본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

2013년 6월 10일 15시 30분 갱신

중소 공급자를 위한 실천적 ISO26262 도입 (3):

최초의 난관 “프로세스 구축”에 어떻게 도전해야 하는가

글: DNV비즈니스・어슈어런스・재팬기능안전부팀 | 출처: MONOist

번역: 이채원・카이젠컨설팅

중소 공급자를 대상으로, ISO 26262에 전념하기 위한 실질적인 방안에 대해서 소개하는 본 연재. 제 3회는, ISO 26262를 추진하는데 있어서의 최초의 난관인 “프로세스 구축”에 대해서 해설합니다. “테일러링”이나 “DIA (개발 인터페이스 협정)”이라는, ISO 26262에서 사용하는 용어에 대해서도 다루도록 하겠습니다.

저번 회에서는, 기능안전 대응에 맞춘 준비 작업에 초점을 맞춰 해설을 했습니다. 이번 회에서는, 도입에 맞춘 최초의 난관인, (본격적인 작업이기도 한) 기능안전 프로세스의 구축에 대해서 해설하고자 합니다.

자사의 책임 범위

그림 1은 ISO 26262에서 정의하고 있는 제품의 기본 구성의 전형적인 모습입니다.

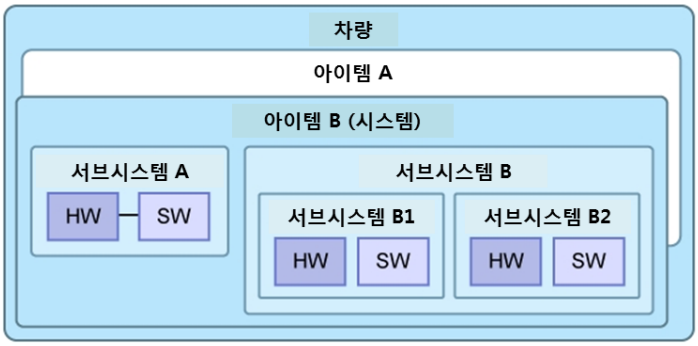

그림 1 차재 시스템의 전형적인 구성

자사 전용의 기능안전 프로세스를 구축해야 하는 범위는 (당연한 이야기입니다만,)자사에서 개발하는 제품이 ISO 26262 대상이 되는 차재 시스템 (아이템) 중에서 어떠한 위치에 있는 지에 크게 의존하게 됩니다. 자동차 제조 회사라면, ISO 26262의 모든 Part를 커버하는 프로세스가 필요할 것입니다. 대기업 공급자는, 자동차 제조 회사와 거의 동등한 프로세스가 필요하게 될 경우도 있고, 시스템 개발

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

(Part4) 이후의 프로세스에 대해서만 대응할 수 있는 경우도 있습니다.

본 연재의 대상인 중소 공급자는, 그림 1의 서브 시스템 A나 B, 서브 시스템 B1이나 B2, 혹은 하드웨어 (HW)나 소프트웨어 (SW)만을 담당하고 있는 경우가 많을 것이라고 생각합니다. 이 경우, 필요한 기능안전 프로세스는, 아마도 시스템 개발 (Part4) 이후, 경우에 따라서는 HW 개발 (Part5)나 SW 개발 (Part6)을 중심으로 한 프로세스*1)에서 대응 가능할 지도 모릅니다.

1) 물론, 제품 개발의 관리나 지원을 규정한 Part2나 Part8, Part9의 프로세스도 필요합니다.

기능안전 프로세스를 구축한 후에는, 자사 제품의 담당 범위가 ISO 26262 요구사항의 어느 Part에 맞는가를 명확하게 해 둘 필요가 있습니다.

특히 중소 공급자의 경우, 인적으로도 예산적으로도 한정된 리소스 속에서 효율 좋은 대응 작업을 해 나가야 하기 때문에, 타겟을 분명히 선정하는 것이 중요합니다. 미리, 다양한 제품이나 개발 패턴을 정의하고, 모든 케이스에 대응 가능한 프로세스를 만드는 전략도 중장기적으로 보면 의미가 있겠죠. 하지만, 최소한의 노력으로 시급하게 기능안전 대응을 실현하는 것에 무게를 둔다면, 먼저 현재 ISO 26262 추진이 가능한 대상 제품이나 개발 패턴에 초점을 맞춰, 그 케이스에 대응한 프로세스를 구축하는 쪽이 현실적입니다.

