“ISO 26262”의 정식 발행으로, “안전”의 의식 개혁이 필수

- 빠른 대응이 승패를 판가름한다.

출처: MONOist

번역: 이채원 • 카이젠컨설팅

2011 년 11 월에 정식으로 발행된 ISO 26262. 먼저 발행된 기능 안전 규격 IEC 61508 이 토대가 된 자동차의 전자 제어에 관한 국제 규격이다. 원래 유럽에서 규격 책정이 추진되어 왔고, 유럽의 제조 회사나 공급자는 이미 적극적으로 임하고 있지만, 일본에서의 대응은 이제 시작이다. 그러한 와중에, 노르웨이에 본 거점을 두고 유럽 사정에 정통한 DNV 비즈니스 어슈어런스 재팬에서는, 전문가와 함께 ISO 26262 의 올바른 인식과 필요성에 대해서 적극적으로 정보 발신을 하고 있다.
기능안전서비스/그룹매니저 竹市正彦씨와 같은 회사 기술 고문을 임하고 있는 동경해양대학의 해양공학부 교수인 佐藤吉信씨에게 일본에서 높아지는 ISO 26262 의 필요성 및 각 회사가 해야 하는 일 등에 대해서 물었다.

라이프사이클이 대상이 되는 기능 안전 규격

전차나 비행기, 산업 플랜트, 병원의 의료 기기 등 컴퓨터는 다양한 시설과 제품 등에 포함되어, 위험을 감지하면 자동 정지하는 등 안전 기능을 실현할 수 있게 되었다. 이러한 컴퓨터를 포함한 시스템 설계, 제조, 사용에 관한 안전의 지침으로써 2000년에 발행된 규격이 IEC 61508 “전기, 전자, 프로그래머블 전자 안전 관련계(이하, 안전 관련계 라고 한다)의 기능 안전”이다.

IEC 61508은, 특정 분야에 한정한 것은 아니지만, 프로세스 플랜트나 공작 기계 등의 분야의 출신자를 중심으로서 만들어졌다. 안전 관련계의 “개념(구상)”의 설정에서, “사용 종료 혹은 폐기” 하기까지의 16 단계로 이루어진 라이프사이클 전체를 대상으로, 각각의 단계를 유기적으로 관련 짓는 요구사항을 규정하고 있다. 안전도 수준(이하, SIL : Safety Integrity Level)에 따라 리스크 및 안전 관련계에 의한 리스크 경감(저감) 성능을 정량적으로 규정하고 있는 것도 특징이다. SIL은 안전 관련계가 그 안전 기능 수행에 성공할지 아닐 지의 확률을 수직적으로 가시화한 지표이다.

이 규격을 기본으로 프로세스 산업의 안전 계장 시스템에 관한 규격(IEC 61511), 산업용 기계류의 전자 제어(IEC 62061), 철도에서의 신호 제어(EN 5012x), 의료 장치(IEC 60601) 등 다양한 분야, 제품 규격이 파생하고 있다. 1994년 이후, IEC 61508 / IEC 61511의 책정/개정 대책 국내 위원회의 간사(현 주사) 및 책정/개정 국제 전문가로 활동해 온 동경해양대학의 해양공학부 교수인 佐藤吉信씨는, “실

제로 일본에서는 2000년 정도에 IEC 61508을 토대로 일본 판 자동차 전자 제어의 안전 기준을 만들어, 장래적으로는 이것을 국제 기준으로 올리려는 움직임이 있었다. ABS의 인정 시험 등에 활용되거나 기능 안전의 사고 방식 보급에 기여할 수 있는 등 성과는 얻었지만, 유감스럽게도 당시 그러한 인식은 퍼지지 않았다" 라고 당시의 국내 실정의 안타까움을 내 비추며 말했다.

