ISSN 1229-1889(Print)
ISSN 2287-9005(Online)
J Korean Soc Qual Manag Vol. 46, No.4: 1001-1014, December 2018
https://doi.org/10.7469/JKSQM.2018.46.4.1001

융복합제품을 위한 모듈방식의 안전인증체계 설계 -자율주행 자동차를 중심으로-

신완선* · 김지원**†

*성균관대학교 시스템경영공학과
**성균관대학교 산업공학과

Designing a Modular Safety Certification System for Convergence Products - Focusing on Autonomous Driving Cars -

Wan-Seon Shin* . Ji-Won Kim**†

*Department of System Management Engineering, Sungkyunkwan University
**Department of Industrial Engineering, Sungkyunkwan University

ABSTRACT

Purpose: Autonomous driving cars, which are often represent the new convergence product, have been researched since the early years of 1900 but their safety assurance policies are yet to be implemented for real world practices. The primary purpose of this paper is to propose a modular concept based on which a safety assurance system can be designed and implemented for operating autonomous driving cars.
Methods: We combine a set of key attributes of CE mark (European Assurance standard), E-Mark (Automobile safety assurance system), and A-SPICE (Automobile software assurance standard) into a modular approach.
Results: Autonomous vehicles are emphasizing software safety, but there is no integrated safety certification standard for products and software. As such, there is complexity in the product and software safety certification process during the development phase. Using the concept of module, we were able to come up with an integrated safety certification system of product and software for practical uses in the future.
Conclusion: Through the modular concept, both international and domestic standards policy stakeholders are expected to consider a new structure that can help the autonomous driving industries expedite their commercialization for the technology advanced market in the era of Industry 4.0.

Key words: Safety Certification System, Convergence Products, Modularization

● Received 5 November 2018, 1st revised 29 November 2018, accepted 30 November 2018
† Corresponding Author(whiteannie31@naver.com)
ⓒ 2018, The Korean Society for Quality ManagementThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-CommercialLicense(http://creativecommons.org/licenses/by-nc/3.0) which permits unrestricted non-Commer-cial use, distribution, andreproduction in any medium, provided the original work is properly cited.
※ 이 논문은 산업통상자원부 국가기술표준원에서 시행한 산업기술혁신사업(국가표준기술력향상사업, 10078275)의 지원을 받아 수행된 연구임.

1. 서 론

2016년 세계경제포럼 (WEF: World Economic Forum)인 다보스 포럼에서 클라우스 슈바프 (Klaus Schwab) 회장이 최초로 언급하며 세계의 이목을 집중시킨 4차 산업혁명은 초연결(HyperConnectivity)과 초지능(SuperIntelligence)을 특징으로 하고 있다.(김남규 외 8명, 2017) 현재 많은 국가에서 초연결, 초지능 개념을 기반으로 한 스마트공장, 스마트시티, 스마트그리드, 스마트교통과 같은 새로운 형태의 산업이 등장하여 관련 기술에 대한 혁신의 바람이 불고 있다.

국내에서는 4차 산업혁명 시대의 신산업에 대응하기 위해 '신산업 민관협의회'가 정부, 기업, 유관 단체의 전문가들로 구성되었다. 또한 2016년 12월 개최된 제 4차 신산업 민관협의회는 미래 산업의 트렌드와 우리나라의 강점 및 민간 부문의 투자 계획을 고려하여 미래에 각광 받을 수 있는 '12대 신산업'을 도출하였으며, 2025년까지 신산업의 수출과 부가가치를 2배 확대하겠다는 목표를 세웠다. 이러한 12대 신산업에 포함되는 업종은 1) 전기, 자율자동차, 2) 스마트, 친환경 선박, 3) IoT 가전, 4)로봇, 5) 바이오 헬스, 6) 항공, 드론, 7) 프리미엄 소비재, 8) 에너지 신산업, 9) 첨단신소재, 10) AR/VR, 11) 차세대 디스플레이, 그리고 12) 차세대 반도체를 포함한다.

본 연구는 스마트카 혹은 커넥티드카 등으로 불리는 자율주행자동차의 안전인증체계를 모듈방식으로 추진할 수 있는가를 다루고 있다. 자율주행자동차는 인간이 직접 운전하지 않아도 자동으로 주행할 수 있는 자동차를 뜻하는데 레이더, GPS, 센서, 카메라 등을 사용하여 주위의 환경을 인식하여 목적지까지 도착하는 과정에서 다양한 기능을 수행한다. 이미 자율주행자동차는 세계적으로 주목 받고 있는 기술이며 기술 수준도 상당히 높은 상황이다. 그러나 아직도 법령 및 안전상의 이유로 상용화 되지 못하고 있다. 우리나라 역시 2018년 현재, 마땅한 안전기준을 결정하지 못한 탓에 이에 대한 안전기준 수립이 시급하다. 특히 2016년 전기자동차와 무인자동차 분야에서 자동차 기술을 선도해 온 테슬라에서 출시한 무인자동차가 자율주행상태로 달리던 중 트럭과 충돌하여 트럭 운전자가 사망하는 사건이 발생했다. 이 사고로 인해 구글, 벤츠, 도요타, GM 등 자율주행자동차 상용화를 추진하고 있는 글로벌 기업들은 상용화 추진에 제동이 걸렸다. 이 사고는 차량의 센서가 밝은 색상의 하늘과 흰색 트럭을 구분하지 못하여 브레이크가 작동하지 않아 발생하였다. 자율주행자동차의 상용화를 위해서는 자율주행기능에 사용되는 소프트웨어, 센서 등과 같이 안전에 영향을 미칠 수 있는 부품들에 대하여 적합한 안전인증을 거친 후 출시되어야 한다. 따라서 자율주행자동차 관련 소비자의 안전을 보증할 수 있는 안전인증체계의 도입과 인증기준 설정이 필요하다.

한국의 국토교통부에서는 2018년 자율주행차의 안전기준을 수립하겠다고 발표하였다. 단일 기능을 하는 일반 자동차와 달리 다양한 정보통신기술이 융합된 자율주행자동차의 경우에는 안전기준의 복잡성이 존재한다. 이에 본 연구는 이러한 복잡성을 해결하기 위해 유럽의 강제인증제도인 CE Mark, E-Mark (유럽 자동차용 전장품 마크)의 적합성평가 제도의 프로세스를 조합하여 모듈방식의 안전인증체계를 제안하고자 한다.

