모델기반 시스템공학 기법을 기반으로 자동차 기능안전표준 ISO 26262에 대한 효과적 대응에 관한 연구

On the Study of Automotive Functional Safety Standard ISO 26262 based on Model-Based Systems Engineering

김 영 민* · 이 재 천*
Young-Min Kim* · Jae-Chon Lee*

Abstract

오늘날 자동차 기술의 비약적인 발전으로, 단순히 이동수단으로만 여겨왔던 자동차는 과거와는 비교 할 수 없을 정도의 안전성과 편의성을 제공하고 있다. 이러한 편의와 안전을 제공하는데 있어서의 핵심은 전자제어 장치의 발달로 이뤄진 결과이다. 최근 개발되는 전자제어 장치는 통합 모듈제어의 형태를 지니고 있어서 설계의 복잡성을 지니고 있다. 따라서 이러한 특성으로부터 발생되는 문제를 기존에 준수해왔던 IEC 61508으로는 해결하지 못해, ISO 26262가 제정되었다. 따라서, ISO 26262의 국내 도입에 따른 발생되는 문제들이 예측되고 있다. 이러한 문제에 대한 분석을 통해, 모델 기반 시스템공학 적용을 통해 해결하고자 노력하였다. ISO 26262의 국내 적용에 따른 가장 유려되는 개발 전체 라이프사이클에 안전성과 신뢰성을 만족하기 위한 개발 프로세스 도입에 대한 문제와 요구사항 분석 및 개발, 그리고 관리 측면에 대해 시스템공학 전산지원도구 활용을 통한 모델기반 시스템 공학 접근 방법을 활용한 방안에 관하여 논의하고 있다. 본 연구 결과를 기반으로 향후 추가 연구를 수행하면, ISO26262의 국내 자동차산업 도입에 따른 문제에 해결하기 위한 과정에 도움이 될 것으로 기대된다.

* 아주대학교 시스템공학과

1. 서 론

과거에 단순히 이동수단에 목적을 두었던 자동차의 역할이 기술의 비약적인 발전으로 더욱 안전하고 편안한 자동차, 즉 서비스 지향적인 자동차로 거듭나고 있다[1]. 이러한 편의와 안전을 제공하기 위해 전자제어 장치의 장착 확대와 전자제어 장치간의 연동을 통한 서비스 개발이 늘어나고 있다. 따라서 이로 인해, 장치 간 통합 및 인터페이스 측면에서의 문제로 인해 설계에 대한 신뢰성 및 안전성 확보에 대한 이슈가 대두되고 있다. 자동차 산업은 1990년대 부품 모듈의 개별 제어수준에서 최근 통합 모듈제어로의 변모된 방식으로 진화하고 있다. 이러한 변화된 방식의 추구는 차량 제어의 혁신을 가져 다 주었지만, 역으로 통합모듈로 인한 전자 제어장치의 복잡성으로 인해 편의성과 안전성 측면에서 보다 신중한 설계가 요구되고 있다. 또한, 기존에는 개별적이고 단편적인 기능 중심의 단편적인 기능 안전 보장 접근방식을 통한 차량개발을 수행한 반면, 최근의 추세는 차량의 개발단계로부터 폐기에 이르는 전 수명주기에 걸친 포괄적이고 체계적인 안전보장이 요구되고 있다.

