ISO 26262 프로세스의 효과적 적용을 위한 소프트웨어 도구 활용

지난해 11월 15일, 자동차 기능 안전성 국제표준 'ISO 26262'가 공식 제정됐다. ISO 26262는 기존의 분석 기법이나 문서관리 방식으로는 규격을 준수하는 것이 불가능할 정도의 복잡도와 난이도를 지닌다. 이런 이유로 검증된 적절한 도구를 통해 효과적이고 능률적인 개발 프로세스를 구축하는 것이 매우 중요하다. 이 글에서는 ISO 26262 내 주요 활동들을 수행할 때 소프트웨어 도구가 어떤 역할을 수행할 수 있는지를 다뤄본다.

글 | **석 민 진** 주임〈minjin@mdstec.com〉
MDS테크놀로지 TA사업팀

현 상황

앞서 언급했듯이 자동차 전자제어 시스템은 갈수록 복잡해지고 그 수 또한 증가하고 있다. 확실히 최근 30년 간 자동차의 중대한 혁신은 전자장비와 관련된 임베디드 시스템(e.g. 에어백, ABS, ESP)을 중심으로 이뤄져 왔으며, 이 같은 트렌드는 향후에도 지속될 것으로 보인다. 따라서 차량 내부에 통합되는 전자 시스템과 관련된 기능 안전의 중요성은 점점 더 커질 수밖에 없다.

최근까지 자동차 제조사들은 전자 임베디드 시스템 개발 과정에서 제품 불량 및 결함을 관리하기 위해 이미 하드웨어 위주의 다양한 분석 기법(e.g. FMEA, FTA)들을 보편적으로 사용해 왔다. 그러나 이러한 과정에서는 시스템의 안전과 관련된 기능들이 충분히 고려되지 못해 잠재적 위험인자들을 늘 안고 가는 형국이었다. 이처럼 자동차 전자제어 시스템의 급격한 발전만큼 안전의 중요성도 커져가면서 그 대응책으로 기능 안전성 국제 규격인 ISO 26262가 공식 제정됐다.

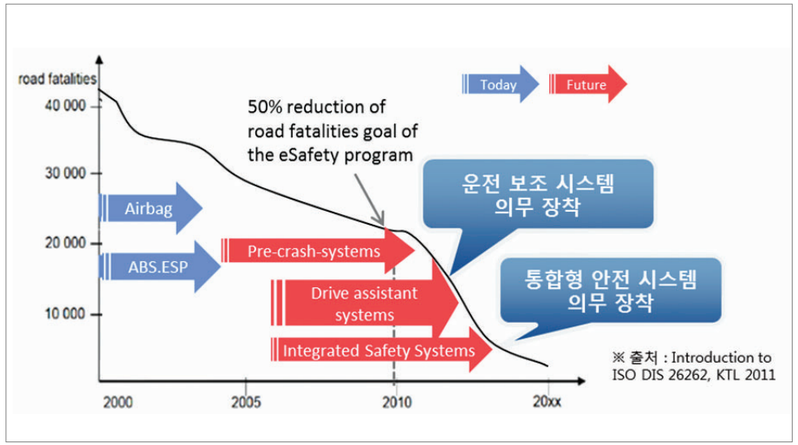
시장에서는 이것이 자동차 산업계에 커다란 영향을 미칠 것으로 보고 있다. 실제로 BMW와 같은 해외 유수의 자동차 제조사들은 이미 현재의 개발, 생산 프로세스 및 시스템을 ISO 26262에 맞춰 새롭게 구축하고 있으며, 관련된 부품 제조사들에게도 ISO 26262 규격에 대한 대응 준비를 요청하고 있다.

How to Start ISO 26262 – Safety Management 도구의 필요성

이러한 변화 속에서 나타날 수 있는 대표적인 문제점은 어떻게, 얼마나 효율적으로 새로운 프로세스를 체계화 시킬 것인지 – How to start 에 대한 정보 부족이다.

