일 반 논 문

자동차 전용 기능 안전 국제 규격 ISO 26262에 대응한 도시바의 대처

■ 야마우치 노부유키 ■ 아오미네 료코 ■ 요미야 히사시

2011년 11월에 발행된 자동차 전용 기능 안전에 관한 국제 규격 ISO 26262 (국제 표준화 구축 규격 26262)에의 대응은, 차재 사업에 있어서 필수가 되었다. 이 규격에는, 하드웨어 고장 이외에 소프트웨어 기인에 의한 시스템 장해에 관해서도 충분한 주의를 요할 것이 요구되고, 소프트웨어 개발 프로세스의 확립이 열쇠가 되고 있다.

도시바는 이러한 대응을 위해, ISO 26262 소프트웨어 개발 프로세스에 관하여 제 3자 인증을 2012년 3월에 취득했다. 그 때, 현장에 용이하게 흡수시키기 위해 프로세스 책정은 기존 프로세스를 바탕으로 하는 등 노력을 기울였다. 현재, 프로세스를 실 제품에 적용하는 대응을 추진하고 있다. 또 해외 거점을 포함한 도시바 그룹 차재 관련 부문의 기능 안전 대응력 강화를 위해, 전사적으로 교육 및 지원 체제를 구축 중이다.

1. 머리말

자동차 전용 기능 안전에 관한 국제 규격 ISO 26262가 2011년 11월에 정식 발행된 것으로, 차재 사업에 변화가 나타나기 시작했다. 고객의 요구사항에 기능 안전이 반영되는 것은 당연한 것이며, 개발 현장에서도 그 대응을 가속시킬 필요가 있다. 이것에는 전장 차량의 개발이 본격화 한 것이 배경이며, 편입된 소프트웨어에 의한 전자 제어의 비율이 증가한 것이 요인의 하나이다.

2. 소프트웨어 개발 프로세스 인증의 취득

당사는, ISO 26262에 관한 소프트웨어 개발 프로세스 인증을 2012년 3월에 취득했다. 이 인증은, 당사의 소프트웨어 개발 프로세스가 ISO 26262 규격의 요구에 따라, 또 당사가 규정된 프로세스에 따라 소프트웨어 개발을 확실히 실시 가능한 기업인 것을 증명하는 것이다.

여기서는, 소프트웨어 개발 프로세스 인증을 취득하는 것에 의의를 두고 개발 프로세스 책정의 단계, 또 프로세스 인증 취득에 따라 가능한 기능 안전 솔루션에 대해서 말한다.

2.1 소프트웨어 개발 프로세스 인증의 의의

ISO 26262에 있어서, 고장은 2종류로 분류된다. 제품의 개발 및 제조 과정에 설계 미스나 프로세스의 불비 등에 따라 발생하는 장해가 원인이 되는 “시스테마틱 고장”과, 제품 운용 중에 발생하는 하드웨어 요소의 장해가 원인이 되는 “랜덤 하드웨어 고장”이다. 기능 안전을 고려한 시스템에서는, 안전 관련 기능에 관한 이들 두 가지의 고장에 대책을 세우는 것이 요구된다.

단지, 소프트웨어의 고장은, 시스테마틱 고장만이 있다라고 한다. 왜냐하면 소프트웨어는 하드웨어와 같이 운용 중에 갑자기 파손되는 것이 아니라, 모든 소프트웨어 장해는 개발 단계에서 잠재적으로 존재하고 있는, 이른바 소프트웨어의 결함에 의한 것이다. 이 때문에, ISO 26262의 소프트웨어의 요구는, 시스테마틱 고장을 막기 위한 것이며, 어느 인증 기관에 의하면 개발 프로세스에 대한 것이 모든 요구의 85%라고 한다.

따라서, ISO 26262 요구를 만족시키는 소프트웨어를 개발하기 위해서는, ISO 26262 요구에 준거한 소프트웨어 개발 프로세스를 책정하고, 이에 따른 개발을 실시하는 것이 가장 중요하다고 말한다.