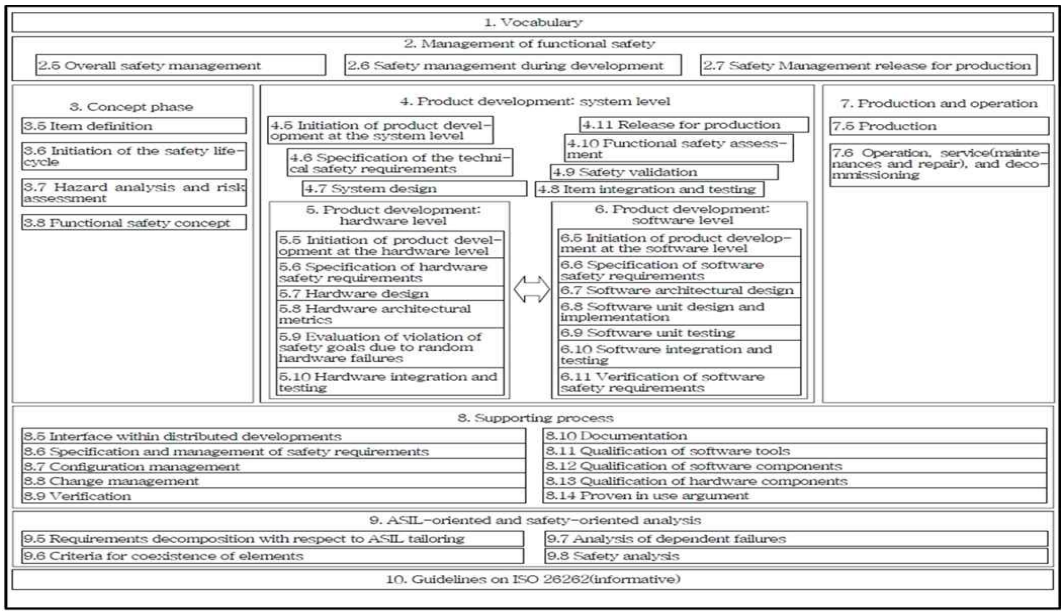
따라서, 안전 분야의 범용 국제표준이라 불리는 IEC 61508[2]에서 벗어나 자동차 도메인 분야에 보다 적용 가능하도록 기능 안전성 개념(Functional Safety Concept)을 자동차 분야에 도입하여 ISO 26262[3] 국제표준이 제정되었다. <Table 1>과 <Figure 1>을 통해서 알 수 있듯이, ISO 26262는 차량의 전기전자장치의 기능 안전성에 대한 요구사항을 정의한 표준으로 총 10개의 파트로 43개의 요구사항 및 권고 사항으로 구성되어 있다. 이에 따라, 글로벌 자동차 공급업체들은 ISO 26262를 연구개발 과정에 도입 및 포괄적인 적용을 통한 차량 안전성 확보 위해 노력하고 있다[4]. 현재까지는 국내 자동차 산업분야에서는 대다수 업체들이 IEC 61508을 통해 차량의 안전성 확보를 위해 노력하고 있지만, ISO 26262가 정식 배포됨에 따라 자동차 산업분야의 발 빠른 대응이 요구된다. 보다 더욱 우려시 되는 일은 기존의 차량 배기가스의 규제가 후발 업체에게는 비관세 무역 장벽화가 되었다는 것을 고려하면 차량의 안전성이란 명목으로 ISO 26262가 추후 더 높은 비관세 무역 장벽이 될 수 있다는 우려가 일본에서 제기되었다[5]. 이러한 전망은 참고문헌 [6]를 통해서도 알 수 있는 사실이다.

Table 1. ISO 26262 Part별 요구사항[3]

Part	관련내용	세부내용
Part 1	용어 (Vocabulary)	- 관련 용어 정리
Part 2	기능 안전성 관리	기능 안전성에 관한 개별 활동을 계획, 조정, 추적하는 요건 정의 전반적인 안전성 관리 요구사항을 정의
Part 3	구상단계	- 개발 품목 정의를 기반으로 해저드 분석 및 위험 심사를 통해 ASIL 판정 안전 목표와 안전 메커니즘 정의
Part 4	제품개발 : 시스템 레벨	제조사 관점의 시스템 통합 전기전자 시스템 외의 타 기술로 구현된 안전 메커니즘 확인 외부 수단으로 구현된 안전개념의 효과 확인 사람의 통제성 및 작동작업에 대한 전제 검증
Part 5	제품개발: HW 레벨	제조사 관점의 시스템 통합 전기전자 시스템 외의 타 기술로 구현된 안전 메카니즘 확인 외부 수단으로 구현된 안전 개념의 효과 확인 사람의 통제성 및 작동작업에 대한 전제 검증
Part 6	제품개발: SW 레벨	- SW 수준 개발에 대해 V-Model 개념에 따른 개발, 통합, 검증 등에 대한 요구사항 정의
Part 7	생산 및 운용	- 품목 생산을 위한 계획, 샘플 생상, 양산, 서비스 등에 관한 요구사항 정의
Part 8	지원 프로세스	안전요구사항 관리, 명세방법, 형상/변경관리, 검증, 문서화, 지원도구 자격 검증, 재사용 SW 자격검증, HW 자격검증, 실제 사용을 통해 입증된 안전성에 대한 요구사항 정의
Part 9	ASIL 및 안전 중심의 분석	- 안전 요구사항 ASIL을 분해하는 방법 안전 관련 구성요소 사이의 상호간섭의 정도, 위험분석 방법 기술
Part 10	가이드라인	주요개념, 안전케이스 ASIL 분해 등 ISO 26262 이해에 도움이 되는 정보 기술