세계 유수의 자동차 기업들조차도 초창기에는 기능 안전에 대해 무엇을 어떻게 시작해야 할지 몰라 큰 혼란을 겪었다. 이런 상황에서 그들이 선택한 해결책은 시장을 선도하고 있는 관련 전문 도구의 적극적인 활용이었다. 같은 맥락에서 이제 막 ISO 26262에 대한 대응 필요성이 대두되고 있는 국내의 경우, 효율적인 기능 안전 규격 프로세스 적용을 위해 이같은 기능 안전 관리 도구를 적극 활용하는 방안이 제조사와 협력사들 사이에서 뜨겁게 논의되고 있다.

시스템의 복잡도가 증가하고 있는 상황에서 충분한 관리적 도구 지원이 없다면 기능 안전 규격이 요구하고 있는 모든 사항들을 만족시키는데 큰 어려움이 따를 수밖에 없다. 다시 말해 안전 전문 관리 도구의 사용은 Safety-Critical 전자 시스템 개발 시 ISO 26262가 요구하는 활동 수행에 매우 용이하다.



[그림 1] 비전제로와 자동차 안전 시스템의 전개 방향

안전 관리도구의 지원을 필요로 하는 대표적인 ISO 26262 규격 준수 활동으로는 아이템 정의, 위험 분석 및 평가 활동, ASIL 등급 결정, ASIL 등급 분해, 안전 목표 정의, 안전 요구사항 할당, V&V 활동, 안전 활동 검증(Safety Assessment), 형상 & 변경 관리 등이 있다.

물론 안전 분석(e.g. FMEA, FTA 등)과 관련된 활동을 지원하는 기법과 도구들은 ISO 26262의 도입 전에도 이미 존재해 왔다. 하지만 규격에서는 특히 안전 분석 활동의 경우 일련의 작업 추적성(traceability)과 일관성(consistency)을 지니고 관리돼야 함을 특별히 강조하고 있으며, 이를 위해서는 무엇보다 기존의 기법과 도구들 간의 통합이 필요하다. 이러한 상황에서 medini analyze는 가장 주목할 수 있는 통합 안전 관리 도구라 할 수 있다.

ISO 26262 규격 준수를 위한 통합 기능 안전 분석 도구 – medini analyze

medini analyze는 ISO 26262 규격 준수를 위한 통합 기능 안전 분석 도구로서 시스템 개발 프로세스에서 ISO 26262의 모든 주요 활동들을 커버하는 것을 특징으로 하고 있다. medini analyze는 위험분석 및 평가 활동을 중심으로 기능 아키텍처 디자인과 기능 안전 분석 작업을 한데 모아 관리하는 통합 안전 관리 도구(Total Safety Management Tool) 다.

기본적인 도구 내 모든 작업 흐름의 구조는 ISO 26262의 V 모델을 기반으로 이뤄진다. ISO 26262 Part 3(Concept)부터 Part 6(소프트웨어 개발)까지의 작업을 프로세스에 맞도록 지원해 기능 안전에 대해 생소한 조직에서도 ISO 26262에 규정된 흐름을 조금만 알고 있다면 손쉽게 ISO 26262 프로세스를 적용해 볼 수 있다.

그렇다면 ISO 26262의 주요 파트 중 하나인 Part 3 위험분석 과정이 통합 기능 안전 분석/관리 도구인 medini analyze를 이용해 어떻게 수행 될 수 있는지 살펴보자.

ISO 26262 Part 3 – 아이템 정의 (Item Definition)

ISO 26262 규격이 Part 3에서 가장 먼저 언급하고 있는 것은 "아이템 정의(Item Definition)"다. 시스템의 기본적인 정의와 역할 등의 정보를 기술해 분석하려는 아이템을 명확히 하는 단계다.