표 1은 제품 개발에 있어서 담당 범위의 기본 패턴을 나타낸 것입니다.

대상	차량/아이템	시스템	서브시스템	HW	SW
대상프로세스	Part3 Concept	Part4 System	Part4 System	Part5 Hardware	Part6 Software
담당	OEM	OEM, Tier1	Tier1, Tier2	HW 제조 회사	SW 벤더
주요 작업	아이템 정의, H&R, ASIL 할당, FSC 정의	TSC 정의, 시스템 설계, 안전 분석, 아이템 통합, 안전 타당성 확인, 기능안전 평가	TSC 정의, 시스템 설계, 안전 분석, HW/SW 통합	HW 안전 요구, HW 설계, 안전 분석, HW 통합	SW 안전 요구, SW 설계, 안전 분석, SW 실장, SW 테스트

표 1 제품 개발의 전형적인 업무 분담

실제 제품 개발에 대해서는 표 1에 나타낸 것과 같이 대략적이고 고정된 담당 구분이 아니라, 제품마다 작업 항목 레벨에서의 분배가 이루어지게 된다고 생각하면 됩니다. 이 경우, ISO 26262의 각 Part의 범위를 보고 자사 전용의 담당 범위를 선정하는 것보다, 실제 계약 조건 또는 지금까지의 실적을 바탕으로 한 자사의 담당 범위 (책임 범위)를 정의하여 선정하는 것이 현실에 입각한 프로세스를 만들 수

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

있다고 생각합니다.

계약상 없어서는 안될 프로세스 영역 (1)

ISO 26262의 Part8의 5절 "분산 개발에서의 인터페이스"에는, 제품 개발에 앞서 자동차 제조 회사와 공급자, 혹은 공급자 간에 합의해 두어야 할 다양한 요구사항이 규정되어 있습니다[*2)]. 이 중에서는, 개발을 의뢰하는 데 필요한 기능 사양 등의 기술 정보뿐만 아니라, 담당 범위나 그 프로세스, Tailoring (칼럼 기사 "프로세스의 Tailoring"을 참조)의 내용 등의 관리적인 요소도 포함되어 있습니다. 즉, 이제부터 계약하는 기능안전 관련 제품에서는, 적어도 여기서 나타내고, 합의하고, 할당된 담당 범위 (책임 범위)의 작업에 관해서는 자사의 기능안전 프로세스로써 구축할 필요가 있는 것입니다.

2) 이 합의 사항을 개발 인터페이스 협정 (DIA) 이라고 합니다.

프로세스의 Tailoring

Tailoring 이란, 요구되고 있는 프로세스를 일정 제약 범위 속에서 순서를 바꾸거나, 통합하거나, 생략하는 것을 허가하는 사고 방식으로, 프로세스를 무제한으로 customizing (시판되고 있는 소프트웨어 등의 기능을 자신이 사용하기 편하게 일부 변경하는 일)하는 것은 아닙니다. 당연히, Tailoring 할 경우에는, Tailoring 사유를 나타낼 필요가 있습니다. 안이한 작업의 생략이나 변경이 가능한 것을 의미하는 것도 아닙니다.

여기서 말하는 Tailoring의 내용은, Tailoring한 결과의 개발 프로세스를 나타냅니다. Tailoring 하지 않으면, 원래의 기능안전 개발 프로세스가 이에 해당합니다. 작업의 통합이나 전략, 지원 툴에 의한 대체 등이 있으면, 그 결과 (프로세스)가 Tailoring의 내용이 됩니다.

부품 인정에 의한 재사용

기본적으로는 위와 같은 사고 방식으로 담당 범위를 추출, 관련한 규격 요구사항을 만족 가능하도록 기능안전 프로세스를 정의해 가게 됩니다만, 몇 가지 예외적 취급이 있으니, 조금 언급해 두고자 합니다.