따라서 ISO 26262는 향후 IEC 61508을 대체할 수 있는 표준으로 거듭날 것이다[6]. 그렇기 때문에 국내 자동차 산업에서 ISO 26262 적용에 대한 발 빠른 대응이 필요한 시점이다. 본 연구팀은 연구수행을 통해, ISO 26262의 국내 자동차산업의 적용과정에서 크게 두 가지 측면의 문제에 대해 인식하였다. 하나는 기존의 차량 기능 안전성 관점의 주안점에서 벗어나 전체 개발 프로세스의 혁신을 요구한다는 것이다. 또 다른 하나의 문제점은 전체 프로세스 이행을 입증하기 위한 문서화를 하는 것이다. 따라서, 이러한 문제점을 해결하기 위해 본 연구를 통해 시스템공학을 적용시켰다.

특히, 문제 해결을 위한 방안으로 모델 기반 시스템공학(Model-based systems engineering, MBSE)을 적용시킨 이유는 기본적으로 시스템공학은 시스템의 안전을 확보하기 위해서 시스템 설계 및 운용 그리고 폐기단계를 포함한 전수명주기 관점에서 위험원을 식별하고 통제하기 위해 필요한 활동들을 착수시키기 위한 과학적이고 공학적인 원리의 응용을 포함 한다[7]. 따라서 안전을 다루기에 적합한 학문이라고 할 수 있겠다.



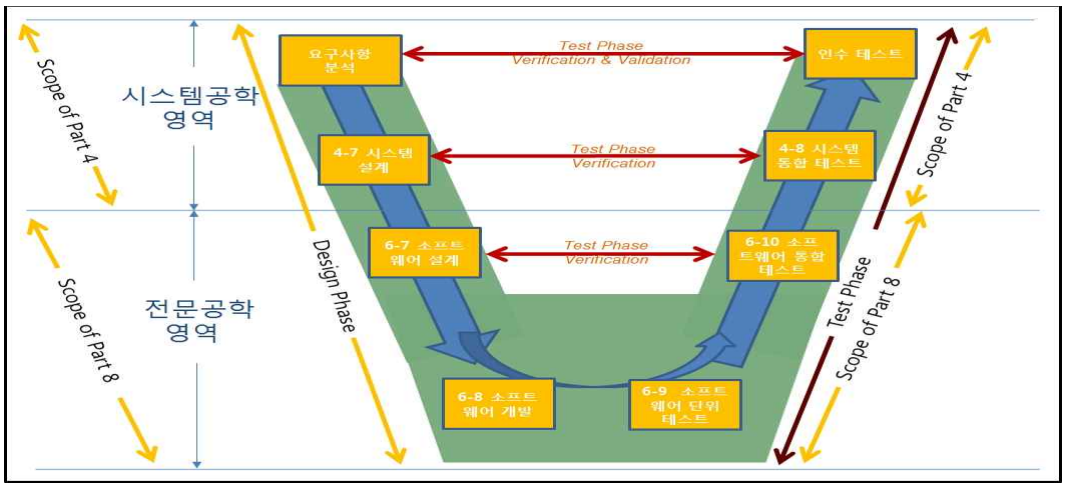
< Figure 1> ISO 26262의 Product Development Life-cycle

또한, 시스템공학 전산지원도구를 활용한 모델기반 설계를 통한, 접근으로 요구사항 생성, 추적성 구현, 형상/변경관리 등을 수행을 보다 효율적으로 할 수 있다. 그밖에, 생성된 모델을 바탕으로 설계 요구사항에 부합하는지 검증과정을 수행 할 수 있고, 전산화된 데이터를 DB화하여 문서출력 또한 가능하기 때문에 ISO 26262를 대응하기 위해 우려되는 문제를 해결 할 수 있는 적합한 학문이며 해결 가능한 메카니즘을 제공한다.

