Journal of KOSSE. (2017. 6) Vol. 13, No. 1 pp. 57-65
DOI: https://doi.org/10.14248/JKOSSE.2016.13.1.057
www.kosse.or.kr

ISSN (print) : 1738-480X
ISSN (online) : 2288-3592

기능 안전과 모델기반 시스템엔지니어링 - ISO 26262/DO-178C 중심으로

박중용* 백승길

한국항공우주연구원

Functional Safety and Model-Based Systems Engineering - focusing on ISO 26262/DO-178C

Joongyong Park*, Seung-Kil Paek

Korea Aerospace Research Institute

Abstract : Recently, the ratio of electrical part and embedded software has grown in automotive industry. ISO 26262, 'Road Vehicles - Functional Safety', was published to guide development of automotive electrical and electronic part in 2011. This paper describes definition of functional safety and analyzes ISO 26262. The comparison of ISO 26262 and DO-178C is made, then difference between them is identified. DO-178C provides guidance for the production of software for airborne system and equipment. The core of DO-178C is a relatively minor update to the previous DO-178B, however, the big changes are captured in the supplemented documents such as DO-331, 'Model-Based Development and Verification Supplement to DO-178C and DO-278A'. Model-based design is important to develop automotive and aircraft meeting the guidelines of ISO 26262 and DO-178C. In this paper, the sample case of applying MBSE(Model-Based Systems Engineering) to AVCS(Active Vibration Control System) software development is discussed.

Key Words : Functional Safety, ISO 26262, DO-178C, MBSE, Active Vibration Control System

Received: November 11, 2016 / **Revised**: June 3, 2017 / **Accepted**: June 12, 2017

* 교신저자 : Joongyong Park, parkjy@kari.re.kr

1. 서 론

2014년 3월에 현대자동차는 2015년 말부터 자사의 신규 자동차 개발에 기능안전 국제표준인 ISO 26262를 전면 적용하겠다고 발표했다[1]. ISO 26262는 자동차 설계부터 개발, 제작 등 완성차가 나오기까지 전 단계에서 '안전'을 확보하기 위한 의무 활동을 규정한다. 전장부품 가운데 안전과 관련 있는 부품이 대상이다. 자동차에서 사용되는 소프트웨어의 양은 이미 웬만한 항공기에 사용되는 소프트웨어 양을 넘어섰다. 그렇기 때문에 전자장비 도입 급증에 따른 오류 가능성을 줄이고자 2011년에 도입됐다. 베엠베와 다임러, 폴크스바겐, 지엠 등 세계의 주요 자동차 업체는 이미 신차 개발에 ISO 26262 적용을 시작했다[1]. 2016년 5월 기준으로 현대자동차와 기아자동차를 비롯한 국내 완성차 업체들은 원칙적으로 ISO 26262 인증서를 요구하지는 않지만 기능별로 인증을 권고하고 있다. 문제는 표준들이 준수해야 할 사항은 있지만 어떻게 준수해야 하는지 규정이 명확하지 않다는 점이다. 이와 같은 어려움을 해소하기 위해 등장한 방식이 모델링 기반 개발이다[2].

항공산업 분야에서는 이미 오래전부터 기능안전을 포함한 시스템 안전에 대한 표준과 규정이 활용되어 왔다. DO-178은 항공용 소프트웨어 안전 표준으로서 ISO 26262의 소프트웨어 부분은 DO-178을 일부 벤치마킹하여 제정되었다고 알려졌다. DO-178은 DO-178B를 거쳐 DO-178C이 최신 버전이다. 항공기 개발 부분에서도 자동차 부분과 마찬가지로 모델을 이용한 개발이 확산되고 있으며, DO-178C의 지침을 모델링 측면에서 지원하는 표준인 DO-331이 활용되고 있다.

본 논문에서는 기능 안전의 개념을 정의하고 ISO 26262가 어떤 표준인지 분석하였다. 그리고 ISO 26262와 DO-178C를 비교하여 두 표준 간에 차이점과 적용 시 중점을 두어야 할 사항을 식별하였다. 마지막으로 모델 기반 개발 기술을 시스템엔지니어링 관점에서 분석하고 민수헬기개발사업에 적용한 사례를 제시하였다.