보통, 기능안전 관련 제품을 개발하는 경우, 대응하는 규격의 Part 별 요구사항을 만족시킨 프로세스로 개발 작업을 실시하지 않으면 안됩니다. 하지만, ISO 26262의 Part8의 12절과 13절에는, 각각 "SW 컴포넌트 인정"과 "HW 컴포넌트 인정"에 대한 조건과 인정 방법이 기술되어 있습니다. 이 조건에 맞는 경우에만, 기능안전 관련 제품의 구성 요소가 될 수 있으며, 전면적인 규격 대응을 하지 않더라도 인정하겠다 라고 여겨지고 있는 것입니다.

예를 들어, 중간 정도의 복잡함을 지닌 HW 컴포넌트나 시판되고 있는 소프트웨어 라이브러리 등은, 각각 대응하는 Part (HW라면 Part5, SW라면 Part6)의 요구사항에 준거한 제품인 것을 증명하지 않더

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

라도 ISO 26262의 Part8의 인정 조건을 만족하고, 부품을 사용하는 측으로부터 부품에 대한 인정을 받았을 경우, 기능안전 관련 제품으로 사용해도 좋다 라는 것입니다. 이 경우, 이들 부품만을 제공하고 있는 공급자는 기능안전 프로세스를 구축할 필요는 없게 됩니다. 하지만, 이 부품에 대한 책임은 부품을 사용하는 측이 갖게 되기 때문에, 제공하는 측에서도 가능한 안전 대책을 세워둘 필요가 있고, 안전에 대한 그 나름의 논증을 확보하고 있어야 합니다.

그러나, 중간 정도의 복잡함을 지닌 HW 컴포넌트에 대해서는, 무엇을 가지고 중간적인 복잡함이라고 하는가 등의 명확한 구분이 실제로는 어렵다는 것이 매우 고민스러운 점입니다. 또, SW 컴포넌트에 대해서도 재사용 기술은 오랜 세월 소프트웨어 업계가 전념해 오고, 좀처럼 성과를 낼 수 없는 어려운 주제이기도 하기 때문에, 간단히 비용 면에서 본 안이한 재사용이 되지 않도록 고려가 필요하겠죠. 어쨌든, 인정에 의한 메리트나 그에 따른 리스크/책임 등, 부품을 사용하는 측과 공급 측에서 신중하게 검토할 필요가 있습니다.

“ARIANE5”의 사고

유럽 우주 기구 (ESA)가 1996년에 쏘아 올린 “ARIANE (아리안) 5” 로켓이 발사 직후에 폭발한 사고가 있었습니다. 이것은, 전 세대의 “ARIANE4”에서 사용된 실적이 있는 소프트웨어를 재사용한 것이 직접적인 원인이 된 것이라고 이야기들 합니다. 수정하지 않은 완전한 재사용 이였지만, 그 소프트웨어에 데이터를 나타내기 위해 전달하는 측의 센서가 새롭게 바뀌었고, 형식이 다른 데이터를 받은 소프트웨어 측이 오작동 해버렸기 때문에 사고가 발생했습니다. 물론, 이러한 중대한 실수를 어째서 끝까지 알아채지 못했던 것인가 하는 것은 프로세스 상의 문제도 있지만, 소프트웨어의 재사용에 관한 매우 중요한 교훈이 된 사고였습니다.

표 2는 예외적인 것을 포함한 공급자의 기본 패턴과, 여러 가지로 필요한 기능안전 프로세스를 정리한 것입니다.

공급자	공급자로서 필요한 기능안전 프로세스
HW 의 기본 부품을 공급하는 공급자 (예:트랜지스터나 저항기 등)	특별히 없음 (기존 프로세스)
HW 컴포넌트로써 인정된 제품을 공급하는 공급자	ISO26262 : Part8 13 절의 인정에 필요한 정보를 제공하기 위한 프로세스 (예:테스트 기록이나 분석 결과 등)
SW 컴포넌트로써 인정된 제품을 공급하는 공급자	ISO26262 : Part8 12 절의 인정에 필요한 정보를 제공하기 위한 프로세스

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

공급자	공급자로서 필요한 기능안전 프로세스
복잡한 HW 컴포넌트를 공급하는 공급자	ISO26262 : Part5 를 중심으로 한 기능안전 프로세스
소프트웨어 시스템을 공급하는 공급자	ISO 26262 : Part6 을 중심으로 한 기능안전 프로세스
시스템 (서브 시스템)을 공급하는 공급자 (예:SW 가 포함된 센서 등)	ISO26262 : Part4, Part5, Part6 을 중심으로 한 기능안전 프로세스

