자동차 분야의 기능 안전 규격 “ISO26262” 라는 것은 무엇인가? (1) :

다시 “ISO26262”의 전체상을 파악해두자

2011 년 8 월 30 일 11 시 13 분 갱신

자동차 분야 전용의 기능 안전 규격 “ISO26262”. 본 고에서는, 정식 발행을 준비하고, 일본의 자동차 업계에서도 대응 작업을 본격화 하고 있는 ISO26262 의 개요, 전체상에 대해서 다시 설명한다.

글: 河野喜一(NEC 컨설팅사업부) | 출처: MONOist

번역: 이채원 • 카이젠컨설팅

자동차 기능 안전 규격 “ISO26262”의 전체 개요

드디어 자동차 전용의 국제 기능 안전 규격 “ISO26262”가 정식 발행 되었습니다. 도대체 “기능안전”이라는 문화--“어떠한 기능, 부품이 고장 나더라도, 시스템의 안전성을 확보한다” 라는 사고방식--은, 유럽에서는 어떻게 해서 소중하게 다루어 온 것일까요.

본 연재의 메인 테마인 ISO26262의 개요를 소개하기 전에, 자동차에 있어서 유럽과 미국, 일본과의 “안전성의 확보”에 대한 사고 방식, 어프로치의 차이에 대해서 간단하게 언급하고 싶습니다.

원래 미국, 유럽과 일본에서는 “안전”에 대한 사고방식이 다르다

유럽, 미국에서는 과거 자동차 부품의 고장률이 높았던 것도 있고, 자동차 제조회사 각 사는 “어떻게 하면 부품이 고장 나도 큰 피해를 내지 않고 끝날까” 라는 관점부터, 자동차의 안전에 관한 검토를 계속 해왔습니다. 이러한 대처가 주춧돌이 되어 유럽, 미국에서는 부품이 고장 나도 안전성을 유지할 수 있는 “기능 안전” 이라는 문화(사고방식)가 침투하고 있었던 것입니다. 제조 규정에는, 부품의 고장뿐만 아니라, “오 조작 시의 안전성 확보”의 사고 방식도 포함하고 있고, 예를 들어 엑셀 페달과 브레이크 페달이 동시에 밟혀진 경우는, 브레이크 페달을 우선해서 작동된다라는 룰도 규정되어 있습니다.

한편, 일본의 자동차 제조회사는 지금까지, 자동차 부품의 고장에 의한 사고를 미연에 방지하기 위해, 자동차 부품 제조회사에 대해서, 자동차 부품의 “품질 개선/품질 향상”을 요구하고, 안전성을 높이는 대책을 강구해 왔습니다. 그 때문에, 일본에서는 “품질=안전” 이라는 생각아래, 품질을 추구하는 것에 의한 안전성 확보 어프로치, “품질 향상의 문화”가 선행해오고 있습니다.

본 연재에서는, 이러한 양쪽(유럽 미국과 일본)의 안전에 대한 사고 방식, 어프로치의 차이를 밟은 다음, 정식 발행을 앞두고 일본의 자동차 업계에서도 대응 작업이 본격화 하고 있는 ISO26262의 개요를 소개해가고자 합니다. 본 연재를 통해서, 다시 ISO26262의 전체상을 잡는다면 좋을 것이라고 생각합니다.

ISO26262 책정의 배경

과거 유럽에서, 고장이 원인이 된 생산 플랜트 사고가 몇 건이 발생했습니다. 산업 플랜트 중에서도 특히 “원자력, 화학 플랜트”의 사고가 발생하면, 지역이나 인명에의 영향도 크게 되기 때문에, 그 손해는 헤아릴 수 없습니다.

그 중, 항공용 소프트웨어의 국제 기술 기준인 “DO-178B” 규격을 참고로 사고, 피해를 방지하기 위해서 방법을 정리한 기능 안전 규격 “IEC61508”이 IEC (국제전기기준회의)에 의해 책정되어, EU (유럽연합)의 법규로써 규정되게 되었습니다.

