ISO 26262 제품개발 프로세스와 연계된 DFSS 로드-맵의 개발

홍성훈¹ · 권혁무² · 김동준¹ · 이민구^{3*}

¹전북대학교 산업정보시스템공학과 / ²부경대학교 시스템경영공학과 / ³충남대학교 정보통계학과

Development of a DFSS Road-map Associated with the ISO 26262 Product Development Process

Sung-Hoon Hong¹ · Hyuck Moo Kwon² · Dong-Chun Kim¹ · Min Koo Lee³

¹Department of Industrial & Information Systems Engineering, Chonbuk National University

²Department of Systems Management and Engineering, Pukyong National University

³Department of Information and Statistics, Chungnam National University

Increasing safety requirements of automobile are asking companies to find out solutions, based on the ISO 26262 which is a functional safety standard. ISO 26262 is an adaptation of the IEC 61508 for automotive electric/electronic systems. ISO 26262 provides a V model for ECU (Electronic Control Unit) development process to secure safety against vehicle. It well describes the requirements, necessary works and their resulting products for each development phase. However, it is difficult to apply to product development for achieving functional safety in the electric/electronic systems of an automobile because it lacks explanation on the working steps to follow and the methodologies and tools to be used in each step.

In this paper, we introduce the outline of the ISO 26262 product development process and present a DFSS (Design For Six Sigma) road-map based on the ISO 26262 product development process as a way to operate efficiently the ISO 26262 product development process. The DFSS road-map consists of five phases: Define, Measure, Analyze, Design, and Verify. The detailed activities, tools, inputs, and work products are given for each phase.

Keyword: DFSS road-map, ISO 26262, product development process

1. 서론

최근 자동차 시장에서 차량의 기능안전성과 관련된 고객의 요구수준이 높아짐에 따라 조작성의성과 안락한 승차환경을 구현하기 위해 장착되는 전자제어장치의 수가 급격히 증가하고 있어 자동차는 기계제품으로부터 전자제품으로 이행하고 있는 중이다(Kwon *et al.*, 2012). 현재 일반적인 고급승용차 한 대에 장착되는 전자제어장치(ECU: Electronic Control Unit)의 수가 적어도 70개 이상으로 추정되며(Bellotti and Mariani, 2010; Mad

et al., 2011), 향후 석유자원 고갈 및 기후변화 대응과 관련하여 개발이 되었거나 개발 중인 하이브리드 자동차와 전기자동차의 등장은 이와 같은 추세를 더욱 가속화시킬 전망이다. 최근 자동차에 장착되는 전자제어장치의 수가 증가함에 따라 자동차의 안전기능에 대한 여러 가지 문제점과 차량 안전과 관련된 사고가 자주 발생하고 있다. 2009년 도요타 자동차 렉서스 ES 350의 가속페달 결함으로 인한 안전사고가 발생한 이후 도요타는 2010년 전 세계 판매량인 827만대를 넘어서는 910만대에 이르는 차량에 대하여 리콜 및 자율수리 조치를 취하였다.

이 논문은 품질혁신기반구축 사업의 지원에 의해 연구되었음.

*연락처 : 이민구 교수, 305-764 대전광역시 유성구 궁동 220 충남대학교 정보통계학과,

Fax : 042-822-0260, E-mail : sixsigma@cnu.ac.kr

투고일(2012년 07월 27일), 심사일(1차 : 2012년 09월 17일, 2차 : 2012년 10월 10일), 게재확정일(2012년 10월 10일).

이로 인해 도요타 자동차는 안전과 품질에 대한 자사 이미지 실추로 인해 시장점유율이 급격하게 줄었다고 알려져 있다. 또한 국내외적으로 자동차의 급발진 사고와 규명되지 않은 자동차와 관련된 안전사고 등이 끊이지 않고 발생하고 있어 자동차의 기능안전성과 관련된 관심이 어느 때 보다도 높아지고 있다. 이와 같이 전자제어장치의 도입 증가는 자동차의 조작을 편하게 해주고, 보다 안락한 차량운전 환경을 제공하지만, 기술적으로는 자동차를 대단히 복잡한 시스템으로 바꿔 이에 따른 여러 가지 부작용을 동반하게 되었다(Kwon *et al.*, 2012). 지난 20년간 하이테크 전자제품에서 원인을 알 수 없는 고장현상이 꾸준한 증가추세를 보이고 있으며 (Brombacher *et al.*, 2005), 일례로 한 미국 자동차회사의 내부조사에 의하면, 사용현장에서의 고장문제 중 35~40%가 시스템 간 상호작용과 관련이 되어 있다고 한다(Yadav and Singh, 2008). 급발진 등 원인을 규명하기 어려운 고장은 단순한 고장의 문제뿐만 아니라 고객에게 재산상, 신체상 치명적인 손상을 입힐 수도 있다. 따라서 자동차의 기능 편의성도 중요하지만 이를 뒷받침할 수 있는 자동차의 기능안전 설계가 매우 중요하다. 이에 따라 자동차 기능안전성을 확보하기 위해 지난 6년 간의 개발기간을 걸쳐 2011년 11월 관련 국제표준인 ISO26262가 제정되었다(ISO 26262-1~9, 2011).

ISO 26262는 자동차 내 전기/전자 시스템(Electrical and/or Electronic System)이라는 응용분야에 특화된 요구에 따라 IEC 61508을 적용한 것이다. ISO 26262는 무게 3.5톤을 넘지 않는 승용차에 장착되는 안전과 관련된 시스템으로서 적어도 하나 이상의 전기 또는 전자시스템을 포함하고 있을 경우에 적용되는 표준이다. ISO 26262에서 규정하고 있는 제반 사항은 법적으로 강제되는 조항은 아니지만 제조물 책임법(PL법)과 연동되어 자동차 제조회사 및 관련 협력사가 따를 수밖에 없는 요건이다. 만약, 자동차 운행 중 사고가 발생했다면 제조회사는 자사의 책임이 아님을 입증하기 위해 현존하는 최고 기술수준을 적용하여 개발, 설계 및 제작되었음을 보증해야만 한다(Bellotti and Mariani, 2010). 이와 관련하여 ISO 26262가 제정됨에 따라 자동차 제조사와 부품업체들의 기술적 결함에 대한 부담은 더욱 커질 것으로 예상된다. 예를 들어 차량 급발진 사고가 발생했을 때 자동차 제조사나 부품업체가 안전을 충분히 고려하여 적합하게 개발, 설계되어 제작하였다는 증거를 제시해야 한다. 만일 ISO 26262에 제시하고 있는 절차에 따라 운전자의 측면에서 차량 안전을 충분히 고려하여 제작되었다면 이는 강력한 증거자료가 될 수 있다(Chae, 2011). 이에 따라 유럽의 선진 자동차 회사들은 자동차에 탑재되는 전자부품에 대해 ISO 26262 요건을 충족할 것을 요구하고 있으며, 향후 모든 자동차 회사가 새로운 제품 혹은 모델을 개발할 때 이 표준을 따를 것으로 생각한다.