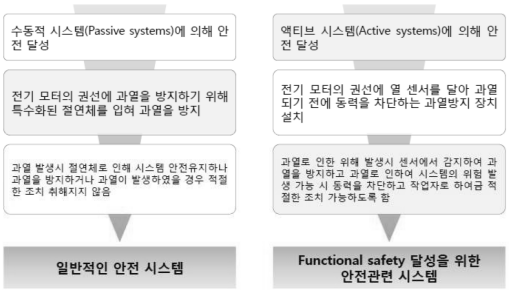
2. 기능 안전

2.1 기능 안전의 개념

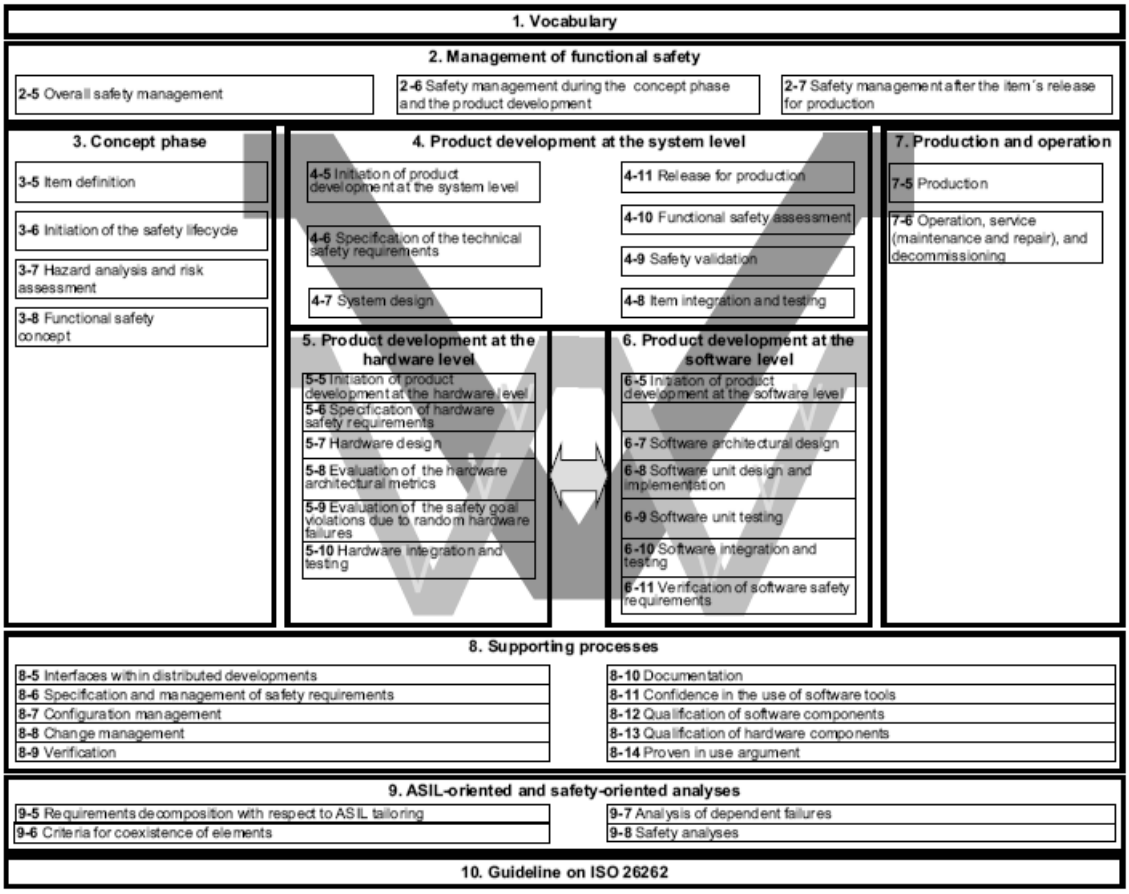
ISO 26262에 따르면 기능 안전이란 전기/전자 시스템의 오동작으로 인해 야기된 해저드(hazards)로 인한 비합리적인 리스크(unreasonable risk)의 제거로 정의된다. 여기서 전기/전자 시스템이란 전기/전자 부품으로 이루어진 시스템을 말하며, 해저드는 아이템의 오동작으로 야기된 상해(harm)의 잠재적 원인을 뜻한다. 비합리적인 리스크는 사회 관습적인 도덕적 개념으로 볼 때 특정 상황에서 받아들이기 힘들다고 판단된 리스크를 뜻한다. 리스크는 상해를 일으킬 수 있는 가능성의 조합이다[3].

일반적인 안전 시스템과 기능 안전 달성을 위한 안전관련 시스템을 비교해서 설명하면 Figure 1과 같다[4].

가장 큰 차이점은 기능 안전 시스템은 능동적 시스템을 통해 안전을 달성하는데 반해 일반 안전 시스템은 수동적 시스템으로 안전을 달성한다는 점이다. 그림에서 알 수 있듯이 모터의 과열을 방지하기 위해 절연체를 입힘으로써 어느 정도의 안전을 보장할 수 있으나 과열 자체를 방지할 수는 없으며 과열이 발생할 경우 적절한 조치가 불가능하다는 것이 일반 안전 시스템의 문제이다. 이에 반해 기능 안전 시스템은 모터에 열 센서를 장착하여 과열이 되면 아예 동력을 차단함으로써 과열을 방지하고 작업자가 적절한 후속조치를 할 수 있게 해준다.