IEC61508은, 위험이 되는 사상부터 인명, 건강, 환경 (지역) 등을 지키기 위해서 “기능”, “장치”를 추가하고, 리스크를 저감해서 안전을 확보한다라는 사고방식으로, 그 시스템의 구성 요소 가운데 컴퓨터나 소프트웨어를 포함한 전기, 전자, 프로그램블 전자(E/E/PES)에 관한 기능 안전 규격입니다. 이 IEC61508은 기능 안전 규격의 기초로, 이 규격으로부터 파생된 생산 기계, 원자력 발전소, 의료 기기 등의 특정 분야에의 안전 사항을 정리한 규격들이 법규로 책정되고 있습니다.

본 연재의 주역인 ISO26262도, IEC61508에서 파생된 자동차 분야 전용의 전기, 전자 시스템 (E/ES)에 관한 기능 안전 규격으로써 자리매김되고 있습니다. 덧붙여서, ISO26262는 현 시점 (2011년 8월)에 정식 발행 “대기” 단계에 들어가 있습니다.

ISO26262 의 정식 발행부터 실제 차량 적용의 시기

계속해서, ISO26262의 정식 발행이 이루어지면 실제로 어떻게 적용되는지에 대해 간단하게 소개하겠습니다.

산업 기계 분야의 소프트웨어나 제어 시스템의 기능 안전 규격이라고 할 수 있는 “ISO13849”의 경우, 정식 발행과 거의 같은 시기에, 규격을 3년 후부터 적용한다는 EU의 선언이 이루어졌습니다. 이러한 사례로 보면, ISO26262에 대해서도 정식 발행과 거의 같은 시기에 EU의 선언이 이루어져 3년 후부터 적용이 될 것으로 예상됩니다.

현 시점에서, ISO26262가, 2011년 8월에 정식 발행 된다고 예측되고 있기 때문에, 자동차 제조회사나 자동차 부품 공급자는, 3년 후인 2014년의 모델부터 ISO26262에 정식 적용할 수 있도록 빠른 템포로

준비를 진행하고 있습니다.

ISO26262 의 개요

그러면, ISO26262에 대해서 조금 더 자세하게 살펴보고 가겠습니다.

ISO26262는, 자동차에 탑재되고 있는 모든 부품 중, “센서로부터, 제어 장치(ECU), 작동 장치(모터)까지 일련의 시스템에 포함된 전기, 전자기기 등의” 하드웨어/소프트웨어를 대상으로 한 안전 규격입니다.

ISO26262에서는, 자동차의 “요구정의 (구상단계)”부터, “개발”, “생산”, “보수, 운용”, “폐차” 에 이르기까지의 라이프사이클 전체라는 광범위한 영역이 대상으로써 정의되고 있습니다. 당연히 자동차 제조회사와 자동차 부품 제조회사 양쪽에서 규격을 준수해야 하기 때문에, 기업을 넘은 대처가 필요합니다.

