한국철도학회논문집
제9권 제5호 2006년 ▌ pp. 601-605

철도신호제어용 소프트웨어 신뢰도 모델링에 관한 연구

A Study on the Reliability of Software for Railway Signalling Systems

박영수† · 이재호*
Young-Soo Park · Jae-Ho Lee

Abstract

Reliability of the Railway signaling system which is safety critical is determined by reliability of hardware and software. Reliability of hardware is easily predicted and demonstrated through lots of different studies and environmental tests, while that of software is estimated by the iterative test outcomes so estimates of reliability will depend on the inputs. Combinations of inputs to and outputs from the software may be mostly combinatoric and therefore all the combinations could not be tested. As a result, it has been more important to calculate reliability by means of a simpler method. This paper identifies the reliability prediction equation applicable to reliability prediction for railway signaling system software, and performs the simulation of onboard equipment of automatic train control for high speed train to review reliability prediction and validity.

Keywords : Reliability Prediction Equation(신뢰도 예측방정식), 철도신호제어(Railway Signaling System), Modeling(모델링), Safety-Critical(안전필수), Automatic Train Control(자동열차제어)

1. 서 론

철도신호분야에서 전자, 통신기술의 발달과 더불어 소프트웨어를 이용한 시스템제어가 급증하고 있다. 신호제어시스템의 경우 과거에서는 기계식과 전기식 등의 순수 하드웨어 기반 제어방식을 사용하여, 고장이나 사고 발생시 원인을 명확히 발견 혹은 규명할 수가 있었다. 그러나 컴퓨터 제어를 이용한 시스템은 상당한 유연성(Flexibility)을 갖지만 고장이나 사고가 발생할 경우에 원인규명이 용이하지 않고 대규모 인명이나 재산의 손실을 초래하여 철도신호분야에서는 안전필수(Safety-Critical) 소프트웨어를 주로사용하고 있다. 그러나 안전필수 소프트웨어를 포함한 전체제어시스템의 정량적 신뢰도 평가에는 많은 어려움이 있다.

컴퓨터를 이용한 제어시스템의 신뢰성은 하드웨어와 소프트웨어의 신뢰도에 의해서 결정된다. 하드웨어의 신뢰도는 상대적으로 많은 연구와 환경적 시험에 의해 신뢰도 평가가 비교적 용이하지만 소프트웨어의 신뢰도는 반복실험 결과를 분석하여 산출해야 한다. 따라서 시스템 신뢰도를 사용개시 이전에 예측하고 입증하기 위해서는 소프트웨어의 신뢰도를 적합한 모델링을 통해 정량적으로 예측하는 것이 중요한 문제로 부각되고 있다. 따라서 본 논문에서는 철도신호제어시스템에 사용되는 소프트웨어의 신뢰도를 예측하기 위한 최적의 신뢰도 예측방정식(Reliability Prediction Equation)을 도출하여 이를 한국형고속철도 자동열차제어(ATC) 차상장치에 적용하여 신뢰도 예측을 실시하였다.

본 논문의 구성은 2.1 및 2.2에서는 소프트웨어 신뢰도의 일반사항을 기술하고, 2.3에서는 소프트웨어 신뢰성 모델링 형태에 대하여 분류하였다.

2.4에서는 선정된 모델과 시운전 데이터를 근거로 시뮬레이션을 실시하여 한국형고속철도 자동열차제어 차상장치의 소프트웨어 신뢰도를 예측하였다. 마지막으로 3장에서는 결론을 기술한다.

2. 본 론

2.1 개요

소프트웨어 신뢰성은 소프트웨어의 품질을 결정하는 중요한 척도중의 하나이다. 소프트웨어가 광범위하게 사용됨

† 책임저자 : 정회원, 건설교통부, 공학박사
E-mail : youngsoo@moct.go.kr
TEL : (02)2110-8255
* 한국철도기술연구원, 전기신호연구본부, 공학박사

에 따라 소프트웨어의 결함은 시간적, 물질적 손실은 물론 인명의 손실과 대규모 재산피해와 같은 치명적 결과를 가져올 수 있는 기능을 수행하게 되었다. 이러한 환경적 변화에 대응하기 위해 소프트웨어의 결함을 제거하여 고품질의 소프트웨어 제작을 위한 연구가 진행되고 있다.