2.2 소프트웨어 개발 프로세스 책정의 단계

2.2.1 프로세스 책정 방침

소프트웨어 개발 프로세스의 책정 방침으로, 완전히 새로운 프로세스를 하나부터 만드는 것이 아니라, 이미 개발자가 운용하고 있는 당사 기존의 소프트웨어 개발 프로세스를 바탕으로, ISO 26262 요구를 보완하는 것이다. 이것은, ISO 26262 요구가 원래 Automotive SPICE[i]이나 CMMI[ii]등의 일반적인 소프트웨어 개발 프로세스와 친화성이 있는 것부터, 당사의 기존 프로세스와 크게 차이가 없는 것이 추측 가능하기 때문이다. 또, 무엇보다도 책정한 프로세스를 실제의 개발에 적용하지 않으면 의미가 없다. 현장의 개발자가 저항감 없이 개발 가능하도록, 가능한 한 기존 프로세스의 형태를 남길 방침이다.

또, ISO 26262를 상세하게 이해하고 있지 않은 개발자라고 하더라도, 프로세스 문서에 기재한 지시의 순서와 성과물 체크리스트 및 성과물 템플릿의 사용에 따라, ISO 26262 요구에 필수적으로 따르게 되는 구조를 책정했다.

2.2.2 Gap 분석

ISO 26262 요구와 기존의 소프트웨어 개발 프로세스의 Gap 분석을 실시했다. Gap 분석의 대상은, ISO 26262의 소프트웨어 요구에 관련한 부분이며 구체적으로는 ISO 26262 Part2 관리의 소프트웨어 개발에 관련한 부분, ISO 26262 Part6 제품 개발: 소프트웨어 레벨의 모든, 및 ISO 26262 Part8 지원 프로세스의 소프트웨어 개발에 관련한 부분이다.

이 범위의 규격에 기재되어 있는 모든 요구 사항에 당사의 기존 프로세스가 대응하고 있는가, 대응하고 있는 경우는 기존 프로세스의 대응 항목 (문서 명, 구체적인 기재 항목)을 기록하고, 대응하고 있지 않은 경우는 부족 항목으로 기록하고, 분석 결과로서 정리되었다.

2.2.3 Gap 분석 결과에 의한 시책

Gap분석의 결과, 당사의 기존 프로세스의 주된 부족 부분은 세 가지로 크게 구분되는 것으로 나타났다. 이들의 Gap 분석에 대해서, 아래와 같이 대책을 검토하고 기존 프로세스에 추가했다.

첫 번째, 기능안전 특유의 개발 관리에 관한 요구이다. ISO 26262는, 기능안전에 관련한 활동의 계획과 관리를 실시하는 안전 관리자를 임명하는 것을 요구하고 있다. 또, 안전 계획이나 안전 분석의 리뷰어와, 안전 감사의 실시자 에게는, 프로젝트나 조직에서의 독립성이 요구되고, 그 독립성 레벨에의 요구는 요구되는 ASIL (Automotive Safety Integrity Level)에 따라 다르다. 이러한 개발 관리에 관한 요구는 기능안전 특유이며, 기존 프로세스에는 없었던 것이다. 거기서, 새롭게 안전 관리자의 역할과 스킬을 규정하고, 프로젝트에 반드시 안전 관리자를 임명하는 것을 규정 문서에 기재했다. 이들에 대해서, 프로젝트 계획서의 체크리스트에 체크 항목을 만들고, 계획 공정의 리뷰에서 확인 가능하도록 했다.

두 번째는, 엔지니어링에 관한 항목이다. 설계나 실장(구축)의 원칙은, 기존 프로세스에서 규격 요구를 거의 만족시키고 있지만 요구 사양 및 설계 사양의 표기 방법이나 테스트 방법, 각 성과물 리뷰 방법 등 ASIL 마다 추천되는 방법은 대책이 필요하다. 이들의 방법의 선택 기준을 규정 문서에 기재하고, 각 성과물 리뷰 시에 사용하는 체크리스트에 체크 항목을 만들었다. 또, 아키텍처 레벨에서의 안전 분석이나 다른 ASIL 레벨의 요소간의 독립성 확보 등, 기능안전 설계를 위한 요구에 대해서도 체크 항목을 만들었다.

