철도소프트웨어 개발 및 평가프로세스 제안

Suggestion of Development and Assessment Procedure for Railway Software

정의진* 신경호**

Joung, Eui-jin **Shin, Kyung-ho**

ABSTRACT

One of the main concerns of railway system is to secure safety. Nowadays digital technology has been rapidly applied to safety critical 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 makes it difficult to predict the software failures. For this reason, the safety criteria are suggested to secure the software safety for the field of railway system. Following them, the railway software have to be examined whether it is properly developed according to the safety criteria and certification process. Because the articles suggested in safety criteria are written in legal term, it is difficult to apply the criteria to develop railway software. This paper suggests and discusses a development and assessment procedure to solve these issues for railway software with more detail description.

1. 서 론

철도시스템의 여러 고려요인 중 안전성이 중요하다는 것은 강조해도 지나치지 않는다. 시스템의 안전성을 확보하기 위해 지금까지는 하드웨어가 고장나지 않아야 한다는 신뢰성 측면의 연구가 많은 부분 진행되었다. 현재 안전성 확보를 위한 연구는 대부분 하드웨어에 대한 시험 및 검증이라고 볼 수 있다. 그러나 안전성 확보라는 것은 시스템 측면에서 검토해야할 사항으로 운영 및 유지보수, 폐기 절차까지 고려해야 하는 광범위한 활동으로 하드웨어에만 국한하여 접근하여서는 않된다.

시스템 측면에서 안전성을 검토하여 하드웨어가 수행하여야 하는 업무, 소프트웨어에서 수행하여야 하는 업무를 정하는 것이 안전계획이며, 이 안전계획에 따라 시스템을 구현하는 것이 안전대책활동이다. 지금까지 하드웨어 측면의 안전대책활동으로 요구사양을 수립하고, 설계, 제작, 시험을 하는 일련의 활동들은 많은 부분 정립되어 있는 상태이지만, 소프트웨어 측면의 안전대책활동이라는 것은 아직 정립되어 있지도 않고 모호한 것이 사실이다.

* 한국철도기술연구원, 전기신호연구본부, 정회원
E-mail : ejjoung@krri.re.kr
TEL : (031)460-5448 FAX : (031)460-5449
** 한국철도기술연구원, 전기신호연구본부, 정회원
E-mail : khshin@krri.re.kr
TEL : (031)460-5488 FAX : (031)460-5449

소프트웨어로 시스템의 기능을 구현할 경우에는 프로세스 처리를 육안으로 확인할 수 없을 뿐만 아니라 의도하는 프로세스가 정확히 수행된다는 것을 보장할 수가 없기 때문에 소프트웨어로 구현한 기기의 정확한 기능 수행 보장 및 품질 및 신뢰성 확보가 무엇보다도 중요하다.

현재 적은 공간에서 빠르게 원하는 기능을 구현할 수 있다는 장점 때문에 안전이 중요한 시스템에서 소프트웨어의 사용이 증대되고 있는데, 이는 아직까지 안전성이 확보되었다는 것이 입증되지 않은 상태에서 소프트웨어를 사용한다고 볼 수 있으며, 만약의 사태로 소프트웨어의 오작동으로 인하여 사고로 이어질 경우 그 손실은 막대하다고 할 수 있다.

따라서 철도소프트웨어에 대하여 안전기준을 새로이 제시하는 연구가 진행 중에 있으며, 제시된 안전기준에 따라 철도소프트웨어가 제대로 개발되었는지 검증하는 체계 또한 연구 중에 있다. 소프트웨어 개발이라는 것은 최종 소스코드 작성만을 의미하지는 않으며, 수명주기 각 단계마다 제시되어야 하는 문서작성 또한 중요하며, 이는 작성된 문서를 근거로 검증 및 평가가 이루어져 소프트웨어의 품질을 보증할 수 있기 때문이다. 본 논문에서는 철도소프트웨어 제시되는 안전기준에 대하여 소개하고, 철도소프트웨어의 수명주기 각 단계마다 수행하여야 하는 업무를 언급하고, 절차, 양식, 기법을 정리한 개발 프로세스에 대하여 논하며, 발주자나 평가자 입장에서 고려할 발주 및 평가 프로세스에 대하여 논하고자 한다.

2. 철도소프트웨어 안전기준

철도시스템에 있어서 품질 좋은 소프트웨어를 만들려는 노력으로 제품자체의 품질을 향상시키는 방법과 제품을 개발하는 프로세스 관리를 통한 문제해결 방안을 생각할 수 있다. 철도소프트웨어의 신뢰성 및 안전성을 확인하고 보증하기 위해서는 제품관점에서 좋은 제품을 만들고, 정확한 시험으로 개발된 제품의 품질이 원하는 수준에 도달했는지를 판단하는 방법이 있을 수 있으며, 이와는 다른 관점으로 좋은 제품은 좋은 조직 체계에서 만들어진다는 프로세스 관점을 생각해 볼 수 있다. 물론 개발 대상 분야에 대한 지식 또한 중요하다. 그림 1은 철도소프트웨어의 품질을 확보하기 위한 각 관점과 관련된 규격들을 분류하여 나타낸 것이다.

