2007년도 대한전기학회 EMECS학회 추계학술대회 논문집 (2007.10.25-10.26)

철도소프트웨어 안전기준의 현장 적용방안 도출

신경호*, 정의진*
한국철도기술연구원

Deduction of the Application Plan for Railway Software Safety Criteria

Kyung-Ho Shin*, Eui-Jin Joung*
Korea Railroad Research Institute

Abstract - In this paper, the safety criteria and framework of railway software which is developing presently is examined. The software development capability and organization of railway company in korea are investigated through interview and are analyzed. Then the application plan for railway software safety criteria is deduced to apply criteria to railway industry effectively.

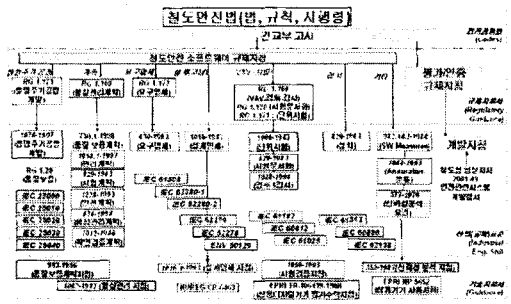
1. 서 론

철도시스템은 규모가 큰 수송 시스템이기 때문에 대형 사고 발생 시 대규모의 인명피해 및 재산 손실이 발생할 수 있으며, 하나의 시스템 장애가 철도 전체 시스템에 영향을 줄 수 있다. 철도에서 사고를 방지하기 위하여 컴퓨터 및 디지털 제어기의 활용이 다양한 분야에서 활용되고 있다. 디지털 제어기가 철도에 적용되는 분야는 신호제어분야, 건널목, 열차의 차상신호 및 제동, 시설물의 감시 및 진단분야 등에 사용되고 있으며, 사용분야가 점차 넓어지고 있어 단순기능에서부터 기능 의존도가 높은 분야까지 다양한 분야에 고루 적용되고 있다. 기능 의존도가 높은 분야에 적용되는 디지털제어기는 고장이 발생할 경우 사고의 직접적인 원인이 될 수 있으며 하드웨어 및 소프트웨어 관점에서의 안전성 확보 활동이 필요하며, 현재까지 주로 하드웨어 관점에서의 안전성 확보 활동들이 수행되어 왔다. 하지만 철도시스템의 안전성을 향상시키기 위해서는 철도시스템에 탑재되는 소프트웨어의 신뢰성, 안전성을 증대를 위한 소프트웨어에 대한 안전성 활동 및 소프트웨어 안전성 검증이 반드시 필요하다. 효과적인 철도 소프트웨어의 신뢰성 및 안전성 향상을 위해서는 철도 소프트웨어의 안전을 확보하기 위한 기준과 평가 및 검증체계의 구축이 필요하며, 현재 건설교통부(건교부) 추진사업인 철도종합안전기술개발사업 중 한국철도기술연구원이 주관으로 수행하는 "철도소프트웨어 안전기준 및 체계구축"과제에서 이에 관한 안전기준 및 안전체계를 개발하고 있다[1].
하지만 현 철도산업계의 기술수준을 무시한 이상적인 안전성 활동 및 평가체계의 도입은 기준과 산업 간의 괴리를 야기할 가능성이 있으며, 국내 철도산업계의 기술 및 체계를 향상시키고 기술의 안정을 도모하기 위해서는 국내 철도소프트웨어 개발업체의 현장조사가 필수적이다.
따라서 본 논문에서는 현재 개발 중인 철도소프트웨어의 안전기준 및 안전체계에 관하여 살펴보고 국내 철도산업계의 소프트웨어 개발수준을 조사하여 철도소프트웨어 안전기준의 효과적인 산업현장 적용방안을 도출한다.