세 번째는, 소프트웨어 툴 인정과, 소프트웨어 컴포넌트 인정, 교정(calibration)의 취급 등 ISO 26262 특유의 요구 군(群)이다. 이들에 대해서도, 먼저 ISO 26262 규격의 요구 내용을 이해하고, 당사로서 어떻게 대처할까를 검토했다. 또, 소프트웨어 개발에 운용할 소프트웨어 툴 인정과 소프트웨어 컴포넌트 인정의 가이드라인을 작성하여 규정 문서에 추가했다.

2.2.4 pilot 프로젝트에 의한 프로세스의 시행

책정한 프로세스를 실제로 실시 가능한 것을 나타내기 위해, 이 프로세스에 따라 기능 안전 대응의 소프트웨어 프로젝트를 시행했다. 최고 레벨 ASIL D의 기술 안전 요구를 가정하여, 안전 계획에 따라서 요구 분석, 설계, 실장(구축) 및 테스트를 실시하고, ISO 26262가 요구하는 활동의 성과물을 작성했다.

2.2.5 인정 기관에 의한 감사

책정한 소프트웨어 개발 프로세스는, 독일의 인증 기관인 TUV SUD Automotive에 감사를 의뢰했다. 모든 규정 문서, 성과물 템플릿, 체크리스트 및 가이드라인과 pilot 프로젝트의 모든 성과물에 대해서 감사를 받았다. 인증 기관은 주로, ASIL마다 추천되는 기술의 선택 기준이 명확하게 되어있는가, 또 그들의 기술이나 방법을 개발자가 확실하게 실행 가능한가를 중요시 했다. 이들에 대해서, 기술 선택 기준을 명확하게 규정하고, 기술 교육 커리큘럼이나 관련 자료의 정비에 따라 현장의 엔지니어가 필요에 의해 기술을 배우고 실천 가능한 체제를 갖추고 있는 것을 나타냈다. 이 감사에 따라, 당사가 개발 현장에서 ISO 26262에 대응한 개발을 확실히 실행 가능한 것이 인정되었다.

2.3 프로세스 인증에 따라 실현하는 기능 안전 솔루션

당사는 현재 ISO 26262 인증을 취득한 소프트웨어 개발 프로세스에 준거하여 당사의 기능 안전을 고려한 마이콤용의 라이브러리를 개발 중이다. 이 라이브러리 제품은, ISO 26262 준거를 나타내는 증거와 함께 유저에게 제공할 예정이다. 또, 기능 안전을 고려한 마이콤은 하드웨어 고장을 자가 진단하는 회로를 갖추고 있다. 이 기술은 IEC 61508 (국제 전기 표준회의 규격 61508)의 SIL 3 (Safety Integrity Level 3)를 실현 가능한 것으로, 2009년에 TUV SUD Automotive로부터 높은 평가 (테크니컬 레포트 수령)을 받고 있다 (그림 1).

고장 진단 기능을 갖춘 마이콤과 인증 프로세스에 준거하여 개발한 마이콤용 라이브러리를 제공하여, 유저는 마이콤의 고장 진단 기능을 용이하게 개발할 수 있다. 또, 유저 시스템 전체에서의 ISO 26262 준거를 나타내는 evidence (safety case) 정비의 일부분을 담당하는 것이 가능하게 된다 (그림 2).

기능 안전은, 마이콤 등의 부품만으로 실현 가능한 것뿐만 아니라, 시스템 전체의 안전 분석에 근거하여 설정된 최상위의 안전 목표를 달성하는 것에 따라 실현되는 것이다. 시스템 레벨에서 설계된 안전 메커니즘은, 시스템을 구성하는 하드웨어 및 소프트웨어 레벨에 요구로 상세화된다. 마이콤이나 소프트웨어에 기능 안전을 서포트하는 기능이나 증거가 갖추어져 있으면, 시스템 전체의 설계를 용이하게 하고 개발 공수를 절감할 수 있다.

이렇게, 하드웨어와 소프트웨어의 연계에 의한 기능 안전 실현의 솔루션은, 유저에 따라 고도의 기능 안전 대응 시스템을 실현하는 동시에, 개발 공수의 절감에 공헌하고 있다.