표 2 공급자에게 필요한 기능안전 프로세스

계약상 없어서는 안될 프로세스 영역 (2)

본 연재에서는, 기능안전 프로세스를 필요로 하는 중소 공급자를 위한 해설이 주안점이기 때문에, 예외적인 논의는 여기까지 하고, ISO 26262: Part8의 5절 "분산 개발에서의 인터페이스"의 이야기로 돌아가고자 합니다.

개발 인터페이스 협정 (DIA)에서 합의한 프로세스가, 고객과 계약하는 데 있어서 최소한으로 필요한 기능안전 프로세스인 것은 전에도 말했었습니다. 이 작업 범위에 포함된 것은 제품 개발을 위한 프로세스, 이른바 엔지니어링 프로세스만이 아닙니다. 제품 개발을 관리하는 매니지먼트 프로세스나, 그에 관련한 지원 프로세스, 제품의 기능안전을 위한 감사와 평가라는 지원 업무도 포함되어 있습니다.

표 3은 DIA의 주된 요구사항을 바탕으로 기능안전 프로세스를 정리한 것입니다. 이 중에서 "기능안전에 필요한 프로세스"란, 어디까지나 예시이기 때문에, 물론 이와는 별개의 구조, 별개의 명칭인 프로세스를 만들어도 아무런 문제가 되지 않습니다.

DIA 에서 합의해야 하는 것	기능안전에 필요한 프로세스	관련 규격 조항
입력 정보	제품 개발 프로세스. 기능 사양서, 안전 목표, 안전 요구 등에 입력 되는 성과물 규정	Part4、Part5、Part6
안전관리자의 임명/계획 입안	안전관리 프로세스. 안전 관리자 임명, 안전 계획서 입안, Tailoring 기준 등 프로젝트 착수 시의 작업과 책임/권한에 관한 규정	Part2 : 6 절
Tailoring 결과	제품 개발 프로세스. 안전 요구사항, 설계, 테스트, 안전 분석 등 엔지니어링 관계의 작업 규정	Part4、Part5、Part6

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

DIA 에서 합의해야 하는 것	기능안전에 필요한 프로세스	관련 규격 조항
수수(교환)하는 성과물	구성관리/문서관리 프로세스, 성과물의 관리와 배포 등 성과물과 문서/기록 등의 버전 관리와 Release 에 관한 규정	Part2 : 6.4.6、Part8 : 7 절、10 절
진척(진행상황) 상황의 보고/이슈 보고	안전관리 프로세스. 진척관리, 문제관리, Escalation 등의 프로젝트 관리 규정	Part2 : 5 절、6 절
변경 발생 시의 대응	변경관리 프로세스. 영향 분석, 변경 시의 승인/보고	Part8 : 8 절
기능안전 감사의 실시	기능안전 감사. 감사 계획, 실시 요령, 감사 보고	Part2 : 6.4.8
기능안전 평가의 실시	기능안전 평가. 평가 범위, 역할 분담(고객/자사)	Part2 : 6.4.9、Part4 : 10 절
생산 시의 대응	생산관리 프로세스	Part7

표 3 DIA를 바탕으로 정리한 기능안전 프로세스 필요 요소

표 3의 "관련 규격 조항"란을 보면, 해당 조항은 어디까지나 DIA와 연관된 규격을 이야기하는 것이며, 이것으로 모든 규격 요구를 만족한 기능안전 프로세스가 구축되지는 않습니다. 하지만, 주가 되는 프로세스는, 거의 포함되어 있기 때문에 이들 프로세스를 골격으로 하여 남은 부분에 살을 붙이면 좋지 않을까 생각합니다. 만약, 기능안전 프로세스의 바탕이 될 수 있는 프로세스 자산이 이미 존재해 있다면, 그것과의 대응 관계를 보면서 부족한 프로세스와 작업을 분명히 하는 것도 좋겠죠.

