철도 소프트웨어 정량적 신뢰성 평가방안 연구

A Study on the Evaluation Method of Quantitative Reliability for Railway Software

조현정*†, 황종규*

Hyunjeong Jo*†, Jonggyu Hwang*

Abstract Recently functions and complexity of embedded SW(software) for railway system have been increased rapidly, there is a growing percentage of potential deficiencies in the SW due to the cause of train accidents and delays. Especially since the fatal error due to the malfunction of SW during the railway operation is directly connected to human accidents, the validation on SW shall be performed by using various methods and the evaluation and verification on it must be available. In addition, the SW testing and verification activities in relation to the international standard for railway SW are already stipulated in terms of 'HR : Highly Recommend '. In this paper, we propose a study of the reliability evaluation methods that provide quantitative prediction of the inherent defects of the railway device embedded software by applying safety assessment procedures and methods in order to prevent potential failures of the railway software.

Keywords **:** Railway software, Safety, Reliability evaluation

초 록 최근 철도시스템 장치에서 소프트웨어의 사용이 급격히 증가함에 따라, 열차사고 및 지연의 원인으로 소프트웨어로 인한 잠재결함이 차지하는 비중이 높아지고 있다. 특히, 철도 운행 중 소프트웨어의 오작동으로 인한 치명적 오류는 인명사고로 즉결되기 때문에 소프트웨어에 대한 사전 검증을 위해 다양한 방법을 이용하여 수행하고, 이를 확인할 수 있어야 한다. 또한, 철도 소프트웨어 관련 국제규격에서 소프트웨어 테스트 및 검증 활동을 이미 'HR : Highly Recommend' 조건으로 규정하고도 있다. 본 논문에서는 철도 소프트웨어의 잠재적 결함에 의한 사고를 미연에 방지하기 위하여, 철도 소프트웨어 안전성관련 평가 절차와 방법을 적용하여 해당 장치의 내재된 결함을 정량적으로 예측하고 추정 가능하게 해주는 신뢰성평가 방안에 대한 연구 결과를 제시하고자 한다.

주요어 : 철도 소프트웨어, 안전성, 신뢰성평가

1. 서 론

최근 철도시스템 임베디드 소프트웨어는 그 기능 및 복잡도가 급격하게 증가하고 있고, 소프트웨어 오류 발생 시 그로 인한 위험 비용이 상대적으로 증가하고 있다. 특히 철도 운행 중 소프트웨어의 오작동으로 인한 치명적 오류는 인명 사고로 즉결됨으로 소프트웨어에 대한 검증을 다양한 방법을 이용하여 수행해야 하고 이를 평가 및 확인할 수 있어야 한다. 철도시스템 개발 중 소프트웨어 신뢰성 확보 및 안전성 평가를 위한 절차가 EN 50128, IEC 62279 등으로 규격화되고 있으며, 특히 IEC 62279의 경우는 평가 절차를 더욱 강화하여 최근 개정되는 등 이 규격을 적용한 철도 소프트웨어의 검증을 요구하고 있다 [1][2].

† 교신저자: 한국철도기술연구원 철도안전인증연구소(hjjo@krri.re.kr)

* 한국철도기술연구원 철도안전인증연구소

그러나 국내 철도 제작사들의 소프트웨어 개발 및 검증에 대한 기술 수준이 아직 국제 규격에서 요구하는 수준을 만족하기에 현실적으로 어려움이 존재하여, 철도안전법 개정에 따라 철도차량 소프트웨어 형식승인이 강제화 되었음에도 불구하고 유예되고 있는 실정이다 [3]. 이는 철도 제작사 즉, 개발자 측면에서는 고객의 다양한 요구사항을 반영하여 개발하고자 하는 시스템이 높은 복잡도와 보다 커진 시스템 규모를 갖게 됨에 따라서 정해진 일정과 비용에 맞추어 고객이 요구한 고품질/고신뢰성/고안전성을 달성하기 어려운 실정이기 때문이다. 그러므로 실제 철도시스템 임베디드 소프트웨어 개발 제품에 국제 규격에서 요구하는 신뢰성 확보를 위한 절차 및 문서화 결과에 대한 검증뿐만 아니라, 소프트웨어 테스트를 통한 분석 및 확인에 대응하기 위한 전략 마련을 위한 구체적인 지원 기술 개발이 매우 필요한 상황이다.

