2011년도 대한전기학회 하계학술대회 논문집 2011. 7. 20 - 22

철도신호시스템 소프트웨어 검증을 위한 경계값 분석도구의 구현

조현정, 황종규, 백종현, 이재호
한국철도기술연구원

Implementation of Boundary Value Analysis Tool for Software Verification in Railway Signaling Systems

Hyunjeong Jo, Jonggyu Hwang, Jonghyen Baek, Jaeho Lee
Korea Railroad Research Institute

Abstract - The railway signaling system is being converted to the computer system from the existing mechanical device, and the dependency on software is being increased rapidly. Though the size and degree of complexity of software for railway signaling system are slower than the development speed of hardware, it is expected that the size will be grown bigger gradually and the degree of complexity will be increased also. Accordingly, the validation of reliability and safety of embedded software for train control system was started to become influential as the important issue. In this paper, we presented boundary value analysis tool for railway signaling system software, and presented its result of implementation.

1. 서 론

철도신호시스템 소프트웨어 안전성 요구사항들이 최근 들어 IEC 61508과 IEC 62279에 의해 국제표준화 되었고[1][2], 또한 국내에서도 철도안전법이 제정되어 이러한 열차제어시스템 관련 국제표준에서 요구하는 각종 소프트웨어 테스팅 및 검증활동을 요구하는 분위기가 조성되고 있다. 하지만 아직까지 소프트웨어 검증은 개발과정에 대한 문서에 주로 의존하고 있으며, 극히 일부만 테스팅에 의한 정량적인 분석이 이루어지고 있다[3][4]. 또한, 국내에서의 국제표준에 따른 열차제어시스템 소프트웨어 테스팅 및 검증을 위한 기준이나 이에 부합하는 기술에 대한 연구는 이제 막 시작하는 초기단계에 불과한 실정이다.

따라서 철도신호시스템 소프트웨어관련 국제표준에서 요구하고 있는 안전성 활동에 대한 문서 검증뿐만 아니라 소프트웨어 테스팅을 통한 분석 및 평가에 대응하기 위한 구체적인 기술 개발이 매우 필요한 상황이다. 특히, 국제표준에서 요구하고 있는 철도신호시스템 소프트웨어 검증 항목 중 하나인 경계값 분석 테스팅은 관련 국제 표준에서 'HR : Highly Recommend' 조건으로 규정되어 있다[1][2]. 이와 같은 철도신호시스템 소프트웨어의 경계값 분석 테스팅은 문서의 검증이나 정성적인 검증방법 보다는 자동화된 도구를 통해서 정확한 분석이 가능할 것이나 국내외에 아직 개발된 적이 없다. 따라서 본 논문에서는 이러한 철도신호시스템 소프트웨어의 검증을 위해서 경계값 분석도구를 설계 및 개발하였다.