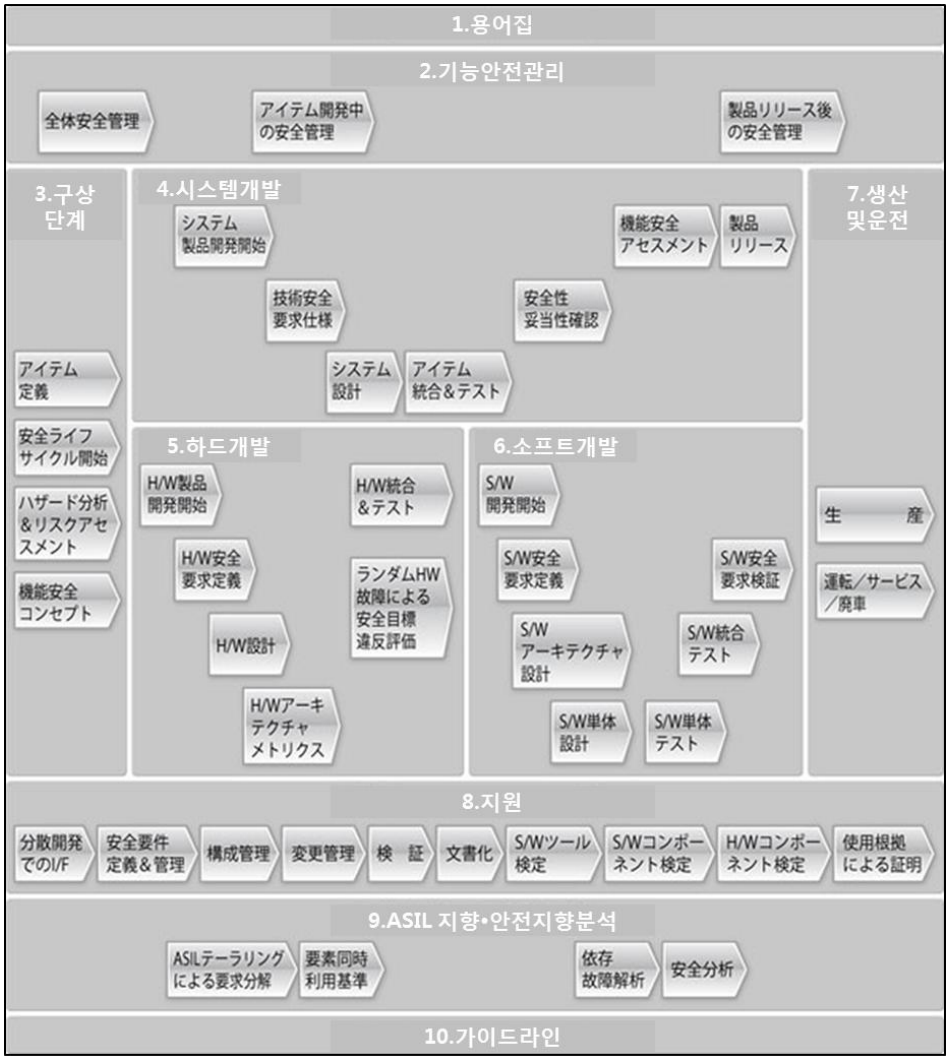

그림1 기능안전규격 전체상

[그림 설명] (시계반대방향으로)

2. 기능 안전 관리 : 전체 안전 관리 → 아이템 개발 중 안전 관리 → 제품 릴리즈 후 안전관리
3. 구상 단계 : 아이템 정의 → 안전 라이프사이클 개시 → 위험 분석 & 리스크 어세스먼트 → 기능안전컨셉
4. 4. 시스템 개발 : 시스템 제품 개발 개시 → 기술 안전 요구 사양 → 시스템 설계 → 아이템 통합 & 테스트 → 안전성 타당성 확인 → 기능 안전 어세스먼트 → 제품 릴리즈
5. 하드 개발 : H/W 제품 개발 개시 → H/W 안전 요구 정의 → H/W 설계 → H/W 아키텍처 매트릭스 → 랜덤 HW 고장에 의한 안전 목표 위반 평가 → H/W 통합 & 테스트
6. 소프트 개발 : S/W 개발 개시 → S/W 안전요구 정의 → S/W 아키텍처 설계 → S/W 단체 설계 → S/W 단위 테스트 → S/W 통합 테스트 → S/W 안전요구 검증
7. 생산 및 운전 : 생산 → 운전/서비스/폐차
8. 지원 : 분산 개발에의 I/F → 안전 요건 정의 & 관리 → 구성관리 → 변경관리 → 검증 → 문서화 → S/W 툴 검정 → S/W 컴포넌트 검정 → H/W 컴포턴트 검정 → 사용 근거에 의한 증명
9. ASIL 지향 • 안전 지향 분석 : ASIL 테일러링에 의한 요구 분해 → 요소 동시 이용 기준 → 의존 고장 해석 → 안전 분석

지금까지의 일본의 자동차 업계에서는, 전 차종과의 “차분(差分:등급을 두어 나눔) 개발”에 중점을 두고 있는 것에 비해, “설계서를 갱신하지 않는다” 라는 문화도 존재하고 있어서, 개발 프로세스를 경시하는 듯한 경향이 적지 않게 있었습니다. ISO26262에서는, 요구 정의를 포함한 개발 프로세스를 필요로 하기 때문에, 규격을 준수하기 위해서는 생각보다 많은 시간을 필요로 하게 될 것입니다.