이렇게 정의된 아이템 역할 분석 데이터를 토대로 관련 기능들을 뽑아내는 순서로 작업이 진행된다. 보통 하나의 아이템이 독립적으로 역할을 수행하는 경우는 매우 드물다. 주로 한 아이템이 여러 개의 아이템들과 신호를 주고받으며 역할을 수행하는 것이 일반적이다.

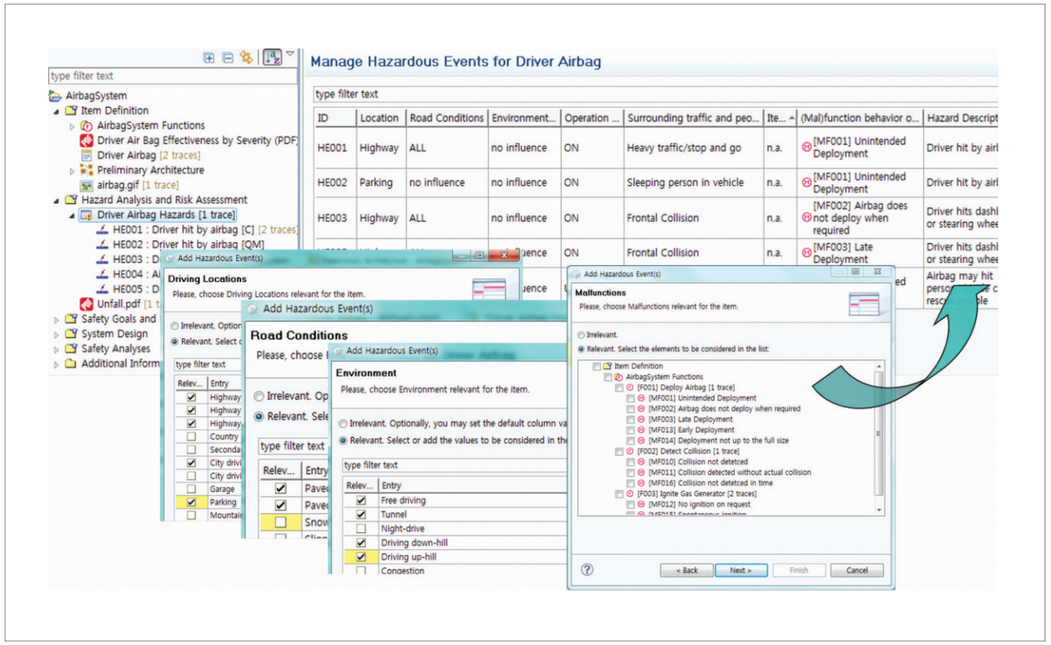
쉬운 예로 순항제어 시스템(Cruise Control)을 생각해 보자. 정속주행 시스템이라고도 불리는 이 장치는, 차량의 속도를 일정하게 유지시키기 위해 회전식 구동축, 속도계 케이블, 바퀴의 속도 센서나 엔진 관리 시스템 등과의 상호작용이 필요하다. 이처럼 각 아이템이 지니는 특성과 아이템 간의 상호작용에 따라 시스템의 기능이 설정되며, 이는 곧 위험 분석 및 평가 활동을 위한 기본 데이터가 된다.

ISO 26262 Part 3 – 위험 분석 및 평가(Hazard Analysis and Risk Assessment)

위험 분석 및 평가 활동은, 아이템의 기능 불량이나 동작 상태, 차량 운행 환경 등의 정보가 포함된 위험 상황 분석 작업을 통해 수행될 수 있다. 여기서 말하는 위험 상황이란, 아이템이 의도하지 않은 동작을 해여 발생할 수 있는 사건을 의미한다. 예를 든 순항제어 시스템의 경우에는 "자동차 실제 속도의 변경 명령이 주어지지 않았음에도 미끄러운 도로 표면으로 인한 의도되지 않은 가속"을 할 수 있다.