Langlois(2002)는 모듈 개념은 '복잡하게 얽혀있는 시스템을 해결할 수 있는 가장 일반적인 방법'이라고 정의하였다. 본 연구는 안전인증체계 설정에 활용될 수 있는 모듈방식을 조사 및 분석하여 자율주행자동차의 안전인증체계의 대안으로 제시하고 이에 따른 한계점과 시사점을 도출하고자 한다.

2. 안전인증에 대한 선행연구

시장에 출시된 제품으로부터 소비자의 안전 확보를 위하여 국가는 법령에 의해 제품 출시 전에 제품에 대한 안전규제 (Safety Regulation)를 지정하고 있다. 여기에서 제품에 대한 안전규제는 위해(Risk), 위해 제품으로부터 소비자의 안전을 확보하기 위한 각종 제품, 업종별로 법률에 의한 안전기준의 설정, 안전담당기관 설치, 안전기준을 위반한 제품에 대한 단속 또는 사업자의 안전준수의무 부과 등과 같은 행정법적인 규제를 말한다. (최병록, 2012)

각 국가에서는 제품에 인증마크를 부착하는 형태로 인증제도를 시행하고 있으며 대표적으로는 유럽의 CE 마크, 미국의 UL 마크, 그리고 한국의 KC 마크 등이 있다. 여기서 인증제도란 특정 제품이나 프로세스 및 시스템이 정해진 규격에 적합하게 제작되고 있는지의 여부를 표준화된 기준에 따라 제 3자가 증명하는 제도를 의미한다. (최금호, 2016)

현재의 많은 안전인증에 사용되는 표준은 프로세스를 기반으로 일련의 개발 기술과 방법을 규정하고 있으며 특히, 제품 기반의 안전인증은 제품이 안전 요구사항을 충족하고 있는지에 대한 보증의 의미로 사용되고 있다고 한다. (Ibrahim Habli, 2006) 미국의 대표적인 인증기관인 UL은 '안전인증이란 수립된 안전 요구사항에 대한 제품 적합성을 평가하는 프로세스' 라고 정의하였으며 국제표준화기구인 ISO는 '적합성평가(Conformity Assessment)'란 제품 등이 요구사항을 충족하는지 직간접적으로 결정하는 것과 관련된 활동이라고 했다. (ISO/IEC Guide2:1996)

Kornecki (2009)은 안전인증의 목표는 '알려진 위험이 있는 상태에서 시스템이 안전하게 작동한다는 것을 공식적으로 보증하는 것' 이라고 하였으며 Jackson (2007)은 안전 기준을 준수한다는 것은 관련 표준에 근거하여 안전 기준을 충족한다는 증거가 될 수 있다고 하였다. 또한, Barbara Gallina (2004)는 자동차 개발 시 일반적으로 ISO 26262(자동차 기능 안전성 국제표준)와 같은 안전표준을 사용하여 인증제도를 운영하는 경우에는 중대한 사고나 위험의 원인을 완화할 수 있다고 하였다. 최근에는 자동차 분야에서 자동차의 개발프로세스, 자동차 안전 무결성레벨(ASILs) 및 추가 요구사항을 제공하기 위해 ISO 26262 기능안전 표준을 도입하였다. (Raghad Dardar et al. 2012) 그러나 ISO 26262 표준은 개발 프로세스를 준수하고 있는지에 대한 확인일 뿐 제품의 개발과 검토 방법에 대한 실제 기준은 제공하지 않고 있으며 기능적 안전성 평가 과정에서 안전성에 대한 논증이 어떻게 평가되어야 하는지를 기술하지 않고 있다. (John Birch et al. 2013) 이와 같이 ISO 26262는 표준화된 프로세스에 의해 제품이 만들어졌는지를 확인할 뿐이며 안전인증제도의 목적인 제 3자로부터 해당 제품이 안전 요구사항을 충족하고 있는지 확인하는 것에는 한계점이 존재한다.

자율주행차 안전기준 개발과 관련 된 활동은 자동차관련 국제기준(UN Regulation)을 제정하는 UN/ECE/WP29와 자동차도로 운행 규약을 제정하는 UN/ECE/WP1을 중심으로 이루어지고 있으며 자율주행자동차에 대한 안전기준 제정 및 개정을 위한 활동을 하고 있다.(민경찬 외 1명, 2015) 또한 현행 자동명령조향기능(ACSF) 기준은 자율주행기능인 차선 유지, 정체 구간 주행, 군집 주행, 하이웨이 오토파이럿 등과 같은 기술의 상용화를 제한하고 있는 관계로 UN Regulation 79의 속도 제한을 향상시키자는 의견에 따라 각국의 정부 대표와 자동차 관련 단체의 이해 관계자들이 참여하여 개정 작업을 진행하고 있다. (이명수, 2016) 또한 2016년 9월 미국 정부에서 연방자율주행차 정책 가이드라인(Federal Automatic Vehicles Policy Guideline)을 발표하였으며, 1년 뒤인 2017년 9월 기존의 연방자율주행차 정책 가이드라인에 안전 지침을 추가하여 자율주행시스템: 안전에 관한 비전 2.0(Automatic Driving System(ADS): A Vision for Safety 2.0)을 공표했으며 기존의 연방자율주행차 정책 가이드라인에서 대체되었다. (양희태, 2017)

대부분의 자율주행자동차의 안전에 대한 선행연구는 설계나 생산 단계에서의 제품안전요소가 아닌 시장 출시 이후 주행단계에서의 발생할 수 있는 기능안전요소에 대하여 연구되고 있다. 그러나 자동차의 경우 생명에 치명적인 위해를 가할 수 있는 제품으로써 시장에 출시하기 전에 적합한 제품안전기준절차에 의하여 이상 여부를 판단하고

인증 기준에 따라 적합성평가를 실시하여 안전 요구사항을 준수하고 있는지 판정 후에 출시하는 것이 바람직하다. 나아가 자율자동차의 경우에는 소프트웨어와 통신기능의 활용도가 높아진 만큼 보안 문제나 개인 프라이버시 보호의 문제도 고려해야 하며 해킹으로부터 발생할 수 있는 사고의 위험을 미연에 방지해야 한다.

본 연구는 복합적인 안전인증 모델과 프로세스 비교분석을 통하여 자율주행자동차에 활용할 수 있는 안전인증체계 방안을 도출하는데 초점을 맞추고 있다. 대표적인 모델인 유럽의 CE Mark 인증제도, E-Mark 인증제도, 그리고 A-SPICE(Automotive SPICE)의 고유 기능을 통합하는 것이 핵심이다. 지금까지 주로 시장 출시 이후 주행기능안전에 대한 문제를 다루고 있는 연구들과 다르게 여기서는 시장출시 이전의 설계 및 생산 단계에서의 제품안전요소를 입증하고 평가하는데 활용할 수 있는 안전인증체계를 제시하고 한다.