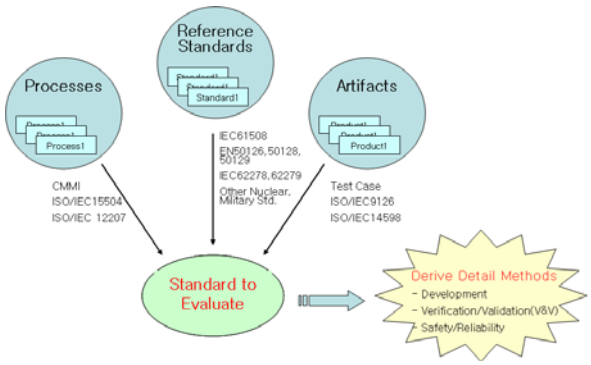

그림 1. 철도소프트웨어 안전과 관련되어 있는 규격의 분류

철도분야의 안전관련 표준으로는 전기전자 규격인 IEC 61508과 철도관련 규격인 IEC 62278, IEC 62279 규격을 대표적으로 들 수 있다. 이중 IEC 62279는 유럽전기전자표준규격인 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 들 수 있으며, 소프트웨어 관련 프로세스에 대하여 성숙도 등급을 매겨 관리하고 있다. 제품 관점으로는 소프트웨어 품질특성을 정의한 ISO/IEC 9126과 소프트웨어 제품의 품질특성 평가를 다루고 있는 ISO/IEC 14598을 들 수 있다. [1]-[7]

국토해양부 사업으로 철도종합안전기술개발사업 중 한국철도기술연구원 주관으로 2004년부터 2008년까지 수행하는 "철도소프트웨어 안전기준 및 체계구축" 과제에서 제시되는 안전기준은 상기 근간이 되는 국제 표준 외에 여러 국제규격(IEC, ISO 등), 국내규격(KS 등) 및 산업체 표준 (IEEE 표준 등) 등과 서로 상충되지 않도록 하며, 국내 환경을 고려하여 안전기준을 제시하고 있다. [8]

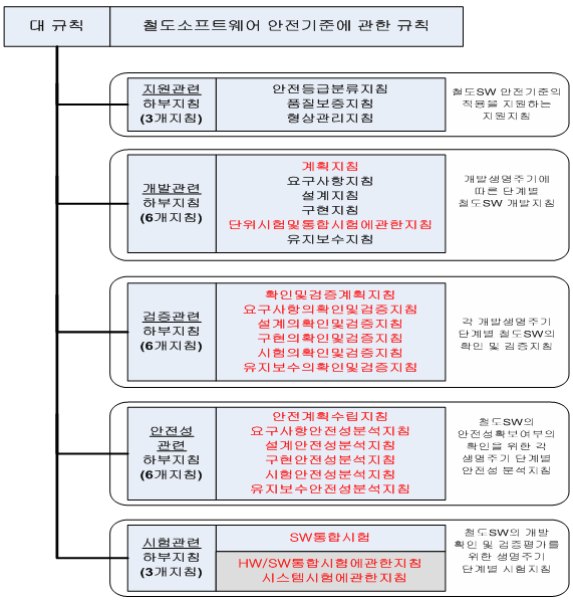

그림 2. 철도소프트웨어 안전기준(안) 구성

본 과제에서 제시하는 안전기준은 철도안전법, 시행령, 시행규칙 하부의 국토해양부 고시수준으로 철도소프트웨어안전기준에관한규칙과 이에 대한 상세기술지침으로 구성되어 있다. 그림 2는 제안한 철도소프트웨어 안전기준(안)으로 규칙과 해당 상세기술지침 목록을 정리하여 나타내었다. 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.

안전기준에 관한 규칙과 상세기술지침은 부처에서 고시하는 일종의 법적인 성격을 갖추다 보니 구체적으로 수행하여야 할 절차가 언급되어 있지 않아 실제로 개발업체나 평가기관에서 안전기준을 적용할 경우에 많은 혼선이 야기될 수 있다. 다음 장에서는 안전기준을 적용하기 위한 개발 및 평가 프로세스에 대하여 논하였다.

3. 철도소프트웨어 안전기준 적용을 위한 세부 절차

3.1 철도소프트웨어 개발프로세스

소프트웨어를 개발하기 위해 개발 조직의 환경과 소프트웨어 및 시스템을 사용할 사용자의 환경에 적합한 소프트웨어 개발방법을 제시하기 위한 프로세스를 일반적으로 방법론이라는 용어를 사용한다. 소프트웨어를 개발하기 위한 개발프로세스의 적용은 1970년대 이후 구조적 방법론을 거쳐, 1980년대의 정보공학 방법론, 1990년 이후의 객체지향 방법론이 제기되었다. 각 방법론마다 장단점이 있어 개발하려는 시스템의 특징을 고려하여 개발프로세스를 채택하여야 한다.