2. 철도소프트웨어 안전기준

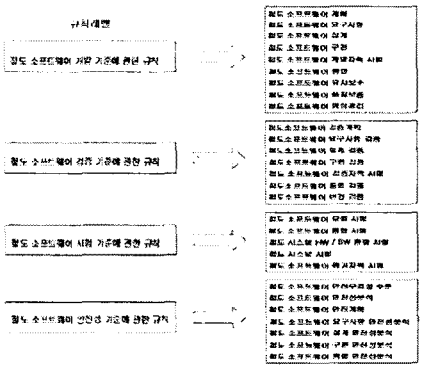
2.1 철도소프트웨어 안전기준

건교부 사업인 철도종합안전기술개발사업 중 한국철도기술연구원 주관으로 2004년부터 2008년까지 수행하는 "철도소프트웨어 안전기준 및 체계구축" 과제의 목적은 철도에 사용되는 컴퓨터 기반 제어기의 소프트웨어 안전성 확보를 위한 안전규제 체계의 개발로서 철도안전법, 시행령, 시행규칙의 하위 법령으로 철도소프트웨어에 대한 안전기준을 마련하고, 이에 대한 해석을 뒷받침할 수 있는 지침을 개발하는 것으로 국제규격, 국내규격, 산업표준 등을 참고하여 건교부 고시 수준에 해당하는 규칙 수준의 수명주기(개발, 검증, 시험, 안전성)별 안전기준(안)과 세부 지침(안)을 개발하고 있다. 철도소프트웨어 안전기준은 건교부 고시수준에 속하는 기준으로 이러한 법령 또는 기준들은 기존의 산업표준이나 기술지침들과 서로 상충하지 않아야 하며 국내외의 관련기준, 표준들을 참조하여야 하며 [그림1]과 같은 관계를 가진다[1].



[그림1] 철도소프트웨어 안전기준과 타 표준간의 관계

[그림2]는 안전기준인 철도소프트웨어 안전기준에 관한 규칙 수준에서의 개발, 검증, 시험, 안전성으로 정의된 4가지 수명주기에 대한 안전기준을 기술적으로 보완 설명하는 지침레벨의 구성을 나타내었다[1].



[그림2] 철도소프트웨어 안전기준 구성 체계

3. 국내 철도시스템 소프트웨어 개발현황 분석

철도소프트웨어 안전기준의 효과적인 적용을 위해서는 국내 철도시스템에 탑재되는 소프트웨어의 개발기술 수준조사 및 현황분석이 필요하며, 분석결과를 반영한 안전기준 및 이에 대한 적용방안의 개발이 필수적이다.

3.1 대상기업

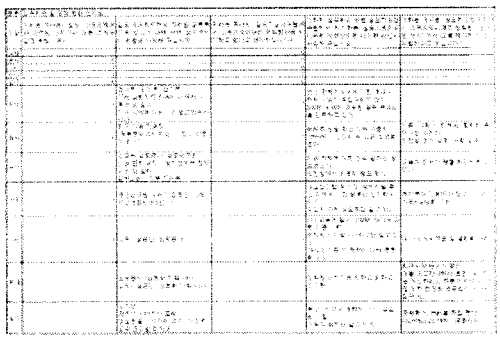
현재 철도시스템과 관련하여 소프트웨어가 탑재되는 제품을 개발 및 생산하고 있는 국내업체를 개발 및 검증 프로세스 대상기업으로 한정하여 현장조사를 수행하였다. 총 12개 업체의 참여가 있었으며 가능한 많은 기업의 참여를 유도하고자 하였으나 기술 보안 등의 이유로 일부 기업에서는 협조를 얻지 못하였다.

3.2 조사방법

협조 기업의 기술 및 연구, 개발 인력에 대한 조사를 위한 방법으로는 여러 가지가 있으나, 시간과 장소에 대한 제약이 따르며 직접 업무를 관찰하고 조사를 할 수 없으므로 조사하고자 하는 사항에 대한 질문들을 도출하여 1차로 사전 설문조사를 수행한 후 2차로 관련 인력들에 대한 인터뷰를 진행하였다. 총 200여개의 문항을 도출하였으며 그 중 간단한 답이 가능한 문항만을 별도로 분류하여 1차 설문을 수행하였다. 철도소프트웨어관련 기업의 상세한 개발 및 검증프로세스 조사는 개발자와 관리자로 나누어 별도의 인터뷰를 통해 진행하였다. 여기에서 관리자란 개발조직이나 개발과제를 관리하는 직책을 가진 사람을 지칭하며, 개발자란 실제 소프트웨어의 개발을 담당하는 사람으로 프로그래밍이나 그 설계를 담당하는 사람을 지칭한다. 인터뷰는 개발자, 관리자 그룹으로 나누어 진행 되었으며, 각 기업별로 개발자 1인 이상 및 관리자 1인 이상의 인력이 인터뷰에 참여하였다. 인터뷰 시간은 개발자 그룹의 경우 대략 2.5시간, 관리자 그룹의 경우 약 30분 정도의 시간이 소요되었다.