동경해양대학 해양공학부 교수 / 佐藤吉信

한편, 같은 시기에 독일과 프랑스가 중심이 되어 자동차 전자 제어의 기능 안전 규격에 대해서 검토가 개시되고, 2005년에 ISO에 제안, 심의가 시작되었다. 일본의 제조 회사나 공급자의 대표자도 규격 책정에 참가, IEC 61508을 바탕으로 자동차 전용의 상세한 요건을 포함하여, 2011년 11월 15일에 ISO 26262를 발행하는 단계가 되었다.

넓은 영역의 자동차 산업에 미치는 영향은 방대

DNV 비즈니스 어슈어런스 / 재팬 기능안전서비스 그룹매니저 / 竹市正彦

ISO 26262 발행에 대해, DNV의 기능안전서비스 그룹 매니저 竹市正彦씨는 "자동차 산업의 비즈니스

체계는, 제조 1회사에 머무르지 않고, 부품 제조 회사, 하청 기업이나 협력 기업이 다수 존재하고 있다. 그 모든 것에, 안전에 관한 부분에 대해서 ISO 26262의 요구사항이 걸린다. 유럽은 2000년 무렵부터 조금씩 준비해 왔지만, 일본에서는 일부 수출을 하고 있는 부품 제조 회사를 제외하고는 아직 대응하지 못하고 있는 실태. 그러나 자동차 산업의 영역은 넓어지고, 미치는 영향은 매우 크다" 라고 지적한다.

대응하지 못하고 있는 배경에는 "안전"의 의식 차이가 있다. 일본의 제조 회사는 부품의 품질을 개선하는 것으로 위험이 발생하지 않는다 라는 생각을 가지고 있다. 이것은 본질적인 원인을 제거한다 라는 "본질 안전"에 관련한 사고 방식이지만, "기능 안전" 이란, 시스템 전체를 대상으로 위험을 허용 가능한 수준까지 저감시키는, 즉 허용 가능한 안전 수준을 달성한다 라는 접근방식이다. 거기서, 그 안전 수준의 정량화에 의한 가시화 즉, SIL이 필요하게 된다.

자동차 분야에 특별히 규격화 되어 발행된 이유는, 자동차가 세계적인 제품이라는 것에 배경이 있다. 佐藤교수는 "자동차 산업은 규모가 크고, 우수한 인재도 풍부하며, 규격에 대응할 만한 힘이 있다" 라고 말한다. 竹市씨는 "차에 포함되는 전자 기기가 매우 늘어나게 된 것도 배경의 하나. 이제까지 그러한 전자 기기에 관한 명확한 안전 지침이 없었고, IEC 61508에 준거시키려고 해도 규격의 성격상 문제로 자동차에 적용하는 것이 꽤 어려웠었다" 라고 말했다.

예를 들어 IEC 61508에서는, 기본 프로세스 제어 계와 안전 관련 계를 분리하는 것이 요구되지만, 자동차에서는 어렵다. 차간 거리 경보 시스템 등, 안전 관련 계가 그들의 기본 제어 기능의 일부로 되어 있기 때문이다. 또 플랜트나 기계라면 물리적으로 인간과 거기를 두어서 안전성을 유지하는 수법이 성립 되지만, 자동차는 운전자와 일체되는 것으로, 분리라는 것은 현실적으로 불가능하다 라는 등, IEC 61508에 적용 시키는 것에는 무리가 있다.

자동차에 특화된 ASIL 을 규정

ISO 26262에서는, 이러한 차이를 고려하고 자동차 전자 제어 분야에 특화 시켜 다시 만들었다. 그 한 가지가 ASIL(Automotive SIL)의 규정이다. "ASIL은 아이템(해당 전자 제어 시스템)이 단위 시간에 어느 정도 위험한 결함이 발생했는가를 나타내는 지표이다. IEC 61508의 고 빈도/연속 모드의 SIL과 호환성이 있어, 이 제품의 안전 수준은 이 수준의 것이다 라고 명확하게 하기 위한 공통의 가시화" (佐藤교수)로, 위험도에 따라 A부터 D까지의 4레벨이 규정되고 있다. 안전상 매우 중요하고, 이것에 문제가 나타나 큰 피해가 발생하는 경우는, 가장 레벨이 높은 D가 되며, 매니지먼트나 하드웨어의 부품, 소프트웨어 설계 등의 요구사항이 어렵고 까다로워 진다.