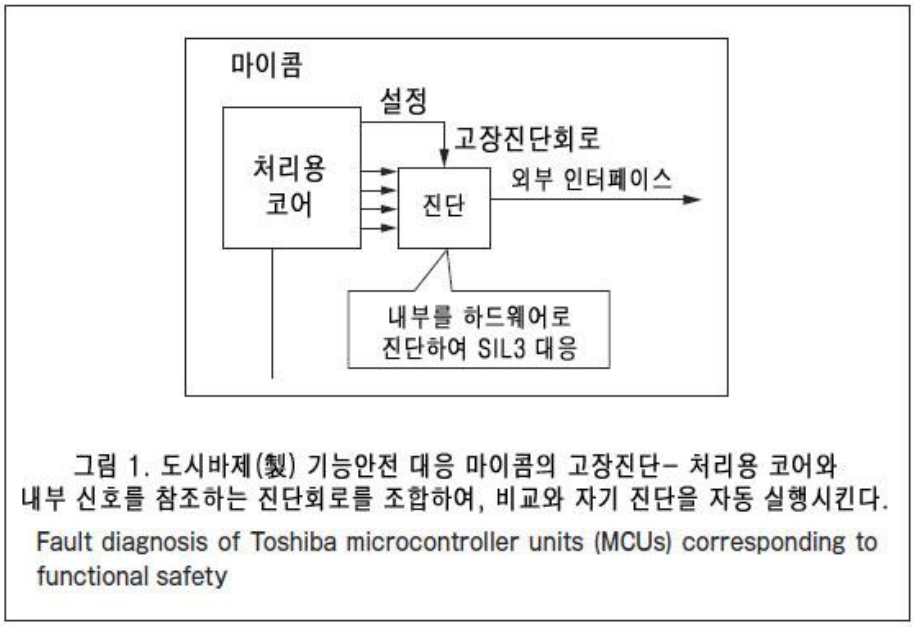

그림 1. 도시바제(製) 기능안전 대응 마이콤의 고장진단– 처리용 코어와 내부 신호를 참조하는 진단회로를 조합하여, 비교와 자기 진단을 자동 실행시킨다.

Fault diagnosis of Toshiba microcontroller units (MCUs) corresponding to functional safety