이러한 측면에서 철도시스템의 소프트웨어 신뢰도(Software Reliability)는 효과적으로 개발 프로젝트를 관리하여 비용과 일정, 품질 및 안전성에 대한 고객의 요구사항을 만족시킬 수 있는 정량적인 기준으로 활용될 수 있다. 이에 따라 본 논문에서는 철도 소프트웨어 신뢰성을 정량적으로 예측하고 평가하기 위한 소프트웨어 신뢰도 모델을 개발하여 제안하고자 한다. 이를 위해 국제 규격에서 요구하고 있는 철도 소프트웨어 안전성관련 평가 절차와 방법을 적용하여, 철도분야 소프트웨어 임베디드 장치의 내재된 결함을 정량적으로 예측하여 평가를 가능하게 해주는 신뢰성 평가 지원도구를 개발하였다. 논문 마지막 부분에 현재 개발하고 있는 도구의 구현 화면 결과를 일부 제시하였다.

2. 본 론

2.1 소프트웨어 정량적 신뢰성예측 평가모델

2.1.1 소프트웨어 신뢰성 평가기술 현황

소프트웨어 신뢰성에 대한 평가는 이미 제품의 신뢰성/정비성/가용성을 분석하여 제품 개발 타당성 및 설계 개선 사항을 도출하는 RAM(Reliability, Availability and Maintainability) 활동을 하고 있는 하드웨어에 비해 상당히 이론적인 접근이 쉽지 않고, 소프트웨어 시험단계에서 얻어져야 측정 가능한 소프트웨어 결함에 관련된 데이터 수집이 쉽지 않다는 커다란 어려움이 존재한다 [4]. 또한, 임베디드 소프트웨어도 하나의 구성품이고 소프트웨어 오류나 에러로 인한 고장이 시스템을 구성하는 하드웨어의 기능 수행에 치명적인 영향을 미칠 수도 있음에도 불구하고, 국내에서는 현재까지 RAM 분석 시 소프트웨어에 대한 분석은 거의 이루어지고 있지 않다는 문제가 있다.

앞서 언급한 바와 같이 Safety-critical 시스템인 철도시스템에서 최근 소프트웨어가 활용되는 규모와 의존도가 늘어남에 따라, 소프트웨어에 대한 신뢰성 분석을 통한 내재된 소프트웨어 에러와 오류로 인한 결함율을 도출하는 것이 매우 필요한 상황이 되었기에 이를 위해 기존 소프트웨어 신뢰성 예측 평가모델을 조사 분석해 보았다. 아직 국내에서는 사용하고 있지 않지만, 신뢰성 평가를 위한 예측 모델 중에 국외에서 널리 알려져 있는 모델로는 RL-TR-92-52, MUSA Model, Putnam Model, SoftRel prediction Models 등이 있다 [5]. 또

한, 최근에 IEEE std. 1633에서는 소프트웨어 신뢰성 예측 및 추정 등 FMEA(Failure Mode and Effect Analysis)에 관한 연구 내용도 제시되고 있다 [6].

본 논문에서는 소프트웨어 신뢰성 예측평가 모델 중에서 로마 실험실 RADC(Rome Air Development Center)에서 만들어 공표한 RL-TR-92-52 모델을 선정하였다 [7]. 그 이유는 다른 모델들에 비하여 수집데이터를 이용한 예측 및 추정에 있어서 계량화가 유동적이었기 때문이었다. 즉, 철도분야의 특수한 개발 현황을 반영하여 RL-TR-92-52 모델의 계량지표 변환을 통해 철도 현장의 적용 가능성을 높일 수 있을 것이라 판단했기 때문이다. 이 외에도 국내에서도 국방분야 무기체계 소프트웨어 개발에 있어서 신뢰성평가 항목을 필수로 적용하기 위한 준비단계에 있음을 조사를 통해 알 수 있었으며, 국방분야에서도 RL-TR-92-52 모델을 기반으로 신뢰성 분석 모델을 개발 중에 있다고 한다.