레벨은 "위해 심각도(S)", "발생 확률 (E), "제어 회피 가능성(C)"의 3가지의 요인을 조합하여 결정된다. (S)는, 아이템에 결함이 발생한 경우, 어느 정도의 피해가 발생할지, 찰과상 정도인가 생명을 위협하는 것인가 라는 피해의 수준이고, (E)는 그것이 어느 정도의 빈도로 발생하는가 라는 것, (C)는 결함이 발

생한 경우, 그것을 운전자가 간단하게 피할 수 있는가? 제어 불능인가? 라는 것이다.

아이템이 ASIL의 어느 레벨에 해당하는지에 따라, 제조 회사는 기능 안전 확보의 대책을 취하는데, 구체적인 아이템에 대해서, 예를 들어 “에어백은 ASIL 등급 C” 라는 식으로 정해지지는 않았다. 구체적인 결정은 각 회사에 맡기고 있다.

佐藤교수는 “어느 회사는 B로 할지도 모르지만, 그렇게 해서 팔릴지 어떨지는 또 다른 문제. 경쟁해서 저비용으로 좋은 물건을 만드는 것이 본래의 경쟁이겠지만, 일률적으로 결정 될지도 모른다” 라고 말한다. 竹市씨는 “업계 간 극단적으로 레벨이 다르면 안 되어서, 어느 정도 맞추는 움직임이 있다. 어쨌든, 안전성의 의식은 높아지고 있다. 조금 전 까지는 A였지만, 어느 샌가 다양한 전제의 인식으로 변화가 일어나서 D가 되거나 하는 경우도 있다” 라고 밝혔다. 竹市씨에 의하면, 아이템의 레벨에 대해서 공적인 자리에서 토론하는 등, 업계에서는 의식의 통일이 이루어지고 있다고 한다.

일본의 제조 회사는, 안전으로의 의식 개혁과 동시에 규격의 올바른 이해가 요구되고, 그 때문에 확실하고 신속한 정보 수집이 해결의 열쇠가 될 것이다 라고 말했다.

ISO26262의 발행과 일본에 미치는 영향

佐藤吉信씨 vs. 竹市正彦씨

유럽과 미국에 비해 10 년 이상 늦어진 일본

- ISO 26262의 발행에 따른 국내에의 영향, 그리고 상황을 말씀해 주십시오.

竹市 : 규격의 공개는, 매우 영향력이 있다고 말해도 과언이 아니죠. 현 단계에서는 법률 등에서 ISO 26262에 대한 적합성을 강요하는 것은 아닙니다만, 부분적으로 법률화 될 가능성이 있다는 소문이 있습니다. 하지만, 규격이 공개된 지금, 자동차의 전자 제어에 관한 부분에서 무언가 트러블이 발생하는 경우, 기업측에서는 규격을 바탕으로 설명하지 않으면 안되도록 되어있습니다. (규격을 바탕으로 설명해야 한다.)

佐藤 : 특히 유럽과 미국에서는 사고가 발생하면 재판으로 이어지는 경우도 적지 않습니다. 그럴 때, 안전 대책에 확실하게 대응하고 있는가 가 논점이 됩니다. 특히 미국의 경우, 제조 회사가 그것을 증명하지 않으면 안됩니다. 그 때, 최소한, 즉 안전 규제나 규칙은 물론 업계 단체의 안전 규격이나 국제 규격을 충족하고 있었는지 어떤지가 기준이 되고, 충족하고 있지 않았다면 패소하게 되어 있습니다. 2010

년에 발생한 일본 차량의 문제에 대해서도, 당시는 전자 제어의 기준이 없었고, 이야기가 일치하지 않는 부분이 많이 있었지만 지금은 ISO 26262가 공개되었으므로 그것에 근거한 판단이 가능하겠지요.

