연재 제95회 요구공학:

ISO 26262에 근거한 안전성 케이스의 적용 사례

국립대학법인 나고야대학 정보연계통괄본부 정보전략실 교수

(전 NTT Data Fellow 시스템과학연구소장) 야마모토 슈이치로

출처: BUSINESS COMMUNICATION

번역: 이채원 • 카이젠컨설팅

ISO 26262에서의 안전성 케이스

ISO 26262 규격 Part 10에서는, 기능안전에 대한 가이드라인을 해설하고 있는데, 그 중 가이드라인 5.3절에서 “안전성 케이스에 대해서 이해한다”라는 제목으로 안전성 케이스에 대해서 소개하고 있다.

안전성 케이스를 기술하는 방법으로는, GSN과 CAE(Claims-Argument-Evidence)가 있으며, 안전성 활동으로는 개발 대상 시스템인 “Product”에 대한 활동과, 시스템 개발이나 Assessment인 “Process”에 대한 활동이 있다.

또, 안전성 케이스의 개발 라이프사이클은, 안전성 라이프사이클과 결합된 반복적인 활동으로 취급할 필요가 있다고 언급하고 있다.

자동차의 기능안전성 확인에 대한 사례 연구

Wagner의 안전성 케이스를 자동차의 기능안전에 적용한 사례를 살펴보면, 안전성 케이스를 기존 차량의 소프트웨어 모델을 대상으로 하고 있다. 구체적으로, MAN Nutzfahrzeuge AG사는 트랙의 주행 제어 컴포넌트에 적용함으로써, 범용적인 안전성 케이스의 아키텍처와 재사용을 분명하게 하고 있다.

덧붙여서, MAN Nutzfahrzeuge AG사가 어떠한 회사인지 알아보기 위해 홈페이지를 찾아 봤더니, 레

이더 센서를 사용하여 선행 차량의 후방을 추적하는 적응 주행 제어(Adaptive Cruise Control)의 기술을 개발하는 회사로 소개되어 있었다.

이어지는 내용에서는, Wagner의 안전성 케이스 작성 방법을 소개한다.

모델 베이스의 개발에서 안전성 케이스의 이용법

Wagner는, 아래와 같이 안전성 케이스를 모델 베이스 개발과 결합하고 있다.

1) 대상 시스템의 아키텍처에 따라 안전성 케이스를 모듈화
2) 개발 모델에 근거하여 안전성 케이스의 정보와 요구사항을 작성
3) 안전성 케이스에 따라 생성되는 전제를 근거로 하여 개발 모델을 작성

이 방법에서는, 안전성 케이스를 대상 시스템의 아키텍처에 근거하여 Top-down으로 전개할 수 있다. 이것은, 아키텍처에 의해 안전성 요구를 분해하는 패턴이다. 이 때, 시스템 개발 모델의 성과물을 안전성 케이스의 Context에 관련 짓는다. 또, 안전성 케이스와 시스템 개발 모델 구조 간 매핑시키기 위해서, 안전성 요구사항을 하위 컴포넌트와 매핑되도록 전개하고 있다.

시스템 개발 모델을 사용하는 것으로, 안전성 활동의 근거를 부여하는 것이 가능하다. 시스템 개발 모델에서는 소프트웨어 컴포넌트의 기능이나 업무와 Bus schedule의 사양을 정의하고 있기 때문에, 이것들과 연결되는 것으로 안전성 케이스를 작성하면 안전성 케이스의 구조는 타당하다고 할 수 있는 근거가 된다.

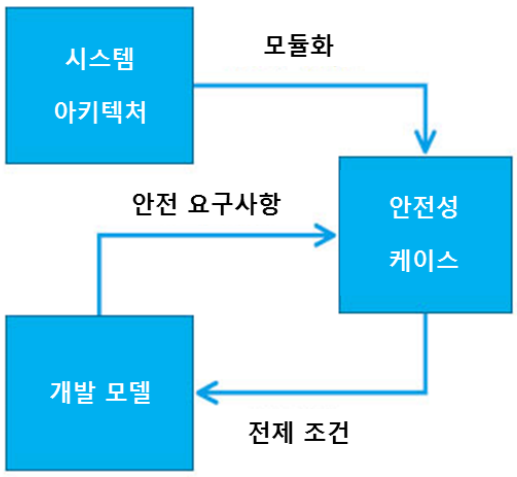

그림1 모델 베이스 개발에서의 안전성 케이스

안전성 케이스 아키텍처

안전성 케이스를 시스템 아키텍처와 연결시키기 위해서는 안전성 케이스를 표1에 나타내듯이 아키텍처를 이용하여 모듈화할 수 있다.