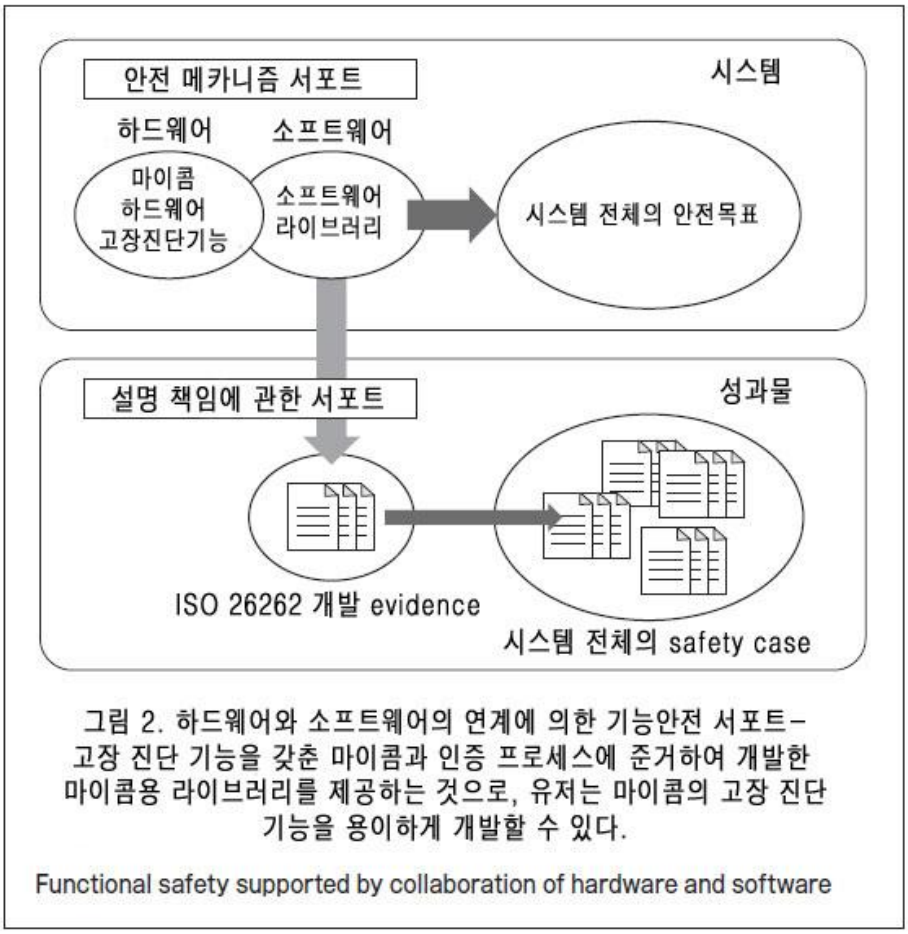

그림 2. 하드웨어와 소프트웨어의 연계에 의한 기능안전 서포트– 고장 진단 기능을 갖춘 마이콤과 인증 프로세스에 준거하여 개발한 마이콤용 라이브러리를 제공하는 것으로, 유저는 마이콤의 고장 진단 기능을 용이하게 개발할 수 있다.

Functional safety supported by collaboration of hardware and software

3. 도시바 그룹 전사의 개발 프로세스 구축에의 대처

도시바 그룹에서는, 다양한 사업 부문이 전사 조직과 함께 차재 전용 제품을 개발하고 있으며, 제품 분야 별 및 전체 제품 개발 프로세스를 갖고 있다. ISO 26262에 준거한 제품 개발을 추진하기 위해서는, 이들의 사업 부문이나 전사 차원의 개발 프로세스가 ISO 26262에 준거할 필요가 있다. 하지만, 개발 프로세스의 수정이나 확인을 위한 시간 및 비용이 문제가 되고 있다.

2장에서 말했던, ISO 26262에 대응한 소프트웨어 개발 프로세스를 그대로 적용하면 제품 분야의 차이나 각 사업 부문과 전사 조직이 갖고 있는 개발 프로세스에 관한 노하우를 계승할 수 없다.

그래서 회사에서는, 기능 안전을 전문으로 하는 전사적인 조직이, 사업 부문이나 전사 그룹의 각각의 개발 프로세스를 ISO 26262에 대응시키기 위한 지원을 실시하고 있다. 이것으로, 개발 프로세스의 수정이나 확인을 위한 시간 및 비용의 문제를 해결하고 있다.

개발 프로세스의 구축은, 다음의 순서대로 실시한다.

(1) 기존의 개발 프로세스를 분석하고, ISO 26262에 대응한 새로운 프로세스의 틀을 결정한다.

(2) 기존의 개발 프로세스에서 만족시키지 못한 ISO 26262의 요구 사항을 추출한다.

(3) (1)에서 결정한 새로운 프로세스에 (2)에서 추출한 만족시키지 못한 요구 사항을 추가하고 수정한다.

(4) (3)에서 얻은 새로운 프로세스가, ISO 26262의 요구 사항을 만족시키고 있는가를 확인한다.

(5) Pilot 프로젝트에서 새로운 프로세스를 시행한다.

(1)의 새로운 프로세스의 틀이라는 것은, 기존의 개발 프로세스와, ISO 26262에서 결정된 용어와의 대응을 정의하는 것, 안전 관리자 등 ISO 26262에서 요구되는 역할을 추가하는 것, 또는 안전 라이프 사이클을 만족하기 위한 단계를 추가하는 것의 3가지가 있다.

(1)은 사업부문이나 전사 조직과 공동으로 추진하고, (2)와 (4)는 전사적 조직이 중심으로 추진하고 있다. (3)에 대해서는, 사업 부문마다의 제품 분야의 차이나 노하우를 흡수하면서 사업 부문이 개발해간다. 필요에 의해, 전사적 조직이 실천으로 활용하는 것을 결정한 가이드나 템플릿의 개발을 지원하고 있다. 가이드는, 예를 들어 FMEA (Failure Mode and Effects Analysis)나 HAZOP (Hazard and Operability Study) 등의 리스크 분석 방법의 실천 순서를 기입한 문서이다. 템플릿은, ISO 26262에 준거하기 위해 기재하지 않으면 안 되는 내용에 누락되지 않도록 포맷을 정한 것이다.