일본에서는 시간도 비용도 만만치 않기 때문에, PL에 관한 소송은 거의 없습니다. 일본에서는, 어떻게 설계 했는가를 제조 회사는 공개 할 필요가 없습니다만, 미국에서는 그것을 감춘 것 만으로도 재판에서 지게 되어있습니다. 일본은 소비자 입장에서의 안전 문화의 의식이 상대적으로 높지 않고, 기업측에서도 기능 안전의 사고 방식이 뒷받침 되어있지 않습니다. 그 배경에는, 처음부터 기술력이 있는 고품질의 물건을 만들고 있고, 상태가 좋지 않는 것은 애초에 만들지 않는다 라는 제조사 측의 자부심이 있겠죠.

한편, 유럽에서는 1990년대에 이미 각국이 움직이고, 2000년에 IEC 61508이 발행되어 이 규격이 베스트셀러가 되는 등 취득 붐이 될 정도였습니다. 사실은, 일본에서도 같은 년도에 IEC 61508의 번역판 JIS C 0508을 만들었고, 저도 관련되었던 것 이였지만 그다지 관심을 갖고 있지 않았습니다. 기능 안전에 대해서는 완전히 10년 이상 늦어버린 겁니다.

竹市： 확실히 꽤 늦고 있다고 느껴지네요. 유럽에서는 산업 기계의 기능 안전에 대해서는 법령화 되고, 저는 그 인증 업무에 종사해 왔습니다. 법령화 된 것은 유럽뿐 이지만, 역사상 유럽의 영향력을 받고 있던 나라는 유럽을 본보기로 합니다. 그리고, 같은 요구를 일본에서도 하고 있습니다. 그렇기 때문에 산업 로봇 등을 수출하는 일본 제조 회사는 민감하게 대응하고 있습니다만, 기능 안전의 인식은 일본 국내에는 퍼져있지 않네요.

설계 단계에서 허를 찌르는 규격

- ISO 26262는 물론이고, 바탕이 된 IEC 61508에 대한 이해가 이루어 지지 않았기 때문에, 기업은 당황하고 있군요. 그럼, 기업은 어떻게 대응해야 할까요?

佐藤：ISO 26262는 IEC 61508과 마찬가지로 라이프사이클의 요구 사항에 대응하지 않으면 안되지만, 이는 예상 밖의 고장이나 실패를 없애기 위해서 하는 것입니다. 따라서, 제품의 구상 단계에서부터 리스크 평가, 개념 설계, 안전요구사양……그 사이에 기능 안전 평가, 적합 확인, 타당성 확인 등 여러 가지 확인을 해야 합니다. 지금까지는 팀 내에서만 확인해도 상관 없었지만, 독립한 제 3자에 의한 확인도 필요하게 되는 등, 할 일이 매우 많습니다. 일본에서는 지금까지 산업계에 있어서 안전이라면, “공장의 안전” 이라는 이미지가 강하고, 설계자는 관련 없다는 입장이였지만, 이 규격은 전원이 관계되어 있습니다. 먼저, 그것을 인식해야겠죠.

竹市： 개발 현장은 매일 업무에 쫓기고 있습니다만, 설계에서 허를 찌르고 있기 때문에 지금까지의 방법으로는 통하지 않습니다. 구상, 기획, 설계 단계에서부터 생각해두지 않으면, ISO 26262에 대응하는 제품은 없을 것입니다. ISO 26262는 요구 항목을 내세우는 것 만으로 200가지 가량이며, 바탕이 되는

IEC 61508과는 차원이 다릅니다. 물론, 지금까지의 품질 관리 활동과 오버랩 되는 부분도 있지만, ASIL 등 지금까지는 없던 개념에 대응해야 합니다. 빠른 시일 내에 지금까지의 활동과의 차이를 판별하여 준비하는 것이 좋습니다.