2. 본 론

2.1 시스템공학 전산지원도구를 통한 ISO 26262 대응의 범위 및 목표

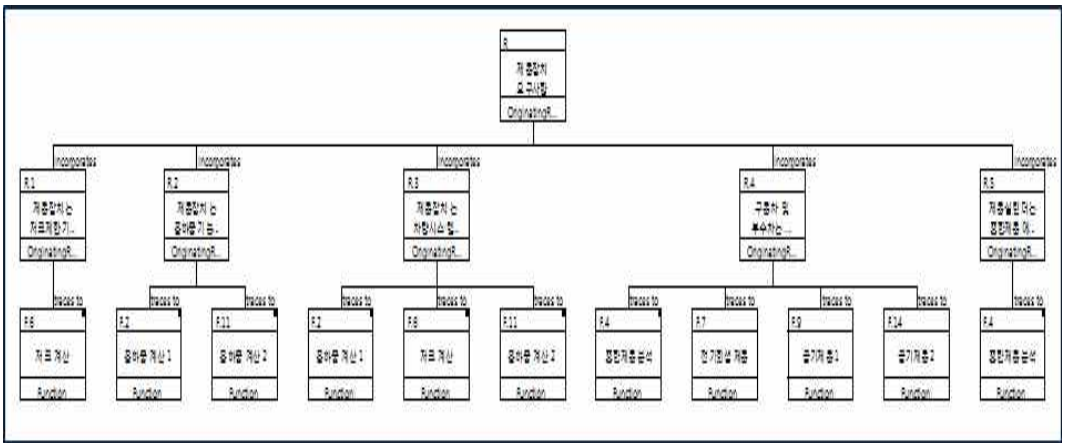
시스템공학 전산지원 도구를 활용한 모델기반 시스템공학 접근법은 <Table 1>, <Figure 1>, <Figure 2>에서 제시하는 것처럼, ISO 26262의 Part 2, Part 3, Part 4, Part 7, Part 8에서 요구하는 활동들은 시스템공학에서 다루는 영역이기에 이 부분에 관련해 제기되는 문제는 해결 가능하다. 따라서 본 연구의 연구 범위를 ISO 26262의 Part 2, Part 3, Part 4, Part 7, Part 8로 한정하려 한다. 또한, 앞에서 문제정의 단계에서 언급한 두 가지 문제점에 대한 달성을 본 연구의 목표로 두었으며, 적용 대상을 철도분야로 선정하였다.



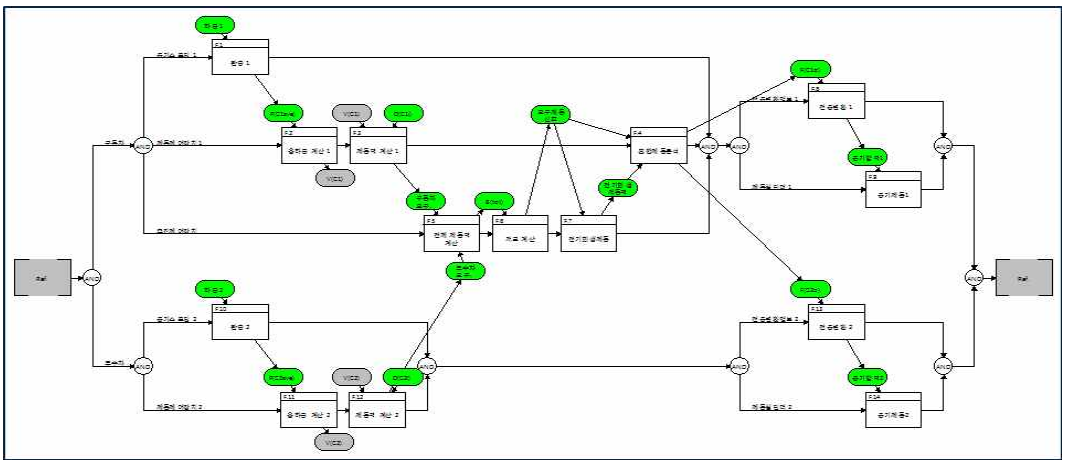
< Figure 2> 자동차 S/W 품질향상을 위한 V-Model 기반의 시스템공학 영역

2.2 모델기반 시스템공학을 통한 전 수명주기 관점 접근의 설계

서두에 언급했듯이, 자동차 산업에서의 안전 추구의 형태는 기능 중심의 안전을 추구에서 벗어나 최근 추세의 특징은 전 수명주기 관점에서 보다 큰 그림으로 시스템 안전성을 추구한다는 것이다. 사실 전문엔지니어가 시스템 수명주기의 전반에 걸쳐서 설계를 관리하기란 매우 어려운 일이다. 따라서 <Figure 2>에서 보이는 것처럼, 설계의 초기 단계 및 최종단계의 수행에 있어서 시스템공학을 통한 차량안전을 추구하고, 그 이하의 세부 상세영역은 전문 엔지니어가 이어서 설계활동을 진행에 나아간다면 ISO 26262에서 추구하는 시스템 개발 전 수명주기 관점 추구에 따른 우려의 문제점을 해결 가능 할 것이다.