3. 모듈 개념과 안전인증제도

3.1 모듈의 개념

모듈의 개념은 특히 컴퓨터공학 산업에서 많이 사용하고 있으며 근래에는 제조 산업에도 사용한다. 제조 및 제품 분야에서Jacobs 등(2007)은 제품 모듈화를 완성품의 조립에 있어 다양한 배열이 가능하도록 표준화 되어 있고 상호 교환적인 부품을 사용하는 것이라고 하였다. Lau 등(2007)은 제품의 모듈화를 생산 시스템에 있어 제품 구성품의 분리성, 특수성, 변환 가능성을 의미하는 연속체라고 하였고 Langlois(2002)는 모듈을 복잡성을 관리하기 위한 일반적인 원칙이며 복잡하게 얽힌 시스템 상호연결을 제거할 수 있는 것이라 정의하였다. 또한 Hoogeweegen 등(1999)은 절차의 모듈화는 독립적인 표준화 된 그룹에 의해 특정지을 수 있다고 하였고, Baldwin과 Clark(2000)은 모듈화를 기업이 신속하게 변화하는 고객의 요구와 기술의 복잡성에 대응하고 차별화 된 대향 맞춤화 역량을 달성하는 데 있어 가장 중요한 요소라고 하였으며, Drucker(1999)는 생산프로세스의 모듈화 방식은 표준화와 유연성의 이점을 동시에 활용할 수 있는 효과적인 방법이라고 하였다.

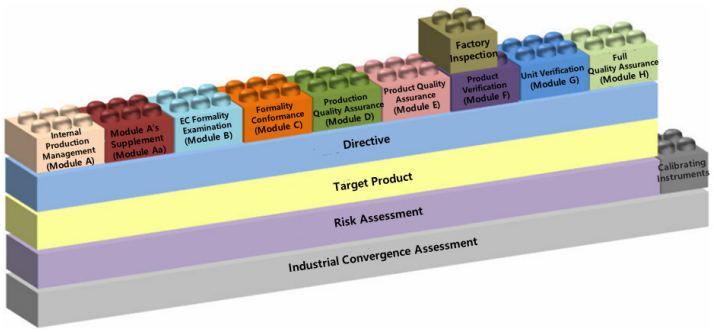

Figure 1. The Concept of Module

이처럼 학자들마다 다양하게 정의하고 있는 모듈 개념은 1960년대에 처음 사용되었음에도 불구하고 아직까지 공통된 정의가 설정되지 못하고 있다. 다만, 정의를 종합하여 볼 때, 모듈 개념의 강점은 프로세스 방식의 복잡성을 해결하는 동시에 표준화의 기반이 될 수 있다는 공통 합의를 이루고 있음을 알 수 있다. 자율자동차의 경우, 기존의 자동차와 소프트웨어가 결합된 형태로써 기존의 일반자동차의 인증에 비해 훨씬 더 복잡한 프로세스를 거쳐야 한다. 따라서 모듈방식에 기초를 둔 자율주행자동차의 안전인증체계는 프로세스 복잡성 개선과 다양한 이해관계자의 안전인증에 대한 공감대 확보에 기여할 수 있을 것이다.

3.2 모듈방식을 활용한 안전인증제도 : CE Mark

CE Mark 인증제도는 유럽에서 판매되는 제품 중 소비자의 건강, 안전, 위생 및 환경보호 차원에서 위험성이 내포되어 있다고 판단되는 제품에 대하여 모두 적용되는 강제 인증제도이다. 유럽연합(EU)의 통합인증 마크로써 유럽연합에 속한 국가 내에서 유통되는 제품 중 CE Mark 제도의 대상 품목에 해당하는 제품은 의무적으로 CE Mark를 부착해야 하며 CE Mark를 부착하지 않을 시 유럽 내에서 유통이 금지된다. CE Mark 인증제도는 해당 제품이 유럽연합 지침(Directive)에 적합하다는 것을 선언하고 인증기관의 적합성평가 절차를 거쳐 소비자로 하여금 안전상의 문제가 없다는 것을 증명하기 위한 수단이 되고 있다.

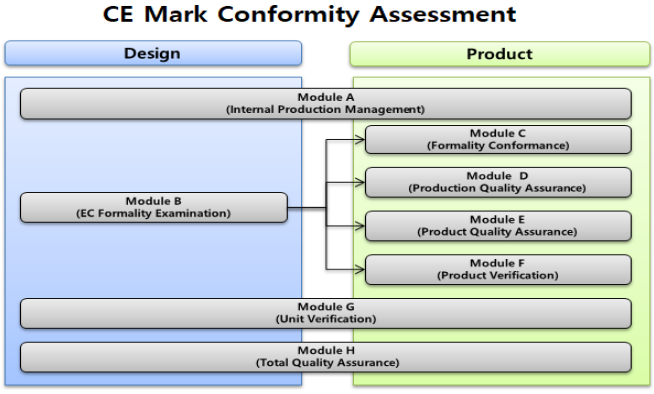

Figure 2. CE Mark Conformity assessment process

CE Mark 인증제도가 다른 인증제도와의 가장 큰 차이점은 적합성평가(Conformity Assessment)이다. 일반적으로 국가별로 각각의 인증제도를 따로 운용하고 있는데, 이와 달리 CE Mark 적합성평가 프로세스는 유럽연합에 해당하는 모든 국가가 통용할 수 있도록 모듈화 되어 있다. 1990년대 이전에는 유럽연합에 속한 국가별로 각자의 기술규격과 국가 표준이 존재하였으나 상이한 기술 규격과 국가 표준은 상품의 유통성을 방해하고 생산비용 증가를 유발하였다. 이에 유럽연합국은 유럽연합 정상회담(1985년)에서 채택된 백서(White Paper)와 1992년에 체결된 유럽연합조약에 근거하여 1993년부터 시장 통합을 진행하였다. 백서의 내용은 1992년 12월 31일까지 상품, 사람, 서비스, 자본의 단일 유럽 시장을 완성한다는 것과 시간표를 설정하고 연합 내에 기술적, 물리적 및 재정적 장벽을 제거한다는 것이었다. 이러한 과정에서 유럽위원회(European Committee)는 무역 장벽에서 발생하는 어려움을 제거하기 위해 각종 기술 규격과 표준 및 인증 제도를 통일하는 것을 목표로 1990년 CE Mark 인증제도를 공표하였다.