2. 본 론

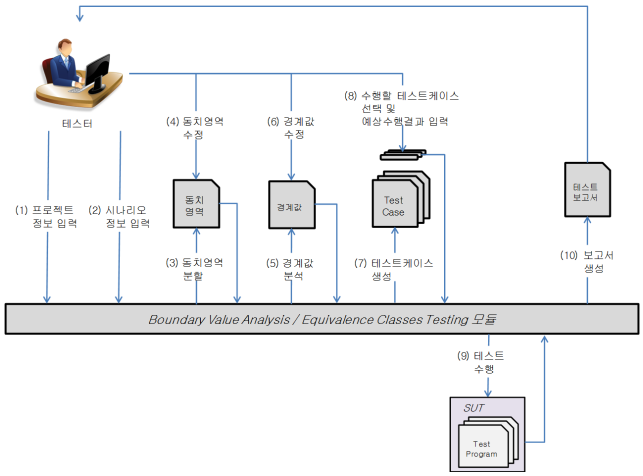
2.1 경계값 분석 도구의 구조 및 설계

경계값 분석도구의 동작 시나리오는 프로젝트 정보 입력, 시나리오 정보 입력, 경계값 분석, 경계값 수정, 테스트케이스 생성, 테스트케이스 예상 수행결과 입력, 테스트 수행, 테스트 보고서 생성 순으로 진행된다. 테스터는 동치영역 분할 후 선택에 의해 영역의 대표값을 이용하여 테스트케이스를 생성할 수도 있고, 추가적으로 경계값 분석 단계를 거쳐 선정된 경계값을 이용해 테스트케이스를 생성할 수도 있다. 경계값 분석 자동화 도구는 시나리오 정보 입력과 테스트 기대 결과값 입력을 제외한 모든 과정을 자동으로 수행하되, 자동 선정된 경계값에 대해서 테스터가 별도로 수정할 수 있는 것이 주요 동작 시나리오의 내용이다. 다음 표 1은 경계값 분석 도구의 기능 리스트를 정리한 것이며, 그림 1은 테스트케이스 입력값 생성 방법 별로 수행하는 동작 시나리오에 대한 그림과 순서에 대한 설명이다.

(1) 프로젝트 정보 입력 : 테스터는 수행할 테스트 프로젝트의 정보를 입력한다.
(2) 시나리오 정보 입력 : 테스터는 테스트할 시나리오 정보를 입력한다.
(3) 경계값 분석 : 경계값 분석도구는 동치영역을 분석하여 경계값을 생성한다.
(4) 경계값 수정 : 테스터는 자동 생성된 경계값의 내용을 확인하고 수정한다.
(5) 테스트케이스 생성 : 경계값 분석 테스팅 도구는 시나리오와 경계값 정보를 이용하여 테스트케이스를 자동 생성한다.
(6) 수행할 테스트케이스 선택 및 예상수행결과 입력 : 테스터는 수행할 테스트케이스를 선택하고 예상되는 수행 결과값을 입력한다.
(7) 테스트케이스 수행 : 경계값 분석 테스팅 도구는 시험대상체계를 제어하여 테스트를 수행한다.
(8) 테스트보고서 생성 : 경계값 분석 도구는 테스트 수행 결과와 테스터가 입력한 예상수행결과값 비교 등의 분석과정을 거쳐 보고서를 생성한다.

<표 1> 경계값 분석 자동화 도구 기능 리스트

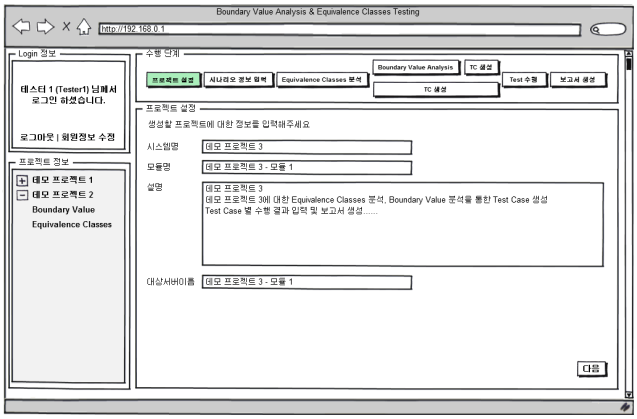
기 능	설 명
경계값 자동 생성	- 분기조건의 경계값 목록을 생성한다. - 테스터는 이를 편집할 수 있으며 최종 정의된 경계값을 저장소에 저장한다.
테스트 케이스 생성	- 생성 및 수정 완료된 경계값을 기준으로 테스트케이스를 자동으로 생성한다. - 생성된 테스트케이스의 기대 결과값을 테스터로부터 입력 받고 이를 저장소에 저장한다.
테스트 수행	- 디버거를 활용하여 대상체계에 테스트케이스 정보를 입력하여 테스트를 수행한다. - 테스트 수행후 출력값을 저장소에 저장한다.
테스트 수행 결과 판단	- 테스트 출력값과 사용자가 기 입력한 기대 결과값을 비교하여 프로그램이 올바르게 수행되었는지를 검증한다. - 검증 결과를 저장소에 저장한다.
테스트 수행 결과 보고	- 테스트 수행 결과 판단 내용을 바탕으로 보고서를 생성한다.