철도소프트웨어의 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 안전의 3분야의 활동으로 구성되어 있으며, 활동들은 주어진 입력을 받아들여 출력을 생성하기 위한 과정을 나타내었다. 양식서는 절차서에서 정의된 입□출력물을 작성하기 위한 format을 정한 것으로 목차 및 그 구성 내용을 설명하고 있다. 이 양식서를 활용함으로써 사용자는 보다 쉽게 프로세스에서 원하는 입□출력물을 확인할 수 있게 된다. 기법서는 절차서에 기술된 활동으로 설명하기에는 보다 기술적인 내용을 포함하고 있는 항목들을 모아둔 것으로 이러한 기법들은 기술이 발전되면서 지속적으로 확대해 나갈 수 있다.

그림 3에 나타낸 철도소프트웨어 개발프로세스는 다음의 7단계로 구성된다.

1) 철도소프트웨어 계획 수립 단계
2) 철도소프트웨어 요구사항 명세단계
3) 철도소프트웨어 설계 단계
4) 철도소프트웨어 모듈 설계 단계
5) 철도소프트웨어 구축 단계
6) 철도소프트웨어 통합 단계
7) 철도소프트웨어 하드웨어 통합 단계

본 프로세스의 절차서에서는 각 수행단계에 대한 활동 및 각 단계의 담당자, V&V담당자, 안전담당자의 담당자들간의 역할을 제시하고 있다. 또한 구체적으로 해당 단계의 입□출력문서 및 수행내용을 기술하였다. 일반 소프트웨어 개발프로세스에서는 V&V담당자가 안전담당자의 역할까지 포함하여 품질관리 관점에서 소프트웨어의 확인 및 검증을 수행하는데 대하여 안전을 중요시하는 철도시스템의 특성상 안전담당자 영역을 따로 구분하여 제시하였고, 안전담당자가 작성□검토한 문건은 바로 발주기관 또는 제 3 안전성 인증기관의 검토 문건이 되어 최종 검토를 받을 수 있도록 구성하였다.

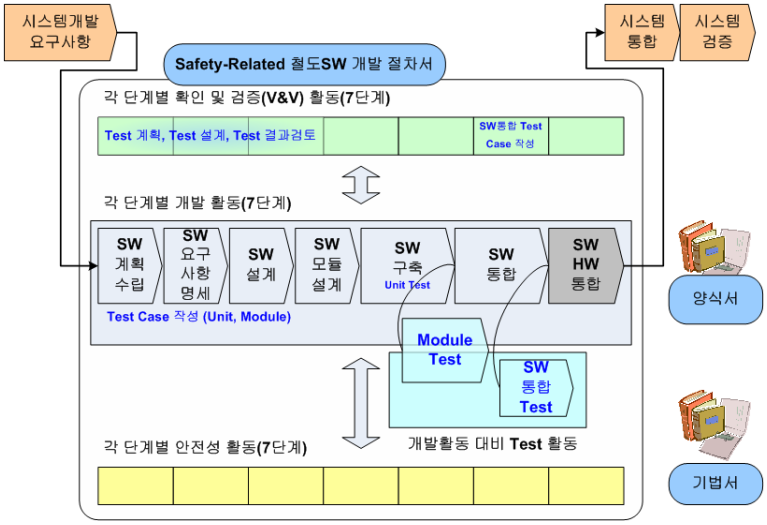

그림 3. 철도소프트웨어 개발프로세스

3.2 철도소프트웨어 발주 및 평가 프로세스

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

본 발주 및 평가프로세스 또한 철도소프트웨어 개발프로세스에서와 마찬가지로 절차서, 양식서, 기법서의 세 부분으로 구성되어 있다. 또한 발주 준비, 공급자 선정, 공급자 관리, 검수의 4개의 단계로 구성된다.

본 발주관리프로세스의 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.

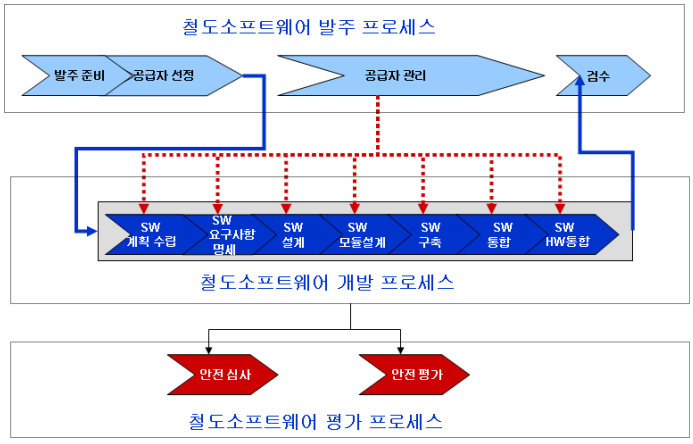

그림 4. 철도소프트웨어 발주 및 평가 프로세스

4. 결　　론

본래 불확실성이 존재하는 소프트웨어를 철도시스템과 같이 안전성이 중요한 시스템에 적용하기 위해서는 철저한 안전성 검증이 필요하다. 이는 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 필요하며, 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 제시한 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. 본 연구가 취약한 기반의 철도소프트웨어 산업의 육성에 기여하길 기대한다.

참고문헌

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 외, 철도소프트웨어 안전기준 및 체계 구축 3차년도 보고서, 한국철도기술연구원, 2007