2.1.2 RL-TR-92-52 모델 선정

RADC(Rome Air Development Center) RL-TR-92-52 모델은 소프트웨어 개발단계에 따른 결함과 관련이 있는 Factor들에 대해 분석하고 신뢰도(결함밀도)를 계산하는 모델이며, 본 논문에서 철도 소프트웨어 신뢰성 예측 모델에 적용하는 것으로 선정하였다. RL-TR-92-52 모델에서의 각 단계별 계산식과 주요 매개변수 factor에 대한 설명과 최종 결함밀도를 구하는 식은 다음 표와 같다.

Table 1 The factors of RL-TR-92-52 model

구분		설명
계산식		δ(초기 결함 밀도) = A * D * (SA*ST*SQ) * (SL*SS*SM*SU*SX*SR)
SDLC	Concept단계	A: Application type(어플리케이션 유형) D: Development environment(개발 환경)
	Requirement /Design단계	SA : Software anomaly management(소프트웨어 예외관리) ST : Software Traceability(소프트웨어 추적도) SQ : Software Quality(소프트웨어 품질)
	Implementation단계	SL : Language type(개발 언어 유형) SS : Program size(프로그램 규모) SM : Modularity(모듈성) SU : Extent of reuse(재사용성) SX : Complexity(복잡성) SR : Software standard review(소프트웨어 표준 검토)

각 단계별 factor 정의는 표 1과 같으며, 각각의 factor를 구하는 자세한 내용과 수식은 [7]과 같다. 기본적으로 본 모델의 신뢰성 산출은 프로그램 소스라인 당 결함밀도를 나타내며, 고유 결점의 총 추정 수를 계산하기 위해 결함밀도는 라인의 예측한 수로 곱해야 하고

여기에 Function Point가 이용된다고 보면 된다. 소프트웨어 개발 단계별 본 모델의 적용 과정을 그림으로 나타내면 다음과 같다.

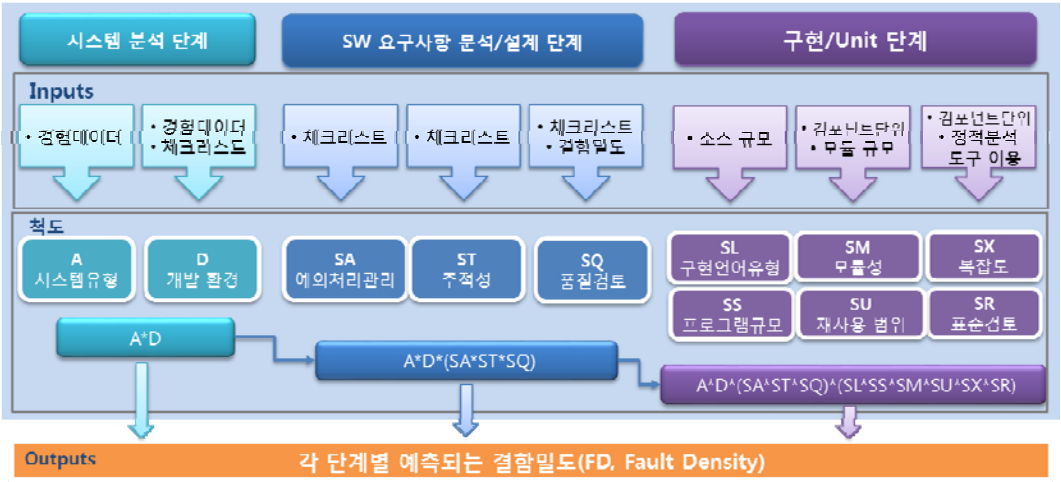

Fig. 1 The application process of software reliability evaluation model

2.2 철도 소프트웨어 신뢰성 예측 평가방안 및 지원도구 설계

2.2.1 기존 관련 국제규격 요구사항 반영

RL-TR-92-52 모델은 체크리스트 및 테스트를 통한 결함데이터를 기반으로 현재 소프트웨어에 잠재하고 있는 결함의 양을 정량화 한다. 철도분야와 같이 대규모 시스템을 제어하기 위해 사용되는 복잡한 소프트웨어의 경우 하드웨어와 달리 정량적으로 내재된 결함을 분석하고 평가하는 것이 쉽지 않으며, 이를 위해 실제 소프트웨어의 개발절차에 따라 반복적인 작업이 이루어져야 하며 안전성관련 평가 절차를 접목한 초기예측과 사후추정을 통해 정략적인 신뢰성 평가 결과를 얻을 수 있는 방안을 도출해야 한다.