다시 말해, ISO 26262 Part 3에서 요구하는 위험 분석 및 평가 활동은 위험한 상황을 발생시킬 수 있는 모든 사건들을 분석해 최종적으로 ASIL 등급 할당과 안전 목표를 설정하는 순으로 진행된다.

문제는 시스템의 복잡도에 따라 발생 가능



[그림 2] medini analyze의 위험 분석 및 평가 활동 수행

한 위험 상황의 수가 수 천, 수 만개까지 만들어 질 수 있다는 사실이다. 더욱이, ISO 26262의 경우 아이템 단계에서부터 시스템 단계까지 정의된 모든 항목들이 추적성과 일관성을 가져야 한다고 명시하고 있다. 따라서 이러한 요구사항들을 준수하며 안전 활동 검증(Safety Assessment) 작업을 수행하는 데에는 안전 관리 도구 없이는 매우 난해한 작업이 될 수밖에 없다. 그렇다면 위의 작업들이 어떻게 도구를 통해 구현 될 수 있는지 그림과 함께 간략하게 살펴보겠다.

그림 2는 medini analyze가 기본적으로 제공하는 운전환경 설정 값과 데이터 입력 자동화 기능을 이용한 위험 분석 및 평가 활동 수행 화면이다. 분석하고자 하는 아이템의 특성에 해당하는 항목들을 선택하면 이에 따라 위험분석 테이블이 자동으로 생성된다. 여기까지의 위험분석 작업이 완료되면 medini analyze가 제공하는 ASIL 등급 결정 마법사를 통해 각 Hazardous Event마다 ASIL등급과 안전 목표를 설정할 수 있다. 안전 목표란 안전 요구사항의 최상위 개념으로서 위험 상황을 예방하기 위한 위험 분석 및 평가 활동의 결과물이다. 즉, 앞서 언급한 순항제어 시스템의 안전 목표는 "표면이 젖어있는 도로에서 차량 운행시 동작을 금한다"로 설정될 수 있다.

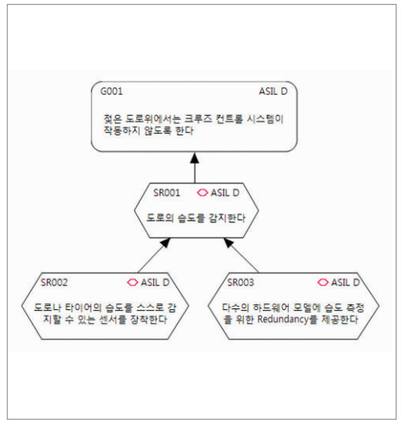
ISO 26262 Part 3 – 기능 안전 요구사항 및 분석(Functional Safety Requirements and Analysis)

위험 분석 및 평가 활동을 통해 각 위험 상황의 ASIL 등급과 안전 목표 설정까지 완료되면, 이를 바탕으로 기능 안전 요구사항들을 도출하게 된다. 기능 안전 요구사항은 쉽게 말해 안전 목표를 충족시키기 위한 하위 조건으로 설명될 수 있는데 이는 **그림 3**을 보면 이해가 쉽다.

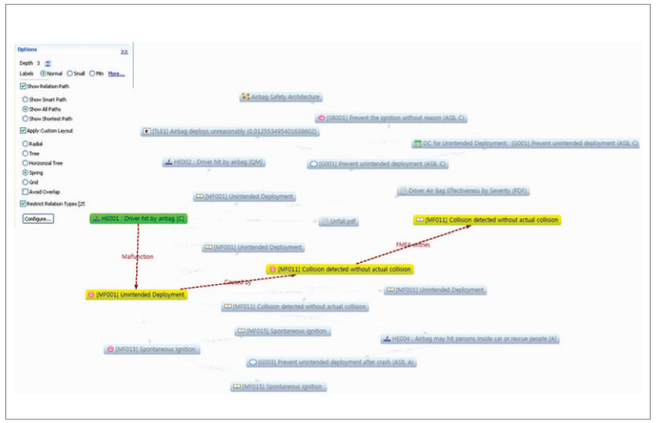
이렇게 안전 요구사항(Safety Requirement)이 도출되면, 이어서 요구사항 분석 및 검증을 위한 시스템의 정성적, 정량적 안전 분석(Safety Analysis) 기법인 FMEA와 FTA 분석 작업을 수행한다.