<Figure 3> 요구사항-기능 추적성 확보 예: 제동장치 기능 분석 샘플 기반



<Figure 4> 기능 분석 샘플: 제동 장치

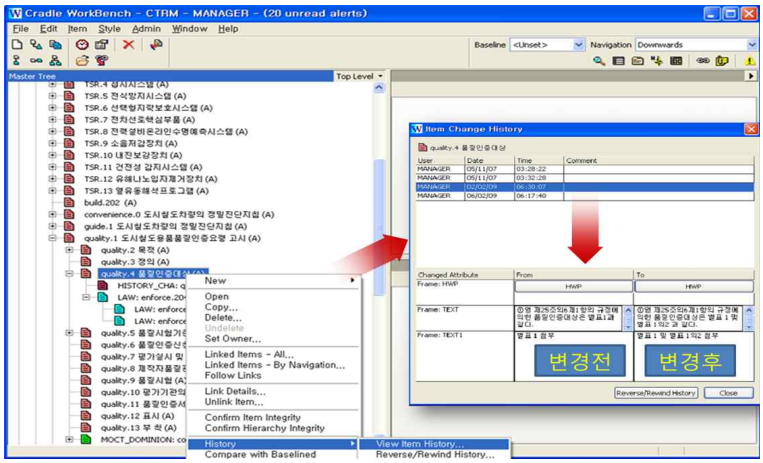
3. 구현

3.1 시스템공학 전산지원 도구를 통한 요구사항 생성 및 추적, 변경, 형상관리

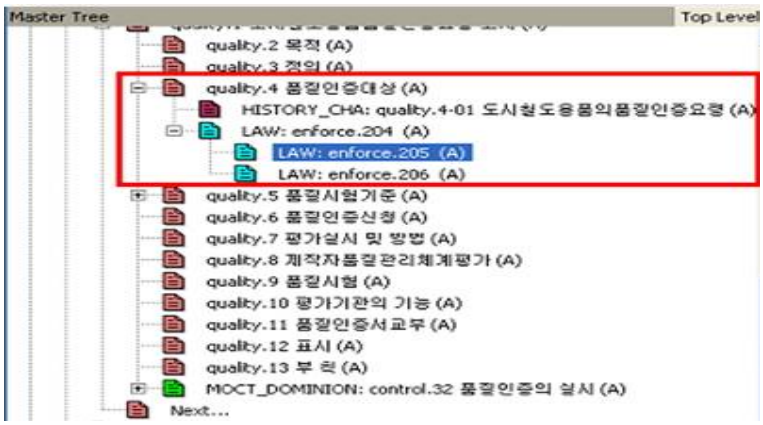
<Figure 2>에서 제시한 V-Model은 국제표준은 아니지만, 시스템공학과 소프트웨어 공학에서 매우 유명한 모델이다. <Figure 2>를 통해서 알 수 있듯이, 모든 설계활동은 요구사항 분석단계를 시작으로 설계활동이 시작된다. 이러한 요구사항은 설계의 초석의 근거를 제공하므로 개발과정의 성패를 좌우할 정도이다. 따라서 요구사항 생성 및 관리의 중요성을 강조하지 않을 수 없다. 전산지원 도구를 활용한 기존 시스템공학 활동을 활용한다면 ISO 26262에서 요구하는 요구사항 추적성을 구현하고, 보다 체계적으로 관리 또한 가능하여 통합 및 인터페이스 변경에 따른 영향 분석 또한 가능하게 할 수 있어 새로운 표준에 대한 효과적 대응이 가능하다. 따라서 ISO 26262 전체 수명주기 프로세스에 따른 각 개발단계에서 수없이 많이 생성되는 요구사항을 관리, 추적성 활용을 통한 체계적인 설계 및 변경, 형상관리를 수행하기 위해서는 현대와 같이 복합 시스템 개발에서 전산지원 도구의 활용을 필수적이라고 말할 수 있겠다. <Figure 5>는 요구사항 내용 및 추적성 변경이력이 가능하다는 것을 보여주는 그림이며, <Figure 3>과 <Figure 6>을 통해서, 서로 다른 요구사항 간에 추적성이 구현된 모습을 확인 가능하다. 특히, <Figure 3>을 통해서 알 수 있듯이, 어떠한 요구사항으로 도출되거나 관련된 기능과의 추적성 구현한 모습을 볼 수 있다.