정량적인 소프트웨어 품질 측정의 한 부류로서 소프트웨어의 복잡도(Complexity) 측정이 있다. 소프트웨어 복잡도 측정의 주된 관심은 프로그램의 크기, 제어흐름(Control Flow), 자료 흐름(Data Flow) 등을 바탕으로 한 프로그램의 정적 구조 분석으로써, 소프트웨어의 사용자관점을 충분히 반영하지 못하는 단점이 있다. 이에 비하여 소프트웨어 신뢰성 모델(Software Reliability Model)을 이용한 소프트웨어 품질 측정은 소프트웨어 개발, 시험 과정에서 발생하는 소프트웨어 고장(Software Failure)을 근거로 통계적 추정을 실시하므로 복잡도 측정에 의한 품질 측정보다 사용자의 관점을 잘 반영한다. 또한, 개발자의 관점에 있어서도 소프트웨어 신뢰도 모델을 이용한 품질 측정은 동적인 요인에 기반한 품질 측정치를 제공한다. 그러므로 이러한 특성은 소프트웨어 개발 과정에서 소프트웨어의 상태를 파악하고, 품질 목표치를 설정하며, 목표치에 도달하기 위한 계획을 수립하는데 도움을 준다. 따라서 소프트웨어 신뢰성은 소프트웨어의 품질을 결정하는 가장 중요한 척도중의 하나이다.

대부분의 소프트웨어 신뢰도 모델들은 동작 프로파일에 기반을 두고 소프트웨어의 동작상태를 관찰해왔다[1,2]. 이런 모델들은 주로 소프트웨어 개발완료 이후 단계에서 소프트웨어가 신뢰도 요구조건을 만족하는지에 대한 여부를 결정하기 위해서 주로 적용되었다. 하지만, 이러한 통계적 수단을 사용하는 모델들의 단점은 테스트 데이터의 불충분과 소프트웨어의 업그레이드에 대한 적용이 용이하지 않다는 것이다.

소프트웨어 개발단계에서는 주로 프로그램의 오류를 중심으로 프로그래밍과 테스팅(Testing)을 수행하여 품질을 관리하고 있으며, 소프트웨어의 규모가 커지고 복잡해짐에 따라 소프트웨어 신뢰도공학(SRE)에서는 모델링을 통한 신뢰성 추정이 활발히 연구되고 있다. 본 논문에서 검토된 모델들은, 각 모델에 대한 가정, 실행을 위한 데이터 요구사항, 형태와 결과의 예측들로 구성된다. 이러한, 모델선정을 통해 얻어지는 예측 값들은 MLE(Maximum Likelihood Estimation)에 근거하며, 본 논문에서는 고장데이터(Failure Data)의 분포형태를 지수(Exponential)구조로 가정한다.

소프트웨어 신뢰성 모델의 개발을 위해 Musa와 Okumoto[3]가 제안한 모델 분류체계를 바탕으로 하면, $M(t)$는 시간구간 t에서의 고장에 대한 임의의 수이고 평균값함수 $\mu(t)=E[(t)]$로 표현된다.

$$\mu(t)=\alpha F_\alpha(t) \qquad (1)$$
$$\lambda(t)=\mu'(t)=\alpha f_\alpha(t)$$

여기서, $R(t)$:신뢰도함수, $\mu(t)$:평균값함수, $\lambda(t)$:고장강도함수, α:상수, $F_\alpha(t)$:각각의 고장 α의 시간에 대한 고장누적분포함수, $f_\alpha(t)$:각각의 고장 α의 시간에 대한 고장확률밀도함수이다.

모델을 간소화하기 위해 소프트웨어의 데이터수집 시점에서 소프트웨어에 존재하는 고장의 수를 N, 그리고, 하나의 고장이 검출되어지면 그것은 즉시 제거되는 것으로 가정하면 다음과 같이 정리할 수 있다.

$$\lambda(t)=N\cdot f_\alpha(t) \qquad (2)$$
$$\mu(t)=N\cdot F_\alpha(t)$$

2.2 모델의 제한과 이슈

수집된 데이터에 대한 모델적용에 있어서 다음과 같은 분석형태에 대한 제한사항을 검토한다.