[Figure 1] Functional Safety Concept[4]



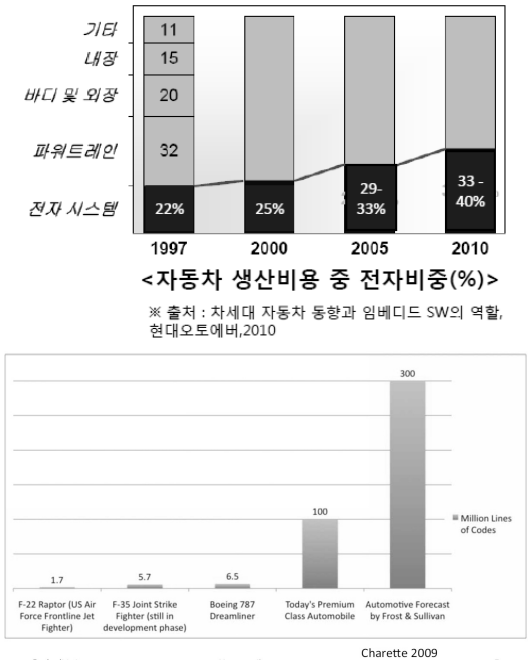
[Figure 2] Structure of ISO 26262[3]

2.2 기능 안전 관련 표준 및 지침

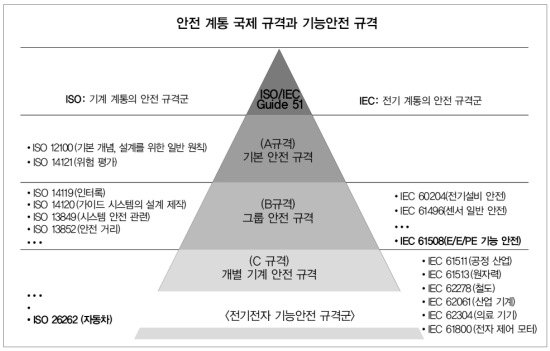
2.2.1 자동차 산업 분야

현재의 자동차에는 다양하면서도 복잡한 기능을 구현할 수 있는 임베디드 소프트웨어가 높은 비중으로 채택되고 있다. Figure 3을 보면 자동차 생산 비용 중 전자 비중이 2010년에 이미 40%에 근접하고 있음을 알 수 있다. 그리고 자동차에 사용된 소프트웨어 라인 수가 이미 항공기와 비교 시 우위에 있음을 알 수 있다.

안전 계통 국제 규격은 Figure 4와 같이 다양한데, ISO 26262는 산업용 전자부품에 적용되는 범용 안전 표준인 IEC 61508을 토대로 2011년에 발간된 표준이다. IEC 61508은 일반 전기전자장치의 포괄적인 기능 안전 표준이므로 자동차 분야의 특수성을 반영하지는 못한다.



[Figure 3] Automotive electric parts and SW LOC



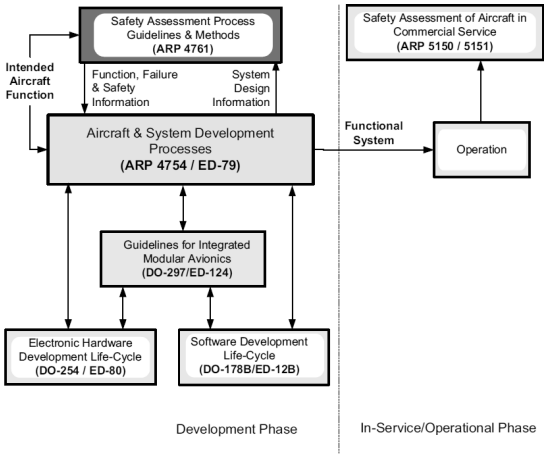
[Figure 4] International Safety Standards[6]

그리고 제조사와 부품공급업체 간의 전문화와 분업화된 자동차 생산 방식에 적합하지 않고 제어시스템과 안전 매커니즘을 별개로 고려한 것이 자동차와 맞지 않는다. 또한 소비자의 관점이 아닌 공급자 관점의 안전에 초점이 맞추어져 있는 한계가 있다[5]. IEC 61508의 한계를 극복하고 최대중량 3.5톤의 양산용 승용차에 장착되는 전기/전자 시스템이 포함된 안전 관련 시스템의 안전 표준으로 제정한 것이 ISO 26262이다.

