연구보고서 2015-002

소프트웨어 안전성 확보 체계에 관한 연구

- 시험, 평가, 인증을 중심으로

A Study on the System of Ensuring SW Safety for a SW Oriented Society - Focus on Testing, Evaluation, Certification

박태형/김태호/진회승

2016.01

SPRi 소프트웨어정책연구소

이 보고서는 2015년도 미래창조과학부 정보통신진흥기금을 지원받아 수행한 연구결과의 보고서로서 내용은 연구자의 견해이며, 미래창조과학부의 공식입장과 다를 수 있습니다.

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

소프트웨어 안전성 확보 체계에 관한 연구 - 시험, 평가, 인증을 중심으로

2. 연구 목적 및 필요성

본 연구는 SW의 안전성을 확보하는 프로세스의 관점에서 예방적 단계를 구성하고 있는 '시험 → 평가 → 인증' 체계에 대하여 국내외의 현황을 검토하고, 국내의 SW안전 확보를 위한 개선 방안을 제안하는 데 그 목적을 두고 있다.

3. 연구의 구성

본 연구는 총 6장으로 구성되어 있다.

제1장은 서론으로서, 본연구의 배경, 필요성, 연구의 목적 등을 기술하였다.

제2장에서는 SW의 안전성을 확보하는 중요한 절차적 요소로서 시험, 평가 등에 대한 이론적 배경을 정리하였다. 시험, 평가, 인증이 무엇이며, 어떻게 유기적으로 연결되는지 등에 대한 개론적 수준에서 논의하고자 하였다.

제3장에서는 미국을 비롯한 해외 주요국의 시험, 평가, 인증 체계의 현황을 검토하여, 국내 환경과의 비교분석의 근거를 마련하고 시사점을 도출하였다.

제4장은 국내 현황분석으로서 , SW공학센터, TTA, KTL 등 국내 주요 시험, 평가, 인증 기관의 조직, 인력, 업무 현황 등을 중심으로 검토, 분석하였다.

제5장에서는 제3장 및 제4장의 시사점 및 문제점을 중심으로 소프트웨어 안전을 확보하기 위한 시험, 평가, 인증 체계의 개선방안을 제시하였다.

제6장에서는 본 연구를 수행함에 있어 논의된 연구의 한계점과 향후 연구방향을 기술하였다.

4. 연구 내용 및 결과

1) 해외 주요국의 소프트웨어 안전 확보 체계 현황 및 시사점

소프트웨어 안전을 위한 표준은 주로 유럽 및 미국 정부에서 위임한 기관, 표준기관, 과 유럽과 미국에 기반을 둔 글로벌 업체에서 관여하여 만들고 있다. 이미 만들어진 표준도 변화하는 제품에 따라 변경되어야 하는 요구 사항, 특히 소프트웨어 분야에 추가되어야 하는 요구사항이 생겨나고 있으며, 여러 기관과 글로벌 업체가 이러한 요구사항을 표준에 반영하기 위한 작업을 하고 있다. 이러한 글로벌 업체는 각 도메인의 제품 및 소프트웨어의 테스트 및 인증도 수행하고 있으며, 그 성장속도가 빠르게 증가하고 있다.

소프트웨어 안전 제고 및 안전 산업 활성화를 위해서는 표준 제정기관 활동에 참여하여 표준 제정에 기여하고, 테스트 기관 및 인증기관으로서 기술력을 높이는 활동이 필요하리라 본다. 또한 기술력을 가지고 있는 글로벌 업체와 활발한 교류로 소프트웨어 안전관련 기술력 향상도 필요하리라 본다.

그리고 도메인별로 나누어진 표준 및 가이드를 비교/분석하여, 소프트웨어 안전 제고 및 안전성 확보 체계 마련에 기반으로 사용해야 할 것이다. 물론 이러한 활동은 정부기관 및 연구소에서도 수행해야 하겠지만, 테스트 및 인증 업체에 위임하여 국내 테스트 및 인증 산업 활성화에도 기여해야 하겠다.