FMEA/FTA – 추적성(Traceability)의 중요성

FMEA나 FTA와 같은 Safety 분석은 이미 자동차 산업에서는 익숙한 기법이다. 잠재적인 불량 인자를 찾고 시스템의 의도되지 않은 결함을 예방하기 위한 방법론으로서 현재까지도 가장 많이 이용되고 있다. 이같은 Safety 분석을 통해 시스템을 구성하는 수백, 수천 개의 부품들과 기능들이 일으키는 결함을 찾고 예방한다. 문제는 이렇게 방대한 양의 항목들을 어떻게 ISO 26262가 강조하고 있는 추적성(Traceability) 요소를 만족시키며 관리 할 수 있는지이다. 예를 들어 순항제어 시스템을 구성하는 여러 개의 센서 중 하나가 결함을 일으켰다고 가정해 보자. 이 경우 FMEA나 FTA는



[그림 3] medini analyze의 안전 요구사항 다이어그램 구성 화면



[그림 4] medini analyze의 추적성 기능

우리에게 해당 센서에 대한 불량률이나 시스템에 미치는 영향 등은 알려 줄 수 있다. 그러나 그로 인해 다른 어떤 센서나 아이템이 영향을 받아 또 다른 위험 상황을 야기할 수 있는지, 위반되는 요구사항은 무엇인지 등의 정보는 파악하기 힘든 것이 사실이다.

이처럼 추적성(Traceability) 요소를 지키며 방대한 양의 데이터를 관리하기 위해 medini analyze는 추적성(Traceability) 기능을 기본적으로 제공하고 있어, 각 아이템을 포함한 시스템 전체의 항목별 영향 분석 시 매우 효율적이라 할 수 있다.

하나의 항목이 각 프로세스 별 어떤 항목, 요구사항들과 연관돼 있는지는 "Dependency View"를 이용하면 **그림 4**와 같이 한눈에 확인이 가능하다.

이 외에도 SysML을 이용한 아이템/시스템 레벨 아키텍처 구성 작업과 각 프로세스 별 검증 기능 등을 지원해 ISO 26262 기능 안전 관리를 위한 도구로서의 역할을 하고 있다.

정리하며

이 글에서 중점적으로 언급한 Part 3 부분은, 아이템의 ISO 26262 프로세스가 안전(Safety) 관점에서 어떻게 흘러갈 것인지 그 방향을 잡는 단계라는 점에서 의미가 크다. 특히 위험 분석 및 평가 활동의 경우 분석하고자 하는 아이템의 ASIL 등급이 어떻게 설정되느냐에 따라 규격에서 요구하는 사항들이 달라진다. 또한 이에 맞춰 수행해야 하는 모든 안전 분석, 검증 활동들이 상호 연관성을 가지고 일관된 프로세스를 구축하도록 관리하는 것이 무엇보다 중요하다. 다시 말해 기능 구현을 위한 기존 개발/관리 프로세스와는 별도로 안전(Safety)에 포커스를 맞춰 방대한 양의 데이터를 얼마나 명확하고 일관성 있게 관리할 것인지가 ISO 26262 규격 준수의 핵심이라고 할 수 있다. 관리하는 방법에 따라 실제 소요 시간과 비용이 달라지므로 효과적인 ISO 26262 프로세스 적용을 위해 medini analyze와 같은 안전 관리 도구의 사용이 매우 바람직하다고 할 수 있다.