CE Mark는 제품 별로 지침(Directive)을 규정하고 지침의 필수 요구사항을 충족하며 제조자, 수입업자, 제 3자 인증기관 중에서 제품 관련된 적합성평가를 수행한다. CE Mark는 신뢰성이나 품질 보증의 목적이 아니라 해당 제품이 유럽 지침에서 규정하고 있는 기술 표준과 필수 요구사항을 준수하고 있다는 것을 의미한다.

3.3 유럽의 자동차 관련분야의 안전인증제도: e-Mark 제도

e-Mark 제도는 유럽의 자동차 분야의 형식승인 제도로써 강제 규격에 해당한다. 유럽에서 차량 및 부품을 판매하기 위해서는 CE Mark와는 별도로 e-Mark 인증 절차를 필수적으로 거쳐야 하며 그렇지 않은 경우에는 유럽 시장에서 판매가 불가하다. e-Mark 인증제도는 1970년 EU 집행위원회에 의하여 처음 도입되었으며, 차량과 부품들이 각종 관련 기술 지침과 규격을 충족시키는지 여부를 확인하기 위한 수단이다.

e-Mark 인증제도는 1992년 이전까지 각 회원국에서 별도의 지침과 규격으로 관리하였다. 이러한 이유로 한 국가에서 e-Mark 인증을 통과했다고 하더라도 유럽 내 다른 국가에서 판매하고자 하는 경우에는 부분적으로 해당 국가의 형식승인을 다시 받아야 했다. 그러나 1992년 8월에 기존의 지침(70/156/EEC지침)을 수정 보완한 'EC Whole Vehicle Type-Approval' 92/53/EEC 지침을 도입하여 1993년 1월부터 유럽 내 한 회원국을 선택하여 e-Mark를 인증 받은 경우에는 다른 유럽 회원국의 형식승인을 받지 않고 유통할 수 있도록 개정되었다.

e-Mark 인증을 받기 위해서는 자동차 제조사로부터 형식승인 요청을 접수해야 한다. 형식승인을 요청받은 국가는 해당 제조사가 안전한 제품을 제조할 능력을 갖추었는지의 여부를 판단하기 위해 공장 설비와 생산 절차를 방문하여 100% 현장 검사를 시행한다. 특히 생산 절차의 적합성 여부는 보통 ISO9000(품질경영시스템)을 기반으로 진행이 되며 이미 제조사에서 국제적으로 인지도가 높은 기관을 통하여 ISO9000을 취득한 경우에는 형식승인 국가의 검사 없이 형식승인을 인가할 수 있다.

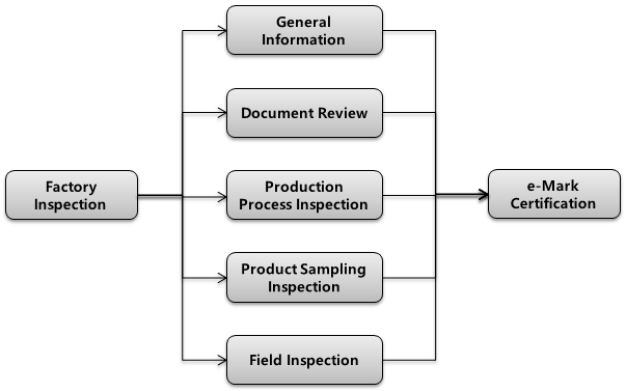

Figure 3. e-Mark Certification Process

주로 공장에 방문하여 진행되는 검사는 일반 현황, 서류 심사, 사내 생산 절차 현황 조사, 제품 샘플링 검사, 현장 검사로 이루어져 있다. 해당 항목 외에도 검사 기관이 필요하다고 판단되는 부분에 대해서 추가 정보를 요구할 수도 있으며 정보에 따라 시험의 항목이 추가되거나 면제되는 경우도 있다.

일반적으로 진행되는 생산 적합성 검사(공장 검사)는 총 다섯 단계로 구분 할 수 있으며 ISO9001 인증 심사와 유사하다. 이를 구체적으로 살펴보면, 일반 현황 단계에서는 회사 개요를 청취하고 책임자 면담을 진행 하며 서류 심사 단계에서 특정 제조 설비와 검사 설비 및 국제 규격 인가에 대한 심사를 진행한다. 사내 생산 절차 현황을 조사하는 단계에서는 제품을 생산함에 있어 적합한 프로세스를 준수하고 있는지에 대한 조사를 진행한다. 제품 샘플링 검사 단계에서는 일부 제품을 샘플링하여 제품에 대한 기술 기준 적합성과 제품의 표시 사항의 준수 여부 등을 검사하게 된다. 현장 검사 단계에서는 제품을 생산하는 전체적인 작업 공정과 설비, 검사 설비 및 계측기의 보유 여부, 계측기 관리 상태에 대해서 검사하는 단계이다. 이러한 e-Mark 제도는 한번 형식승인을 받고 나서 특별한 변화나 결함으로 인해 취소 조치가 없다면 인증은 계속 유효하다.

3.4 자동차 분야 소프트웨어 프로세스 수행능력 평가표준 모델: A-SPICE

A-SPICE(Automotive Software Process Improvement and Capability dEtermination)는 기존의 SPICE모델을 자동차 분야에 적합하게 사용할 수 있도록 변형한 모델이다. SPICE는 ISO에서 국제표준으로 지정된 프로세스 수행능력 평가표준 프레임워크이며 정식 명칭은 ISO15504이다. SPICE는 1991년 6월 스톡홀름에서 개최된 총회에서

토의과제로 선택해 규정을 만들어가고 있다. (이영식 외 2명, 2002) SPICE 모델은 ISO12207의 소프트웨어 생명주기 프로세스로부터 파생된 모델로서 소프트웨어 개발단계에서 획득, 공급, 개발, 운영, 발전, 지원 활동을 계획하고 개선하는데 사용되며 소프트웨어 심사를 목적으로 한다. (이영식 외 2명, 2002)

최근 자동차 산업계는 전자제어장치(ECU)가 필수적으로 탑재됨에 따라 소프트웨어 품질관리 이슈가 크게 부각되고 있다. A-SPICE(Automotive SPICE) 모델은 이러한 이슈에 대응하기 위하여 유럽 기업인 폭스바겐, BMW, 아우디, 포르쉐, 다임러크라이슬러로 구성된 HIS(Hersteller Initiative Software) 컨소시엄에 의해 ISO15504(SPICE모델)를 참고하여 2005년에 자동차 산업에 적합한 형태로 제정되었으며 '자동차분야 소프트웨어 개발 프로세스 수행능력 평가표준'이라고 명명되었다.