2) 국내 소프트웨어 안전 확보 체계 현황 및 시사점

국내 소프트웨어 안전 관련 업체들은 현재까지 주로 저부가가치 서비스인 제품 개발 최종단계에 이루어지는 품질 중심의 테스팅 및 컨설팅을 주로 하고 있어, 고부가 가치 서비스인 제품 개발 초기 단계부터 이루어지는 안전 분석, 설계 컨설팅 및 인증으로의 작업 전환이 필요하다. 『국내 소프트웨어 안전(Safety) 산업동향 조사』에 따르면 국내 업계에서 보는 해외 선진사와의 가증 큰 차이는 다양한 산업별로 보유하고 있는 레퍼런스라고 느끼고 있는 것으로 나타났다. 따라서 국내 업체가 각 산업군별로 안전 수행 작업을 하여 관련 레퍼런스를 쌓아 한 단계 발전할 수 있도록 하는 정책적 지원도 필요하겠다.

국내에서 이미 수행하고 있는 소프트웨어 품질 관련 인증들도 현 상황을 반영하여 수정 보완 작업이 필요하다. GS 인증, SP 인증 등은 소프트웨어 안전 특성 반영에는 미흡점이 있다. 기능 안전 관련 국제 표준 내용을 분석하여 품질 및 프로세스에 대한 내용에 소프트웨어 안전 기능 요소에 대한 반영이 필요하다.

3) 소프트웨어 안전 확보 체계 개선 방향

(1) 소프트웨어 안전 개념의 확립

현재 국내는 소프트웨어와 관련된 품질(Quality), 보안(Security), 안전(Safety) 간의 개념이 명확하지 못하다. 특히 소프트웨어 품질, 보안, 안전 사이의 개념 구분이 모호하여, 소프트웨어 안전에 대한 연구 범위 및 정책 방향 설정이 이루어지고 있지 않았다. 소프트웨어 안전에 대한 개념이 확립되지 못하는 경우, 국제 표준을 적용하는 데 어려움을 겪을 수밖에 없으며, 이로 인해 글로벌 진출에 있어, 국제적 안전 수준을 충족하지 못해 실패하는 상황이 발생하게 되는 문제가 있다.

(2) 정보공유를 통한 소프트웨어 안전성 제고 역량 강화

국내의 경우, 소프트웨어 안전을 시험・평가・인증하는 기관이 상대적으로 분산되어 있어, 각 산업분야 별로 안전점검 기관 및 인허가 담당기관이 달라서 정보공유를 통한 협업이 원활하지 않은 상황이며, 안전 관련 기관 간 해외 수출 지원이나 인증 관련 업무 등에 어려움을 겪고 있다. 또한 담당 부처 및 전담기관의 분산으로 인해 소프트웨어 안전 관련 공통기술의 활용도가 낮아 중복투자 또는 예산 낭비가 발생할 가능성도 존재한다.

소프트웨어 안전 관련 신기술, 위험요인, 대응방안 등의 정보 공유를 위한 협의체를 구성하고 활성화 될 수 있도록 지원할 필요가 있다. 인허가를 관장하는 전담기관 간의 정보공유 체계를 강화하고, 공통기술, 사고사례, 문제해결 사례 등을 적극 공유해야 한다. 나아가 소프트웨어 안전사고 대응 모범사례집 발간을 통해 역량 강화와 인식을 제고하는 노력도 필요하다.

(3) 소프트웨어 안전성 확보를 위한 기술 역량 강화

산업 분야별로 소프트웨어 안전 관련 기능안전성 국제 표준이 존재함에도 불구하고, 여전히 국내 적용에 대한 연구활동이 미흡하다. 특히, 산업별로 안전성 보장 및 사고 예방을 위한 위험요소 및 분석 등에 대한 연구활동이 저조하여 소프트웨어 개발 단계 중 설계 단계에서 안전성이 제대로 반영되지 못한다.