<그림 1> 경계값을 이용한 테스트 수행 시나리오

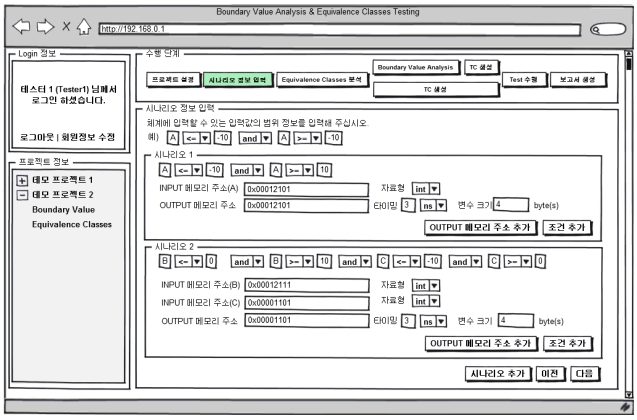
2.2 경계값 분석 도구 구현 결과

다음 그림 2와 같이 프로젝트 설정 입력 화면은 테스터가 새로운 테스트 프로젝트를 생성할 때 표시된다. 테스터는 시험할 시스템과 모듈의 이름, 테스트의 설명 및 시험을 수행할 대상 서버 이름을 입력 한다.



〈그림 2〉 프로젝트 설정 입력 화면 구성

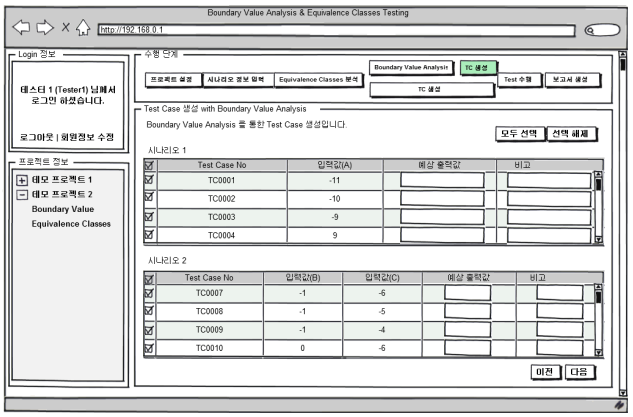
그림 3의 시나리오 정보 입력 화면에서는 시나리오별로 분기 조건, 입/출력 메모리 정보등을 입력할 수 있는 환경을 제공한다. 다수의 시나리오를 입력할 경우 '시나리오 추가' 버튼을 클릭하면 새로운 시나리오를 입력할 수 있는 폼이 표시된다. 하나의 시나리오에는 다수의 조건과 출력 메모리 주소가 존재하며, 입력된 조건의 변수마다 입력 메모리 주소를 입력할 수 있는 폼이 생성된다. 시나리오의 조건을 추가하거나 다수의 출력 메모리를 검사할 필요가 있을 경우에는 각각 '조건 추가', 'OUTPUT 메모리 주소 추가' 버튼을 통해 해당 사항을 입력할 수 있는 환경을 추가할 수 있다.



