

Safety Engineering for AI

“AI Testing - Exploratory Test Method”

최근 자율주행 자동차 및 자율로봇과 같은 AI 기반 고위험 시스템들이 도입되고 있습니다. 이러한 AI 기반 시스템들은 기존 차별화된 기능과 성능을 제공함으로써 거대한 신규시장의 창출을 가능하게 하지만, 높은 자유도로 인해서 오동작 시 심각한 위험을 야기할 수 있습니다.

특히, 심층학습(Deep Learning) 등 훈련기법에 의존적인 현재의 AI 기술들은 훈련 시에 주어지지 않은 미지 사례(Unknown Cases)에 대해서 예측되지 않는 동작을 수행하기 때문에 보다 폭넓은 검증이 필요합니다. 하지만, 검증을 위해서 기존의 테스트 기법들을 적용하기 어려운데, 이는 기존 기법들이 입력-출력 관계에 대해 정의하는 요구사항 명세에 기반하기 때문입니다. AI는 학습 데이터에 의해서 훈련되지 명세에 의해서 개발된 것이 아니어서, 입력-출력에 대한 요구사항 명세를 작성하기 힘든 경우가 대부분입니다.

이러한 문제를 해결하기 위해서 탐색적 테스트 기법(Exploratory Test Method)이 적용될 수 있습니다. 탐색적 테스트 기법은 AI 시스템의 입력 영역에 대해서 추출/조합 기법을 적용하여 다양한 테스트 케이스를 생성하고, 그 결과를 확인하는 과정을 자동적으로 반복하면서, 통계적인 평가를 통해서 위험도를 분석함으로써, 부족한 요구사항 명세를 가지고도 폭넓은 검증을 수행할 수 있습니다.

탐색적 테스트 기법은 개략적으로 다음과 같이 구성됩니다.

1. 입력 영역 정의
2. 테스트 케이스 생성 - 다양한 추출/조합 기법 적용
3. 테스트 수행 - 시뮬레이션 환경 활용
4. 테스트 결과 확인 - AI 커버리지 측정 및 변성관계(Metamorphic Relation) 기반 테스트 판정
5. 통계적 위험도 분석

■ 탐색적 테스트 기법(Exploratory Test Method)