이러한 문제는 소프트웨어 안전사고의 예방이라는 측면에서 접근할 때, 예방 실패 가능성을 높이게 되고, 그 결과로 막대한 사회경제적 피해나 인명 피해를 초래하게 된다.

우선적으로 산업군별 공통 적용 가능한 표준 모델을 개발하고, 이를 기반으로 산업군별 특화 모델을 개발, 보급할 필요가 있다.

소프트웨어 안전성 관련 요구사항 도출 및 관리, 설계, 개발, 테스팅 등의 단계에서 시스템의 안전성을 분석하고, 이에 따른 안전 메커니즘에 대한 설계 및 구현을 위한 체계 및 도구를 개발・지원해야 한다.

한편, 민간의 역량을 강화 하기 위해 소프트웨어 안전 관련 국가 차원의 R&D 지원을 통해 해외 의존도가 높은 소프트웨어 안전 확보 기술을 국산화할 필요가 있다. 특히, 인증으로 이어지는 테스팅 및 정적 분석 도구 분야의 지원사업을 강화하고 국내 운용사례 확보를 통해 기술을 고도화해야 할 것이다.

(4) 소프트웨어 안전 전문인력의 육성 및 역량 강화

소프트웨어 안전성을 확보하기 위해서는 개발에서부터 시험, 평가, 인증에 이르는 체계 속에서 지식과 기술을 활용할 수 있는 전문인력이 양성되어야 함에도 불구하고, 현재 국내의 경우에는 품질 및 프로세스 중심으로 소프트웨어 공학 교육이 이루어지고 있어, 소프트웨어 안전 전문인력을 양성하기에는 어려움이 있다.

나아가, 소프트웨어 안전 분야에 종사하는 인력의 전문성을 강화하기 위한 교육기관도 없는 실정이어서 체계적인 교육이 이루어지지 못하고, 현장에서 실무경험을 축적하는 수준에 머무르고 있다.

전문 인력 확보를 위해서는 소프트웨어 안전 관련 사회/산업적인 기반 성숙이 선행되어 소프트웨어 안전 산업에 대한 인식 제고, 소프트웨어 안전 서비스에 대한 대가의 현실화, 국내 TIC업체의 고부가가치 서비스로의 전환 등이 이루어지고, 이를 통해 수준 높은 전문인력이 유입 또는 육성되는 선순환 구조를 마련해야 한다.

대학 및 대학원 등 제도권 교육을 통해 신규인력을 양성하여 시장에 공급함과 동시에 재직자를 위한 소프트웨어 안전 전문 교육프로그램을 개설하여 전문역량을 강화시키는 것도 중요하다. 이와 연계하여 소프트웨어 안전분야에 국가자격제도를 도입하고, 신뢰성 있는 전문가로의 위상 강화도 고려해 볼 필요가 있다.

(5) 법제도 개선을 통한 소프트웨어 안전성 강화

해외 선진국에서는 주요 산업 도메인별 소프트웨어 안전 표준이 준수 될 수 있도록, 직간접적으로 법/규정을 제정하고, 관리감독 기관에서 감독하고 있다. 법/제도에서 표준 준수 여부를 정부 기관이 관리/감독하거나, 허가 받은 업체가 인증을 수행함으로써, 표준이 준수될 수 있도록 제도화 하고 있다.

일관된 소프트웨어 안전 관련 개념을 확립하고 정책을 시행하기 위해 소프트웨어 안전법과 같은 기본법을 제정할 필요가 있다. 기본법 제정을 통해 산업군별 소프트웨어 안전성을 확보하는 계기를 마련해야 한다. 또한 산업별 특성을 고려하여, 소관 부처 및 전문기관과의 협력을 통해 기존의 관련 규정 및 지침에 소프트웨어 안전 내용을 반영하여야 한다.