- 주어진 모델에 대한 가정을 명확히 해야 한다. 만약 선택된 모델이 사건발생시간의 차이를 통한 추정을 전제로 하는 경우에, 수집된 데이터의 시간간격이 모두 같은 크기라고 가정되면, 해당 모델은 주어진 데이터의 유형에 맞지 않으므로 적용이 적합하지 않다.
- 추정의 한계를 명확히 해야 한다. 만약 소프트웨어의 테스트 환경이 데이터가 수집된 환경과 일치하지 않는다면 예측된 결과의 신뢰수준은 저하된다.

2.3 소프트웨어 신뢰도 측정절차 및 모델링 분석

신뢰도 모델을 통한 신뢰도추정의 절차는 그림 1과 같이

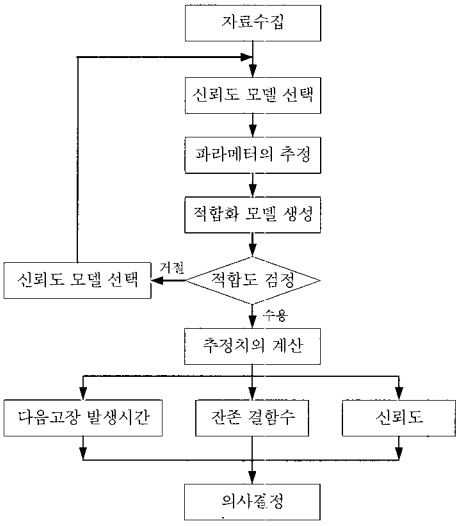

그림 1. 소프트웨어 신뢰도를 측정하는 절차

먼저 고장자료를 수집하여 데이터 특성에 적합한 신뢰도 모델을 선택한다. 모델이 선택되면 모델에 필요한 파라메타를 추정하여 이를 모델에 대입한 후 모델의 적합성을 확인한다. 다음으로는 실제고장자료로부터 얻어진 모델의 정확성을 평가하기 위하여 적합도 검증(Verification)을 실시한다. 검증의 결과를 통해 모델의 유도추정치를 획득하고 마지막으로 유도추정치를 바탕으로 의사결정을 수행하는 단계로 구성된다.

2.3.1 신뢰도 모델링분석

소프트웨어 신뢰성 모델의 분석이 올바르게 수행되고, 적용분야에 대한 고장특성을 고려한 모델간의 연관관계가 분석되면, 신뢰성 모델을 선택하는 방법의 문제가 대두된다. 소프트웨어의 신뢰도를 정량적으로 추정하여 평가하기 위해 다음의 3가지유형의 모델이 발표되었다.

- Weibull and Gamma Failure Time Class of Model
  -S-shaped reliability growth model
- Infinite Failure Category Model
  -Geometric Model
  -Musa-Okumoto logarithmic Poisson
- Exponential Failure Time Class of Models
  -Jelinski-Moranda de-eutrophication model[4]
  -Non-homogeneous Possion Process(NHPP) model
  -Schneidewind's model
  -Musa's basic execution time model

위와 같은 3가지 신뢰도 모델유형 중 전자부품의 고장특성인 지수고장을 따르는 모델인 Schneidewind's model을 이용하여 한국형고속철도 자동열차제어 차상장치의 소프트웨어 신뢰도를 예측하였다. Schneidewind's model은 미국 우주 왕복선의 기내시스템 소프트웨어의 신뢰성을 예측하기 위해 사용되었다.

Schneidewind's Model은 신뢰도 예측구간에 따라 다음의 3가지 모델로 나뉘게 된다.