덧붙여서 (필자의 경험에 의하면), 해외에서의 차분 개발의 경우는, 기존 문서에 차분 부분을 장치시켜 자동적으로 설계서를 갱신하는 구조가 도입되고 있는 케이스가 많고, 개발이 프로세스를 준수하여 잘 진행되고 있다는 인상을 받았습니다.

ISO26262 의 Part 와 관련된 부문

ISO26262는 기능 안전의 사고 방식에 근거해서, 안전한 자동차를 개발하기 위한 유효한 방법이나 기준 등을 체계화 한 것으로, 전체 “10”의 Part로 구성되어 있습니다.

전체 Part들은, 각 Part 간 여러 부문이 관계되어 있고, 그 담당 범위를 자동차 제조회사 (Part 3 : 구상

단계 ~ Part 4 : 시스템 개발)와 자동차 부품 제조회사 (Part4 : 시스템 개발 ~ Part 5 : 하드웨어 개발, Part 6 : 소프트웨어 개발)로 분류하는 것이 가능합니다.

그림2 기능안전규격과 관련부문 예

일본에서는 “몇 개의 안 또는 의견을 맞대어 조정하는 문화”가 조성되어 있고, “Part3 : 구상 단계”나, “Part4 : 시스템 개발” 을 실시하는 문화가 별로 없었기 때문에, 당황스러움을 느끼고 있는 기업이 늘어나고 있는 것으로 파악됩니다. 또, “Part2 : 기능 안전 관리” 에서는, 품질 보증 부문도 관련되어있기 때문에, 자동차의 특성을 잘 알고 있는 품질 보증 담당이 필요하게 되고, 지금까지의 품질 보증의 개념을 크게 바꾸게 됩니다.

덧붙여, 해외에서의 많은 회사들은 “Part3 : 구상 단계”와 거의 같은 프로세스로 요구를 확실하게 정의하고 있고, “Part4 : 시스템 개발”과 같은 프로세스에서 시스템 개발을 실시하며, “Part2 : 기능 안전 관리”에서 요구되는 부문 지식을 갖춘 품질 보증 담당이 존재하기 때문에 현재 일본보다는 적용하기 쉬운 규격이라고 말할 수 있습니다.

이와 같이, 유럽과 미국의 출발로 유럽과 미국의 문화가 많이 받아들여지고 있는 ISO26262 입니다만, 일본의 자동차 제조회사나 자동차 부품 제조회사 중 규격 책정에 참가한 멤버도 있어서 당초 생각보다는 일본에 적용하는데 있어서도 “느슨한 규격”으로 받아들여지고 있습니다. 단지, “느슨하다” 라고 해도, 규격으로 정의되고 있는 범위가 넓고, 적용하려면 큰 수고와 비용이 필요하게 됩니다. 수고와 비용을 줄이기 위해서는, 유럽과 미국에서 채용되고 있는 ISO26262 준거의 여러 가지 툴을 적용하고, 작업의 효율화를 진행시킬 필요가 있습니다.

자, 다음 회에서는, 현재 국내에서도 실시되고 있는 비교적 프로세스 개선에 착수하기 쉬운 “ISO26262의 소프트웨어 개발”에 대해서 말씀 드리고자 합니다. 기대해 주세요!

필자 소개

河野喜一（こうのよしかず: 코우노 요시카즈） / NEC 컨설팅 사업부

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

생산기기개발, 통신기기개발, ALM벤더, 편입 컨설팅을 걸쳐, 현직. 전문분야는, 개발자 관점에 의한 개발 프로세스 개혁(관리측면, 개발측면), 규격 적용 컨설팅. 현재, 편입 개발의 개발 프로세스 개혁, ISO26262 적용 컨설팅에 종사.

원문 | http://monoist.atmarkit.co.jp/mn/articles/1108/30/news002.html