3.2 시스템공학 전산지원 도구를 통한 검증 및 Reporting 기능 구현

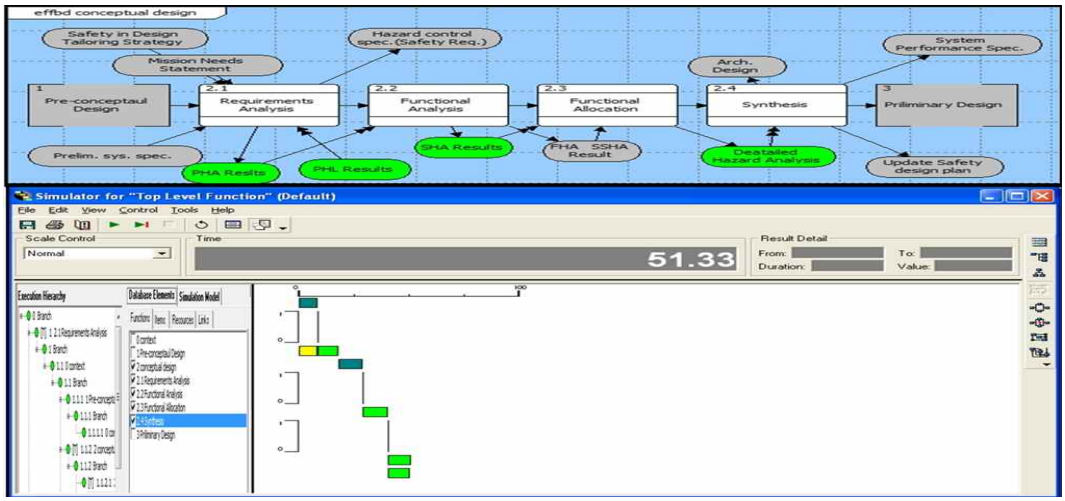
시스템공학 전산지원 도구를 통해, 통합과정에서 초기 계획되었던 설계 요구사항과 부합되는지 검증하기 위해서 <Figure 4>와 <Figure 7>에서 제시하는 것처럼, 기능 흐름의 분석을 통해서 논리적 오류가 없는지 검사가 가능하다. 이러한 모델 기반 검증의 수행을 통해, ISO 26262 Part 4-8에서 요구하는 성능 테스트에 대한 지원을 통해 충족 가능하다. 이러한 테스트를 통해, 주어진 시스템 자원을 최적화 할 수 있는 시스템 아키텍처 설계가 가능해 질 수 있다. 또한, ISO2626는 요구사항 이행을 증명하기 위해 추적성 확보 및 문서화를 필수적으로 요구하고 있다. 따라서 <Figure 8>을 통해서 알 수 있듯이 정의된 요구사항이 출력 가능한 모습을 통해 ISO 26262 수행에 따른 문제되는 요소들에 대해 모두 대응이 가능하다는 것을 알 수 있다.