(6) 국제 표준 준수 및 국제 활동 지원 강화

소프트웨어 안전성 관련 국제표준이 존재하고, 각 산업분야 별로 세분화되고 있다. 모표준으로서 IEC 61508을 토대로 국내 실정에 맞는 공통 기준이 마련되어야 한다. 나아가 소관 부처 및 전문기관과의 협력을 통해 산업별 특화된 소프트웨어 안전 기준을 마련하고, 산업별 기존의 안전 관리 규정에 SW안전 기준을 현실적으로 반영할 필요가 있다.

또한 소프트웨어 안전 관련 국제표준에 대응하고, 국내 적용을 위해서 관련 국제 회의 및 기구 등에 적극 참여할 수 있도록 지원체계를 강화할 필요가 있다. 이는 글로벌 경쟁력 강화에도 큰 기여를 하는 문제이기도 하다.

따라서 현재, 국내의 국제표준화 활동 지원사 업이나 국가 표준기술력 향상 사업 등 국제 표준화 기반 강화와 전문가 양성 등을 목표로 하는 지원 사업을 보다 확대 지원할 필요가 있다.

5. 정책적 활용 내용

본 연구의 결과물은 SW중심사회에서의 소프트웨어 안전성 확보를 위한 정책 수립에 있어 기초자료로 활용할 수 있다.

먼저, 산업 분야별 소프트웨어 안전 확보 관련 시험, 평가, 인증체계에 대한 이해에 큰 도움이 될 것으로 판단한다.

또한 해외 주요국의 소프트웨어 안전성 확보 현황을 참고하여 소프트웨어 안전성을 확보하는 국내 시험, 평가, 인증 기관의 효율적이고 유기적인 체계 개선 정책 수립에 활용할 수 있다.

6. 기대효과

본 연구를 통해 소프트웨어 안전성 확보의 중요성을 인식하고, 시험, 평가, 인증체계의 개선을 통해, 단기적으로는 대상 소프트웨어 또는 시스템의 안전성을 제고함과 동시에 중기적으로는 국가 전반의 안전성을 확보할 수 있을 것으로 기대한다.

또한 장기적으로는 고부가가치 산업으로서의 소프트웨어 안전 분야에서 기업의 경쟁력을 강화하여 글로벌 시장에서 제도적·기술적 선도적인 국가로서의 위상을 확보할 것으로 기대한다.

SUMMARY

This study is designed to review the current status of the "test → assessment → certification" system at home and abroad, which composes the preventive phases from the perspective of the process that secures S/W safety; and to propose methods of improving the aforementioned system to secure software safety at home.

If we look at the present situation of the systems for securing software security in major overseas countries, standards are mainly established by the organization authorized by the European and U.S. governments as well as global companies based in Europe and U.S. However, a well-established standard still needs to be amended when a product is changed or modified and, in particular, whenever it is necessary to add a new requirement to the software area. Several organizations and global companies are working on the project to reflect such requirements in the standard. Global companies also test and verify the product and software in each domain, and the growth of the test and verification business is gaining momentum.

We need to contribute to the establishment of standards by participating in the activities of organizations responsible for establishing standards, and perform activities aimed at improving our technical skills as a test agency and certification authority, in order to improve software safety and establish a safe industry. We also need to enhance technical skills related to software safety through active exchange with global companies with advanced technical skills.

In addition, the standards and guidelines divided by each domain should be compared and analyzed, and used as the basis for improving software safety and security safety. Of course, these activities should be also performed by government agencies and laboratories. However, if these activities were delegated to test and certification service companies, it would contribute greatly to promoting the domestic test and certification industry.

Until now, a testing and consulting service centered largely on quality has been provided in Korea, which is a low added-valued service performed at the final phase of product development. As a result, it should be switched to a high-added-value service comprising safety analysis, design consulting and certification, all of which are performed from the early phase of product development. According to "Research on the trend of the domestic software industry," the domestic industry believes that advanced overseas companies have various references in each industry, and that is the biggest difference from our own domestic industry. Therefore, policy support is also needed in order to enable domestic companies to take a step forward, by

accumulating references after conducting safety work for each industry group.

