ISO 26262

ISO 26262 개요

ISO 26262는 3.5톤 미만의 승용차 내 안전 관련 전기/전자 장치에 적용되는 기능 안전성(Functional Safety) 국제 표준입니다.

자동차 내 전장 시스템 활용은 기능 고도화와 함께 급격하게 증가하여 자동차는 움직이는 컴퓨터로 보여지기도 합니다. 따라서, 복잡도 관리가 필요하며, 자동차는 특히 운전자 및 보행자의 안전과 직결되어 있어 안전의 중요성이 부각되고 있습니다.

10개국 27개 완성차업체 및 공급사가 참여하여 ISO 26262 표준은 2011년에 제정되었고, 2018년에 개정되었습니다.

총 12개의 파트로 구성되어 있으며, 이 표준에는 총 588개의 요건을 규정하고 있습니다. 이전 IEC 61508과 같은 기능 안전에 대한 범용적인 표준이 있어 왔지만, 각 산업별 특성을 반영하지 못하고 있었습니다. 이에 자동차 분야에 적합한 ISO 26262 표준이 제정되었습니다.

ISO 26262 고객

국내외 자동차 OEM 고객으로부터 ISO 26262 인증 결과를 얻고자 하는 협력업체

자동차에 적용되는 전장제품을 개발하는 업체로서 ISO 26262에 따라 제품을 개발하고자 하는 업체

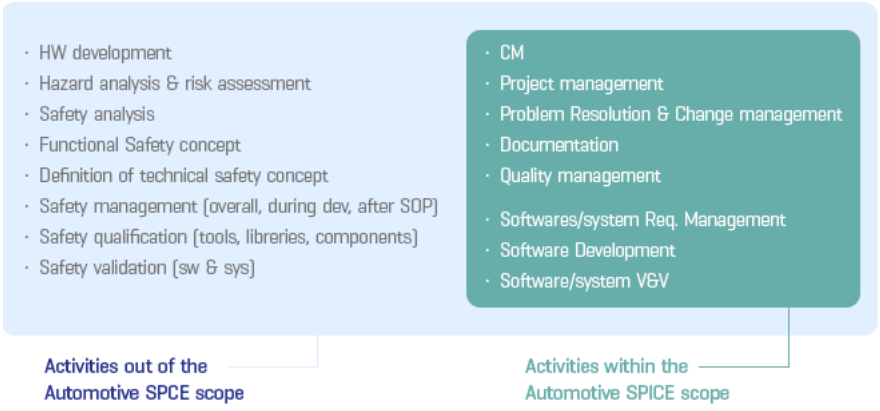
Automotive SPICE를 추진한 후 ISO 26262로 확장하고 싶은 업체

ISO 26262 적용 현황

ISO 26262는 민간 인증 기관을 중심으로 인증 기준으로 사용되고 있습니다. 즉, 자동차 전장품(아이템이라고 함)이 ISO 26262 인증을 받았다는 것은 해당 전장품이 ISO 26262의 요건들을 충족하면서 개발·운영되고 있음을 의미합니다. ISO 26262는 또한 안전성을 확보하기 위한 최신 기술(State-of-Art)을 적용하고 있다는 의미로 해석되어, PL 법 상의 소송 회피, 시장 위험의 대응, 향후 법규로 진행될 가능성에 대비하고자 하는 목적으로도 사용됩니다.

국내외 OEM들은 부품사들에 대해 ISO 26262를 요구하고 있습니다. 제3의 공인기관을 통한 인증을 요구하기도 하고, 또는 OEM에서 납품된 부품에 대해 ISO 26262 요건 준수를 확인하기도 합니다. 국내 자동차 OEM(현대, 쌍용 등) 및 부품사(모비스, 만도, LG전자 등)에서 ISO 26262 추진팀을 구성하여 고객 요구에 대응하고 있으며, 일부 인증을 받은 사례가 보고되고 있습니다. 해외 OEM에 수출하는 일부 국내 부품사의 경우 고객의 ISO 26262 인증 요구사항에 대응하여 전담팀을 구성하여 추진하고 있습니다.

한편, 일본과 유럽은 국가 차원에서 ISO 26262에 올바르게 대응하기 위한 가이드라인을 마련하였습니다. ISO 26262 에 포함된 프로세스의 많은 부분이 Automotive SPICE에 의해 구현가능하기 때문에 상호보완적인 방법으로 활용됩니다. 즉, ISO 26262의 Functional safety Audit를 Automotive SPICE 심사와 함께 수행가능하며, 대부분 OEM에서는 협력업체에 대해 Automotive SPICE Level 2 이상의 수준을 요구하고 있기 때문에 ISO 26262의 기반 조건으로 Automotive SPICE 추진을 함께 진행하는 것을 권장합니다.



ISO 26262 모델 내용

ISO 26262는 자동차용 전장 부품의 관리, 개발, 생산, 운영, 서비스, 폐기까지의 안전 생명주기를 제공하고 이 생명주기 과정에서 필요한 활동을 조정하도록 지원하기 위한 표준입니다. 총 12개의 파트로 구성되어 있고, 각 파트에서 커버하는 내용은 다음 그림에 나타나 있습니다.