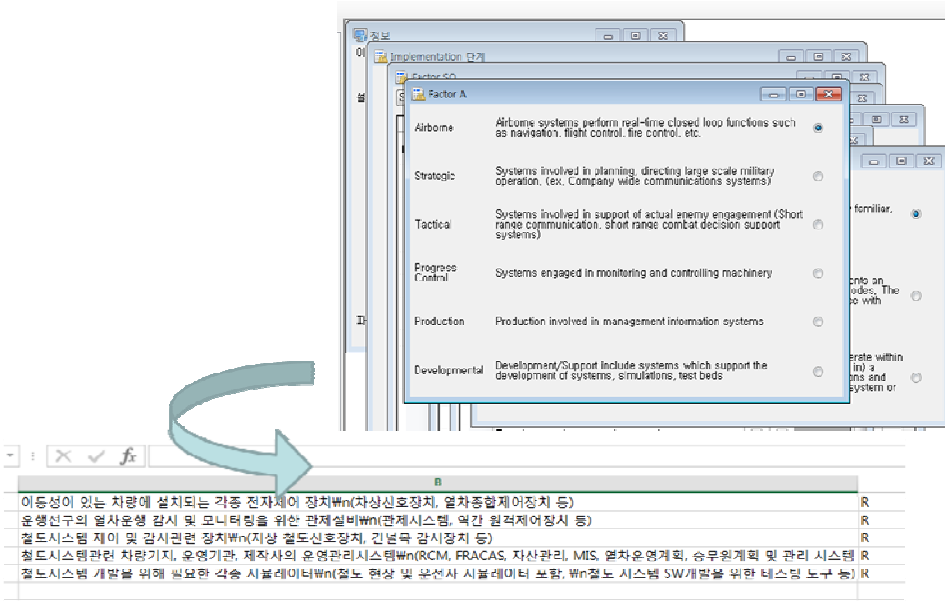

Fig. 2 Developed procedure of railway software reliability model

본 논문에서는 철도 소프트웨어 신뢰도 분석을 통한 초기예측을 통해 정량적 결함율을 얻고 나면, 테스팅 이후 과정에서의 실제 신뢰도 사후추정을 하기 위한 방향을 제시할 수 있도록 사용 가능한 철도 신뢰도 예측 모델을 개발하였으며, RL-TR-92-52 모델의 factor들을 철도분야에 적합하도록 수정 보완하였다. 수정 보완하여 제시한 factor들 중에서, Concept 단계에서의 'A' factor를 사례로 들면 그림 2와 같다. 즉, 기존 RL-TR-92-52 모델에서는 국방분야 특히 항공분야의 개발 소프트웨어에 적용한 내용을 철도분야에서 준수해야 하는 국제규격을 반영 및 수정하여 철도 소프트웨어 신뢰도 분석모델을 개발한 결과이다.

이와 같은 방법으로 Concept 단계뿐만 아니라, Requirement & Design 단계, Implementation 단계에 따라 결함밀도를 계산할 수 있도록 철도 소프트웨어 신뢰도 분석 모델을 개발하였으며, 특히 Implementation 단계에서는 소스코드 기반 척도에 대한 factor 값들은 해당되는 대상 시스템에 맞는 정적분석 도구를 이용하여 도출할 수 있다. 다만, 각각의 factor 값들을 도출할 때 적용되는 정량적인 기준들은 철도분야 규모 및 복잡성에 맞춰 재정립하여 모델에 보완 반영하였다. 또한, 정성적인 체크리스트를 사용하여 값들이 도출되는 factor들의 경우는 IEC 62279 및 EN 50128에서 제시하고 있는 요구사항을 분석하여 필요에 따라 추가, 삭제 그리고 수정할 수 있도록 설계하였다.