Certification related to software quality, which has been already performed in Korea, needs to be modified and supplemented by reflecting the present conditions. GS Certification and SP Certification are not sufficient to fully reflect the characteristics of software safety. The content of international standards related to functional safety needs to be analyzed, so that software safety functional elements can be reflected in the quality and process content.

When the present domestic situation is compared with that of major overseas countries, the following improvement methods can be proposed.

First, a concept of software safety should be established. Currently, the conceptual difference between quality, security and safety related to software remains unclear in Korea. In particular, the scope of research on software safety and policy direction has not yet been fixed due to the ambiguous conceptual definition of software quality, security and safety. If the concept of software safety cannot be established, we will inevitably have difficulty in applying international standards, which will in turn cause the failure of global market entry as a result of our inability to satisfy the international safety standard.

Second, software safety capability should be strengthened by sharing information. A consultative group needs to be formed and supported for promotion, in order to share information on new technologies related to software safety, risk factors, and methods of response. Also, the information sharing system among organizations dedicated to license management should be strengthened; and common technologies, incident cases, and problem-solving cases should be actively shared. Furthermore, efforts to strengthen competence and improve awareness are needed, including the publication of a book of case studies on response to software safety incidents.

Third, technological competence should be enhanced to secure software safety. A standard model that can be commonly applied to each industry group should be developed, and specialized models based on that standard model should be developed and diffused. System safety should be analyzed during the phase of requirement identification and control, design, development and testing related to software safety. Then, the system and tools for designing and implementing safety mechanisms should be developed and supported.

Fourth, software safety experts should be fostered and their competencies strengthened. A virtuous cycle needs to be created in which the social/industrial foundations related to software

safety is matured in advance, awareness of the software safety industry is raised, the price of software safety services is rationalized, domestic TIC companies switch to high added-value services and, finally, high-level experts are either brought in or nurtured. It is also important to nurture a new workforce through institutional education (e.g., colleges, graduate schools) and supply it to the market, and launch a training program specialized in software safety to allow workers to improve their specialized capability. In tandem with these activities, we need to consider the introduction of a national qualification system in the software safety area, and strengthening workers' position as reliable experts.

Fifth, software safety needs to be strengthened by improving the legal system. We need to enact a fundamental law such as the "Software Safety Act" to establish a consistent concept related to software safety and implement the relevant policies. An opportunity should be created to secure software safety by industry, by enacting a fundamental law. In addition, details of software safety should be reflected in existing related regulations and industry in cooperation with the ministry and office concerned and specialized organizations, after considering the characteristics by industry.

Lastly, international standards should be observed, and support for international activities should be increased. Currently, there are international standards related to software safety that are sub-divided by industry area. Common criteria that fit the present domestic conditions should also be prepared, based on the IEC 61508 as a "mother" standard. Furthermore, we should establish a software safety standard specialized in each industry through cooperation with the ministry and office concerned and professional organizations, and practically reflect the software safety standard in the existing safety control regulation for each industry. In addition, we need to strengthen the support system, so that the domestic industry can actively participate in related international conferences and organizations in order to respond to international standards related to software safety and apply them to the domestic industry. It could also make a significant contribution to strengthening global competitiveness. Therefore, the number of support projects aiming at consolidating the foundation of the international standard and at fostering experts should be increased, including domestic support projects for international standard activities and projects for enhancing national standard technical skills.

CONTENTS

제1장 서 론

제1절 연구의 배경 및 필요성

1. 연구의 배경

안전이라 함은 “자연적 혹은 인위적 위험요인이 없거나, 이러한 위험 요인에 대한 충분한 대비가 되어 있는 상태”를 말한다.[1] 안전한 상태를 유지하기 위해서는 홍수, 가뭄, 폭설, 산사태 등 자연재해로 인해 발생되는 다양한 위험요인을 제거하는 노력 뿐만 아니라, 인간의 편리와 효율을 위해 구축한 인위적인 것으로부터 피해를 입지 않도록 하는 노력이 필요하다.