ISO 26262는 전기전자장치를 이루는 하드웨어와 소프트웨어의 기능 안전을 다루고 있다. ISO 26262는 총 10개의 파트로 구성되어 있다. 여기에는 44개의 프로세스가 있다. Figure 2에서 브이(V) 자는 시스템엔지니어링의 브이 모델과 유사하다. 즉, 시스템 수준에서의 개발에서부터 시작하여 하향하며 하드웨어와 소프트웨어를 개발하되 각 파트는 요구사항 정의부터 검증까지의 프로세스를 포함한다. 이러한 제품 개발 파트가 4, 5, 6 파트에서 서술되고 있고 그 전 후 단계인 구상 단계와 생산 및 운용 단계가 파트 3과 7에서 설명된다. 파트 8은 이 모든 파트를 지원하는 지원 프로세스를 정의하며 파트 9는 자동차 안전 무결성 수준(Automotive Safety Integrity Level, 이하 ASIL) 중심의 분석을 설명한다. 마지막으로 파트 10은 ISO 26262의 가이드라인이다.

2.2.2 항공 산업 분야

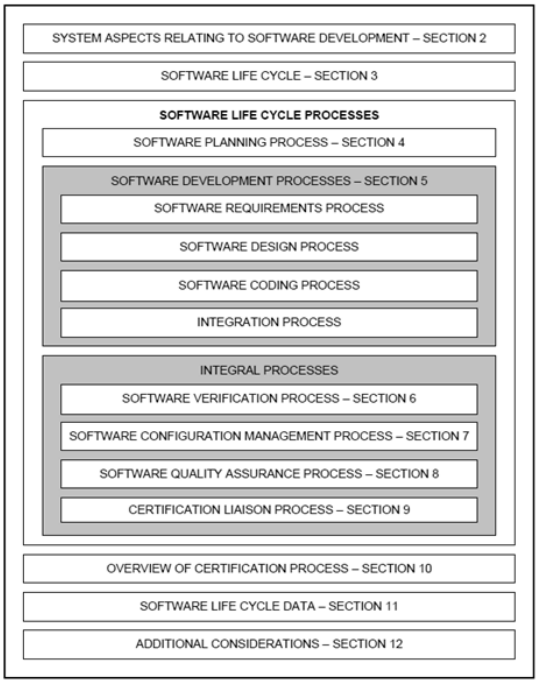
항공기 개발 시 준수해야 할 대표적인 안전 관련



[Figure 5] Aircraft safety guideline documents[7]

규정은 미국의 연방항공청(Federal Aviation Administration, FAA)에서 제정한 연방항공청 규정(FAA Regulation, 이하 FAR)이 있다. FAR는 항공기 종류에 따라 여러 규정으로 다시 나뉘며, 유럽이나 우리나라에서도 FAR와 유사한 규정을 제정하여 항공기 개발 시 규정을 준수했음을 입증하도록 한다. DO-178C는 FAR 규정을 최상위 규정으로 하여 여러 단계를 거쳐 하부로 내려오면서 생성된 가이드라인이다. Figure 5는 관련 규정을 보여준다.

- FAR25.1309(장비, 시스템, 장착) : 항공기에 장착되는 시스템이나 장비에 대한 일반적인 요구사항. 헬리콥터는 FAR 27과 FAR 29의 1309임.
- FAR25 Advisory Circular 1309 (AC25.1309) : FAR25.1309를 만족하기 위한 수행 가이드라인으로 안전성 평가에 대한 기법들이 소개되어 있음.
- SAE ARP4754A(민수용 항공기와 시스템 개발을 위한 가이드라인) : 민간 항공기 또는 시스템 개발 지침으로서 시스템엔지니어링 개발 프로세스를 적용함.
- SAE ARP4761(민수용 항공기 시스템과 장비의 안전성 평가 프로세스 수행을 위한 방법과 가이드라인) : 민간 항공시스템 또는 항공장비의 안전성 평가 지침 및 방법을 명시함.



[Figure 6] Structure of DO-178C[8]

AC25.1309에서 소개한 안전성 평가에 대한 상세 지침을 소개함.

- RTCA DO-178C(항공기 시스템과 장비 인증을 위한 소프트웨어 고려사항) : 항공시스템 또는 항공장비 인증 시 소프트웨어 측면에서 고려해야 할 사항을 명시함. 구조는 Figure 6 참고
- RTCA DO-331(DO-178C와 DO-278A를 지원하기 위한 모델 기반 개발 및 검증) : 모델기반 개발 및 검증 기법이 사용될 때 DO-178C의 요구사항 충족을 지원하기 위한 지침을 명시함.
- RTCA DO-254(항공기용 전자 하드웨어를 위한 설계 보증 가이던스) : 항전장비 중 하드웨어 설계 지침을 명시함.

