2011년 11월 21일 11시 27분 갱신

자동차 분야의 기능 안전 규격 “ISO26262” 라는 것은 무엇인가? (4):

ISO26262 Part.8 지원 (검증 프로세스 등)

자동차 분야 전용 기능 안전 규격 “ISO26262”. 이번 회는, 시스템, 하드웨어/소프트웨어에 관한 “ISO26262 Part.8 지원”의 연속으로, “검증 프로세스”에 대해서 논의한다.

글: 河野喜一(NEC 컨설팅사업부) | 출처: MONOist

번역: 이채원 • 카이젠컨설팅

자동차 기능 안전 규격 “ISO26262” 지원 (검증 프로세스 등) 개요

지난 회에서는 기능 안전 규격의 “지원 (관리 프로세스)”에 대해 개요를 설명했습니다.

이번 회는 ISO26262 Part.8 지원의 연속으로 “지원 (검증 프로세스 등)”에 대해서 설명합니다.

주목은 받고 있지만, 실시하기 어려운 활용/재사용 프로세스

임베디드 소프트웨어 개발에서는 기존 제품의 소스코드의 활용에 의한 제품 개발이 많아졌지만, 재사용하기 위해 필요한 정보가 제대로 정리되지 않는 경우를 많이 볼 수 있습니다. 또 선행 개발이나 시작(試作)개발로는 재사용을 전제로 한 개발을 하고 있지 않기 때문에, 실제로 재사용할 때 그 때마다 소스코드를 분해하여 사양을 확인하거나, 설계서를 쓰기 시작하거나 하는 경우가 많습니다.

ISO26262에서는 소프트웨어 부품이나 하드웨어 부품이 ISO26262에 준거하여 개발되고 있는 것은 물론, 활용/재사용에 필요한 정보를 문서로 남기는 것 등이 요구됩니다. 즉, 소스코드의 활용이나 재사용으로 인해 발생하는 결함을 방지하기 위한 “컴포넌트 검증 프로세스”를 정의해야 합니다.

ISO26262 지원 (검증 프로세스)

ISO26262의 지원 (검증 프로세스)에서는, 검증 대상이 되는 부품을 미리 선정해 두고, 프로젝트 계획 시 검증 계획을 수립하는 것이 요구됩니다. 이를 위해서 요구사항 정의 (Item 정의)가 끝난 후에 차종마다 공통된 요구사항이나, 등급 등에 따라 변경되는 부분을 가장 먼저 확실하게 분석해 둘 필요가 있습니다. 이 때문에 상품 기획 단계에서 Item을 어떠한 등급으로 정의하고 있는지, 차종 간에 있어서 공

통 요구사항은 무엇인지 등을 명확하게 하는 것을 전제로 합니다.

예) 엔진을 공통화 하는 것 등

ISO26262의 검증

ISO26262의 검증 프로세스는 개발 프로세스에서 설계서의 검증과 구축 후의 테스트 양쪽 모두 적용됩니다. 이 검증 프로세스에서는 “검증 계획 수립”, “검증 사양서의 작성”, “검증 결과 레포트”의 3가지가 세트로 요구됩니다.

ISO26262에서는 설계서를 검증하기 위해 시뮬레이션이 요구되는 경우가 있습니다. 그 때문에 구축 후의 테스트뿐만 아니라, 설계서 검증에서도 시뮬레이션 계획을 수립하고, 설계서를 검증하는 것이 요구됩니다.

또 단순하게 시뮬레이션 하는 것뿐만 아니라, 요구사항을 망라하고 있는가를 확인하는 요구 베이스 테스트나, 기능 간의 상태 부정합에 의한 이상 제어와 같은 내용도 테스트하여야 합니다.

“설계서 리뷰만 수행하면 몇 시간이면 끝나는데, 왜 시뮬레이션까지 하는가?”라는 이야기도 있습니다만, 오류에 대한 수정 공수는 초기 설계 단계 쪽이 이후의 공정보다도 크게 적어집니다. (후기 공정 10분의 1에서 초기 공정은 100분의 1로 적어지는 것으로 알려져 있다). 특히 소프트웨어에는 오류가 잠재하고 있는 경우가 많기 때문에, “보다 상위 공정에서 오류를 검출해 두는 것이 효율이 좋다”라고 말할 수 있겠죠.

문서화

검증 프로세스와는 조금 다릅니다만, ISO26262 Part.8 지원에서는 문서화의 요구도 정의되고 있습니다.

설계서는 물론, 테스트를 실시하기 위한 테스트 사양서, 테스트 결과 등의 모든 성과물을 문서로 하는 것이 요구되고 있습니다. “문서로 남긴다”라는 행위는 제 3자에 의한 리뷰를 하기 위해 필요한 것뿐만 아니라, 개발한 소프트웨어나 하드웨어를 재사용할 경우에도 필요하게 됩니다.

또 모든 문서에는 “작성자”, “승인자”, “버전”, “변경 이력” 등의 포맷을 채용하는 것이 요구되고 있습니다.