3.3 현황분석결과

1차, 2차 현장조사를 통한 국내 철도산업계의 철도소프트웨어 개발 및 검증 프로세스 현황은 총 19개의 카테고리로 분류하여 분석하였으며 [그림3]과 같이 각 카테고리별로 엑셀파일을 만들어 분석자료의 정리를 효율화하였다.



[그림3] 소프트웨어 개발 검증프로세스 현황분석자료

- 정부기관 및 정책 관련 인지도

철도 소프트웨어의 관리 또는 개발과 연관이 있는 정부 기관 및 정책에 대한 인지도를 조사하였으며 많은 기업들이 한국철도기술연구원, 철도공사, 시설공단 등을 언급하였다.

- 소프트웨어 관련 규격 및 기준에 대한 인지도

현재 기업이 적용하고 있거나 관심이 있는 소프트웨어 관련 규격에 대하여 조사하였다. 이미 인지하고 있는 규격이나 기준이 있는 경우 또는 기적용하고 있는 규격이나 기준이 있는 경우 현재 추진 중인 과제의 산출 결과를 적용하는데 용이 할 수 있다. 그러나 분석결과 대부분의 기업 관련자들이 인지하고 있는 규격의 수와 종류가 다양하지 않고 그 인지 수준 또한 높지 않은 것으로 파악되었다.

- 소프트웨어 안전에 대한 인지도

개발자들의 소프트웨어 안전에 대한 인지도는 높지는 않으나 어느 정도 필요성은 인지하고 있으며 관리자들의 소프트웨어 안전에 대한 인지도는 개발자 대비 낮은 것으로 파악되었다. 또한 개발자 및 관리자와의 인터뷰 시 철도 관련 제품의 발주와 평가를 담당하는 기관의 인력이 철도 소프트웨어에 대한 특징을 제대로 파악하지 못하고 있는 것으로 파악 되었다.

- 개발자 및 평가자에 대한 신뢰도

일부 조직의 경우 개발자와 평가자의 구분이 모호한 경우가 있었고, 분리가 되어 있는 조직의 경우 제품 신뢰성을 시험에 전적으로 의존하고 있는 개발 현실에 비춰 개발조직과 평가조직간의 상호 신뢰도가 높은 것으로 파악되었다.

- 소프트웨어 품질 및 관련 규격에 대한 인지도

대부분의 개발자들의 경우 소프트웨어 자체의 품질에 대하여는 개념을 정확히 파악하고 있지 못하며, 국내외 관련 규격에 대해서도 알지 못하는 경우가 대부분인 것으로 파악 되었다.

- 관련 전문가 집단에 대한 인지도

소프트웨어 관련 전문가와 교수 등의 전문 지식인들과의 교류 또는 자문 등의 실태를 파악하기 위하여 시도하였으나, 현재 소프트웨어 관련 전문가와 직접적인 관계를 가지고 기술적 도움이나 관련 정보를 제공 받는 등의 시도는 많이 부족한 것으로 파악되었다.

- 제품분류에 대한 인지도

현재 개발자들이 분류하는 일반 소프트웨어와 내장소프트웨어의 구분을 확인하고 그들이 개발하고 있는 제품군의 특징을 조사하였다. 대체적으로 일반소프트웨어와 임베디드 소프트웨어를 정확히 구분하고 있었으나, 일부 개발자의 경우 내장소프트웨어와 실시간소프트웨어를 혼돈, 구분하지 못하였다.

- 검증 및 확인 과정에 대한 인지도

검증과 확인 과정이 무엇인지, 누구에 의해서 어떻게 이루어져야 하는지, 잘 인지하고 그대로 수행 되고 있는지 파악하기 위한 문항들로 구성되어 있다. 개발자, 관리자 모두 확인 및 검증 과정에 대한 정확한 이해는 부족하였으며, 각 과정을 정확히 수행하는 개발 조직 또한 없는 것으로 파악되었다.

- 임베디드 시스템 및 개발 제품군에 대한 인지도

임베디드 시스템과 critical 시스템의 정의 및 현재 각 기업이 개발하고 있는 제품의 분류와 관련된 문항을 개발자들을 대상으로 조사하였다. 대체적으로 safety critical system에 대하여는 잘 구분 하고 있는 반면, 나머지의 개념은 부족한 것으로 판단되며 따라서 개발자 자신이 개발하고 있는 소프트웨어 제품의 안전성이 실제 사회에 미치게 되는 영향에 대한 인지도도 낮은 것으로 파악되었다.