2.3.2 Schneidewind's model의 3가지 유형

본 논문에서는 신뢰도를 예측하기 위한 모델로 Schneidewind 모델을 선택하였다. Schneidewind 모델의 경우 고장밀도함수 $\lambda(t)$와 평균고장함수 $m(t)$는 다음과 같다.

$$m(t)=\int_0^t \lambda(s)ds \tag{3}$$

여기서, $\lambda(t)$와 $m(t)$는 다음과 같다.

$$\begin{aligned}\lambda(t)&=\alpha e^{-\beta t}\\ m(t)&=(\alpha/\beta)[1-e^{-\beta t}]\end{aligned} \tag{4}$$

Schneidewind 모델을 적용하기 전 먼저 두개의 파라메터 α와 β를 추정해야 한다. 여기서 α는 $t=0$에서의 초기 고장률이고, β는 상수이다. 이 두 파라미터가 정해지게 되면 4개의 테스트 자원을 얻을 수 있다.

① $[0,t]$시간동안 나타나는 고장발생의 수 예측
$F(t)=(\alpha/\beta)[1-e^{-\beta t}]$

② 위의 특징을 사용해 $[t_1,t_2]$시간 구간 내에서의 고장발생의 수를 예측
$F(t_1,t_2)=(\alpha/\beta)[1-e^{-\beta t}]-X_{0,t_1}$
X_{0,t_1} : $[0,t_1]$에서의 고장발생의 수

③ 소프트웨어의 life($t=\infty$)동안 발생할 최대 실패의 수 예측
$F(\infty)=\alpha/\beta$

④ ①,②,③을 이용하여 t에서 시스템에 남아 있을 수 있는 최대 고장발생요인의 수 예측
$R(t)=(\alpha/\beta)-X_{0,t_1}$

Schneidewind 모델은 다시 3개의 모델로 나뉘어 진다.

• 모델 1

전체 시간 구간을 n이라고 했을 때, 시간 구간을 동일한 간격으로 나누게 되고 동일한 가중치를 사용하게 된다. 첫 번째 모델을 사용한 경우 아래 식을 이용하여 α, β을 추정하게 된다.

$$\frac{1}{e^{\hat{\beta}}-1}-\frac{n}{e^{\hat{\beta}n}-1}=\sum_{k=0}^{n-1}k\frac{f_{k+1}}{F_n}$$

$$\hat{\alpha}=\frac{\hat{\beta}F_n}{1-e^{-\hat{\beta}n}},$$

$F_n=\sum_{i=1}^{n}f_i$, f_i : 실제 나타나는 고장의 수

• 모델 2

전체 시간구간을 n이라고 했을 때$[1,s-1]$까지 구간은 무시하고, $[s,n]$까지 구간만을 이용해 α와 β을 추정하게 된다. 이 때 α와 β을 추정하기 위한 수식을 다음과 같다.

$$\frac{1}{e^{\hat{\beta}}-1}-\frac{n-s+1}{e^{\hat{\beta}(n-s+1)}-1}=\sum_{k=0}^{n-s}k\frac{f_{k+s}}{F_{s,n}}$$

$$\hat{\alpha}=\frac{\hat{\beta}F_{s,n}}{1-e^{(-\hat{\beta}(n-s+1))}},$$

$$F_{s,n}=\sum_{i=s}^{n}f_i$$

• 모델 3

모델3의 경우 모델1과 모델2의 복합 형태로 $[1,s-1]$까지 구간은 누적시켜 첫 번째 발생고장의 데이터처럼 사용하게 되고, $[s,n]$구간은 각각 독립적인 실패의 수로 사용되게 된다. 이 때 α와 β을 추정하기 위한 수식은 다음과 같다.

$$\frac{(s-1)F_{s-1}}{e^{\hat{\beta}(s-1)}-1}+\frac{F_{s,n}}{e^{\hat{\beta}}-1}-\frac{nF_n}{e^{\hat{\beta}n}-1}=\sum_{k=0}^{n-s}(s+k-1)f_{s+k}$$

$$\hat{\alpha}=\frac{\hat{\beta}F_n}{1-e^{-\hat{\beta}n}}$$

2.4 신뢰도 예측 시뮬레이션 및 결과 고찰

2.4.1 입력데이터

한국형고속철도 자동열차제어 차상장치의 소프트웨어 신뢰도 분석을 위해 사용된 데이터는 현재 고속철도기술개발사업에서 수행중인 시운전 기간에서 소프트웨어 고장발생의 수를 체크 하여 24시간 단위로 누적된 결함의 수를 입력데이터로 사용하였다. 2004년 11월 1일부터 2005년 10월 19일까지 총 116회 동안 장치를 가동하여 소프트웨어를 실행하였으며 이 중 표 1과 같이 4회의 소프트웨어 관련 장애가 발견되었다.