ISO 26262는 10개 부분으로 구성되어 있다. 제 1부에서는 용어를 정의하고 있으며, 제 2부는 기능안전성 관리, 제 3부는 개념단계, 제 4부는 시스템 수준의 제품개발, 제 5부는 하드웨어

(HW) 수준의 제품개발, 제 6는 소프트웨어(SW) 수준의 제품개발, 제 7는 생산 및 운용, 제 8부는 지원 프로세스, 제 9부는 ASIL (Automotive Safety Integrity Level: 안전 무결성 수준) 및 안전 기반 분석 그리고 제 10부는 ISO 26262에 대한 지침을 다루고 있다. 이 중 제품개발 프로세스는 제 3부에서부터 제 7부까지에 걸쳐 기술하고 있으며, ISO 26262의 제품개발 프로세스는 상기 각 단계별로 해야 할 구체적이고 상세한 내용들을 다루고 있다. 따라서 자동차 업체나 부품업체에서 ISO 26262의 제품개발 프로세스에 따라 제품을 개발하면 자동차의 기능안전성을 달성하는데 많은 도움이 될 것으로 기대한다. 그러나 ISO 26262의 제품개발 프로세스를 진행하다 보면 HW 설계와 SW 구현의 단계에서 HW와 SW의 개발을 하나의 독립적인 과제로 진행해야만 하는 경우가 자주 발생한다. 하지만 ISO 26262의 제품개발 프로세스는 제품의 기능안전 요건에 국한되어 있기 때문에 제품의 전체적인 개발 프로세스 관점에서 보면 HW나 SW의 개발 과제들을 효율적이고 효과적으로 관리하지 못한다. 따라서 ISO 26262에서 기술하고 있는 제품개발 프로세스를 충실하게 반영하면서 HW 설계 및 SW 구현에 대한 효율적이고 효과적인 관리 방법이 필요하다. 6시그마는 모든 종류의 프로세스에서 결함을 제거하고 목표로부터 이탈을 최소화하여 조직의 이익창출과 함께 고객만족을 최대화하고자 하는 혁신전략으로 시스템적인 접근 방법을 통해 프로젝트들의 진행을 효율적이고 효과적으로 관리 한다. 6시그마의 진행 로드맵은 그동안 많은 기업에서 사용되었으며 그 효과가 이제 입증된 단계에 이르렀다. 특히 6시그마 DFSS의 로드맵은 제품의 전체적인 개발 프로세스에 있어 매우 효율적이고 효과적인 방법임이 여러 기업들에서 입증되었다. 이러한 점에 근거하여 본 논문에서는 ISO 26262 제품개발 프로세스를 효과적이고 효율적으로 운영하기 위하여 ISO 26262 제품개발 프로세스와 연계된 DFSS 로드-맵을 개발하고자 한다. 본 논문의 구성은 다음과 같다. 제 2장에서는 ISO 26262 제품개발 프로세스를 살펴보고 이를 기반으로 제 3장에서는 ISO 26262 제품개발 프로세스와 연계된 DFSS 로드-맵을 제시하고 각 단계에서 수행해야 할 활동들에 대해 살펴본다.

2. ISO 26262의 제품개발 프로세스

ISO 26262 제품개발 프로세스(V-모델)의 핵심 단계를 살펴보면 <Figure 1>과 같다. 제품개발 프로세스는 제 3부의 개념단계, 제 4부~제 6부의 제품개발 및 제 7부의 생산운용 단계로 구성되어 있다. 일반적인 제품개발 프로세스와 같이 ISO 26262 제품개발 프로세스도 프로세스를 구성하는 각 단계의 산출물은 다음 단계의 입력물이 되거나 참조되어 후속작업이 이루어진다. ISO 26262에서는 제품개발의 각 단계에서 해야 할 활동과 산출물이 구체적으로 제시되어 있다. 이에 대한 자세한 내용은 참고 문헌(ISO 26262-3~7, 2011)을 참조하기 바란다. 본 장

에서는 ISO 26262 제품개발 프로세스의 각 단계에서 수행되어야 할 주요 작업들을 중심으로 ISO 26262 제품개발 프로세스를 개략적으로 살펴본다.

2.1 개념 단계

개념 단계에서 수행할 일은 아이템 정의, 안전수명주기의 설정, H&R (Hazard analysis and Risk assessment : 위험원 분석과 리스크 평가), 기능안전성 개념의 설정이다.

아이템 정의는 시스템의 기본적인 정의와 역할 등을 기술함으로써 개발하려는 아이템을 명확하게 정의하는 것이다. 일반적으로 한 아이템이 독립적으로 작용하는 경우는 드물고 여러 아이템과 신호를 주고받으며 역할을 수행하기 때문에 아이템 자체에 대해 기술하고, 주변 환경이나 타 아이템과의 의존관계 및 상호작용에 대해 기술함으로써 개발하고자하는 아이템에 대해 올바르게 이해할 수 있도록 하여 후속 단계의 활동 수행에 지장이 없도록 해야 한다. 아이템의 정의 단계의 주요 산출물은 아이템 기술서이다.

안전수명주기의 설정은 새로운 아이템의 개발과 기존 아이템의 수정을 구별하고, 안전수명주기 상 기존 아이템의 수정시 진행되어야 할 활동들을 정의하는 것이다. 이를 위해서 수정에 따른 영향도 평가가 선행되어야 하고, 그 결과를 반영하여 개량된 안전 계획이 수립되어야 한다. 안전수명주기의 설정 단계의 주요 산출물은 영향분석(Impact analysis) 결과서와 안전 계획서(Safety plan)이다.

H&R는 아이템의 오작동으로 초래될 수 있는 위험원들을 식별 및 분류하고, 안전과 관련된 부당한 위험을 피하기 위해 위험 사건의 방지 혹은 완화에 관련된 안전 목표를 설정하는 것이다. 여기서 위험원이란 아이템이 의도되지 않은 동작을 하

여 발생할 수 있는 사건을 야기하는 원인들을 나타낸다. H&R의 세부 활동으로서 상황을 분석하여 위험원을 식별하고 그 영향도와 노출 확률 및 통제 가능성을 추정한다. 추정 결과에 따라 ASIL 등급이 정해지고 그에 따른 안전 목표가 결정된다. 참고로 ASIL 등급 결정시 고려되는 요소는 심각도, 노출 확률 및 통제가능성이다. 그리고 H&R 및 안전 목표는 아이템의 오작동으로 인한 위험 상황 및 위해를 빠짐없이 취급하고 있는지, 아이템 정의에 부합되는지, 관련된 H&R과 일관성이 있는지, 위험 사건을 빠짐없이 포괄하고 있는지, 위험사건에 대해 할당된 ASIL 등급에 일관성이 있는지 등을 입증하기 위한 검증 절차를 거쳐야 한다. H&R 단계의 주요 산출물은 위험원 분석과 리스크 평가서, 안전 목표 수준 및 이들의 검증·검토 보고서이다.