중소 공급자에게 있어서의 기능안전 평가

표 3에 나타낸 프로세스 중에서, 중소 공급자 입장에서 기능안전 프로세스를 생각한다면 조금 귀찮은 일인 것이 기능안전 평가일 것입니다. 기능안전 평가는, ISO 26262: Part2에 나와있는 표 2의 정의에 의하면, "item"의 기능안전을 평가[*3)]하는 것이라고 되어있습니다. Item의 구성 요소만을 담당하는 중소 공급자가, Item 전체에 관한 기능안전에 대해서 합격 여부를 판정한다는 것은 어려운 일이기 때문에, 규격 요구를 그대로 받아들이는 것은 현실적이지 않겠죠. 보통, 안전 목표를 달성하기 위한 안전 방책은, Item level 또는 차재 시스템 전체로 생각하기 때문에, 구성 요소 단독으로 안전을 평가하는 것에는 한계가 있습니다.

3) 대상 제품에 ASIL-C 또는 ASIL-D가 할당될 경우에만 해당. ASIL-B의 경우는 추천.

중소 공급자라는 입장에서 현실적으로 가능한 것은, 기능안전 평가의 요구 전체를 짊어지는 것이 아니

본 내용은 [일본 IT MONOist] 매거진에 등재된 기사 원문을 ㈜카이젠컨설팅이 번역한 자료임을 알려 드립니다.
본 내용에 대한 저작권은 일본 ITmedia Inc.에 있으며 내용의 개편 및 수정이 불가합니다.

라, 전체 중의 일부분만을 담당하는 사고 방식이라고 생각합니다. 시스템 전체로써의 기능안전은 평가할 수 없지만, 담당한 제품이 요구에 따라 올바른 프로세스로 개발된 것을 분명히 평가한다 라는 접근입니다. 예를 들어, 자사의 담당 범위 내에서 실시되는 검증 활동의 결과와 기능안전 감사의 결과를 평가하고, “안전 요구가 확실히 전개되고 있는가”, “테스트가 충분히 실시되고 있는가”, “미해결 문제가 남아있지는 않은가” 라는 항목에 대해서 객관적인 시점으로 평가한다는 것입니다. 객관적인 시점에서의 평가는, 개발의 당사자가 알아차리기 힘든 사실을 발견하는 효과적인 수단입니다.

하지만, 구체적인 방법과 평가 관점, 대상 범위와 평가의 깊이 등은 계약자(고객)과의 사이에서 조정하고, 합의할 필요가 있겠죠. 고객이 실시하는 경우도 있습니다. 어쨌든, 이 검토를 위해서는 전 회에서도 언급했던 것처럼 (자)조직의 사정도 충분히 고려하여 조금이라도 효과를 높일 수 있는 활동을 생각해야 합니다.

보충: DIA에 대해서

이번 회에서는, 방대한 규격 요구사항 중 기능안전 프로세스를 구축하는 데 있어서, DIA를 바탕으로 최소한으로 필요한 프로세스 요소를 압축해 보았습니다.

하지만, 현실의 비즈니스를 생각하면 이 DIA 자체도 어디까지의 범위에서 필요한 것인지 알 수 없다 라는 질문을 받은 적이 있습니다. 예를 들어, 일본의 개발 현장에서 자주 볼 수 있는, 제품 개발을 위탁하는 것이 아니라 제품 개발에 필요한 기술 서비스(인력 소싱)를 제공하는 경우는 어떻게 되는 것인가 라는 질문입니다. 타사의 소프트웨어 기술자가 자사에 상주하여 개발하도록 하는 경우의 일입니다.

DIA는, 제품의 분산 개발을 실시하는 경우, 책임도 각각 분담하자 라는 사고 방식이라, 성과물 책임을 지지 않는 이러한 경우에는 DIA를 결부시키는 것은 어려운 일이라고 생각합니다. 당연히 DIA를 결부시키지 않는다면 책임은 분담할 수 없다(책임은 발주자가 진다)라는 것이 되기 때문에, 발주하는 측은 이에 상응하는 작업 관리가 필요하게 되겠죠.

원문 | http://monoist.atmarkit.co.jp/mn/articles/1306/10/news014.html

http://monoist.atmarkit.co.jp/mn/articles/1306/10/news014_2.html

http://monoist.atmarkit.co.jp/mn/articles/1306/10/news014_3.html