DO-178C는 총 12개의 섹션으로 구성되어 있다. 섹션 1은 개요이고 섹션 2는 소프트웨어 개발과 연관된 시스템 생명주기 프로세스를 설명한다. 소프트웨어로 할당되는 시스템 요구사항, 시스템 생명주기 프로세스에 고려되어야 할 소프트웨어 등의 내용이 포함된다. 섹션 3는 소프트웨어 생명주기 프로세스에 대해 설명한다. 섹션 4부터 섹션 9까지는 크게 3단계로 분류된 소프트웨어 생명주기 프로세스를 상세히 설명한다. 소프트웨어 개발 계획을 수립하는 섹션 4, 소프트웨어 개발 프로세스를 설명하는 섹션 5, 그리고 소프트웨어 검증, 형상관리, 품질 보증, 인증 등의 업무를 총괄하는 통합 프로세스를 섹션 6~9에서 설명한다. 나머지 섹션 10은 인증 프로세스의 개요를 설명하고, 섹션 11은 소프트웨어 생명주기에서 산출되는 데이터를 식별하며, 마지막으로 섹션 12는 사용하는 도구 보증과 같은 기타 고려할 사항들을 설명한다. 부록으로 각 섹션별 프로세스의 목표와 그 목표를 달성해야 하는 소프트웨어 수준을 연결하고 생성되는 산출물을 식별한 표를 제공하여 DO-178C를 적용했을 때 DO-178C의 요구사항이 개발계획서에 반영되었는지와 이를 충족시켰는지 여부를 확인하는데 유용하다.

2.2.3 ISO 26262와 DO-178C 비교

ISO 26262와 DO-178C를 비교 분석하였다. Matthias Gerlach가 연구한 ISO-26262와 DO-178B 비교 연구 결과를 참조하되[9], ISO 26262에서 상대적으로 자세히 언급한 소프트웨어 수준을 분해하는 기법, 그리고 위험도를 예측하는 지침에 대해 추가로 분석하였다.

항공용 소프트웨어 안전 표준으로 인식되는 DO-178B는 1992년 민간 항공기 소프트웨어 안전에 대한 지침을 제공하기 위해 만들어 졌으며, 1993년 미국의 연방항공청 문서인 AC 20-115B에서 FAR에 부합하기 위한 지침으로 채택되었다. 2011년에 발표된 DO-178C가 최신 버전이다. DO-178C와 B는 근본적인 차이는 없으나 2011년에 DO-178C를 지원하는 DO-331이 함께 발간된 점에 주목하면 모델 기반 설계를 강조했음을 알 수 있다[10].

ISO 26262는 DO-178C와 달리 소프트웨어 뿐만 아니라 하드웨어 개발 영역까지 다루고 있다는 점에서 가장 큰 차이가 있다. 그 밖의 주요 차이점을 확인 방법(Confirmation Measures), 생명주기

프로세스, 산출물의 세 가지 측면에서 비교하였다.

1) 확인 방법(Confirmation Measures)

확인 방법이란 제품이 규격의 요구사항을 어느 정도 만족시켰는지 확인하는데 필요한 측정지표를 뜻한다. 관련 법 규정이 있는 경우엔 확인 방법은 인증으로 연결될 수밖에 없다. DO-178C는 항공전장품 영역의 인증과 깊은 관련이 있음이 명백하나 ISO 26262는 공식적인 인증의 지표로 효력을 발휘하지 않는다. ISO 26262의 경우는 기능 안전 관리자가 안전 프로세스와 측정지표의 올바른 구현을 책임지나 DO-178C는 인증 당국과 상호작용하는 담당자가 별도로 있다. 두 표준 모두 인증이나 양산은 최종 통합된 항공기나 자동차가 최상위 수준의 안전 요구사항을 만족했을 때 인정된다. 즉, 소프트웨어 개발 산출물과 검증 기록은 제품의 안전 평가 전체의 일부에 불과하며, 소프트웨어 자체는 인증가능하다는 의미이지 인증을 받은 것은 아니다. 양 표준은 모두 제품/아이템의 수준을 다섯 단계로 규정하고 있다. 안전에 영향이 없는 최하위 단계는 ISO 26262는 품질 관리(Quality Management, QM), DO-178B는 E로 정의한다. 이 단계의 아이템은 기본적인 품질 관리만을 필요로 한다. 윗 단계로서 ISO 26262는 ASIL A에서 D로 점점 안전에 대한 요구사항이 높아진다. 반대로 DO-178C는 D에서 A로 안전에 대한 요구사항이 까다로워진다.

ISO 26262는 세 가지 종류의 확인 방법을 정의했다.

첫째, 안전성 감사(safety audit)는 프로세스가 정의되고 요구된 대로 수행되었는지 확인한다.

둘째, 확인 검토(confirmation review)는 개발 기간 중 만들어진 산출물의 내용을 검증한다.