기능안전성 개념의 설정은 안전 목표로부터 FSR(Functional Safety Requirements : 기능안전성 요구사항)들을 도출하고, 이들을 아이템의 예비 아키텍처 엘리먼트 및 외적 수단에 할당하는 것이다. 기능안전성의 개념은 결함 탐지 및 고장 완화, 안전 상태로의 전환, 결함 방지 메커니즘, 결함 탐지 및 경고 신호, 최적제어 로직 등을 취급해야만 한다. 기능 안전성 개념 역시 안전 목표에 부합되고 일관성이 있는지, 위험사건을 피하거나 완화시킬 수 있는지의 검증절차를 거쳐야 한다. 기능안전성 개념의 설정 단계의 주요 산출물은 기능 안전성 개념 기술서와 기능안전성 개념 검증 보고서이다.

2.2 제품개발 단계

제품개발 단계는 시스템 수준, HW 및 SW 수준의 제품개발과 기능안전성 평가 및 검증의 단계로 구성되어 있다. 각 단계별 활동을 간략하게 살펴보면 다음과 같다. 자세한 내용은 참

Figure 1. Product Development Process on ISO 26262 (V-Model)

고문헌(ISO 26262-3~6, 2011)을 참고하기 바란다.

(1) 시스템 수준의 제품개발

시스템 수준의 제품개발 목적은 시스템 개발의 각 하위단계에서 수행 할 기능안전 활동을 결정하고 계획하는 것이다. 시스템 수준의 제품개발 진행은 시스템 수준의 제품개발 착수, TSR(Technical Safety Requirements : 기술안전 요구사항) 작성 및 시스템 설계의 순서로 수행된다.

시스템 수준의 제품개발 착수는 위에서 열거한 제품개발의 각 하위단계에서 기능안전과 관련된 활동들을 결정하고 계획하는 것이다. 또한, 필요한 지원 프로세스들도 정한다. 이 활동의 주요 산출물은 프로젝트 계획서, 안전 계획서, 아이템 통합 및 시험 계획서, 검증계획서 및 기능안전성 평가 계획서를 들 수 있다.

TSR 명세서는 기술적인 안전 요구사항들을 명시하고 있으며, 기능안전 개념 및 예비 아키텍처를 기본으로 기능안전 개념을 구체화하고 TSR이 FSR에 부합되는가를 분석하여 검증하는 것이다. 즉, 아이템 수준의 FSR을 시스템 수준의 TSR로 구체화하는 것을 의미한다. 또한 TSR은 시스템 혹은 엘리먼트의 안전에 영향을 미치는 자극에 대한 반응을 명시해야만 한다. 이 활동의 주요 산출물은 TSR 명세서, 시스템 검증 보고서 및 검증 계획서이다.

시스템 설계는 FSR과 TSR 명세에 부합되는 기술안전개념 및 시스템 설계를 수행하고 검증하는 것이다. 시스템 설계 및 기술안전개념은 기능안전 개념으로부터 유도된 TSR 명세에 기초하여 개발한다. 만약 시스템이 하부 시스템들로 구성되어 있다면 이 작업은 반복적으로 시행된다. 시스템 아키텍처 설계를 위해서 FSR, TSR, 그리고 안전과 관계없는 요구사항들도 구현되어야 한다. 즉, 이 단계에서는 안전에 관계된 요구사항들과 안전과 관계없는 요구사항들을 하나의 개발프로세스 내에서 수행되어야 한다. 시스템을 설계하는 동안 시스템 아키텍처가 확립되고 TSR이 아이টে를 구성하는 HW와 SW에 할당되며, 필요하다면 다른 기술에도 할당된다. 또한, HW와 SW간 HSI(Hardware Software Interface: 인터페이스)를 포함하여 시스템 아키텍처로부터 발생하는 TSR들을 추가하고 기존의 TSR들을 개선한다. 이에 따른 주요 산출물은 기술적 안전 개념서, 시스템 설계 명세서 및 HSI 명세서를 들 수 있다.

(2) HW 수준의 제품개발

HW 수준의 제품개발도 <Figure 1>의 V 모델을 따르며, HW 제품개발 착수, HSR(Hardware Safety Requirements: 하드웨어 안전 요구사항) 명세서 작성, HW 설계, HW 아키텍처 지표 평가, HW 우발고장에 의한 안전목표 침해 평가, HW 통합 및 시험의 순서로 진행된다. HW 수준의 제품개발의 주요 산출물은 HW 수준의 제품개발 착수를 위한 요구사항 명세서, HSR 명세서, HW 설계도, HW 아키텍처 평가표 및 HW 우발 고장으로 인한 안전 목표 및 HW 통합과 시험 결과서 등이다.

(3) SW 수준의 제품개발

SW 수준의 제품개발 프로세스 역시 <Figure 1>의 V 모델을 따라 SW 제품개발의 착수, SSR(Software Safety Requirements: 소프트웨어 안전 요구사항) 명세서 작성, SW 아키텍처 설계, 단위 SW 설계 및 구현, 단위 SW 시험, SW 통합 및 시험, SSR 입증 순서로 진행된다.

SSR을 정의할 때 안전 요구사항의 명세서 작성 및 관리, 특정 시스템 및 HW 아키텍처, 관련 HW 설계 명세서 내의 요구사항, 시간적 제약, 외부 인터페이스, SW에 영향을 주는 차량, 시스템 혹은 HW의 운전 모드 등을 고려해야 한다. SSR 명세서는 이해가 가능하고 모호하지 않아야 하며, 하나의 기능을 제공하고 내적 일관성이 유지되어야 하며, 그리고 실현 및 검증이 가능해야 한다. 이 단계의 주요 산출물은 SW 수준의 제품개발 착수를 위한 요구사항 명세서, SSR 명세서, SW 아키텍처 설계도, SW 유닛 설계도, SW 유닛 시험 보고서 및 SSR 입증서 등이다. HW 수준의 제품개발과 유사하게 SW 개발에서 구현해야 할 SW 유닛이 여러 개인 경우, 하나의 유닛을 하나의 단위 프로젝트로 나누어서 진행하는 것이 좀 더 효율적이고 효과적이다.

(4) 제품개발의 기능안전성 평가 및 검증

HW 및 SW 수준의 제품개발이 완료되고 나면 아이টে 통합 및 시험, 안전성 입증, 기능안전성 평가, 생산 이전 순으로 검증 및 생산 준비 작업이 수행된다.

2.3 생산운용 단계

생산운용 단계의 목적은 자동차에 설치될 안전과 관련된 엘리먼트나 아이টে에 대한 생산 프로세스를 개발하고 유지하며, 프로세스에 책임이 있는 관련 제조사나 개인 또는 기관(차량 제조사, 공급자, 하위 공급자 등)에 의해 생산하는 차량의 기능 안전성을 확보하는 것이다. 이를 부연하여 설명하면, 생산 이행에서 아이টে이 차량 수준에서의 기능 안전 요구사항에 부합된다는 것을 확인하는 것을 의미한다. 생산 이행에 필요한 문서로서 이행 책임자의 이름과 서명, 이행 아이টে의 버전, 이행 아이টে의 형상, 관련 문서들의 참고 문헌, 이행 날짜 등을 들 수 있다.

