위험 분석과 테스팅 프레임워크 표준의 연계: 위험 분석을 통해 식별된 위험 요인 기반의 테스팅 방안

서준호

한국정보통신기술협회

jhseo@tta.or.kr

Integration of Risk Analysis and Standards for Testing Framework: A Testing method based on causal factors identified through Risk Analysis

Junho Seo

Telecommunications Technology Association

요 약

본 논문은 위험 분석과 CPS 안전·신뢰성 프로필 주도 테스팅 프레임워크 표준을 연계한 테스팅 방안을 제안한다. 다양한 위험 분석 기법에 비해 위험 분석의 결과인 위험 요인은 구체적인 형태나 통일성이 없어 위험 요인을 활용해 체계적인 테스팅을 수행하기 어렵다. 이러한 위험 요인에 대해 필수 속성을 정의하고, 테스트 환경 구성 및 테스팅 수행 방법을 제공하는 CPS 안전·신뢰성 프로필 주도 테스팅 프레임워크를 연계하면 테스터는 위험 요인을 활용하여 테스트 항목을 쉽고 빠르게 도출하고 일부 테스트 절차를 자동화함으로써 효율적이고 체계적인 테스팅을 수행할 수 있다.

Ⅰ. 서 론

위험 분석은 사고를 유발할 가능성이 있는 시스템의 상태나 조건들을 식별하고 원인을 분석하는 일련의 활동을 말한다[1]. 위험 분석 기법에는 FTA(Fault Tree Analysis), FMEA(Failure Mode and Effect Analysis), 등과 같이 하나 이상의 오작동으로 시스템의 실패나 위험을 초래한다는 전제를 기반으로 하는 순차적 사고 모델 기반의 분석 기법과 STPA (System- Theoretic Process Analysis)와 같이 시스템 내의 컴포넌트간의 유기적인 상호관계를 고려한 시스템 이론에 기반한 사고 분석 모델 기반의 분석 기법이 있다. 각각의 위험 분석 기법은 잠재된 위험을 식별한다는 공통점이 있지만, 위험 분석을 통해 식별되는 위험 요인의 형태가 구체화되지 않고 위험 분석 기법에 따라 주관적인 요소를 반영할 수 있어 위험 요인의 통일성이 없기 때문에 위험 요인을 활용한 체계적이고 효과적인 테스팅 수행이 어렵다.

“사이버-물리 시스템(CPS)의 안전·신뢰성 확보 지침 - 제5부: CPS 안전·신뢰성 프로필 주도 테스팅 프레임워크” 표준에서는 ‘위험요소-위험대책-검증방안’으로 구성된 CPS 안전·신뢰성 프로필을 활용해 효율적이고 효과적으로 테스팅을 수행할 수 있는 프레임워크가 제안되었다[2]. 이 테스팅 프레임워크에서는 CPS의 안전·신뢰성 사고의 원인이 되는 결함요인을 활용해 테스팅할 수 있도록 테스트 환경 및 테스팅을 위한 구성요소, 테스팅 과정 등을 제공한다.

본 논문에서는 위험 분석을 통해 식별되는 위험 요인의 필수 항목들을 정의하고, 이를 활용해 테스팅을 체계적이고 효과적으로 수행할 수 있도록 관련 표준을 연계하는 방안을 제안한다.

Ⅱ. 본론

본 논문에서는 <그림 1>과 같이 위험 분석의 결과인 위험 요인의 필수 속성을 정의하고 이를 CPS 안전·신뢰성 프로필 주도 테스팅 프레임워크의 일부와 연계하였다. 이 연계 방안으로 테스팅을 수행하는 일련의 과정은 ‘위험 분석 수행 - 테스트 항목 설정 - 테스트 케이스 생성 - 테스트 스크립트 생성 및 실행 - 테스트 결과 리포트’의 흐름이다.

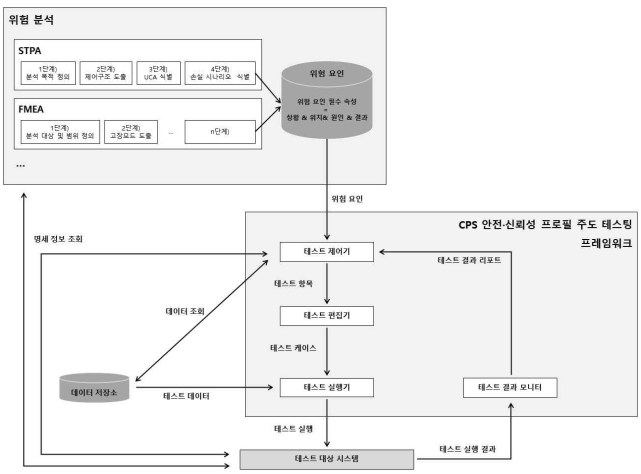

그림 1. 위험 분석을 통해 식별한 위험 요인 기반의 테스팅 방안

ⅰ. 위험 분석 수행

시스템 상황 및 테스트 환경에 적합한 위험 분석 기법을 설정하여 위험 분석을 수행한다. 위험 분석 결과로 식별되는 위험 요인은 구조화된 데이터 형태나 평문으로 구성할 수 있지만, 본 논문에서는 위험 요인에 위험 요인이 발현하는 ‘①상황’과 ‘②위치’, 위험 요인을 발현 시키는 입력 값과 같은 ‘③원인’, 위험 요인이 발현함으로써 발생하는 오류와 같은 ‘④결과’를 필수 항목으로 정의한다. 필수 항목을 포함하여 위험 요인을 구조화하