셋째, 기능안전평가(functional safety assessment)는 안전성분석 산출물(safety case)의 올바른 작성 여부를 검증한다.

이 때 ASIL이 높을수록 안전 검토의 독립성의 정도가 높아진다.

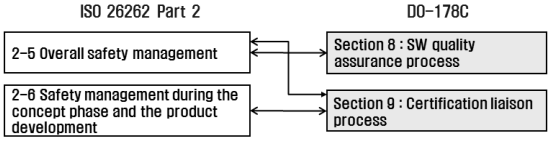
DO-178C는 인증 위임 프로세스를 통해 개발 기간 동안 지속적으로 검토를 수행한다. DO-178C는 독립성의 수준을 정의하지는 않았지만 소프트웨어의 안전 수준이 높을수록 독립성을 가지고 검증되어야 할 목표를 더 많이 명시한다. ISO 26262는 독립성을 정의하기 위한 역할과 구조를 설명하고 있고 DO-178C는 객관적인 평가를 보장하고 소프트웨어 품질 보증을 위한 보완 활동 권한을 정의했다.

2) 생명주기 프로세스

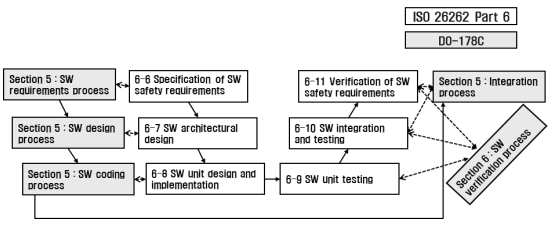
생명주기 프로세스 수를 비교하면 ISO 26262가 DO-178C의 4배 이상이다. 이와 같이 개수에 큰 차이가 나는 이유는 다음과 같다.

- DO-178C는 소프트웨어 개발에만 관련된 내용이지만 ISO 26262는 시스템 수준과 하드웨어 수준의 개발까지 포함한 내용이다.
- ISO 26262는 생산과 운영 프로세스를 포함하지만 DO-178C는 포함하지 않는다.
- ISO 26262는 방법 중심의 접근법이기 때문에 프로세스 정의가 좀 더 상세하다.

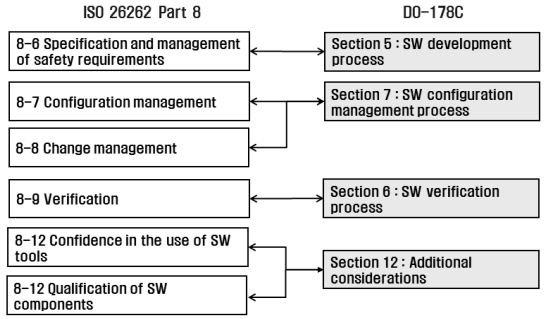
ISO 26262와 DO-178C의 프로세스를 1:1로 맵핑하기는 어렵다. 다만, ISO 26262에는 있지만 DO-178C에는 없는 프로세스로 뚜렷이 식별되는 것은 파트 5 제품 개발 : 하드웨어 레벨과 파트 7 생산 및 운영이다. ISO 26262에서 소프트웨어와 관련된 파트 2, 6, 8과 DO-178C의 프로세스 비교는 Figure 7, 8, 9와 같다.



[Figure 7] ISO 26262 part 2 vs DO-178C



[Figure 8] ISO 26262 part 6 vs DO-178C

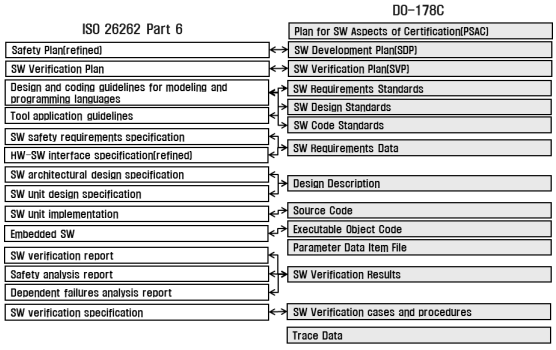


[Figure 9] ISO 26262 part 8 vs DO-178C

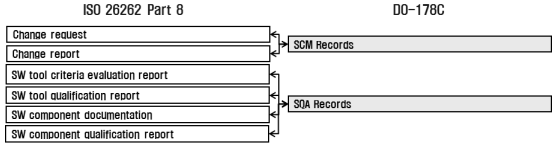
ISO 26262의 파트 6-10 프로세스에는 소프트웨어 통합과 검증 업무가 수행되므로 DO-178C의 섹션 5와 6의 업무가 혼재되어 있다. ISO 26262의 파트 6-11 프로세스에는 소프트웨어 안전 요구사항이 상위 시스템 요구사항을 충족하는지 검증하면서 하드웨어와 소프트웨어의 통합 업무가 포함되므로 DO-178C의 섹션 5와 6의 업무와 관련이 있다.