이 표에서는, 세로축에 수준, 가로축에 Product, 환경, 유저, 프로세스를 배치하고 있다.

수준에는, 기능을 논리적으로 정의하는 개념 수준, 기구적인 요소와 회로적인 요소를 통합하는 통합 수준, 기구, 회로, 소프트웨어 별 기능을 분해하는 기능 수준이 있다. Product에 대해서, 이 3개의 수준별로 안전성을 정의하기 위한 안전성 케이스 모듈을 작성하는 활동을 실시한다. 이 때, 환경, 유저와의 상호 작용을 확인하고, 유저의 행동에 대해서 판정(운전수의 반응 시간 등)이나 환경 조건(도로의 경사, 노면 상황, 풍속 등)을 기술하기 위해, 환경, 유저에 관한 안전성 케이스 모듈을 작성한다.

이렇게, 환경, 유저에 대해서 안전성 케이스를 모듈화 해두면, 다른 유사한 제품에 대해서도 재사용 할 수 있다.

또, 개발 프로세스에 대해서도 제품과 같이, 안전성 케이스를 수준마다 모듈화하여 작성하는 것이 가능하다. 해당 문헌[2]에서는, 프로세스에 대한 안전성 케이스에 대해서는 구체적인 내용은 기술되어 있지 않다.

주행 제어 시스템에 대한 기능 레벨의 안전성 케이스 모듈 구성 내용과 분석 대상을 표2에 나타냈다.

기구 모듈에서는 온도 경계, 부품의 위치 등을 기술하고 검증한다. 이 때, CAD모델, 평가 기준에 대해서 분석한다.

회로 모듈에서는, 전자 회로의 타당성, 피해 회복성에 대해서 기술하고 검증한다. 이 때, 센서 신호와 신호 전달의 타당성에 대해서 분석한다.

배치 모듈에서는, 소프트웨어를 배치하는 물리적 대상 관계에 대해서 기술하고 검증한다. 이 때, 실행 환경에서 결함 발생 시 영향에 대해서 분석한다.

소프트웨어 모듈에서는, 소프트웨어의 정당성에 대해서 기술하고 검증한다. 이 때, 주행 제어기, FPGA가 실행하는 소프트웨어 기능을 Simlink/TargetLink로 검사하거나 형식 검증을 실시한다.

공급 부품 모듈에서는, 공급자가 제공하는 부품의 요구사항 및 제품으로의 통합에 대해 기술하고 검증한다. 공급 부품에 대해서는 내용이 블랙박스화 되어 있기 때문에, 블랙박스 안전성 케이스 모듈에 의한 분석을 실시한다.

표1 안전성 케이스 아키텍처

수준	설명	제품	환경, 유저	프로세스
개념	논리 기능을 정의	개념 product 에 대한 안전성 활동	시스템 안전성에 대해 환경, 유저와의 상호작용을 확인 유저 행동에 대한 판정(운전수의 반응 시간 등) 환경 조건(도로의 경사, 노면 상황, 풍속 등)	개념 개발 프로세스 안전성 활동
통합	기구, 회로 요소의 통합	통합 product 에 대한 안전성 활동		통합 개발 프로세스 안전성 활동
기능	기구, 회로, 소프트웨어의 기능 분해	기능 product 에 대한 안전성 활동		기능 개발 프로세스 안전성 활동

표2 기능 레벨 안전성 케이스 모듈의 구성

모듈	내용	분석대상
기구	기구 부분에 대해서 온도 경계, 기계 부품의 위치 등을 검증	CAD 모델, 평가 기준
회로	전자회로의 타당성, 피해 회복성에 대한 검증	센서 신호와 기능의 신호 전달의 타당성
배치	소프트웨어를 배치하는 물리적 대응 관계에 대한 검증	실행 환경에서의 결함의 영향
소프트웨어	소프트웨어의 정당성에 대한 검증	주행 제어기, FPGA 가 실행하는 소프트웨어 기능을 Simlink/TargetLink 에 의한 검사 및 형식 검증
공급 부품	공급자가 제공하는 부품의 요구사항 및 제품의 통합에 대한 검증	블랙박스 안전성 케이스 모듈에 의한 분석

안전성 케이스의 Top-down 작성 방법

Wagner에 의한 안전성 케이스의 작성 방법의 순서는, 그림 2에 나타냈듯이 Top-down 검증 프로세스이다. 먼저, 대상 시스템의 Hazard를 식별한다.

원문 | http://www.bcm.co.jp/site/youkyu/youkyu95.html