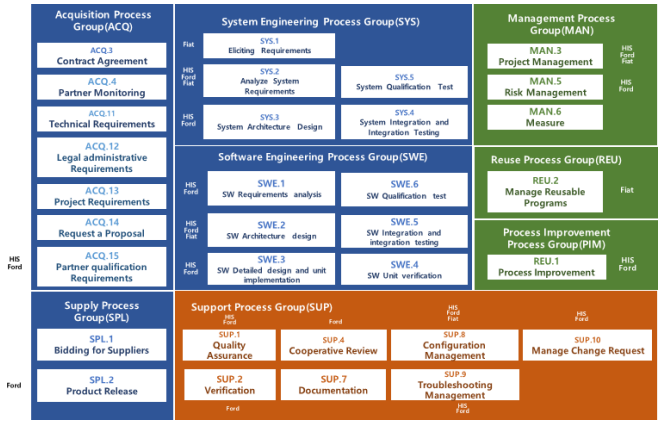

Figure 4. A-SPICE (Automotive SPICE) Model

A-SPICE는 3개의 생명주기, 8개의 그룹, 32개의 프로세스로 구성되어 있다. 여기서 3개의 생명주기란 기본적(Primary) 생명주기 프로세스, 지원(Supporting) 생명주기 프로세스, 조직(Organizational) 프로세스로 분류한다. (Suneel Sabar, 2011) A-SPICE 인증을 받기 위해서는 32개의 모든 프로세스를 필수적으로 받아야 하는 것은 아니다. A-SPICE 모델은 업체에 따라 필요한 범위(Scope)에 따라 일부 프로세스만을 선택하여 인증 받을 수 있다. 모든 프로세스를 거치지 않고 업체에 따라 필요한 프로세스만을 선택하여 사용할 수 있다는 점은 모듈의 강점과 맥락이 같다. 특히 시중에서는 HIS그룹에 포함된 자동차 기업들이 채택하고 있는 HIS Scope가 많이 활용되고 있다. HIS Scope는 A-SPICE의 전체 프로세스 중 16개 프로세스에 대한 심사를 받으며 모든 적용 프로세스에 대해서 3수준 이상이 될 것을 권장하고 있다.

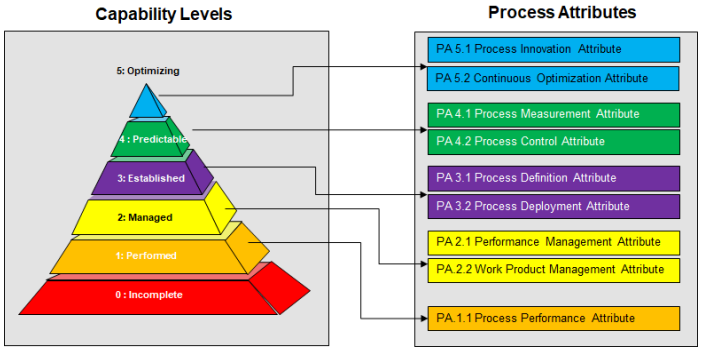

Figure 5. A-SPICE Level criteria

A-SPICE는 <그림 5>와 같이 따라 0에서 5까지의 단계로 수준을 결정할 수 있다. A-SPICE 모델은 ISO 15504와 달리 국제표준은 아니지만 HIS외에도 글로벌 완성차 업체인 미국의 포드, GM에서도 A-SPICE를 요구하고 있다. 이처럼 A-SPICE는 의무적으로 받아야 하는 표준은 아니다. 그러나 ISO 26262(자동차 기능 안전성 국제표준)에서도 A-SPICE Level 2 이상의 수준을 요구하고 있으며 글로벌 완성차 업체 대부분에서 인지도와 신뢰도를 인정받아 산업계에서는 표준처럼 사용되고 있다.

4. 모듈방식의 안전인증체계 설계

4.1 안전인증제도의 프로세스 비교 분석: CE Mark, e-Mark, A-SPICE

프로세스 비교 분석을 위해서는 대상이 필요하다. 본 연구에서는 프로세스의 비교를 위해 CE Mark 인증제도와 e-Mark 인증제도 A-SPICE 모델을 대상으로 선정하였다. 그러나 A-SPICE는 CE Mark와 e-Mark처럼 제품형태의 인증프로세스가 아닌 소프트웨어 개발 프로세스 평가를 위한 모델이므로 비교가 불가하여 별도로 분류하였다. 또한 CE Mark와 e-Mark를 비교하여 A-SPICE에서 필요한 프로세스를 도출하여 하나의 모델로 구성하였다.

A-SPICE는 업체에 따라 필요한 프로세스만을 선택하여 인증 받도록 설계되어 있는데 전 세계적으로 가장 인지도가 높은 HIS Scope에서 요구하고 있는 프로세스를 선택하였다. HIS Scope 프로세스는 <그림 6>과 같이 3개의 카테고리에 4개의 그룹이 해당되며 총 15개의 프로세스를 인증 받아야 한다. 국내의 자동차 기업도 협력사로부터 A-SPICE Level 3을 요구하고 있다. 이런 수준을 충족시키기 위해서는 표준 프로세스가 존재해야 하며 해당 프로세스는 맞춤화와 피드백을 통해 개선할 수 있어야 한다.(Bernd Hindel, 2015)