이렇게 해서 구축한 사업 부문과 그룹 전사 각각에 특화한 ISO 26262 소프트웨어 개발 프로세스가 실제로 운용 가능한 것을, pilot 프로젝트에 의해 확인하고 있다.

이 밖에 전사적 조직에서는, ISO 26262 프로세스를 구축할 때에, 동시에 Automotive SPICE나 CMMI에 대해서 전문가에 의한 지원이 가능한 체제를 정비하고 있다.

이러한 메리트는, 개발 프로세스 구축까지의 시간과 비용 이외에, 다음 2가지에 정리하는 것이 가능하다.

(1) 사업 부문은 요구사항의 추가 (전기 (3))에 주력할 수 있다.

(2) Automotive SPICE나 CMMI에도 준거한 개발 프로세스의 구축이 가능하다.

이 대응에 의해, ISO 26262에 대응한 프로세스의 구축을, 사업 부문이나 전사 그룹만으로 프로세스

를 구축하는 경우에 비교하여, 약 1/2의 기간으로 실현하고 있다.

4. Competence 의 구축

ISO 26262에 준거한 제품 개발에서는, 안전 관리자나 개발자의 육성과 적성의 관리가 중요하다. 하지만, 이들을 도시바 그룹의 각 사업부문에서 실시할 경우, 개발자 육성을 위한 교육을 독자적으로 준비하기에는 시간이 너무 많이 걸린다. 제 3자 인증 기관 등의 외부에 위탁할 때에는 교육의 실시 시기에 제약이 있거나, 비용이 너무 많이 들거나 하는 문제가 있다.

당사에서는, ISO 26262에 관한 competence를, 개발 프로젝트에서의 역할에 의해 필요한 직무 경험(종류와 연수) 및 수강해야 하는 교과목을 정하여 육성하고 관리하고 있다.

교육에 관해서는, ISO 26262의 교육을 자사에서 개발하고 있다. 그 교육 체계를 그림 3에 나타냈다. 여기서는, 직무 경험에 관한 요건은 생략하였다.

“기능안전 설계교육 기초편”은, 안전에 대해서 용어와 개념 등을 넓게 이해하기 위한 교육으로, IEC 61508을 주로 한 교육 내용이다. 기능안전에 대해서 기초 지식뿐만 아니라, FMEA나 HAZOP등의 리스크 분석 방법에 대해서, 연습을 통하여 습득할 수 있는 것도 특장이다.