3. ISO 26262와 연계된 DFSS 로드-맵의 진행절차

ISO 26262의 제품개발 프로세스를 실행하다 보면 HW 수준의 개발 단계와 SW 수준의 개발 단계에서 HW 설계와 SW 구현을 독립적으로 진행해야만 하는 경우가 발생한다. 그러나 ISO 26262의 제품개발 프로세스는 제품의 기능안전과 관련된 사항에 국한되어 있기 때문에 제품의 전체적인 개발 프로세스 관점에서 보면 HW나 SW의 개발 과제들을 효율적이고 효과적으로 관리하지 못한다. 따라서 ISO 26262에서 기술하고 있는 제

품개발 프로세스를 충실하게 반영하면서 HW 설계 및 SW 구현에 대한 효율적이고 효과적인 관리 방법이 필요하다. 이러한 점에 근거하여 본 장에서는 ISO 26262 제품개발 프로세스를 효과적이고 효율적으로 운영하기 위하여 ISO 26262 제품개발 프로세스와 연계된 DFSS 로드-맵을 제안 한다. 먼저 DFSS 로드-맵을 제시한 후, 로드-맵을 구성하는 각 단계별 실행절차에 대하여 기술한다.

3.1 DFSS 로드-맵

본 논문에서는 ISO 26262 제품개발 프로세스와 연계된 DFSS 로드-맵으로 6시그마 설계 방법론의 주요 로드-맵 중 하나인 DMADV(Define, Measure, Analyze, Design, Verify) 로드-맵을 적용한다. <Figure 2>는 DMADV 로드-맵에서 수행해야 할 활동들을 나타낸 것이다.

정의(Define) 단계의 주요 활동은 OEM 요구 아이템 중 기업의 경영 목표와 회사의 경쟁력을 높일 수 있는 아이템의 ASIL을 프로젝트의 목표로 선정하고 정의하는 것이다. 아이템을 개발하는 프로젝트의 수행 주체는 임원이나 해당 개발팀장으로 프로젝트의 목적은 아이템의 안전 목표를 달성하는 것에 맞추어야 한다. 프로젝트의 리더는 DMADV의 전체 과정 동안 전반적인 기능 안전성 관리 요구사항의 정의, 진행 및 관리를 담당한다. 정의 단계에서는 아이템의 선정 및 정의의 활동을 진행한다.

측정(Measure)단계는 해당 아이템의 안전수명주기 설정, H&R을 통한 ASIL 및 안전 목표를 결정하는 활동을 진행한다.

분석(Analyze) 단계는 기능 안전성 개념 설정 및 이를 토대로 FSR 및 TSR 명세서를 작성하며, 이를 바탕으로 시스템 수준의 제품을 개발하는 단계이다. 이를 위해 시스템 개념설계를 진

행한다.

설계(Design) 단계에서는 필요한 경우 시스템은 다시 여러 개의 서브 시스템으로 분해하여, 이를 바탕으로 상세 시스템을 설계한다. 설계 단계의 주요 활동은 시스템을 구성하는 HW 설계와 SW 구현이며, 이를 위해 HW 설계와 SW 구현을 하나의 독립된 과제로 나누어서 진행한다. 참고로 프로젝트 리더는 아이템을 구성하는 HW 설계와 SW 구현을 가장 잘 수행할 수 있는 담당자를 선정하여 프로젝트를 진행할 필요가 있으며, 선정된 프로젝트가 잘 진행될 수 있도록 효율적이고 효과적인 지원 및 관리를 해야 한다. 설계 단계에서의 주요 산출물은 HSR 명세서, HW 설계, SSR 명세서, SW 아키텍처 설계 등이다. 또한 설계 단계에서는 아이템을 구성하는 HW 설계와 SW 구현을 완료한 다음 HW 요소 별 시험 및 SW 유닛 별 시험을 실시하여 시스템 설계에 부합하는지를 검토하고 피드백 한다.

입증(Verify) 단계는 설계 단계에서 완료한 HW 설계와 SW 구현을 통합하고 시험하여 안전목표 달성 여부를 확인한 후 생산으로 이전 준비를 한다. 입증 단계의 세부 진행은 SW 수준 통합 및 시험, SSR 입증, HW 수준 통합 및 시험, 안전성 입증, 기능안전성 평가, 생산 이전의 세부 활동을 진행한다. <Figure 3>은 ISO 26262 제품개발 프로세스와 DFSS 로드-맵의 관계를 나타낸 것이다. 다음 장에서는 DFSS 로드-맵의 세부 실행절차에 대해 살펴본다.

3.2 DFSS 로드-맵의 세부 실행 절차

(1) 정의 단계

정의 단계의 세부 진행사항은 아이템 선정 및 아이템 정의이다. 아이템 선정 활동에서는 OEM에서 요구한 아이템 중 기

Figure 2. Project Progress Roadmap

Figure 3. The Framework of DFSS Process for ISO 26262

업의 경영 목표와 회사의 경쟁력을 높일 수 있는 아이템을 개선 대상 프로젝트로 선정하는 것이 바람직하다.

아이템을 정의하는데 있어 해당 아이템 자체에 대해 기술하고, 주변 환경이나 타 아이템과의 의존관계 및 상호작용에 대해 기술함으로써 후속 단계에 지장이 없도록 하는 것이 중요하다. 아이템의 정의는 정의하고자 하는 아이템과 관련된 기존의 정보들을 활용하여 아이템을 정의한다. 예를 들면 아이템의 아이디어, 프로젝트 스케치, 관련된 특허, 기존 아이템과 관련된 기술 문서 및 다른 독립적인 아이템의 관련 정보들을 활용한다. 정의 단계의 주요 결과물은 프로젝트 아이템, 아이템 정의의 기술서 등이다.

<Table 1>은 정의 단계의 세부 진행 내용, 사용도구, 입력요소 및 결과요소를 정리한 것이다. 세부 진행 단계별 수행해야 할 구체적인 내용이나 방법은 ISO 26262의 제 3부를 참조하기 바란다.

(2) 측정 단계

측정 단계에서는 해당 아이템의 안전수명주기 설정, H&R를

통한 ASIL 목표 설정 및 안전 목표를 결정한다.

안전수명주기의 설정 활동에서는 새로운 아이템의 개발과 기존 아이템의 수정을 구별하고, 안전수명주기 상 기존 아이템을 수정 시 수행해야 할 활동들을 결정한다. 새로운 아이템을 개발할 경우에는 H&R와 함께 안전수명주기의 설정이 진행되어야 하며, 기존 아이템을 수정하는 경우에는 수정에 따른 영향도 평가가 선행되어야 한다. 그리고 평가 결과를 반영하여 개량된 안전계획이 수립되어야 한다.

H&R에서는 아이템의 오작동으로 초래될 수 있는 위험원들을 분류하여 분석하고, 위험을 평가하여 ASIL 등급을 설정한다. 또한 부당한 위험을 피하기 위하여 위험 사건의 방지 혹은 완화에 관련된 안전 목표를 설정한다. H&R의 세부 활동으로서 상황을 분석하여 위험원을 식별하고 그 영향도와 노출확률 및 통제가능성을 추정한다. 이에 따라 ASIL의 등급이 정해지고 관련 안전 목표가 결정된다. 안전 목표는 각 위험 사건별로 ASIL과 함께 정해지는데, 만약 비슷한 안전 목표들이 정해지면 하나의 목표로 합칠 수도 있다.