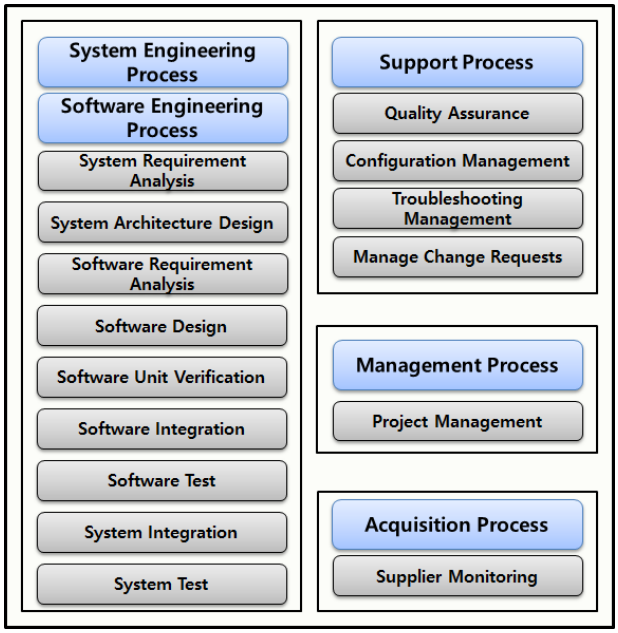

Figure 6. HIS Scope Process

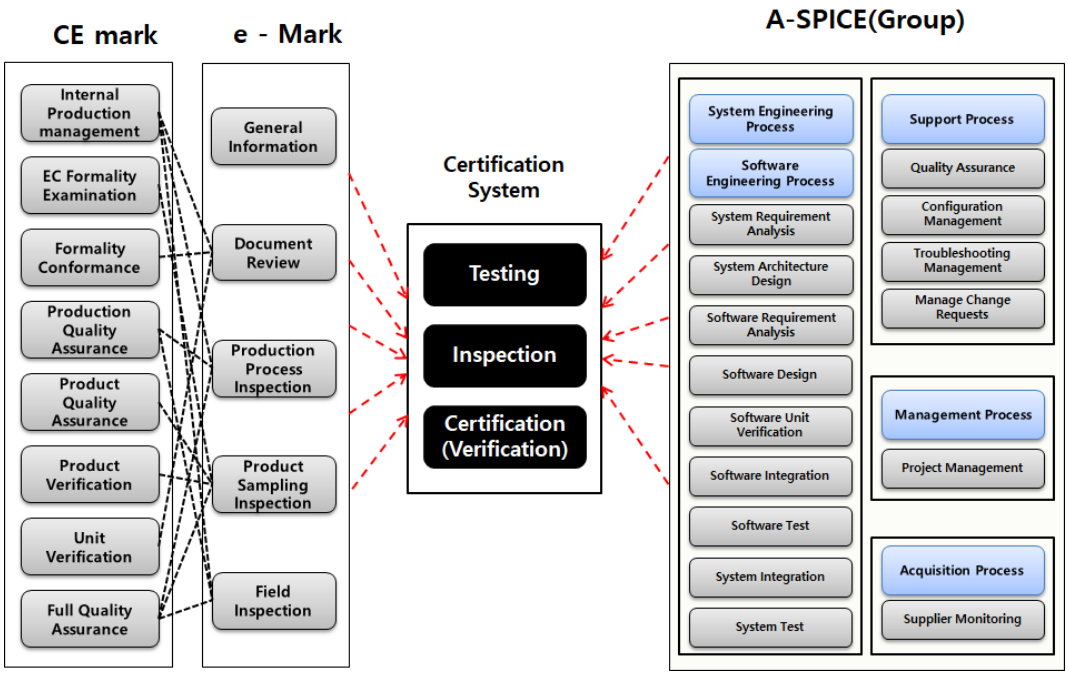

Figure 7. A Comparative Mapping of CE Mark, e-Mark, and A-SPICE

우리나라의 국가기술표준원(KATS)에서 인증제도(Certification System) 운영은 시험(Test)과 검사(Inspection), 인증(Certification) 3가지로 운영된다. 본 연구는 안전인증체계를 설계하는 것이 목적이므로 각 인증 체계의 세부 프로세스 중 핵심 키워드인 Test, Inspection, Certification(Verification)을 활용하였고 추가로 안전(Safety), 보안(Security) 키워드를 활용하여 각 안전인증제도의 세부 프로세스를 비교하였다. e-Mark의 인증프로세스는 '일반현황' 외에 모든 프로세스가 CE Mark에 모두 종속되었다. 여기서 '일반 현황' 이란 심사 전 책임자로부터 회사 소개를 청취하고 심사에 대해서 면담하는 단계를 의미하며 ISO9001의 '경영자 면담' 절차와 유사하다고 볼 수 있다.

CE Mark와 e-Mark의 차이점은 CE Mark는 e-Mark의 절차를 더욱 세분화 시켜 놓은 형태이나 유럽의 경우 자동차의 안전인증은 CE Mark가 아닌 e-Mark인증을 받도록 되어 있다. CE Mark 프로세스는 e-Mark에 비하여 절차가 더욱 세분화 되어있다. 따라서 본 연구가 제시하는 모델의 프로세스는 현재 자동차 전장 용품 인증에 사용되고 있는 e-Mark 인증프로세스를 기반으로 설계하였으며 자율자동차 안전인증에 필수적으로 요구되어야 하는 프로세스 요소를 추가하였다. 모델을 구성하기 위해 A-SPICE 모델을 활용하여 소프트웨어 인증에 필요한 프로세스를 도출하여 하나의 모델로 통합하였다.

4.2 모듈방식의 안전인증 통합모델

CE Mark와 e-Mark의 비교에서 '일반현황' 프로세스는 맵핑이 되지 않았으나 '일반현황' 프로세스에 해당하는 경영자 면담은 본 연구의 목적인 자율주행자동차의 안전인증체계와는 관련성이 높지 않아 본 통합 모델에서 제외하였다. CE Mark와 e-Mark는 프로세스 내용상으로 큰 차이가 없으며 A-SPICE 모델에서 사용하고 있는 프로세스를 주로 활용하였다. 이는 자율주행자동차는 기존의 자동차와는 달리 자율주행 기술이 탑재되어 있어 소프트웨어가 필수적으로 설치되기 때문이다.

