information Technology-Process Assessment-Part 1~5"
[5] ISO/IEC 12207 "Information Technology- Software lifecycle processes"
[6] ISO/IEC 9126 "Information Technology-Software Quality Characteristics and Metrics-Part 1,2,3"
[7] ISO/IEC 14598 "Information Technology-Software Product Evaluation-Part 1~6"
[8] 정의진, 철도소프트웨어 안전기준 및 체계 구축 3차년도 보고서, 한국철도기술연구원, 2007