2.2.2 철도 소프트웨어 신뢰성 예측 평가지원 도구 설계

앞 절에서 언급한 방법으로 철도 소프트웨어 신뢰도 분석모델을 개발하였으며, 개발한 모델을 적용하여 실제 현장에서 적용할 수 있도록 지원도구로서 제작하기 위해 아래 그림과 같은 프로세스 구조를 갖도록 설계하였다.

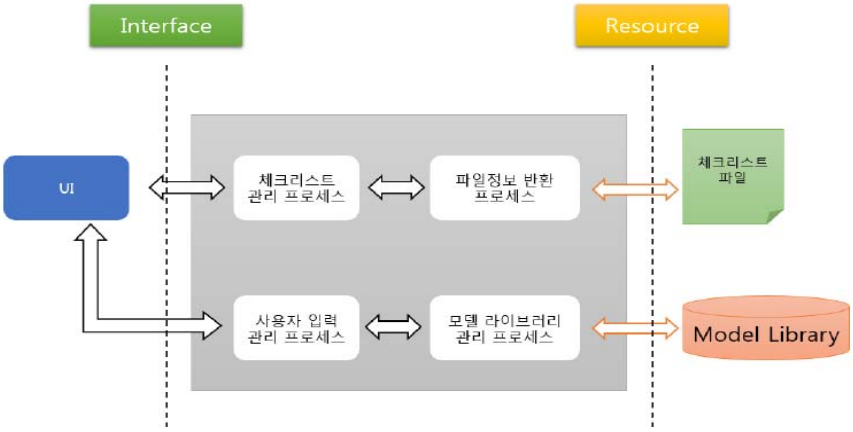

Fig. 3 Process architecture of railway software reliability prediction tool

Factor 입력 형식이 체크리스트일 경우에는 yes/no 항목의 선택 수를 통해 값이 계산되며, 입력 형식이 항목 선택인 경우에는 각 항목에 부여된 factor 값이 있기 때문에 사용자의 선택에 따라 부여된 값으로 변환하는 과정이 필요하다. 여기서 각 항목에 부여된 factor 값은 본 논문에서 개발한 철도 소프트웨어 신뢰도 분석모델을 지원도구 프로그램 Library로 적용하여 설계하였다. 현재 프로토타입 형태로 아래와 같이 화면 구현 중에 있으며 설계 결과로서 몇

가지 화면 구현 결과를 제시하였으며, 각각의 단계별로 결함밀도가 산출되어 도식화될 수 있도록 하였다.