면, 테스팅 수행 시 과정의 일부(테스트 케이스 생성)를 자동화할 수 있는 장점이 있다.

ii. 테스트 항목 설정

위험 분석의 결과인 위험 요인과 테스트 대상 시스템의 명세 정보 등을 기반으로 테스트 항목(테스트할 위험 요인, 테스트 실행 시 사용될 입력 값 정보, 테스트 순서)을 설정하며, 테스트 항목 설정 과정은 다음과 같다.

a) 시스템 및 기능 등의 명세 정보를 기반으로 위험 요인 중 테스트 대상 시스템에 테스트할 위험 요인을 식별함
b) 위험 요인의 원인을 참고하여 데이터 저장소에서 테스트 실행 시 입력할 입력 값을 식별함
c) 위험 요인 내용에 심각도가 포함된 경우 심각도에 따라 테스트 순서를 결정함

iii. 테스트 케이스 생성

테스트 케이스는 테스트 수행을 위한 입력 값, 기대 출력 등의 집합으로, 테스트 케이스를 생성하면 테스트 누락을 방지하고 테스트를 투명화할 수 있다. 본 논문의 테스팅 방안에서 생성하는 테스트 케이스의 형태는 <표 1>과 같으며, <그림 2>와 같이 위험 요인의 필수 속성을 테스트 케이스와 매핑하여 테스트 케이스 생성 과정을 자동화할 수 있다. <표 1>의 테스트 케이스는 최소한의 항목이며 테스트 실행 단계, 의존 테스트 케이스 등을 고려하여 테스팅 상황에 맞게 속성을 추가할 수 있다.

표 1. 위험 요인 활용 테스트 케이스

속성	설명
테스트 케이스 ID	테스트 케이스를 구분하는 식별자
테스트 대상	테스트 대상 컴포넌트 혹은 기능
입력 명세	테스트 입력 값
출력 명세	테스트 케이스 실행 시 기대 출력
사전 조건	테스트 케이스 실행을 위한 환경정보를 포함한 모든 사전 조건

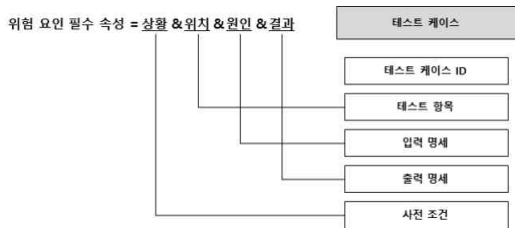

그림 2. 위험 요인 필수 속성과 테스트 케이스 매핑

iv. 테스트 스크립트 생성 및 실행

테스트 케이스를 기반으로 다음과 같이 테스트 스크립트를 구성하고 실행시켜, 테스트를 수행한다.

a) 테스트 케이스의 사전 조건을 활용하여 소프트웨어 및 하드웨어 환경을 포함한 전체 테스트 환경을 구성함
b) 테스트 케이스의 입력 명세를 참고하여 테스트 입력 값을 구성함
c) 테스트 스크립트가 실행되는 위치와 실행 시 기대 결과는 테스트 케이스의 테스트 대상 및 출력 명세를 각각 참고함
d) 구성된 테스트 환경에서, 입력 값에 대한 결과를 확인하는 일련의 절차를 구체화하여 테스트 스크립트를 작성하며 이를 실행함

v. 테스트 결과 리포트

테스트 실행 결과는 <표 2>와 같이 리포트하여, 테스트 결과를 분석한다.

표 2. 테스트 결과 리포트

속성	설명
테스트 실행 결과 ID	테스트 실행 결과를 구분하는 식별자
기대 결과	테스트 스크립트 실행 시 기대 출력 결과로 관련 테스트 케이스의 출력 명세를 참고함
실제 결과	통과(Pass) 혹은 실패(Fail)

Ⅲ. 결론

본 논문에서는 위험 분석과 테스팅 프레임워크 표준을 연계하여, 테스팅을 효율적으로 수행할 수 있는 방안을 제안하였다. 테스팅 프레임워크에 활용하기 위해 필수 속성을 정의한 위험 요인은, 다양한 위험 분석 기법을 분석하여 좀 더 구체적이고 상세화한 속성을 정의한다면 테스트 커버리지를 향상시키고 좀 더 체계적인 테스팅 수행이 가능하다. 또한 표준의 테스팅 프레임워크는 활용하는 위험요소가 기존에 미리 정리되어 있기 때문에, 본 논문에서 위험 분석을 통해 식별되는 위험 요인은 데이터 저장소와 같은 기존의 구성요소와 유기적인 흐름이 다소 부족하다. 이는 제안된 연계 방안을 활용한 사례 연구 수행함으로써, 데이터 저장소 등의 기존의 프레임워크의 구성요소를 테스트 활동을 위험 분석 결과에 특화하여 보완하고 구체화할 필요가 있다.

참 고 문 헌

[1] “STPA를 활용한 위험분석 가이드,” 2018.12.

[2] “TTAK.KO-11.0268-Part5.사이버-물리 시스템(CPS)의 안전·신뢰성 확보 지침 - 제5부: CPS 안전·신뢰성 프로필 주도 테스팅 프레임워크,” 2023.12