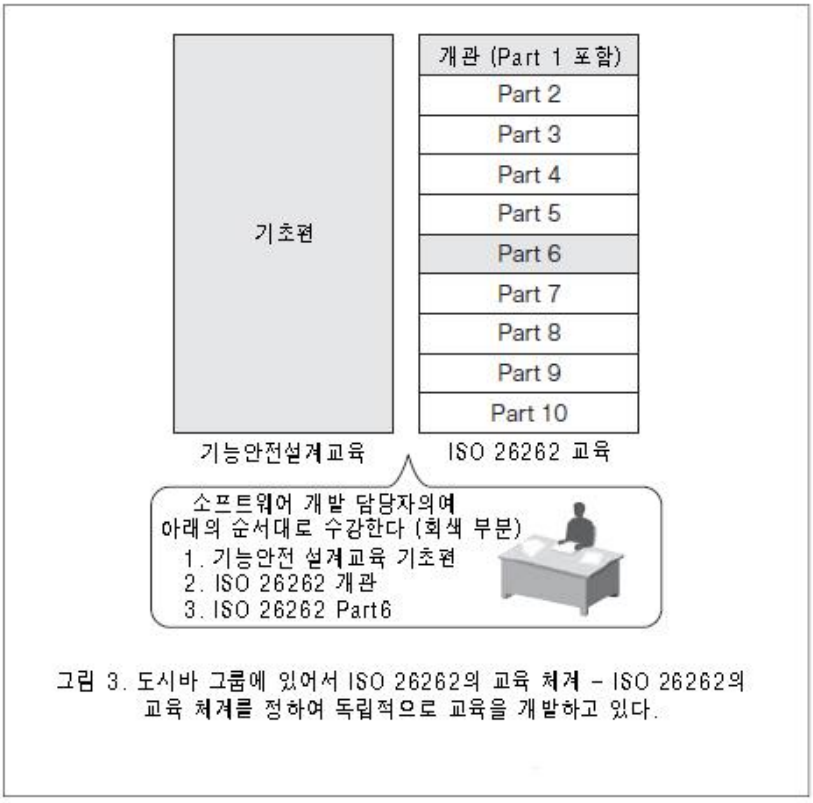

그림 3. 도시바 그룹에 있어서 ISO 26262의 교육 체계 – ISO 26262의 교육 체계를 정하여 독립적으로 교육을 개발하고 있다.

“ISO 26262 개관”은, ISO 26262에 대해서 규격의 구성이나 내용을 단기간에 습득할 수 있다. 그 외에, ISO 26262의 각 Part에 대응한 교육을 준비하고 있다.

이들 교육은, 개발 프로젝트에서의 역할에 의해, 개발 프로젝트의 개시 전까지 적절한 타이밍으로 수강할 수 있도록 운용하고 있다.

이들의 교육 체계의 메리트는, 다음과 같다.

(1) 안전 일반이나 교육 안전에 관한 기초적인 교육을 준비하는 것으로, 전 개발자의 안전에 대한 지식을 높이는 것이 가능하다.

(2) 개발 프로젝트의 개시 시기에 맞춘 교육을 사업 부문 내에 빠르게 실시 가능하다.

(3) 개발 프로젝트에서의 역할에 의한 인재를 효율적으로 육성 가능하다.

이 교육은, 차재 전용 제품을 개발하는 사업 부문이나 그룹 회사에 대해, 국내뿐만 아니라 인도 등 해외에서도 실시하고 있고, 안전 관리자나 개발자를 적절히 육성하고, 적성을 관리하고 있다.

5. 마치며

당사는 기능안전에의 대처의 일환으로, ISO 26262에 대응한 소프트웨어 개발 프로세스에 대해서 제3자 인증을 취득했다. 또, competence를 만족한 안전 관리자나 개발자를 육성하는 체제도 구축 중이다. 이들을 살려, 또 반도체와 소프트웨어 및 그들의 교육의 상승 효과를 배경으로, 앞으로도 자동차의 안전성 향상에 공헌하고 싶다.

문헌

(1) 야마우치 노부유키 외. 자동차의 전자화, 전동화를 지지하는 소프트웨어 기술과 과제. 도시바리뷰. 66, 2, 2011, p.17-20.

(2) 요미야 히사시 외. 소프트웨어를 중심으로 한 안전설계기술. 도시바 리뷰. 65, 7, 2010, p.37-40.

山内　信之　YAMAUCHI Nobuyuki
사회 인프라시스템 사 철도, 자동차 시스템 사업부 자동차 시스템
통괄부 참사. 자동차 전용 기반 소프트웨어 기술의 개발에 종사.
Railway & Automotive Systems Div.

青峰　亮子　AOMINE Ryoko
semiconductor&storage사 시스템, 소프트웨어 추진센터
소프트웨어개발기술 담당 주무자(主務). 편입용 소프트웨어 개발기술
및 개발 프로세스의 관리 업무에 종사.
System & Software Solution Center

余宮　尚志　YOMIYA Hisashi
소프트웨어 기술 센터 소프트웨어 설계기술 개발 담당 주무자(主務).
소프트웨어 설계기술의 연구, 개발과 소프트웨어 개발 프로젝트의
관리 업무에 종사. 정보처리학회 회원.
Corporate Software Engineering Center

[i] Automotive SPICE는, Verband der Automobilindustrie e.V.

[ii] CMMI는, 미국 카네기멜론대학의 등록상표.