<Table 2>는 측정 단계 세부 진행내용, 주요 입력요소, 출력

Table 1. Define Phase

세부진행 단계	진행 내용	입력요소	출력요소	사용도구
아이템 선정	프로젝트를 진행할 대상 아이템을 결정하는 활동	OEM 요구사항	프로젝트 아이템	CTQ 세부전계, Pareto Chart, Technology Roadmap, Technology Tree 등
아이템 정의	아이템의 기술, 환경이나 타 아이템과의 의존관계 및 상호 작용을 기술하여 후속 단계 활동에 지장이 없게 하는 활동	프로젝트 아이템	아이템 정의 기술서	

Table 2. Measure Phase

세부진행 단계	진행 내용	입력요소	출력요소	사용도구
안전수명 주기 설정	신제품인지 기존 제품인지를 구별하고 수행하여야 할 활동 계획 수립	아이템 정의 기술서	안전계획 수립서	FMEA, 특성요인도, FTA, HAZOP 등
H&R 분석	위험원 분석을 통한 안전 목표 결정	아이템 정의 기술서	ASIL 등급, 안전목표 H&R 분석표	

요소 및 사용도구를 정리한 것이다. 진행 단계별 수행해야 할 구체적인 내용이나 방법은 ISO 26262의 제 3부와 참고문헌 (Kim and Jang, 2011)을 참조하기 바란다.

(3) 분석 단계

분석 단계에서는 기능안전성 개념 설정 및 시스템 설계를 포함한다.

기능안전성 개념의 설정은 안전 목표로부터 FSR들을 도출하고 이들을 아이템의 예비 아키텍처 엘리먼트 및 외적 수단에 할당하는 것이다. 기능안전성 개념에는 안전 목표에 부합될 수 있도록 아이템의 아키텍처 엘리먼트에 구현될 안전 메커니즘 등 안전 수단 및 FSR들이 포함되어야 한다. 또한 기능안전성 개념은 결함 탐지 및 고장 완화, 안전 상태로의 전환, 결함 방지 메커니즘, 결함 탐지 및 경고 신호, 최적 제어 로직 등을 포함해야 한다. 시스템 설계는 ISO26262의 안전과 관련된 아이템 개발을 위한 기준 단계 모델의 제 4부에 해당하는 활동들이다. 세부 진행 사항은 시스템 수준의 제품개발 착수, FSR에 기반한 TSR 도출 및 시스템 설계로 구성되어 있다. 시스템을 설계하는 동안 시스템 아키텍처가 확립되고 TSR이 HW와 SW에 할당되며, 필요 시 다른 기타 기술에도 할당된다. 또한 TSR이 좀 더 구체화되고 HSI가 포함된 시스템 아키텍처에서 발생한 안전과 관련된 요구사항이 추가된다. 그리고 아키텍처의 복잡도에 따라서 시스템의 요구사항이 반복적으로 생겨 날 수도 있다.

시스템 수준의 제품개발 착수에서는 제품개발의 각 하위단계에서의 기능안전 활동들을 결정하고 계획하는 것이다. FSR에 기초한 TSR 도출에서는 기능안전 개념 및 예비 아키텍처를 토대로 기능안전 개념을 구체화하고 TSR이 FSR에 부합되는지를 분석하여 검증한다. 즉, 이는 아이템 수준의 FSR을 시스템 수준의 TSR로 구체화하는 것이다. TSR은 시스템이나 아이템 엘리먼트 간, 아이템과 기타 시스템 간의 안전과 관련된 종속성을 명시해야 한다. 또한 TSR에는 안전 목표 달성에 영향을 끼치는 시스템이나 엘리먼트의 반응이 명시되어야 한다. 이들 요구사항에는 고장, 서로 관련된 각각의 운영모드와 정의된 시스템 상태가 결합하여 발생할 수 있는 자극들을 포함한다. 예를 들어 ACC (Adaptive Cruise Control : 적응형 크루즈 컨트롤) ECU(Engine Control Unit)가 브레이크 시스템 ECU에 의해서 차량 안정성 제어기능이 작동되지 않는다는 정보를 받는다면, 이 ACC ECU는 ACC 기능을 작동시키지 않는다.

시스템 설계에서는 FSR과 TSR에 부합되는 시스템 및 기술적 안전 개념을 개발하고 이들이 TSR과 부합하는지를 검증하는 것이다. 또한 시스템 아키텍처를 정하고 TSR들을 HW와 SW에 적절하게 할당하는 작업도 포함한다. 이 단계는 시스템이 여러 하위 시스템들로 구성되어 있다면, 반복하여 적용할 수 있다. 시스템 아키텍처를 설계하기 위해서, FSR과 TSR, 비-안전관련 요구사항들을 고려하여야 한다. 안전 및 비-안전과 관련된 요구사항들은 시스템 개발 단계에서 같이 다루어진다. 또한 TSR들은 시스템 설계 엘리먼트에 할당되어 시스템 설계에 구현되어야 한다. 이 때, 시스템 설계 검증 능력, 기능안전 달성에 관련된 HW 및 SW의 기술적 능력, 시스템 통합 시 시험 수행 능력 등을 고려하여 설계하여야 한다. 시스템 및 하부 시스템 아키텍처는 상응하는 ASIL 등급에서의 TSR과 부합되어야 하는데 각 엘리먼트는 TSR로부터 ASIL 최상위 등급을 상속받는다. HSI 명세서는 HW와 SW의 상호작용을 기술해야 하고 기술 안전개념과 일치되어야 한다. HSI는 SW에 의해 제어되는 컴포넌트의 HW 디바이스 및 SW 실행을 지원하는 HW 자원을 포함한다. 또한 HW 및 SW의 상호작용을 진단할 수 있는 능력도 명시되어야 한다. 그리고 시스템 설계는 시스템 설계 검사, 시스템 설계 검토, 시뮬레이션, 시스템 시작품 및 차량 시험, 시스템 설계분석 등을 통해 기술 안전개념과의 부합성 및 완전성이 ASIL 등급에 따라 적절하게 검증되어야 한다. 본 활동에서는 아이템 통합 및 시험 계획, FSR 명세서, 사전 아키텍처안, 기능 개념 및 기능안전 개념 등의 정보를 활용할 수 있다.

분석단계에서 사용할 수 있는 주요 도구는 QFD/KJ법, PFD, FBD, 벤치마킹, 창의적 사고, Risk Management, 시뮬레이션, TRIZ, FMEA, FTA, ETA(Event Tree Analysis), 마코브 모형 등이다. <Table 3>은 분석 단계 세부 진행내용, 주요 입력요소, 출력요소 및 사용도구를 정리한 것이다.

(4) 설계 단계

ISO 26262와 관련하여 설계 단계에서는 <Figure 1>과 <Figure 3>의 제 5부와 제 6부에 해당하는 아이템의 HW와 SW를 개발하기 위한 절차로 구성되어 있다. 설계 단계에서는 HW 설계와 SW 구현을 위해 이들을 하나의 독립된 과제로 나누어서 진행한다.

HW 설계는 HW 제품의 개발 착수, HSR 명세서 작성, HW 설계, HW 아키텍처 지표 평가, HW 안전목표 침해 평가 및 HW 요소 별 시험의 순으로 진행한다.

