중소 공급자를 위한 실천적 ISO26262 도입 (1)

ISO26262 대응을 시작하기 전에 이해해 두어야 할 것 (2/3)

글: DNV 비즈니스 • 어슈어런스 • 재팬기능안전부팀 | 출처: MONOist

번역: 이채원 • 카이젠컨설팅

규격 대응에 앞서

ISO26262 대응을 위한 활동을 시작하기 전에, 먼저 “리스크”라고 하는 것에 대해서 이해해 두지 않으면 안됩니다. 리스크라는 단어나 리스크 관리라는 사고 방식은, 좀처럼 일본에는 친숙하지 않고, 일본 기업의 약점이 되고 있다 라는 논리를 자주 듣습니다. 이것은 기업 레벨에만 국한되지 않습니다. 후쿠시마 제1원자력 발전소 사고에서는, “안전 신화”라는, 리스크를 완전히 무시한 최악의 케이스를 직접 행한 것이라고 할 수 있습니다.

한편, 유럽과 미국 사람들은 “인간은 실수를 범한다”, “기계는 고장 난다” 라는 전제에서 생각하기 때문에, 리스크가 제로가 되는, 매우 안전하다 라는 사고 방식을 갖고 있지 않습니다. 존재하는(제로가 되지 않는) 리스크를 명확하게 식별해, 그 리스크의 정도에 응한 최적인 대책을 세우는 것이, 제품 개발자의 책임이라고 하는 사고 방식입니다. 물론, 그 판단 경위를 포함한 활동 결과는 제 3자에게도 보이는 형태로 되어있지 않으면 안됩니다. 이 사고 방식의 차이로 고생한 것이 2009년에 발생한 도요타자동차의 미국에서의 집단 소송 문제입니다[*1)]

[*1)] 최종적으로는 NHTSA와 NASA로부터 전자 제어의 안전성의 확증을 얻는 것으로 결론지어지고 있습니다.

ISO26262도 이러한 전제에 있어서, 의도한 기능이 고장이 난 경우에, 안전을 위협할 가능성이나 그 피해 정도[*2)] 를 평가해서, 그 결과에 응한 대책을 세우는 것을 요구하고 있습니다. 그 대책에 대해서, 리스크의 정도에 따라 정리한 결과가 ISO26262의 규격서 속에서, 안전요구 레벨인 ASIL(Automotive Safety Integrity Level) A~D로 나누어 분류되고 있는 것입니다.(표1)

[*2)] ISO26262에서는 콘트롤러빌리티 라는 개념이 더해져, 정확하게는 세 개의 척도로 평가한다.

수법		ASIL A	ASIL B	ASIL C	ASIL D
1a	비형식기법	++	++	+	+
1b	준형식기법	+	++	++	++
1c	형식기법	+	+	+	+

표1. ASIL 레벨에 맞춰 요구된 대책의 예. 소프트웨어 아키텍처 설계를 위한 기법과 ASIL 레벨을 대응시킨다.

많은 사람들은, 이 ASIL 레벨마다 나열되어 있는 요구사항 자체에 주목하고, 단기적인 시점에서 어떻게 대응할까 하고 생각하기 십상입니다. 하지만, 이들의 대책은, 추상적인 표현으로는 이용자에게 이해되지 않기 때문에, 현재의 기술 수준부터 생각할 수 있는 가장 타당한 대책을[*3)] , 가능한 한 구체적으로 나열해 놓았다고 이해해야만 합니다. 물론, 기술이 진화하면 그 대책도 바뀌어야 할 것입니다.

[*3)] "state of the art"라는 용어가 자주 사용 되고 있다.

ISO26262를 이해하는 데 있어서 가장 중요한 것은, ASIL 레벨마다 나열해 놓은 대책・수법 등이 아니라, 전제한 리스크에 대한 사고 방식입니다. 즉, "리스크를 신중하게 식별"해서, 자신들이 실시하는 대책이나 개발 활동이 "식별한 리스크를 충분히 경감(허용)할 수 있는 레벨인가의 판단"을, "조직"이 철저히 의식하면서 개발을 진행한다는 점을 함께한다는 것입니다. 이것이 ISO26262라는 규격의 베이스에 있는 사고, 의식, 정신인 것이라고 생각합니다.

리스크를 의식하고 있지 않으면, 요구된 ASIL 레벨과, ASIL 레벨이 요구하는 대책을 수행하는 것만이 관심사가 되어, 항상 단기 요구나 비용 제약 등에 노출되는 개발 현장에서, 안전 활동은 소홀하게 되버릴 수 있는 사태를 부를 수 있습니다. 물론, 공정 후반부에서 새로운 해저드(위험 요소)가 발견[*4)] 되는 것도 아니며, 또한 ISO26262가 목표하는 건전한 "안전 문화" [*5)] 도 양성되지 않겠죠.

[*4)] ISO26262의 Part9에서, 새로운 해저드(위험 요소)를 발견한 경우의 취급이 명기되어 있다.

[*5)] Part2에서 안전 문화에 대해서의 요구가 명기되어 있다.

ISO26262 의 전체상

앞서 말한 대로, ISO26262는, 매니지먼트, 시스템 개발, 하드웨어 개발, 소프트웨어 개발, 양산에 이르는 제품의 설계・개발 전체에 사용되는 규격입니다. 본 연재는, 규격 그 자체의 해설은 주된 목적은 아니기 때문에, 규격 문서의 각 Part의 상세한 것에 대해서는, MONOist의 해설 기사를 참고해 주세요.

그림2는, 자동차의 개발 프로세스에 있어서 자동차 제조 회사, 티어1 공급자, 티어2 공급자, 이들 공급자의 하청이 되는 하드웨어 제조 회사, 소프트웨어 판매자 각각의 담당 범위와, 규격 문서의 Part2~9

까지의 관계를 대략적으로 나타내고 있습니다. 하지만, 이것은 어디까지나 규격 요건 내용으로부터 본 전체상이며, 실제로는 개별 계약*6) 에 따라 담당이나 책임의 범위가 다르게 정해지게 될 것이라고 생각합니다.

*6) Part8 중에서 "분산 개발의 인터페이스"로써 계약에 대한 요구가 명시되어 있다. 이 계약은 일반적으로 DIA라고 불린다.

그림2. 자동차 개발 프로세스에 있어서의 ISO26262의 담당 범위와 규격 문서 각 Part의 관계

원문 | http://monoist.atmarkit.co.jp/mn/articles/1212/25/news055_2.html