<Figure 5> 구축된 요구사항의 변경관리



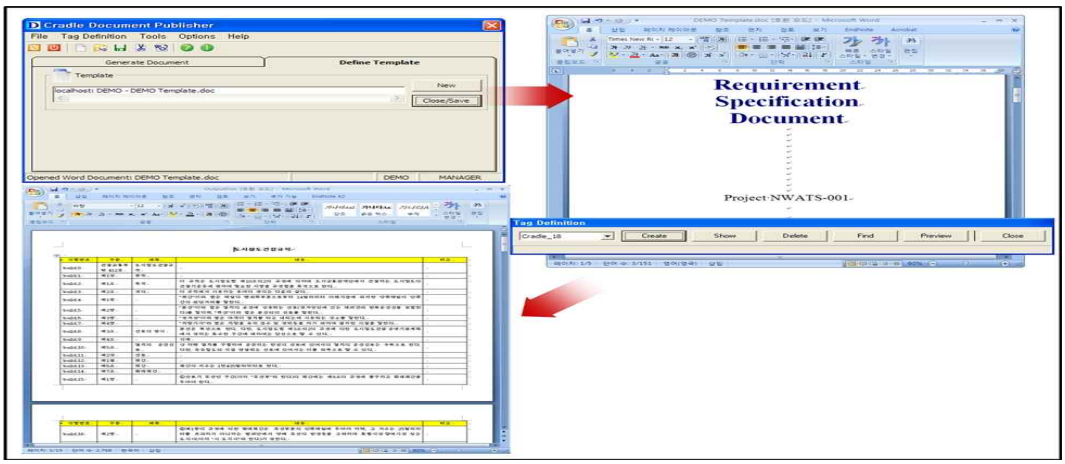
<Figure 6> 요구사항 추적성 구현



<Figure 7> 시뮬레이션을 통한 설계 기능안전 검증

4. 결론 및 향후 연구 방향

오늘날 기술의 고도화에 따른 자동차 산업 또한 차량 시스템의 구성이 복잡해지고 있다. 차량 역시 과거와는 달리 전자제어 장치의 발달로 인해 사용자로 하여금, 편의성과 안전성을 제공하고 있다. 하지만, 이러한 편의성과 안전성은 전자 제어 장치의 오류가 없는 조건에서 보장되는 것 일 것이다. 따라서 오늘날 보다 복잡해진 전자 제어 장치 기능을 효율적으로 설계하고, 기존에 준수하던 IEC 61508에 의해서는 자동차의 전자장치 설계에 있어서 많은 문제점을 노출해, 자동차 분야에 특화된, ISO 26262가 제정되었다.



<Figure 8> 요구사항 정의에 따른 출력

ISO 26262에서 제시하는 핵심은 2가지이다. 첫째, 개발 전체 수명주기에 걸친 안전성과 신뢰성 만족을 위한 프로세스, 또 다른, 하나는, ISO 26262에서 제시하는 프로세스 수행에 따른 요구사항을 이행에 따른 추적성 확보 및 문서화가 핵심이다. 이러한 측면은, 전 수명주기 관점에서 설계에 접근하는 시스템공학 접근법을 활용하여 상위레벨의 설계단계에서는 시스템공학을 통한 접근을 통해 해결하고 그 이하의 레벨, 즉 상세설계 단계의 경우 전문 엔지니어의 설계활동을 이어서 수행한다면, ISO 26262에서 요구하는 설계단계의 전 수명주기적 설계안전도를 높일 것이다. 또한, 요구사항 생성 및 관리, 문서화 또한 시스템공학 전산지원 도구를 통한, 모델기반 시스템공학 방법을 적극 활용한다면 시스템 설계 초기 단계에 집중하고 있는 시스템공학 학문을 통해, ISO 26262의 Part 2, 3, 4에서 요구하는 사항들에 대한 해결이 가능할 것이다. 본 연구를 통해서, ISO 26262 제정에 따른 국내 자동차 산업의 도입에 있어서 야기되는 문제를 모델기반 시스템공학 접근법을 통해 접근해 해결 가능해짐에 따라 추후 활용적 가치에 기여하였다고 생각 한다. 후속 연구 활동 또한 활발히 진행되었으면 한다. 추후 연구에서는 연구범위를 확장시켜 ISO 26262에서 제시하는 다른 Part의 적용을 통한 대응에 관한 연구가 필요할 것이다.

5. 참 고 문 헌

[1] 한태만, 조진희, "자동차 전자제어 장치용 소프트웨어 기술 및 표준화 동향", ETRI, 자동차융합플랫폼연구팀, Tech Rep., pp. 69-82.(2010)

[2] “Functional safety of electrical/electronic/programmable electronic safety-related systems“, in IEC 61508

[3] ISO DIS 26262 Road Vehicles - Functional safety, July, (2009)

[4] Robert N. Charette, “This Car Runs on Code,” http://www.spectrum.ieee.org/greentech/advanced- cars/this-car-runs-on-code, Feb, (2009)

[5] D. Mizuguchi, “A Report of the Current Situation on Software Certification in Japan,” http://www.jaist.ac.jp/joint-workshop/verite/ 06JaistAist_mizuguchi.pdf

[6] MISRA Guidelines for Safety analysis of vehicle based programmable systems, Nov,(2007)

[7] I. Clifton and A. Ericson, “Hazard analysis techniques for system safety.”, Hoboken, New Jersey: John Wiley & Sons, Inc., (2005)