2.4.2 모델의 신뢰성 테스트

본 논문에서는 소프트웨어 신뢰도모델링 방식 중 전자부품의 고장특성인 지수고장특성의 모델링에 해당하는 Schneidewind 모델 식 (4)를 적용하여 고장정보를 바탕으로 자동열차제어 차상장치 소프트웨어의 신뢰성 검사를 수행하였다. 먼저 그림 1의 모델검정에서와 같이 선택된 Schneidewind 모델이 적용대상과 부합하는지를 검증하기 위해 s값에 따른 추정치를 비교해야 한다.

Schneidewind 모델 2의 경우 s=1이면 모델 1과 동일한 모델이 된다. 모델 3에서의 최적의 s값은 모델 2의 s값보다 1 큰 값이 일반적이다. 따라서, 표 2에서와 같이 동일한 $\hat{\alpha}$와 $\hat{\beta}$에 대한 모델들의 추정치가 동일함에 따라 Schneidewind 모델의 적용 적합성을 검증하였다.

고장정보의 수집기간에 따라 3가지 모델로 세분화 되는 Shneidewind모델은 자동열차제어 차상장치 소프트웨어의 수집된 고장정보에 적합한 세부 모델을 선택해야 한다.

모델2의 경우 추정시간을 줄여줄 수 있고 s값을 추정하는 명확한 근거가 제시되어 있는 장점이 있어 모델2를 사용하여 에러를 추정하고자 하였으나, 모델2의 경우 초기에 발생하는 에러를 무시하게 되는데 실험데이터의 특성이 처음 1-5회 사이에 에러 데이터의 대부분이 존재하기 때문에 모델2를 사용하게 되면 에러 데이터의 예측에 영향을 미치게 되는 대부분의 에러 데이터를 무시한 후 각 파라메터를 추정하게 되기 때문에 예측에서 많은 오차 성분이 포함된다. 따라서 수집된 고장정보와 같이 초기에 고장발생이 분포된 경우에는 모델 2를 사용할 수 없다. 따라서 현재와 같은 실험데이터의 경우 모델 1 또는 모델 3을 선택해야 한다. Schineidewind 모델 3은 구간별로 가중치를 두어 신뢰도를 예측하는 반면 Schineidewind 모델 1은 모든 구간에 동일한 가중치를 두고 신뢰도를 예측한다. 즉, 이와같이 고장이 일부구간에 집중된 경우에는 Schineidewind 모델3을 이용하여 신뢰도를 보다 정확하게 예측할 수 있다.

따라서 본 논문에서는 Schineidewind 모델3을 적용하여 한국형고속철도 자동열차제어 차상장치의 소프트웨어 신뢰도를 예측한다.

2.4.3 신뢰도 예측 시뮬레이션

입력데이터에 대한 평균, 분산, 표준편차 값을 다음 표 3과 같다.

이렇게 얻어진 실측데이터를 근거로 하여 Maximum Likelihood Estimation 방법을 이용하여 파라메터 $\hat{\alpha}$, $\hat{\beta}$를

표 1. ATC차상장치 시운전 중 소프트웨어관련 장애이력

가동일	운행 횟수(회)	장애 건수(건)	장애내역
2004.11.03	1	2	데이터 입력 오류
2004.11.08	1	1	통신프로세스 오류
2004.12.14	1	1	증속대비 프로그램 오류

표 2. 모델1, 모델2(s=1), 모델3(s=2)

	$\hat{\alpha}$	$\hat{\beta}$	시스템내에 잔존 가능한 에러 수(예측)
모델1	0.6974	0.1744	6.584e-009
모델2	0.6974	0.1744	6.584e-009
모델3	0.6974	0.1744	6.584e-009