소프트웨어 툴 검증

2011년 11월 21일 11시 27분 갱신

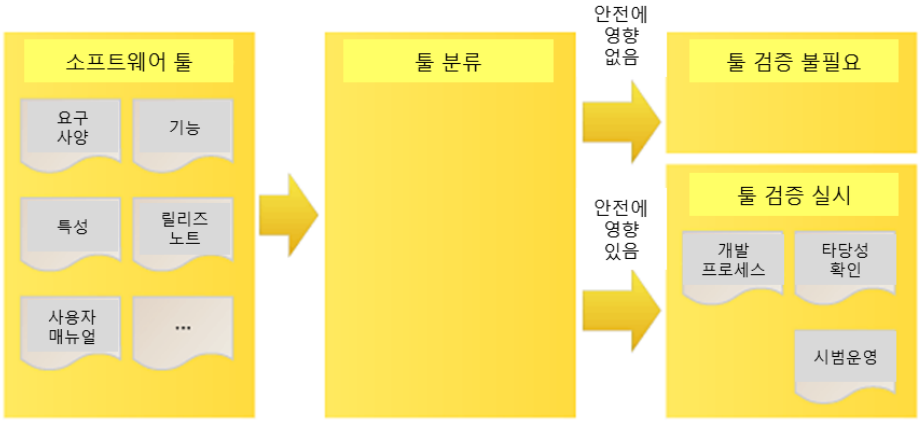

그림1 소프트웨어 툴 검증 전체상

ISO26262의 소프트웨어 툴 검증에서는 개발에 사용하는 소프트웨어 툴을 사전에 검증하기 위한 프로세스가 정의되어 있습니다.

대상은 “안전성과 관련된 모든 소프트웨어 툴”이 되기 때문에, 설계서나 사양서를 기술하기 위한 에디터나 모델링 툴, CAD 툴, 코딩 지원 툴, 컴파일러&링커, 테스트 툴 등이 대상이 됩니다. 또, 특수한 툴로 HILS (Hardware-In-the-Loop Simulation)도 소프트웨어 툴 검증의 대상으로 포함됩니다.

소프트웨어 툴 중에서도 코드 자동 생성이나 테스트에 사용하는 소프트웨어 툴의 검증은 다른 툴과 비교하여 특히 어렵습니다.

가장 처음으로 해야 하는 일은 소프트웨어 툴 검증을 위한 검증 계획을 수립하는 것입니다. 계획을 수립하기 위해서는 여러 가지 문서나 정보가 필요합니다만 프리웨어 툴의 경우는 문서나 정보를 모으지 못한다는 Risk도 있습니다.

다음으로 소프트웨어 툴이 안전성에 관한 툴인지, 안전성과 관련된 경우라면, 고장이나 오류 발생 시에 그것을 검출할 수 있는지 여부를 확인하여 툴을 분류합니다. 그 결과 소프트웨어 툴이 안전성과 관계없이 고장이나 오류 발생 시에 검출 가능한 경우는 검증의 대상 외로 취급됩니다.

실제 검증에서는 “사용 과정에 의한 보증”, “툴 개발 회사의 프로세스 인증”, “툴의 타당성 확인”을 실시하는 것이 요구되고 있습니다.

여기에서 특히 주의가 필요한 것은 툴 개발 회사의 프로세스 인증도 요구되는 점입니다. 그 때문에 CMMI나 Automotive SPICE (내장 툴에 유효)라는 인증, 더불어 IEC 61508이나 ISO26262와 같은 어려운 인증에 준거할 필요가 있다라는 것입니다.

이것도 프리웨어인 경우 “개발한 기업이 어디인지? 누구인지? 프로세스는 있는지?” 등을 파악할 수 없다라는 Risk가 발생하기 쉽다라고 말할 수 있습니다. 게다가 프리웨어이기 때문에, 어떠한 검증을 했는지, 타당성 확인을 했는지도 명확하게 파악하는 것이 곤란하므로. 툴 검증을 실시하기 위해서는 “프리웨어를 테스트하기 위한 테스트 환경”을 준비할 필요도 있습니다.

이런 점을 고려하면 ISO26262 인증된 “상용 툴”을 이용한 경우는, 소프트웨어 툴 검증을 생략 가능하고, 게다가 신뢰성을 인증 기관이 보증하고 있다라는 큰 메리트가 있습니다. 덧붙여, CMMI 등의 프로세스 인증을 취득하지 않은 상용 툴 벤더는 이후 프로세스 인증 취득이 요구될 가능성이 나옵니다.

또 소프트웨어 툴 검증은 소프트웨어 툴의 버전이 바뀔 때마다 실시할 필요가 있기 때문에 내부 공수를 최소한으로 억제하기 위해서는 소프트웨어 툴의 종류를 필요 최소한으로 줄이는 것과, ISO26262 인증된 상용 툴을 이용하는 것이 중요합니다. 또 마찬가지로 소프트웨어 툴의 타당성 확인을 위한 작업 공수를 최소한으로 줄이기 위해서도 타당성 확인을 자동화 하는 것이 요구됩니다. 이렇게 되면 소프트웨어 툴의 버전이 바뀌는 경우에도 재확인의 공수를 최소한으로 하는 것이 가능합니다.