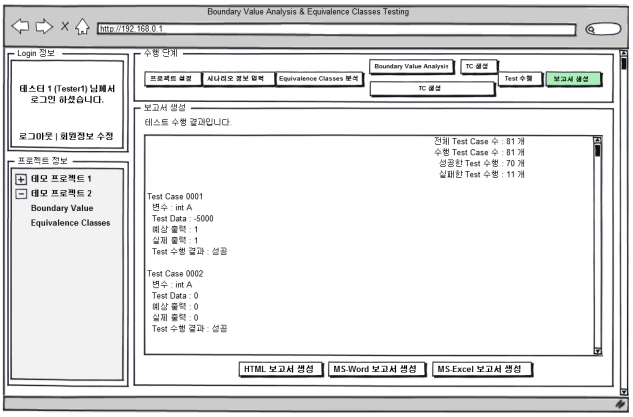
〈그림 3〉 시나리오 정보 입력화면

기 입력된 시나리오 정보를 바탕으로 자동 생성된 경계값을 출력한다. 단, 한 분기 내 다수의 입력 변수가 존재할 경우 각 변수별로 별도의 경계값 표시란을 출력한다. 테스터가 새로운 값을 추가하기를 원한다면 '경계값 추가' 버튼을 클릭하여 새롭게 표시된 창에서 값을 입력하여 추가할 수 있으며, 자동 분석된 경계값을 수정하기를 원한다면 현재 경계값이 출력된 입력창의 값을 수정하고 '저장' 버튼을 클릭하면 된다. 또한, 기 정의된 경계값 정보를 바탕으로 생성된 테스트케이스 목록을 그림 4에서와 같이 출력한다. 테스터는 테스트케이스 수행후 기대되는 예상 출력값과 비고 사항을 각 테스트케이스의 '예상 출력값', '비고' 입력란에 입력할 수 있으며, 특정 테스트케이스만 수행하고 싶을 경우 원하는 테스트케이스의 체크박스를 지정하여 선택할 수 있다.

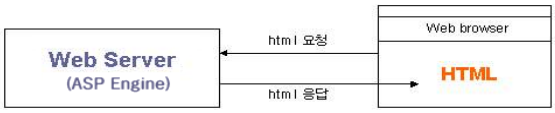
테스트의 수행 시, 수행엔진은 테스트 수행을 마무리 할 때까지 해당 화면을 출력한다. 마지막으로 수행된 테스트의 요약 결과와 각 테스트케이스별 결과를 출력하는 화면은 그림 5와 같다. 테스터는 하단의 'HTML 보고서 생성', 'MS-Word 보고서 생성', 'MS-Excel 보고서 생성' 버튼을 클릭하여 각 형식별로 보고서를 생성할 수 있다. 이러한 경계값 분석 자동화 도구의 화면 구현방식으로서 그림 6과 같이 사용자 인터페이스는 ASP 기반의 웹페이지 형태로 구현하였다. 테스터는 웹 브라우저를 통해 도구에 접근하여 대화식으로 테스트를 준비하고 진행할 수 있다.



〈그림 4〉 경계값을 이용한 테스트케이스 생성 및 예상출력값 입력화면



〈그림 5〉 도구 수행결과 보고서 생성 화면



〈그림 6〉 ASP 수행 개념

3. 결 론

최근 들어 컴퓨터 기술의 발달에 따라 철도신호시스템이 컴퓨터 소프트웨어에의 의존성이 급격하게 증가하고 있으며, 이러한 기술발전에 따라 바이탈한 철도신호시스템 소프트웨어에 높은 신뢰성과 안전성이 요구되고 있다. 이에 따라 철도신호시스템 소프트웨어관련 국제표준에서 의무사항으로 요구하고 소프트웨어 검증 항목 중 하나인 경계값 분석 테스팅에 대한 정확한 검증을 위해 본 논문에서 국내외 처음으로 개발한 자동화 도구를 제시하였다. 먼저 개발한 철도신호시스템 전용 소프트웨어 경계값 분석 동작 시나리오에 대해 설명하였고, 그 구현 결과를 구체적으로 보여주었다.

이러한 철도신호시스템 소프트웨어 경계값 분석 자동화도구는 기본적으로 소프트웨어 검증 단계에서 활용될 도구이며, 동시에 소프트웨어 개발과정에서도 충분히 활용도가 높을 수 있다고 본다. 본 도구를 소프트웨어 검증 및 개발 단계에서 널리 이용한다면, 이를 통해 바이탈한 철도신호시스템 소프트웨어의 오류를 미연에 방지하여 안전성과 신뢰성을 확보하는데 크게 기여할 수 있을 것이다.

[참 고 문 헌]

[1] IEC 61508, "Railway Applications - The specification and demonstration of RAMS", 1998.

[2] IEC 62279, "Railway Applications - Software for railway control and protection systems", 2002.

[3] M. Fewstar, D. Graham, "Software Testing Automation: Effective use of test execution tools", ACM Press, Addison Wesley, 1999.

[4] J.D. Lawrence, "Software qualification in safety applications", Reliability Engineering & System Safety, Vol. 70, No. 2., pp. 167-184, 2000.