표 3. ATC 차상장치 소프트웨어 고장 데이터

입력개수	평균(mean)	분산(var)	표준편차(std)
116	0.0345	0.0510	0.2258

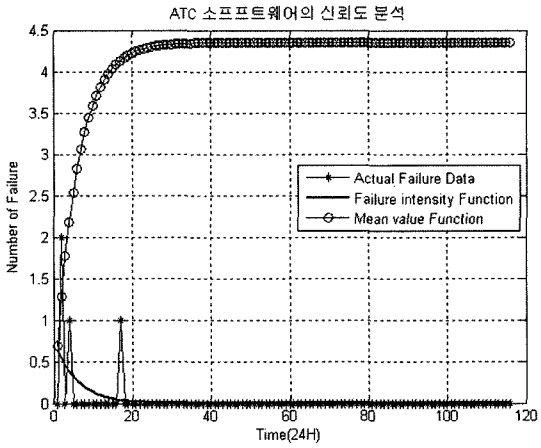

그림 2. ATC 차상 장치의 소프트웨어 신뢰도 분석을 위한 $\lambda(t)$, $\mu(t)$

표 4. 모델3을 이용한 신뢰도 예측

	F(1, 116)	F(117, ∞)
장치가동시 얻은 결함 수	4	·
Schneidewind 모델 3	4.000006989	1.4705e-006
신뢰도	99.99985%	

추정하게 되면 다음과 같은 추정치를 얻게 된다.

$$\hat{\alpha}=0.5065,\ \hat{\beta}=0.1266,\ s=15 \tag{5}$$

얻어진 파라메터를 Schneidewind 모델 3에 적용하여 $F(117\sim\infty)$에서의 고장을 예측하면, 그림 2와 같은 추정 결과를 얻을 수 있다.

신뢰도함수 $R(t)=1-F(t)$이므로 앞으로 예측될 $F(t\sim\infty)$ 구간에서의 신뢰도는 $1-F(t,\infty)$가 된다. 따라서, 예측된 $F(t,\infty)$의 추정치를 이용하여 신뢰도를 산출하면 표 4와 같이 신뢰도는 99.99985%로 예측할 수 있다.

3. 결 론

안전필수시스템인 철도신호제어시스템의 신뢰성은 현재까지 주로 하드웨어에 집중하여 연구가 수행되어왔으나 컴퓨터기반 제어기의 활용증가로 인해 소프트웨어의 신뢰도 평가에 대한 연구가 요구되었다.

따라서 본 논문에서는 철도신호제어시스템에 적용되는 소프트웨어의 신뢰도를 예측하기 위한 기초적 연구로써 여러 가지 신뢰도 모델을 제시하였고, 그 중 전자부품의 고장특성인 지수고장모델을 분석하였다. 분석한 지수모델은 미국 우주왕복선의 기내시스템 소프트웨어의 신뢰도를 예측하는데 사용되었던 Schneidewind 모델로, 한국형고속철도 자동열차제어 차상장치의 소프트웨어 신뢰도 예측을 위해 선택하였다.

타당성이 검증된 Schneidwind 모델 3을 이용하여 2004년 9월에서 2005년도 10월에 이루어진 116회 시운전데이터를 이용하여 한국형고속철도 자동열차제어 차상장치 소프트웨어의 신뢰도를 예측한 결과 신뢰도 99.99985%를 얻을 수 있었다.

향후에는 이러한 방식의 타당성 검증과 효율화 방안에 대한 연구를 지속하여 철도신호제어시스템의 신뢰성예측에 적용될 수 있도록 연구를 진행할 것이다.

참 고 문 헌

1. Cheung R. C., "A User-Oriented Software Reliability Model", IEEE Transactions On Software Engineering, 6(2), pp.118-125, March 1980.
2. Farr W., "Software Reliability Modeling Survey", In M.R. Lyu editor, Handbook of Software Reliability Engineering, McGraw-Hill Publishing Company and IEEE Computer Society Press, New York, pp.71-117, 1996.
3. Musa, J.D., Okumoto, K, "A Logarithmic Poisson Execution Time Model for Software Reliability Measurement", Proceedings Seventh International Conference on Software Engineering, Orlando, Florida, pp. 230-238.
4. Moranda, P.L., and Jelinski, Z., Final Report on Software Reliability Study, McDonnel Douglass Astronautic Company, MADC Report Number 63921, 1972.