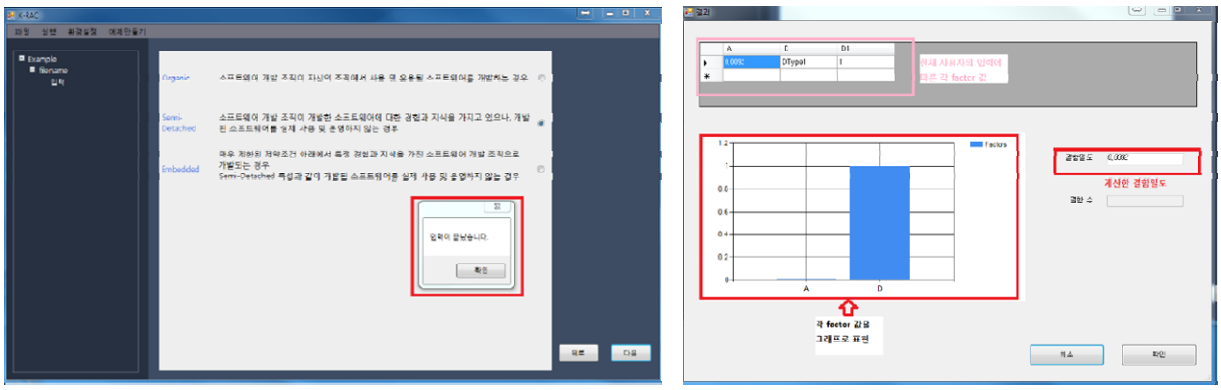

Fig. 4 Screen design results of railway software reliability prediction tool

3. 결 론

최근 컴퓨터 기술의 발달에 따라 철도시스템들이 컴퓨터 소프트웨어에의 의존성이 급격하게 증가하고 있으며, 이러한 기술발전에 따라 바이탈한 철도 소프트웨어에 높은 신뢰성과 안전성이 요구되고 있다. 이에 따라 철도시스템 소프트웨어관련 국제표준 및 국내 철도안전법 개정 이후 형식승인 기술기준에서도 소프트웨어의 테스트 및 검증을 의무사항으로 요구하고 있으나, 현재까지 RAM 분석 시 소프트웨어에 대한 분석은 거의 이루어지고 있지 않다는 문제가 있다. 이에 따라 실제 철도시스템 임베디드 소프트웨어 개발 제품에 국제 규격에서 요구하는 신뢰성 확보를 위한 절차 및 문서화 결과에 대한 검증뿐만 아니라, 소프트웨어 테스트를 통한 분석 및 확인에 대응하기 위한 전략 마련을 위한 구체적인 기술지원을 위해 본 논문에서 철도 소프트웨어 신뢰성 예측 도구를 제안하였다.

이에 따라 본 논문에서는 일반적으로 널리 알려져 있는 소프트웨어 신뢰성 예측평가 모델을 조사분석 하였으며, 그 중 예측 및 추정에 있어서 계량화가 가장 유동적인 RL-TR-92-52 모델을 선정하여 본 모델을 기반으로 하는 철도 소프트웨어 신뢰도 분석모델을 개발하였다. 개발한 철도 소프트웨어 신뢰도 분석 모델을 적용하여 각각의 단계별 도출되어야 할 factor 값들을 철도분야에 적합하도록 국제 규격 내에서의 요구사항을 반영하여 수정 보완하였다. 이와 같은 과정을 거쳐 철도 소프트웨어 정량적 신뢰성을 평가할 수 있도록 지원도구를 만들기 위해 개발한 모델을 적용하여 설계한 자세한 내용을 본론에 제시하였다. 마지막으로 현재까지 설계한 철도 소프트웨어 신뢰성 평가 지원도구에 대한 프로토타입 버전 결과 구현 화면을 보여주었다.

이와 같이 본 논문에서 개발하여 제안하는 철도시스템 소프트웨어 신뢰성 예측평가 지원도구는 개발 프로젝트를 관리하여 비용과 일정, 품질 및 안전성에 대한 고객의 요구사항을 만족시킬 수 있는 정량적인 기준으로서 널리 활용될 수 있다. 즉, 기본적으로 철도 운영기관 등의 수요처에서 철도시스템의 소프트웨어 품질 확인 및 검증을 위해서 활용될 수 있는 도구이며, 동시에 철도 관련 산업체들의 소프트웨어 개발과정에서도 해당 개발품의 단계별 결함율 측정

을 통한 단위 혹은 통합 테스트 전략수립 및 테스트 소요기간 단축 등에도 활용도가 충분히 높을 수 있다고 본다. 또한 철도분야 소프트웨어 임베디드 장치의 내재된 결함을 정량적으로 예측하여 평가를 가능하게 해주어, 철도 소프트웨어의 내재된 오류를 제로화 함으로써 운영지연과 발생 가능한 사고를 미연에 방지함으로써 안전성과 신뢰성 확보하는데 크게 기여할 수 있을 것으로 기대된다.

참고문헌

[1] EN 50128(2011), "Railway Applications – Communication, signaling and processing systems – Software for railway control and protection systems".

[2] IEC 62279(2015), "Railway Applications – Communication, signaling and processing systems – Software for railway control and protection systems".

[3] Railroad Safety Act(2015), *Law No. 13436,* Partial revision

[4] H.M. Choi (2002), Function-oriented evaluation model for embedded software, *software and application*, 32(12), pp. 1192-1204.

[5] RAC (2004), Introduction to software reliability, *RAC(Reliability Analysis Center)*, pp. 93-108.

[6] IEEE Std. 1633(2008), “IEEE Recommended Practice in Software Reliability”.

[7] McCall, J., Randell, W., Dunham, J., and Lauterbach, L. (1992), Software reliability measurement and testing guidebook, *Technical Report RL-TR-92-52*, *Rome Laboratory USAF*, pp. 201-203.