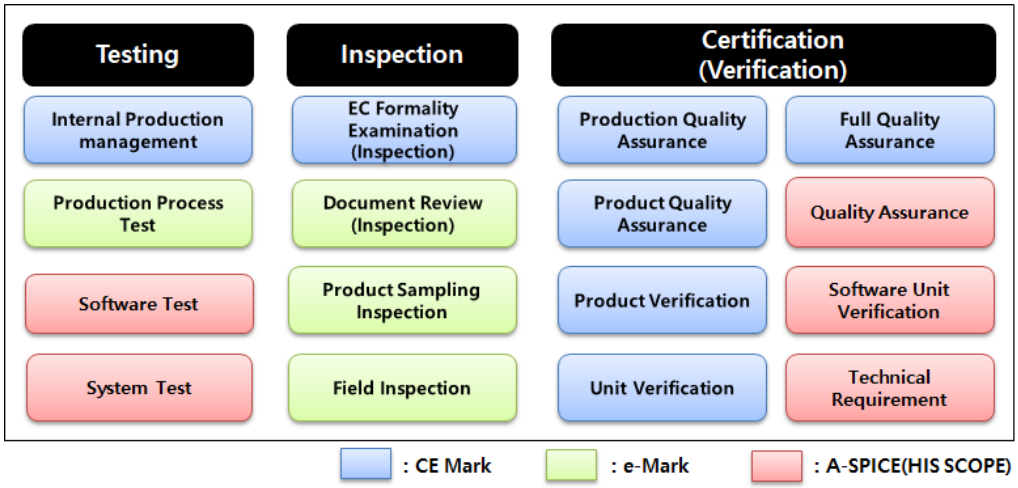

Figure 8. An Integrated Model using e-Mark and A-SPICE

A-SPICE는 총 32개의 프로세스로 설계되어 있으나 HIS Scope를 참고하여 이에 해당하는 프로세스 중 2개 그룹 4개 프로세스를 추가하였다. HIS Scope에 포함되는 프로세스의 내용 중에서 Testing, Inspection, Certification(Verification), Safety, Security 키워드가 포함된 프로세스를 도출하여 추가하였다. 또한 '취득 프로세스(Acquisition Process)' 의 기술 요구사항 프로세스는 HIS Scope에 해당하지 않지만 추가하였다. 이는 2015년 독일 VDA에서 발간한 A-SPICE의 매뉴얼이라고 볼 수 있는 'Automotive SPICE Process Assessment/ Reference Model'의 '기술 요구사항 프로세스'에서 안전과 보안에 대한 기술 요구사항을 직접적으로 다루고 있기 때문이다. 동 매뉴얼에 따르면 기술요구사항 프로세스를 사용했을 경우에는 기술 요구사항에는 환경 영향 평가, 안전, 보안에 관련 된 표준을 포함하여 기타 관련된 표준을 준수하였는지에 대해서 평가가 가능하다고 제시하고 있다.

한국지식재산보호협회에서 발표한 세계 스마트카 기술의 특허 출원 추이를 살펴보면 안전/보안 분야가 41%로 가장 많았다.(이병윤, 2016) 이러한 동향으로 볼 때 출시 이전에 개발 단계에서 안전, 보안을 위한 '기술 요구사항 프로세스'는 필수적이라고 할 수 있다. 또한, 엔지니어링 프로세스 그룹에 포함되어 있는 소프트웨어 단위 검증(Software Unit Verification)에 대해서 소프트웨어 상세 설계 및 비기능적 소프트웨어 요구사항을 준수하는지에 대한 검증을 목표로 제시한다. 소프트웨어의 세부 단위를 검증하고 요구사항 준수 여부와 소프트웨어에 추적성에 대해서 검증하는 것에 초점을 맞추고 있다.

소프트웨어 및 시스템 테스트 프로세스는 소프트웨어 아키텍쳐 디자인과 시스템과 잘 통합되었는지에 대해서 검증하는 프로세스이다. 지원프로세스 그룹의 '품질보증 프로세스'의 목적은 제품이나 프로세스가 사전에 정의된 기준과 계획을 준수하고 부적합 사항이 원만하게 해결되었는지에 대한 여부와 해당 부적합 사항이 반복되지 않도록 독립적이고 객관적인 보증을 제공하는 것이다. 이를 통해 관련 요구사항이 있는 작업에 대해서 산출물, 프로세스 및 활동의 부적합 사항을 식별할 수 있으며 해당 내용을 기록하여 관련 이해 관계자에게 공유하고 역추적하여 재발을 방지할 수 있다. 다만, 소프트웨어는 제품처럼 물리적인 형태가 아닌 논리적인 형태로 공유된다. 물리적인 제품의 경우처럼 100% 정확한 시험 및 검사를 보장하기 힘들다는 점을 인정해야 하는 상황이다.

5. 결론 및 한계점

본 연구는 자율주행자동차의 안전인증체계를 모듈방식으로 추진하는 방안에 초점을 맞추었다. 모듈 개념을 표준화 프로세스를 활용하면 사각지대에 해당되는 기준을 미연에 방지할 수 있다는 사실에 착안하여 기존 e-Mark 모델에 포함되어 있지 않은 소프트웨어 안전에 대한 인증 프로세스를 통합하는 방안을 새롭게 시도하였다. 자율주행자동차는 많은 기능이 소프트웨어에 의존하는 경우가 많다. 소프트웨어 오류로 인하여 급발진이나, 오작동이 발생하게 될 경우에는 치명적인 인명 사고로 이어질 수 있음을 의미한다. 본 연구에서는 이러한 문제를 개선하기 위하여 제품의 설계 단계부터 소프트웨어의 안전에 대해서 평가할 수 있도록 새로운 모델을 제안하였다.

본 연구는 유럽에서 통용되고 있는 CE Mark에 기반을 두고 e-Mark와 A-SPICE에서 자율주행자동차의 안전인증체계에 영향을 미치는 요인들을 선별하여 추가하였으므로 연구 결과물인 모듈방식은 실제 적용에 필요한 타당성 분석을 크게 요구하지 않는다. 이미 사용하고 있는 안전인증 프로세스 요소 기준에 대한 오류들이 걸러진 상태로 볼 수 있기 때문이다. 완전히 새로운 안전인증체계의 개발보다는 기존 인증체계의 모듈화 개념을 이용하여 적용 범위와 다양한 상황에 대한 대응성을 높이려고 주력하였다. 독일의 베언트 힌델(Bernd Hindel)은 A-SPICE는 전 세계 자동차 엔지니어링 분야에서 가장 많이 사용할 개발 프로세스평가 모델이 될 것이라고 하였다. 2005년 A-SPICE 2.0 버전이 최초로 개발된 이후, 2010년 3.0 버전이 나오기까지 7번의 개정을 거쳤으며 2017년 11월 현재로써 최종 버전인 3.1버전으로 업데이트 된 상태이다. 모듈 개념에 기초를 둔 표준체계의 강점은 적용 기준과 방식의 업그레이드가 쉽다는 점이다. 따라서 본 연구가 제시하는 모듈 방식도 현재 A-SPICE의 일부 프로세스를 사용하고 있으나 새롭게 개정된 모델이 출시될 경우 필요한 해당 프로세스만 교체하는 유연성을 갖게 된다. 이러한 부대 효과는 안전인증체계 유지관리 과정에서 비용과 시간(인증기간)을 저감시키는 효과로 이어질 수 있다.

모듈화의 개념은 표준화의 개념과 유사하다. 표준화된 프로세스를 통용하기 때문에 다양한 상황에도 동일한 테스트를 거칠 수 있으며 이는 일관된 인증 과정을 의미하며 품질을 일관성을 보장할 수 있다. 그러나 A-SPICE는 구입해서 사용할 수 있는 프로세스가 아니고 여러 모범 사례와 이를 어떻게 학습해 나가야 하는지에 대한 아이디어다. 모듈방식의 안전인증은 학습요점 파악과 지속적인 관리를 통해서 자율주행자동차의 실질적인 안전 수준을 확보하는데 활용되어야 한다.