- 소프트웨어 고장에 대한 인지도

소프트웨어에 있어 error, bug, fault, failure등의 개념 파악 여부와 그에 따르는 처리 또는 예방 방법에 대한 개발자들의 인지도를 파악하기 위한 질문들로 구성했다. 이 질문들에 대하여 대부분의 개발자들은 error와 failure를 혼돈하고 있는 경우가 많았고 또한 그에 대한 적절한 대응 법을 알고 있는 경우도 거의 없었다.

- 개발환경 관련 인지도

현재 개발에 활용하고 있는 개발환경(Development Environment)을 파악 하고 개발자들이 이 도구들을 어떤 역할로 얼마만큼 사용하고 있는지 파악하고자 하였다. 대부분의 기업들이 Microsoft사의 Visual Studio를

활용하여 C/C++언어로 개발을 하고 있었으며, 임베디드 소프트웨어의 개발을 위하여 Windriver사의 Tornado를 사용하는 경우가 주류를 이루었다. 임베디드 소프트웨어의 경우 실시간운영체계(RTOS)로 VxWorks를 활용하여 응용소프트웨어를 개발하는 경우가 대부분이었으며, CTC 등의 관제소프트웨어의 경우 Microsoft사의 Windows 운영체계에서 동작하는 응용소프트웨어를 개발하고 있었다.

- 개발조직 및 인력에 대한 인지도

현재의 기업 내 개발조직과 그 인력 구성과 관련 지식에 대한 인지도를 파악하고자 하였으며 대부분의 기업들은 2~4명으로 구성된 1개 정도의 소프트웨어 개발팀을 운영하고 있으며, 소프트웨어의 설계와 구현을 분리하지 않고 개발자 1~2인이 담당하여 개발과정을 진행하는 것으로 파악되었다.

- 개발경험 및 관련지식에 대한 인지도

개발자와 관리자들의 소프트웨어 개발경험과 개발 관련 기술지식에 대한 인지도를 파악하는 것으로 대체로 개발자들은 5년 이상의 개발경력을 가지고 있었다. 소프트웨어에 대한 전공지식을 가지고 있는 개발자는 많지 않았으며 대개 전기, 전자공학 등의 전공지식을 가지고 있고, 교육기관, 독학 등을 통해 소프트웨어 개발능력을 익힌 것으로 파악되었다. 따라서 안전기준 및 체계를 적용하기에 앞서 개발자들에 대한 안전필수 소프트웨어 체계와 개발방법론에 대한 인지도를 높이는 작업이 선행되어야 한다.

- 외주개발에 대한 인식

대부분의 기업들은 기업 자체적으로 소프트웨어를 개발하고 있었다. 이것은 철도시스템에 탑재되는 소프트웨어의 규모가 하드웨어 대비 크지 않고, 중요성을 심각하게 고려하지 않는 발주처나 기업 관리자에 의해 판단되고 있기 때문이다.

- 소프트웨어 시험관련 지식 인지도 및 활용도

요구사양에 관한 지식의 보유 및 활용정도를 확인하기 위한 질문들에 대하여 개발자나 관리자 모두 그 중요성은 인지하고 있으나 요구사양의 분석 및 관리방법에 대한 지식은 거의 갖고 있지 않았다.

- 개발 프로세스 및 방법론 관련 지식 인지도

대부분의 설문참가자가 개발 프로세스나 방법론에 대한 지식은 가지고 있지 않았지만 개발 프로세스 및 방법론에 대한 필요성은 인지하고 있었다.

- 정형기법 관련 인지도

대부분의 설문참가자가 정형기법에 대하여 모르고 있었다. 정형기법을 적용한 경험이 있는 기업도 있었으나 시험적용 또는 외부에서 정형기법으로 분석된 요구사양을 근거로 소프트웨어를 개발한 것으로 파악되었다.

- 조직구성 및 제품구성, 인력관리, 조직경력부분 정보

설문 참가기업의 조직구성은 제품별 개발에 초점이 맞춰진 조직으로 파악되었다. 효율적인 소프트웨어 안전을 확보하기 위해서는 소프트웨어 개발 및 시험인력의 보충과 함께 소프트웨어 개발특성을 고려한 인력 및 조직의 관리가 필요한 것으로 파악되었다.