Table 3. Analyze Phase

세부진행 단계	진행 내용	입력요소	출력요소	사용도구
기능안전성 개념	안전 목표로부터 FSR을 도출하여 아키텍처 엘리먼트 및 외적 수단에 할당	아이템 정의 기술서, H&R 분석표, 안전목표	FSR 목록	HAZOP QFD/KJ법, PFD/FBD, 벤치마킹/ 창의적 사고, Risk Management, 시물레이션, TRIS, FMEA/FTA/ETA, 마코브 모형 등
시스템 수준의 제품개발 착수	제품개발의 각 하위 단계에서 기능안전 활동들을 결정/계획, 필요한 지원 프로세스 결정	기능안전개념, 입증 계획, 안전목표, 기능개념 등	TSR 명세서, 시스템 입증 보고서, 개정된 입증 계획 등	
FSR에 기반한 TRS 명세 도출	기능안전개념 및 예비 아키텍처를 토대로 기능 안전 개념을 구체화하고 TSR이 FSR에 부합되는지 검증, 아이템수준의 FSR을 시스템 수준의 TSR로 구체화 하는 활동	기능안전개념, 입증 계획, 안전 목표, 기능개념 등	TSR 명세서, 시스템 입증 보고서, 개정된 입증 계획 등	
시스템 설계 (컨셉 디자인)	FSR과 TSR에 부합하는 기술 안전개념 및 시스템 설계를 개발하고 검증, TSR 명세에 기초하여 시스템 아키텍처 개발, TSR의 HW/SW에 배정하는 활동, HSI 명세 작성	아이템 통합/시험 계획, TSR 명세서, 개정된 입증 계획, 기능개념 등	기술안전개념, 시스템 설계 규격, HSI 명세서, 시스템 입증 보고서, 안전분석 보고서 등	

HW 제품개발 착수의 목적은 HW 개발을 위해 수행해야 할 기능 안전 활동을 결정하고 계획하는 것이다. HW 제품개발을 위한 필수 활동과 프로세스에는 기술적 안전 개념의 HW 구현, 잠재적인 HW의 결함과 그 영향 분석, 그리고 SW 개발과의 협력 사항이 포함되어야 한다. 또한 아이템의 HW 개발 절차는 방법과 도구를 포함하여 HW 개발의 모든 하위 단계에서 일관되어야 하고 시스템과 HW 개발 하위 단계와 일치하여 차량의 기능안전과 관련된 요구사항의 흐름이 HW를 개발하는 동안 정확성과 일치성을 유지할 수 있도록 해야 한다.

안전요구사항 명세 작성의 목적은 HSR을 명시하는 것과 HSR이 기술적 안전 개념과 시스템 설계 명세서와 일치하는지를 검증하는 것이다. 안전 요구사항에 대한 내용은 기술적 안전 개념과 시스템 설계 명세서로부터 도출된다. TSR은 HW와 SW에 각각 할당되며, HW와 SW 양쪽에 할당된 요구사항은 HW만을 위한 안전 요구사항을 도출하기 위해 더 나누어진다. 그리고 HSR은 설계 제약사항과 설계 제약사항이 HW에 미치는 영향을 고려하여 더 세분화 된다. 이를 위해 기술적 안전 개념, 시스템 설계 명세서, HSI 명세서 등의 정보를 활용할 수 있어야 한다.

HW 설계의 목적은 시스템 설계 명세서와 HSR에 따라 HW를 설계하고 시스템 설계 명세서와 HSR에 대한 HW 설계를 검증하는 것이다. HW 설계는 HW 아키텍처 설계와 HW 상세 설계를 포함하고 있다. HW 아키텍처 설계는 모든 HW 요소들과 다른 요소들과의 상호작용을 나타낸다. HW 상세 설계는 하드웨어 요소를 구성하는 HW 부품 간 상호연결을 나타내는 전기적 설계의 수준에서 이루어진다. 그리고 단일 HW 설계를 개발하기 위해 모든 비 안전 요구사항은 물론 모든 HSR를 준수해야 한다. 따라서 HW 상세 설계에서는 안전 및 비 안전 요구사항은 하나의 개발 프로세스 내에서 처리된다.

HW 아키텍처의 지표 평가는 제품의 안전 결함과 관련된 요

구사항에 대해 HW 아키텍처 메트릭(Metric)을 이용하여 아이템과 관련된 HW 아키텍처의 안전성을 평가하는 것이다. 이를 위해 HSR 명세서, HW 설계 명세서, HW 안전 분석 보고서 등을 활용하여 아이템의 아키텍처 효용성 분석, 평가 및 검토 보고서를 작성한다.

HW 안전목표 침해 평가는 아이템의 HW 우발고장으로 인한 안전목표가 침해될 수 있는 잔여 위험이 충분히 작다는 것을 판단할 수 있는 기준을 만드는 것이다. 이를 위해 HSR 명세서, HW 설계 명세서, HW 안전 분석 보고서 등을 활용하여 안전 목표 침해 평가서와 H&R 분석표를 작성한다.

HW 요소 별 시험은 설계된 HW를 구성하는 각 요소들에 대하여 시스템 설계 시 의도한 대로 구현이 잘 되었는지를 알아보는 것이다. HW 요소 별 시험에서는 개정된 아이템 통합 및 시험 계획, HSR 명세서, HW 설계 명세서 등을 활용하여 HW 요소 시험 보고서를 작성한다. HW 아키텍처 지표평가와 HW 우발고장에 의한 안전목표 침해 사항에 대한 구체적인 평가 방법은 참고문헌(ISO 26262-5, 2011)을 참고하기 바란다.

SW 구현의 진행은 HW 제품개발과 비슷하게 V 모형을 따라 SW 개발 착수, SSR 명세서 작성, SW 아키텍처 설계, SW 유닛 설계 및 구현 그리고 SW 유닛 시험의 순서로 진행한다.

SW 개발 착수는 SW 개발의 하위 단계 동안 수행해야 할 기능 안전성과 관련된 활동을 계획하고 착수하는 것이다. 이 활동에서는 개정된 프로젝트 계획, 안전 계획, 아이템 통합 및 시험 등의 정보를 이용하여 SW 입증 계획, 모델링 및 프로그램 언어의 설계 및 코딩 지침 등을 마련해야 한다.

SSR 명세서를 작성할 때 안전 요구사항의 명세 및 관리, 특정 시스템 및 HW 아키텍처, HSI 명세서, 관련 HW 설계의 요구사항, 시간적 제약, 외부 인터페이스, SW에 영향을 주는 차량, 시스템 혹은 HW의 운전 모드 등을 고려해야 한다. SSR 명세서는 이해가 가능하고 모호하지 않아야 하며, 하나의 기능을 제공

하고 내적 일관성을 유지해야 하고, 실현 및 검증이 가능해야 한다.

SW 아키텍처 설계는 SSR을 구현하는 SW 아키텍처 설계를 개발하고 구현을 입증하는 것이다. 이를 위해 SSR 명세서, HSI 명세서, 시스템 설계 명세서 및 SW 입증 계획을 활용하여 SW 아키텍처 설계도, 개정된 SSR 명세서, 안전 분석 보고서 및 개정된 SW 입증 계획 등을 작성한다.