3) 소프트웨어 개발 산출물

양 표준 모두 개발 기간 중에 특정 산출물을 생성할 것을 요구한다. DO-178C는 섹션 11에서 명확하게 각 산출물의 목적을 기술하고 있다. 반면 ISO 26262는 각 프로세스의 작업 산물로 정의한다. Figure 10과 11을 참고한다.



[Figure 10] ISO 26262 part 6 output vs DO-178C output



[Figure 11] ISO 26262 part 8 output vs DO-178C output

ASIL Determination		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

[Figure 12] Criteria for determining ASIL[3]

4) ISO 26262의 기타 특징

아이템이나 엘리먼트의 ASIL을 결정하는 방법은 식별된 해저드의 심각성(S), 발생가능성(E), 조정가능성(C)의 등급을 정해서 Figure 12에 따라 결정할 수 있지만 등급을 정하는 것이 쉽지 않다.

자동차기술협회(Society of Automotive Engineers, SAE)에서는 방대한 과거 자동차 사고 기록을 바탕으로 S, E, C를 쉽게 결정할 수 있는 J2980을 2015년에 발간했다[11]. 이 문서를 활용하면 ASIL 결정이 용이하다.

아이템의 ASIL이 등급이 높아질수록 충족해야 하는 요구사항이 많아지므로 되도록 등급을 낮추는 것이 좋다. 이를 위해 아이템의 ASIL을 분해해서 낮은 등급의 ASIL로 재조합하는 기법이 만들어졌으며 ISO 26262는 이 방법에 대해 상세히 설명하고 있다[3]. 예를 들어 ASIL이 최고 등급인 D인 아이템이나 엘리먼트의 경우 C와 A, B와 B, D와 QM 등급의 아이템이나 엘리먼트로 분해가능하다.

3. 기능 안전을 위한 MBSE

3.1 기능 안전 MBSE 방법론과 도구

현대의 복잡한 시스템을 ISO 26262와 DO-178C의 요구사항을 적용하면서 개발하려면 모델 기반 개발을 채택하는 것이 효과적이다. DO-178C의 경우는 모델 기반 개발을 효과적으로 수행할 수 있도록 DO-331을 추가로 제시하였다. DO-331의 항목들은 DO-178C와 거의 같고, 단지 모델 기반 개발

및 검증을 수행하는데 필요한 사항에 대한 지침을 추가했다. 도구개발 회사들은 DO-331의 지침을 쉽게 수행할 수 있는 도구들을 제품으로 내놓았다. 모델을 상용 도구를 이용해서 작성하면 최초 요구사항부터 기능 분석을 거쳐 아키텍쳐를 구성하고 소프트웨어 코드까지 추적성을 확보하면서 작성 가능하다. 마지막으로 작성된 코드가 요구사항을 충족시키는지 확인할 수 있는 검증 업무까지 도구를 통해 수행할 수 있다.

3.2 DO-178C/DO-331 적용 예

능동진동제어시스템(Active Vibration Control System, 이하 AVCS)은 항공기에 발생하는 진동을 능동적으로 감쇠시키는 장치이다. 소형무장헬기(LAH) 연계 소형민수헬기(LCH) 개발사업에서는 국외업체가 이전하기를 꺼려하는 핵심기술 세 가지를 개발 중에 있다. 이 중의 한 가지 기술이 AVCS 개발 기술이다. AVCS는 헬리콥터 진동 수준을 고정익 항공기 수준으로 저감할 수 있는 능동진동제어시스템이다[12].

AVCS는 제어기 컴퓨터와 가속도 및 타코미터 센서, 구동기 및 와이어하니스로 구성되는데, 제어기 컴퓨터에 탑재될 진동제어 구동 소프트웨어(Application SW)의 소프트웨어 개발에 DO-178C의 설계보증수준(DAL : Design Assurance Level) C급 인증기준을 적용하고 있다.

DO-178C 기준에 따라 소프트웨어 개발 절차 및 각 소프트웨어 개발 프로세스 목적을 만족할 수 있도록 소프트웨어 생명주기를 설정하였다.

먼저 소프트웨어 개발 관련 표준으로 소프트웨어 요구사항 표준, 소프트웨어 설계 표준, 소프트웨어 코드 표준 등의 개발 표준을 설정하였다. 본 연구에서는 모델기반 소프트웨어 개발 방식을 추구하고 있기 때문에 DO-331[13]에서 요구하는 소프트웨어 모델 표준을 수립하였다[14].

소프트웨어 요구사항은 요구사항 표준서에 따라 개발하며 상/하위 요구사항 간의 연관성 및 추적성 관리는 DOORS[15]를 사용한다.