구체적으로는, 안전 기능이라는 것이 대 전제로, 그것이 어떠한 방향으로 전달되고 있는가, 모두 관련지어져 있어서 반드시 관리되지 않으면 안되고, 관련 문서의 한 문장 한 구절이 어떠한 형태로 바뀌어 왔는가 라는 것도 추적하여 설명할 수 없으면 안 됩니다. 안전에 대한 사고 방식을 몸에 익히는 등 기술자의 교육도 필수입니다.

자동차에는 차종에 따라서는 100 이상의 CPU가 포함되어, 수많은 안전 기능이 존재합니다. 각각의 개발 단계 등도 설명 가능하도록 하지 않으면 안됩니다.

진화하는 규격의 움직임을 내다보고 대응을.

- 자동차의 고성능화가 이러한 규격을 선동하고 있는 것 같네요. 앞으로의 전망을 알려주세요.

佐藤 : 지금의 자동차는 아직 멈추기도 하고, 돌고 있는 기능의 수행 시스템에 기계적인 결함이 존재합니다. 안전은 최종적으로 이 기계적 부분에 의거할 수 있습니다. 하지만, 비행기나 선박처럼 자동차 시스템도 완전 전자화 될 가능성이 있습니다. 그렇게 되면, 완전히 기능 안전의 세계가 됩니다. 기능 안전의 의식을 높이지 않으면 일본의 기술은 위험하겠죠.

竹市 : 실제, 제조 회사로서는 ISO 26262에 대응한 설계나 개발의 방법 등에 익숙해 지면, 다음에는 새로운 기술에 도전하게 될 것입니다. 그것을 생각해보면, 기능 안전은 꽤 중요합니다. 지금, 국내 제조 회사는 ISO 26262에 대해서, 어떻게 해야 하는 것인지 부정적인 반응이지만, 이것을 기회로 기능 안전 규격을 이용하여 고부가 가치 기술에 의한 경쟁력도 늘겠죠.

DNV에서는 그 때문에 지원을 전문가인 佐藤교수를 기술 고문으로 맞이하고 충실하게 배우고 있습니다. 기계 산업에 의해 인증 기관이 적극적으로 관련된 정도의 구속력은 지금은 없지만, 일본에서는 기능 안전의 사고 방식에 이해가 깊지 않아서, 국제적인 논의에 참가하는 사람도 적습니다. 우리들은 일본 국내에서만 통용되는 사고 방식에 빠져들지 않고, 세계 수준에 통용하는 정보를 제공하고 그 시선에서 이야기하고 향후 자동차 산업의 발전에 공헌해 가고 싶습니다.

현 시점에서는 보급 활동을 중심으로 움직이고 있지만, 먼저 평가에 의해서 자사가 어느 정도인가 인식하는 것을 권장하고 있습니다. 제 2자에 의한 확인은 사내의 독립적인 부서에서의 실시가 가능하지만, 사내의 인재로는 대응하기 어려운 경우도 있겠죠. 그 때, 우리를 이용하여 평가 해주셨으면 합니다. 또, 트레이닝도 실시하고 있으므로, 보다 올바른 인식을 얻기 위해서 활용해 주셨으면 좋겠네요.

규격에 대해서는, 개정이 진행되는 등 움직임이 조금씩 바뀌어 가고 있습니다. 기능 안전의 해석도, 자

동차 기술도, 시시각각 진화하고 있습니다. 그래서 판단이 어려운 다음 규격의 방향성도 내다보지 않으면 미리 준비할 수 없습니다. 전문 기관이나 전문가의 충고는 빼놓을 수 없겠죠. 그러한 전문가의 힘을 빌리고, 잘 임하고 싶습니다.

원문 | http://monoist.atmarkit.co.jp/mn/articles/1204/09/news001.html