본 연구에서 제시된 모듈방식의 자율주행자동차 안전인증 모델은 초기 모델로서 실제로 적용하기 위해서는 모델에 대한 타당성을 검증하는 절차가 필요하다. 실질적인 도입 이전에 모델을 다양한 관점에서 분석하고 관련 전문가의 의견을 바탕으로 모델의 한계점을 도출하고 보완하는 후속 연구가 선행되어야 할 것이다.

또한 본 연구에서 제안된 모델은 모듈의 장점을 활용하여 기존 융복합제품의 인증에서 발생할 수 있는 프로세스의 복잡성을 개선하고 자율자동차 출시 이전 설계와 개발 단계에서 자율주행자동차에 사용되는 부품과 소프트웨어의 안전 및 보안 검증을 동시에 진행하는데 초점을 맞추고 있다. 이는 자율주행자동차의 부품 결함이나 소프트웨어 오류로 발생할 수 있는 사고를 미연에 방지하는 효과를 거둘 것으로 기대되며, 모듈방식의 안전인증체계가 산업 4.0 시대에 다른 융복합제품의 안전인증에도 활용될 수 있다.

REFERENCES

Antonio, KW Lau, CM Yam Richard, and Esther Tang. "The complementarity of internal integration and product modularity: An empirical study of their interaction effect on competitive capabilities." Journal of Engineering and Technology Management 26:305-326.

Baldwin, Carliss Young, and Kim B. Clark. 2000 Design rules: The power of modularity. MIT press.

Birch, J., Rivett, R., Habli, I., Bradshaw, B., Botham, J., Higham, D., and Palin, R. 2013. "Safety cases and their role in ISO 26262 functional safety assessment." International Conference on Computer Safety, Reliability, and Security. Springer, Berlin, Heidelberg.

Cha, W. Y., 2016. “US Autonomous Driving Policy and Implications of Google's Autonomous Car Patent.” KISTEP Research Report.

Cho, J. H., Jung, Y. J, Jun, S. H., Han, T. M. and Kim, H. S. 2010. “An Implementation of automotive development methodology Based on ISO 26262.” Transactions of the Korean Society of Automotive Engineers, Autumn Conference and Exhibition, 2052-2059.

Cho, J. H., Park, K. M., Han, T. M., Jung, Y. J., Jeon, S. H. and Kim, H. S. 2009. “An Analysis of ISO 26262 and its applications.” Transactions of the Korean Society of Automotive Engineers. Autumn Conference and Exhibition 1697-1702.

Choe, G. H. 2016. “Standardization test certification guidebook in international trade required for technical barriers.” IICS, ISBN: 979-11-959002-0-6.

Choi, B. R. 2012. “Product Safety Certification and Product Liability(focused on Liability of State and Manufacturer for defective Products of Product Safety Certification.“ The Korean Consumer Safety Association 2:15-38.

Dardar, R., Gallina, B., Johnsen, A., Lundqvist, K., and Nyberg, M. 2012. "Industrial experiences of building a safety case in compliance with ISO 26262." Software Reliability Engineering Workshops (ISSREW), IEEE 23rd International Symposium on IEEE.

Drucker, Peter F. 1990. "The emerging theory of manufacturing." Harvard Business Review 68:94-102.

Gallina, Barbara. 2014. "A model-driven safety certification method for process compliance." Software Reliability Engineering Workshops (ISSREW), IEEE International Symposium on IEEE.

Habli, Ibrahim, and Tim Kelly. 2006. "Process and product certification arguments: getting the balance right." ACM SIGBED Review 3:1-8.

Hoogeweegen, M. R., Teunissen, W. J., Vervest, P. H., and Wagenaar, R. W. 1999. "Modular network design: Using information and communication technology to allocate production tasks in a virtual organization." Decision Sciences 30:1073-1103.

ISO/IEC Guide2:1996(Standardization and related activities - General vocabulary)

Jacobs, Mark, Shawnee K. Vickery, and Cornelia Droge. 2007. "The effects of product modularity on competitive performance: do integration strategies mediate the relationship?." International Journal of Operations & Production Management 27:1046-1068.

Kim, N. K., Kim. Y. J., Heo, J. W., Choi, J. Y., Choi, J. Y., Kim, Y. S., and Cho, S. R. 2017. “The need for 5G in the Age of Fourth Industrial Revolution and a Standardization Trends about 5G Mobile communication” The Korea Institute of Communications and Information Sciences 739-740.

Kornecki, Andrew, and Janusz Zalewski. 2009. "Certification of software for real-time safety-critical systems: state of the art." Innovations in Systems and Software Engineering 5:149-161.

Langlois, Richard N. 2002. "Modularity in technology and organization." Journal of economic behavior & organization 49:19-37.

Lee, B. Y. 2016. “Trends and prospects of autonomous driving technology development at home and abroad.” Korea Institute of Information and Communication Engineering 33:10-16.

Lee, M. S. 2016. “The Trend of International Safety Standard on Autonomous Vehicles.” Auto Journal 38:22-26.

Lee, Y. S., Kim, H. M. and Hwang, S. M. 2002. “A Study on Architecture Analysis of SPICE and CMMI model.”

Korea Multimedia Society 51-54.

Min, K. C. and Lee, M. S. 2015. “The Trend of Temporary Operating Permit and Safety Standard on Autonomous Vehicles in Korea and Abroad.” Auto Journal 37:53-58.

Ministry of Trade, Industry and Energy. 2016, “A Study on Industrial Policy Direction for Activating Ecosystem of Smart Automobile Industry.”(Final Report).

Park, S. G. 2017. “Current and Future of Autonomous Vehicles.” Korea Robotics Society 14:11-17.

Sabar, Suneel. 2011. "Software Process Improvement and Lifecycle Models in Automotive Industry.".

Seol, H. J. 2007. “Methodology for process benchmarking and modularization.” Seoul National University Graduate School of Industrial Engineering(PhD thesis).

VDA QMC Working Group 13/ Automotive SIG. 2015. “Automotive SPICE Process Reference Model/Process Assessment Model(Ver.3.0).”.

Yang, H. T. 2017. “Guidelines for autonomous vehicles with deregulation of the US government.” Science and Technology Policy Institute 27:4-9.