아이템을 기준으로 자동차에 특화된 위험-기반 접근방법을 통해 ASIL(Automotive Integrity Levels)을 결정하도록 하고 있습니다. ASIL은 A에서 D까지 등급으로 나뉘며, ASIL D가 가장 높은 수준의 안전 요건을 충족시켜야 합니다. 예를 들어 크루즈 컨트롤은 ASIL A이며, 에어백은 ASIL C 등으로 정해지는데, 이는 대부분 OEM에서 사전에 결정하는 경우가 많습니다. 이렇게 결정된 ASIL에 따라 협력업체에서는 개발을 진행하게 됩니다.
ISO 26262에서는 ASIL 수준별 적용해야 하는 기법과 수단(measures)을 정의하고 있습니다. 예를 들어 SW 아키텍처 설계를 위한 기법들은 ASIL에 따라 다음과 같이 권장된다. 즉, ASIL D로 갈수록 적용해야 하는 기법들이 더 강력해짐을 알 수 있습니다.

	설명	ASIL			
		A	B	C	D
1a	소프트웨어 구성 요소의 구조 설계	++	++	++	++
1b	구성 요소의 크기 제한	++	++	++	++
1c	인터페이스의 크기 제한	+	+	+	+
1d	각 소프트웨어 구성 용소의 높은 응집도	+	++	++	++
1e	소프트웨어 구성 요소 간의 결합(외부 조인) 제한	+	++	++	++
1f	적절한 스케줄 한 반지	++	++	++	++
1g	인터럽트의 사용 제한	+	+	+	++

++ : 강력히 추천(필수 요구사항), + : 추천

아이템이 기능안전 요구사항에 따라 개발되었는지 확인하는 방법은 크게 확인 검토, 심사, 평가의 3가지로 나뉩니다. 평가 대상, 결과, 시기별 차이가 있으며, ASIL에 따라 확인자의 독립성도 보장되어야 합니다. 예를 들어 ASIL C 이상에서는 감사와 심사는 독립적인 주체가 수행하여야 합니다.

구분	확인검토 (Confirmation Review)	기능 안전 검사 (Functional Safety Audit)	기능 안전 심사 (Functional Safety Assessment)
평가 대상	작업 산출물	프로세스	아이템 자체
결과	확인 내용 검토 보고서	기능안전 감사 보고서	기능안전 감사 보고서
안전 생명주기 상 시기	해당 안전 활동의 완료 후	해당 프로세스의 수행 중	각 개발 단계 종료 시점 & 제품 릴리즈 전
범위 및 정도	안전 계획서에 따름	안전 계획서 참조 또는 감사자가 결정	기능 안전에서 요구되는 프로세스 및 안전 조치에 대한 리뷰

에이비앤아이 컨설팅의 특장점

통합 프로세스 접근 방법

통합 프로세스 모델 구축 접근방법을 통해 Automotive SPICE, SS 7740 등의 다양한 모델을 함께 진행합니다. (아래 그림 참조)
컨설팅 및 심사 후 갭 분석 서비스를 통해 고객이 지속적으로 역량을 확보할 수 있도록 지원합니다.
국내 다수의 인증기관과 network를 구축하고 있어 인증 추진이 용이합니다.

지식 및 경험

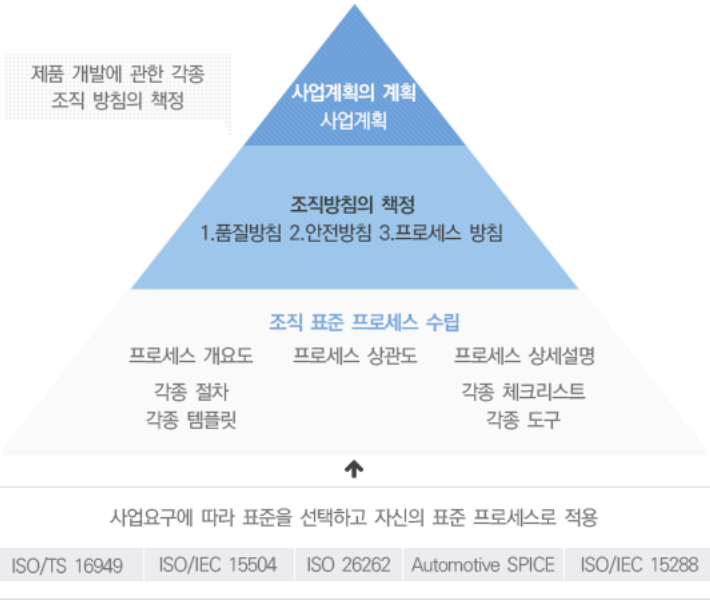
전기자동차 배터리 관리 시스템(BMS) 개발, 차량용 OS 개발, 네비게이션SW 개발을 포함하여 자동차의 다양한 응용 분야에 대해 컨설팅 경험을 보유하고 있습니다.

Automotive SPICE 뿐 아니라 현재 개정되고 있는 SPICE 표준에 대해 최신 지식을 적용하며, ISO 26262, SS 7740과 같은 타 표준에 대해 효과적으로 대처할 수 있도록 지원합니다.

인프라

오랜 경험을 통해 확보한 **통합 프로세스 자산(Process Asset :** 프로세스 및 산출물 세트 포함)을 활용하여 단기간에 최적화된 프로세스 구축하고 실현하게 합니다.

프로세스에 최적화된 공개 SW 기반의 **ALM(Application Lifecycle Management)** 도구를 구축하여 프로세스와 도구의 시너지 효과를 기대할 수 있습니다.



본사 : 서울특별시 서초구 서초중앙로6길 7, 501호(서초동, 홍빌딩) 지사 : 대전광역시 유성구 신성남로 111번길 24, 201호
전화번호 : 02-523-6112 팩스 : 02-3486-6112 E-mail : abni@abni.net