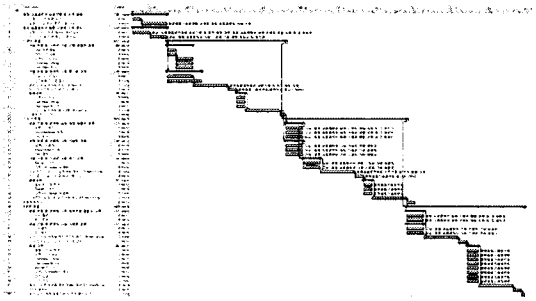
4. 현장적용방안 도출

4.1 철도소프트웨어 개발 프로세스 현황

국내 철도소프트웨어 개발수준 및 개발현황을 분석한 결과 개발기업만의 자발적인 참여를 통해 철도소프트웨어의 안전기준의 현장적용은 불가능하며, 발주기관의 적극적인 적용 노력이 없다면 철도소프트웨어 안전기준의 국내철도산업에 대한 적용은 쉽지 않을 것이다. 따라서 철도 소프트웨어의 안전성을 확보를 위해서는 소프트웨어 자체의 특성과 철도시스템의 특성 그리고 적용되어야 하는 안전성 확보 관련 기술에 대한 지식을 겸비한 인력과 조직이 철도 소프트웨어를 발주하는 기관에서 확보가 되어야하며 이러한 조직이 발주과정 전반과 제품의 평가에 주도적인 역할을 하여야 한다. 또한 현황조사에 협조한 기업 중 해외 철도 사업에 대한 관심이 있는 기업들은 국내 철도 소프트웨어의 안전성을 인증해 줄 수 있는 기관의 필요성을 피력하고 있었으며 한국철도기술연구원에서 이러한 인증기관의 역할을 해 주는 것이 적합하다는 의견도 제시하고 있었다. 따라서 국내 철도 소프트웨어의 안전성 확보와 대외적인 기술력 제고를 위하여 철도소프트웨어 안전기준은 국제 기준과 대등 하거나 그에 비추어 우월한 기준이 필요할 것이다.

4.2 단계별 적용방안

철도소프트웨어 안전기준의 국내철도산업현장 적용을 위해서 가장 먼저 필요한 것은 개발기업과 발주기관에서의 철도소프트웨어에 대한 인식제고가 필요하며, 관련 인력을 대상으로 교육 등을 통한 철도소프트웨어의 안전성 확보의 필요성과 안전기준의 상세절차 및 안전기준 적용 시 얻을 수 있는 안전성 향상효과에 대한 홍보가 필요하다. 이러한 제반 사항들의 준비가 완료되면 개발 및 평가담당자들의 업무 수행능력의 향상이 필요하며, 철도소프트웨어 안전성 향상에 필요한 소프트웨어 설계, 평가 등에 대한 기술교육을 통해 가능하다. 현재 분석된 국내 철도소프트웨어 개발기업의 인식 및 기술수준을 고려할 때, 철도소프트웨어 안전기준의 적용을 위해서는 총 9년의 기간 동안 3단계로 구분된 적용계획을 수립하였으며 각 단계별 수행기간은 3년이다. 1단계는 소프트웨어의 요구사양 분석, technical writing, test case 작성 등을 강조 하는 단계로 구성하였다. 2단계는 소프트웨어 설계방법 및 관련 문서와의 연관관계 정리에 대한 중점 관리 단계로 구성하였다. 3단계는 전체 개발 과정에 대한 품질 관리 단계로 구성하였다. [그림4]는 총 9년 동안의 철도소프트웨어 안전기준의 적용계획을 나타낸다.



[그림4] 철도소프트웨어 안전기준의 단계별 적용계획

5. 결 론

철도소프트웨어의 안전을 확보하기 위해서는 안전기준 및 평가/검증체계의 구축이 필요하며, 현재 건교부 추진 사업인 철도종합안전기술개발사업 중 "철도소프트웨어 안전기준 및 체계구축"과제에서 이에 관한 안전기준 및 안전체계를 개발 중에 있다. 본 논문에서는 현재 개발 중인 철도소프트웨어의 안전기준 및 안전체계에 관하여 살펴보고 국내 철도산업계의 소프트웨어 개발수준을 조사/분석하였으며 철도소프트웨어 안전기준의 효과적인 산업현장 적용계획을 도출하였다.

[참 고 문 헌]

[1] 정의진, "철도 안전필수 소프트웨어를 위한 안전기준 도출", 대한전기학회 하계학술대회 논문집, 2007