SW 유닛 설계 및 구현은 먼저 SW 아키텍처 설계와 관련된 SSR에 따라 SW 유닛을 정의한 다음, SW 유닛을 구현한다. SW 유닛을 설계하고 구현 한 후, 설계 명세서에서 정의한 대로 완료되었는지를 확인한다. 이를 위해 모델링과 프로그래밍 언어를 위한 설계 및 코딩 지침, 개정된 SW 입증 계획, SW 아키텍처 설계 명세서, 개정된 안전 계획 및 개정된 SSR 명세서 등을 활용하여 SW 유닛 설계 명세서, SW 유닛 실행 및 개정된 SW 입증 보고서를 작성한다.

SW 유닛 시험은 SW 유닛이 SW 유닛 설계 명세서를 충족하며 필요 없는 기능은 포함되지 않았다는 것을 증명한다. SW 유닛 시험에서는 개선된 HSI 명세서, 개정된 SW 검증 계획, 개정된 안전 계획, SW 유닛 설계 명세서 및 SW 유닛 구현을 활용하여 개정된 SW 입증 계획, 개정된 SW 입증 명세서 및 개정된 SW 입증 보고서를 작성한다.

설계 단계에서 프로젝트 리더는 HW 설계와 SW 구현을 위한 책임자를 선정하여 과제를 진행하며, 선정된 과제가 잘 진행될 수 있도록 효율적이고 효과적인 지원 및 관리를 해야 한다. 또한 HW 설계와 SW 구현을 진행하는 동안 프로젝트 리더

는 HSR 명세서와 SSR 명세서가 시스템 명세서와 일치하는지 검증하고 피드백 해 주며, 분석 단계에서 도출된 HSI가 시스템 설계에 부합하는지 여부를 확인하고 피드백 하며, HW 설계와 SW 구현의 진도관리를 철저히 해야 한다. <Figure 4>와 <Figure 5>는 설계 단계의 세부 진행 절차와 입력, 출력 및 사용 도구를 기술한 것이다.

(5) 입증 단계

입증 단계는 설계 단계에서 개별적으로 완료한 HW 설계와 SW 구현을 통합하고 시험하여 안전 목표 달성 여부를 확인한 후 생산으로 이전 준비를 하는 단계이다. 입증 단계의 세부적인 진행절차는 <Figure 6>과 같이 HW 통합 및 시험, SW 통합 및 시험, SSR 입증, 안전성 입증, 기능안전성 평가 및 생산 이전의 활동을 포함한다.

HW 통합 및 시험에서는 시험을 통해 개발된 HW가 HSR을 준수함을 보장하는 것이다. 이는 적합한 ASIL에 따라 HSR의 준수를 입증하기 위해 HW 엘리먼트 통합 및 HW 설계 시험을 목적으로 한다. HW 통합 및 시험은 ISO 26262의 제 8부에 해당하는 HW 컴포넌트 활동의 인증과는 다르며, ISO 26262를 준수하여 개발된 아이템 부품, 시스템 또는 엘리먼트의 부분으로 사용하기 위한 중간 수준 HW 컴포넌트와 부품의 적합성에 대한 증거를 제공한다. HW 컴포넌트 활동의 인증에 대한 자세한 내용은 참고문헌(ISO 26262-8, 2011)을 참조하기 바란다.

SW 통합 및 시험에서는 SW 엘리먼트를 통합하고 SW 아키텍처 설계가 임베디드 SW에 의해 구현된다는 것을 증명하는

Figure 4. Design Phase(I)

Figure 5. Design Phase(II)

Figure 6. Verify Phase

것이다. 이 활동에서는 HW와 개정된 HSI 명세서, SW 아키텍처 설계 명세서, 개정된 안전 계획, SW 유닛 구현, 개정된 SW 입증 계획, 개정된 SW 입증 명세서 및 개정된 SW 입증 보고서를 활용하여 개정된 SW 입증 계획, 개정된 SW 입증 명세서 및 임베디드 SW를 만든다.

SSR 입증에서는 임베디드 SW가 SSR을 충족한다는 것을 증명한다. SSR 입증의 목적은 임베디드 SW가 목표 환경에서 안전 요구사항을 만족한다는 것을 증명하는 것이다. 이 활동에서는 SW 아키텍처 설계 명세서, 개정된 안전 계획, 개정된 SSR 명세서, 개정된 SW 입증 계획, 개정된 SW 입증 명세서, 개정된

SW 입증 보고서 및 통합 시험 보고서를 활용하여 SW 입증 계획 수립, SW 입증 명세서 및 SW 입증 보고서를 다시 개정하는 것이다.

아이템 통합 및 시험은 다음과 같이 3단계로 진행된다. 첫 번째 단계는 아이템이 구성하는 각 엘리먼트의 HW와 SW의 통합이다. 두 번째 단계는 완전한 시스템을 만들기 위해 아이템을 구성하는 엘리먼트의 통합이다. 세 번째 단계는 차량 내부 및 차량 자체의 타 시스템과 아이템을 통합하는 것이다. 아이템 통합 프로세스의 목적은 각 명세서와 ASIL 분류에 따라 각 안전 요구사항을 준수하는지 시험하는 것과 안전 요구사항을 포함하는 시스템 설계가 전체 아이템으로 정확히 구현되었는지를 검증하는 것이다. 이 활동에서는 안전목표, 기능안전 개념, 아이템 통합 및 시험 계획, 기술적 안전 개념, 시스템 설계 명세서 및 HSI 명세서를 활용하여 개정된 아이템 통합 및 시험 계획, 통합 시험 명세서 및 통합 시험 보고서를 작성한다.

안전성 입증은 안전목표에 부합되고 기능안전 개념이 아이템의 기능 안전에 적절하다는 증거를 제공하기 위해 실시한다. 또한 안전목표가 올바르며 차량 수준에서 충분히 달성될 수 있고 완전하다는 것을 입증하기 위해 실시된다. 차량에 통합된 아이템의 안전성 입증은 의도된 사용의 적절성에 대한 증거를 제공하고 동일 혹은 동종 차량에 대한 안전 수단의 적절성을 확인하기 위해 실시한다. 안전성 입증은 검사 및 시험을 토대로 안전목표가 적절하고 충분히 달성되었음을 보증하는 것을 포함한다. 그리고 안전성 입증은 제어 가능성, 우발 및 계통적 고장을 제어하기 위한 안전 수단의 유효성, 외적 수단의 유효성, 그리고 타 기술 엘리먼트의 유효성을 차량 수준에서 평가하여 시행한다. 이 활동에서는 H&R, 안전목표, 기능안전 개념 및 개정된 입증 계획을 활용하여 개정된 입증 계획과 입증 보고서를 작성한다.

기능안전성 평가는 아이템으로 구현된 기능안전성을 평가하는 것이다. 기능안전에 책임을 지는 차량 제조업자 혹은 공급자는 기능안전성 평가를 착수하여 아이템에 의해 달성되는 기능안전성을 평가해야 한다. 이를 위해 안전 케이스, 안전 계획, 확인 수단 보고서, 심사 보고서, 기능안전성 평가 계획이 사전에 구비되어 있어야 한다. 기능안전성 평가는 한 명 이상의 담당자를 지정하여 실행해야 하며, 담당자는 충분한 수준의 기술과 재능 및 자격요건을 갖춘 사람으로 정해야 한다. 담당자는 평가 후 기능 안전성 평가 보고서를 제출해야 한다.