소프트웨어 컴포넌트 검증

ISO26262의 소프트웨어 컴포넌트 검증이란 소프트웨어 아키텍처 설계로 정의한 “소프트웨어 컴포넌트” 단위로 재사용하기 위한 검증 프로세스입니다. 여기에서는 “소프트웨어 컴포넌트에 대해서 어떠한 이상 검출이나 이상 제어의 단계가 존재하는가, 그 외에 함께 이용하지 않으면 안 되는 소프트웨어 컴포넌트는 무엇이 있는가”라는 내용이 요구됩니다.

소프트웨어 컴포넌트 검증을 위해서는 먼저 검증 계획을 수립하고 검증을 행하게 됩니다. 검증의 수준은 소프트웨어 컴포넌트의 어플리케이션 매뉴얼을 정비하는 등의 사전 준비 정도로 검증 자체는 타당성을 확인하기 위한 요구 베이스 테스트를 실시하는 정도로 검증을 수행하면 됩니다.

재사용하는 경우는 소프트웨어 컴포넌트의 산출물 세트를 구성 관리 프로세스의 베이스라인으로 설정하고, 산출물 세트의 버전이나 갱신 이력을 관리해야 합니다. ISO26262에 따라 구성 관리/변경 관리를 실시하기 때문에, 변경 관리된 산출물 세트를 용이하게 취급하는 것이 가능합니다.

단지, 소프트웨어 컴포넌트 자체가 독립된 것이라는 사항을 전제로 하고 있기 때문에, AUTOSAR 등에 따라 계층화하고, 계층 간의 교환에 API를 사용할 필요가 있습니다.

하드웨어 컴포넌트 검증

ISO26262의 하드웨어 컴포넌트 검증에서는 ISO26262에 따라 개발한 하드웨어 컴포넌트 (부품)를 재사용하기 위해 검증을 실시합니다. 하드웨어 컴포넌트 검증도 사전에 계획을 수립한 후에 검증을 실시하게 됩니다.

2011년 11월 21일 11시 27분 갱신

하드웨어 컴포넌트 검증 자체는 소프트웨어 컴포넌트 검증과 달리, “분석 (한계 초과 테스트, 열화 가속 테스트)에 따라 성능을 증명하는가, ISO16750에 따라 테스트를 실시하여 성능을 증명하는가” 중 한쪽을 선택하여 실시합니다. 덧붙여, 이 증명에는 고장 모델이나 고장 분포의 증명도 포함됩니다.

사용 근거에 의한 증명

사용 근거에 의한 증명은 검증이 필수인 소프트웨어 컴포넌트 및 하드웨어 컴포넌트에 적용되고, 사용 근거에 의한 ASIL (안전 레벨)의 향상이 인정된다라는 수법이 됩니다. 사용 근거를 취득하기 위해서는 판매 후의 고장률을 집계하여야 하는데, 이를 위해서는 OEM 등으로부터 고장 정보를 입수할 필요가 있습니다.

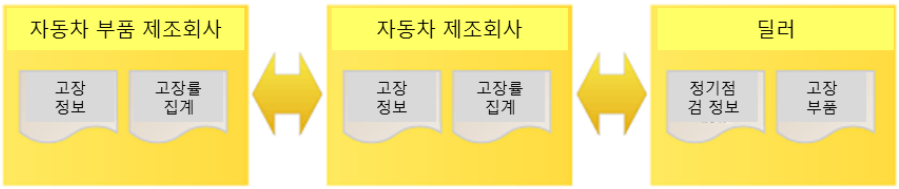

그림2 딜러부터 자동차 부품 제조회사까지의 전달

또한 현재 상태에서는 사용 근거에 의한 증명은 ISO26262의 프로세스에 따라 개발된 컴포넌트를 대상으로 하고 있는 것이기 때문에, ISO26262를 준거하여 개발을 실시한 후에 수행하는 프로세스입니다.

지금까지 “ISO26262 Part.6 소프트웨어”와 “ISO 26262 Part.8 지원”의 개요를 설명했습니다. 다음 회는 ISO26262 Part.6 소프트웨어에 기재되어 있는 “수법”에 포커스를 두고자 합니다. 기대해 주세요. (다음 회에 계속됩니다.)

필자 소개

河野喜一 코우노 요시카즈

2011년 11월 21일 11시 27분 갱신

NEC 컨설팅 사업부

(http://www.nec.co.jp/service/consult/vision/softconsul/safety_05.html)

산업기기개발, 통신기기개발, ALM벤더, 임베디드 컨설팅을 걸쳐, 현직. 전문 분야는, 개발자의 시점에 의한 개발 프로세스 혁신(관리 측면, 개발 측면), 규격 적용 컨설팅. 현재, 임베디드 개발의 개발 프로세스 혁신, ISO 26262 적용 컨설팅에 종사.

원문 | http://monoist.atmarkit.co.jp/mn/articles/1111/21/news004.html

http://monoist.atmarkit.co.jp/mn/articles/1111/21/news004_2.html