소프트웨어 설계는 MATLAB/Simulink와 Enterprise Architect[16]라는 UML도구를 사용한다. MATLAB/Simulink는 진동제어를 위한 제어기 모델을 설계하는데 사용하였고, UML 도구는 전체 소프트웨어 구성, 제어기 파라미터 데이터의 로딩, 제어기로의 데이터 입출력 부분의 설계에 사용하였다.

DOORS 내에 정의된 요구사항과 MATLAB/Simulink 모델의 블록 사이에 링크 생성을 위해, 먼저 DOORS-MATLAB 인터페이스 프로그램을 MATLAB에 설치하고, 해당 Simulink 모델에서 요구사항 추적성 세팅를 통해 DOORS를 지정한 후 DOORS의 특정 요구사항과 해당 Simulink 블록을 링크시킨다.

소프트웨어 산출물인 소스코드의 사용 언어는 C 언어이며 MATLAB/Simulink 로 구성된 제어기 모델로부터 MATLAB Embedded Coder라는 자동코드 생성도구를 이용하여 생성하며, UML 도구로 설계된 부분은 핸드 코드로 작성하고 있다.

AVCS에 사용된 제어기 컴퓨터의 제어기 하드웨어로는 텍사스 인스트루먼트사(Texas Instrument, 이하 TI))의 TMS320F28335급 디지털 신호 처리기를 사용하기 때문에 TI 의 Code Composer Studio를 이용하여 실행코드(Executable Object Code)를 생성한다. 개발된 프로그램 모듈에 대한 디버깅을 위하여 스펙트럼 디지털 사의 eZdsp 평가보드를 사용한다[14].

소프트웨어 검증 중 코드 표준 준수 여부 확인과 같은 정적분석, 테스트케이스 생성, 하위수준 요구사항 만족 여부 및 구조적 커버리지 분석을 위해 LDRA[17]를 사용한다.

4. 결 론

자동차, 항공기 등에 임베디드 소프트웨어가 많이 사용되면서 주목을 받게 된 기능 안전의 개념을 정의하고 자동차 산업의 기능 안전 표준인 ISO 26262가 어떤 내용으로 구성되어 있는지 분석하였으며 항공전장품의 소프트웨어 안전 표준인 DO-

178C와 비교하였다. ISO 26262가 소프트웨어뿐만 아니라 하드웨어, 시스템까지 다루고 있어서 DO-178C보다 영역이 넓으나 소프트웨어 부분만 비교하면 상당히 유사하다는 점을 알 수 있다. ISO 26262와 DO-178C의 요구사항을 충족하기 위해서는 모델 기반 설계를 도입하는 것이 효과적이며 요구사항부터 소프트웨어의 소스코드까지 추적성을 갖는 모델 수립이 상용도구를 통해 가능함을 능동 진동제어시스템 개발 사례를 통해 소개하였다.

후 기

본 논문은 산업통상자원부 소형무장헬기 연계 민수헬기 핵심기술개발사업 연구결과 중 일부임.

References

1. http://www.etnews.com/news/article.html?id=20140318000196
2. http://www.etnews.com/20160531000226
3. ISO 26262 Road Vehicles - Functional Safety, 2011
4. Sooyeon Lee, "Overview and prospect of Automotive Functional Safety International Standard(ISO 26262)", 27 Oct. 2011
5. mds technology, "Solution for Automotive Functional Safety International Standard ISO 26262"
6. Automotive Software, "Beyond functional level and quality of Functional Safety Standard ISO 26262", August/September 2010
7. SAE ARP4754A Guidelines for Development of Civil Aircraft and Systems, 2010
8. RTCA DO-178C Software Considerations in Airborne Systems and Equipment Certification, 2011
9. Matthias Gerlach 외, "Can Cars Fly? From Avionics to Automotive: Comparability of Domain Specific Safety Standards", Embedded World, 2011
10. Bill Potter, "Complying with DO-178C and DO-331 using Model-Based Design", 12AEAS-0090, MathWorks, Inc., 2012
11. SAE Surface Vehicle Recommended Practice J2980 "Consideration for ISO 26262 ASIL Hazard Classification", 2015
12. Paek, S.-K., Song, K.-W.., and Kim, S.-H., "Current Status of Helicopter Active Vibration Control System and Development Plan," Proceeding of the 2013 KSAS Spring Conference, 2013, pp. 888-891
13. RTCA DO-331 Model-Based Development and Verification Supplement to DO-178C and DO-278A, 2011
14. Paek, S.-K., "Software Development Plan for an Active Vibration Control System," Proceeding of the 2016 KSAS Spring Conference, 2016, pp. 630-631
15. https://www.ibm.com/developerworks/downloads/r/ordng/
16. http://www.sparxsystems.com/
17. http://www.ldra.com/