생산 이전에서는 아이템 개발 완료 시 생산을 위한 이전 기준을 명시하는 것이다. 또한 생산을 위한 이전 아이템이 차량 수준의 기능안전성 요구사항에 부합한다는 것을 확인하여야 한다. 생산 이전에 필요한 문서로서 이행 책임자의 이름과 서명, 이행 아이템의 버전, 이행 아이템의 형상, 관련 문서들의 참고 문헌, 이행 날짜 등이 있다.

입증 단계에서 프로젝트 리더는 HW 설계와 SW 구현을 아이템 단위로 통합하여 안전성 입증과 기능안전성 평가에 필요한 지원, 책임자 선정, 진도 관리 및 지연사항의 Follow Up을 실

시하며, 개발된 아이템이 안전 목표를 달성 했는지 여부를 검토하고 피드백 한다. 또한 유지관리 계획/문서화를 통하여 프로젝트의 최종 성과를 정리하고 프로젝트 결과를 이관하기 위한 자료를 만들고 이를 생산부서에 이관한다.

4. 결 론

본 논문에서는 ISO 26262 제품개발 프로세스를 효과적이고 효율적으로 운영하기 위하여 ISO 26262 제품개발 프로세스와 연계된 DFSS 로드-맵을 제안하였다. 개발된 DFSS 로드-맵은 기존 6시그마의 DFSS 로드-맵 중 하나인 DMADV(Define, Measure, Analyze, Design, Verify)를 적용하였다. 제안된 로드-맵의 각 단계별 실행절차를 ISO 26262의 제품개발 프로세스와 연계하여 설명하였으며, 각 단계에서 사용하는 도구, 입력물 및 출력물을 정리하였다. ISO 26262의 제품개발 프로세스는 많은 요구사항과 복잡한 구조로 이루어져 있기 때문에 기존의 산업 관행에서 볼 때 구현이 매우 어렵다. 또한 ISO 26262의 제품개발 프로세스는 제품의 기능안전에 요건에 국한되어 있기 때문에 제품의 전체적인 개발 프로세스 관점에서 보면 HW나 SW의 개발 과제들을 효율적이고 효과적으로 관리하지 못한다. 따라서 본 논문의 목적은 ISO 26262의 모든 요구 사항을 충족시키는 제품개발을 위하여 보다 체계적이고 포괄적으로 사용할 수 있는 모델을 제공하는 것이다. 그러나 본 논문에서 제안한 모델을 실제로 제품개발 프로세스에 적용해 보지는 못하였다. 하지만 본 논문에서 제안한 모델은 실제 ISO 26262 제품개발 프로세스에 따라 제품개발을 진행하는 과정에 발생 가능한 여러 어려움을 피할 수 있을 것으로 생각한다. 본 논문에서 제안한 모델이 완벽하지는 않지만 ISO 26262의 제품개발 프로세스를 진행하는데 필요한 롤 모델로 진화하기를 기대하며, 우리나라 자동차 부품 산업의 경쟁력 확보에 도움이 될 것으로 기대한다.

참고문헌

- Bellotti, M. and Mariani, R. (2010), How future automotive functional safety requirements will impact microprocessor design, *Microelectronics Reliability*, 50, 1320-1326.
- Brombacher, A. C., Sander, P. C., Sonnemans, P. J. M. and Rouvroye, J. L., (2005), Managing product reliability in business processes under pressure, *Reliability Engineering and Systems Safety*, 88, 137-146.
- Chae, S. Y. (2011), Changes in the automotive market by ISO 26262, *Communications of the Korean Institute of Information Scientists and Engineers*, 29(1), 42-47.
- International Organization for Standardization (2011), ISO 26262-1 Road vehicles-Functional safety-Part 1 : Vocabulary.
- International Organization for Standardization (2011), ISO 26262-2 Road vehicles-Functional safety-Part 2 : Management of functional safety.
- International Organization for Standardization (2011), ISO 26262-3 Road vehicles-Functional safety-Part 3 : Concept phase.

International Organization for Standardization (2011), ISO 26262-4 Road vehicles-Functional safety-Part 4 : Product development at the system level.
 International Organization for Standardization (2011), ISO 26262-5 Road vehicles-Functional safety-Part 5 : Product development at the hardware level.
 International Organization for Standardization, 'ISO 26262-6 Road vehicles-Functional safety-Part 6 : Product development at the software level,' 2011.
 International Organization for Standardization (2011), ISO 26262-7 Road vehicles-Functional safety-Part 7 : Production and operation.
 International Organization for Standardization. (2011), ISO 26262-8 Road vehicles-Functional safety-Part 8 : Supporting processes.
 International Organization for Standardization (2011), ISO 26262-9 Road vehicles-Functional safety-Part 9 : Automotive Safety Integrity Level(ASIL)-oriented and safety-oriented analyses.

Kim, K. Y. and Jang, J. S. (2011), Quantitative assessment procedure for the hardware of ISO 26262 ASIL, *2011 Spring Conference on the Korea Reliability Society*, 271-279.
 Kwon, H. M., Hong, S. H., Lee, M. K., and Koh, S. G. (2012), ECU Development and Design process for Asil requirements and Some Considerations, *Spring Conference on the Korea Reliability Society*, 1-13.
 Mader, R., Griebnig, G., Leitner, A., Kreiner, C., Bourrouilh, Q., Armengaud, E., Steger, C., and Weiß, R. (2011), A Computer-Aided Approach to Preliminary Hazard Analysis for Automotive Embedded Systems, *18th IEEE International Conference and Workshops on Engineering of Computer-Based Systems*, 169-178.
 Yadav, O. P. and Singh, N. (2008), Perspectives and challenges for product reliability assurance in the product development process, *Int. J. Product Development*, 5, 4-16.

홍성훈

고려대학교 산업공학과 공학사
 한국과학기술원 산업공학과 공학석사
 한국과학기술원 산업공학과 공학박사
 현재 : 전북대학교 산업정보시스템공학과 교수
 관심분야 : Six Sigma, 통계적 품질관리, 공정 최적화, 품질공학

권혁무

서울대학교 경영학과 경영학사
 한국과학기술원 산업공학과 공학석사
 한국과학기술원 산업공학과 공학박사
 현재 : 부경대학교 시스템경영공학부 교수
 관심분야 : 로버스트 설계, 안전품질, Six Sigma, 통계적 품질관리

김동준

한양대학교 기계공학과 공학사
 George Washington Univ. 기계공학과 공학석사
 George Washington Univ. 기계공학과 공학박사
 현재 : 전북대학교 산업정보시스템공학과 겸임교수
 관심분야 : 그린 6시그마, 녹색경영, 안전품질

이민구

아주대학교 산업공학과 공학사
 한국과학기술원 산업공학과 공학석사
 한국과학기술원 산업공학과 공학박사
 현재 : 충남대학교 정보통계학과/산업대학원 산업공학과 교수
 관심분야 : Six Sigma, 통계적 품질관리, 공정 최적화, 품질공학