그러나 최근 세월호 사고, 의정부 아파트 화재, 지하철 2호선 충돌 사고 등 대형 재난안전 사고의 발생으로 안전에 대한 국민의 인식은 어느 때보다 높다. 이러한 상황에서 정부는 재난·안전 관리체계에 대한 혁신방안인 「안전혁신 마스터플랜」을 관계부처 합동으로 마련하고, 추진 중에 있다. 이에 따라, 산업 환경의 안전, 생활 환경의 안전, 교육 환경의 안전 등 여러 분야의 안전 확보를 위한 장치들이 구축되고 있는 실정이다.

한편, SW중심사회는 주요 산업별로 SW비중이 갈수록 증가하고 있으며, SW의 품질이 시스템 운영에 큰 영향을 미치고 있다. 당연한 결과겠지만, SW의 복잡성과 SW에 대한 의존성이 증대할수록, SW가 시스템의 품질과 성능 및 성패를 좌우하는 핵심요소로 인식되고 있는 것이다.

일반적인 SW 고장(failure)은 불편하지만, 심각하거나 장기간 손해를 입히지 않기 때문에 우리가 감내할 수 있다. 그러나 그 고장이 안전의 문제와 결부될 때, 또는 경미한 고장도 방지해야 하는 중대한 시스템(critical system)인 경우에는 상황이 다르다.

SW 오류에 의해 발생되는 사고가 빈번하지는 않지만, 몇가지 사례를 예로 들어 보면, 1991년 2월, 걸프전쟁에서 패트리어트 미사일 방어 시스템에서 발생한 사고에서는 소프트웨어를 통한 시간 계산의 오류로 인해 발생한 사고로서 당시 28명의 생명을 잃었다. 또한 2009년 8월, 한국 첫 우주 발사체 나로호에서 발생한 사고는 헬륨 탱크의 압력을 측정하는 소프트웨어의 결함으로 발사를 중지하게 되어 경제적 피해를 유발하기도 하였다.

---

1) 행정자치부, 국가안전관리기본계획 2010-2014

이처럼 경미하거나 사소한 SW오류가 사람의 생명을 앗아가거나 막대한 경제적 피해를 초래하기도 하는 것이다. 안전의 관점에서 이러한 사례를 바라볼 때, 심각한 경제적·물질적 피해를 초래하거나 인간의 생명에 막대한 위협이 되는 경우에는 보다 거시적이고, 체계적인 대응이 필요하다는 것을 의미한다.

SW안전을 확보하는 일의 가장 우선시 되어야 하는 것은, SW 오류나 고장으로 인해 사고가 발생하지 않도록 하는 '예방'의 노력이다. 모든 안전 분야가 그렇듯이, 사고가 발생하지 않는 상태를 유지하는 것이 가장 중요하다.

2. 연구의 목적

SW가 개발되는 프로세스에서 필요한 안전성 확보 수단은 시험, 평가, 인증 등으로 구분할 수 있다. 정확하고 투명한 '시험 → 평가 → 인증'의 단계를 거치면서 최소한의 SW안전성 확보 요건을 충족했다고 할 수 있다. 그만큼 시험, 평가, 인증은 매우 중요한 절차적 요건이다.

본 연구는 SW의 안전성을 확보하는 프로세스의 관점에서 예방적 단계를 구성하고 있는 '시험 → 평가 → 인증' 체계에 대하여 국내외의 현황을 검토하고, 국내의 SW안전 확보를 위한 개선체계를 제안하는 데 그 목적을 두고 있다.

3. 연구의 구성

본 보고서는 총 6장으로 구성된다.

제1장에서는 서론으로서, 본연구의 배경, 필요성, 연구의 목적 등이 기술된다.

제2장에서는 SW의 안전성을 확보하는 중요한 절차적 요소로서 시험, 평가, 인증 등에 대한 이론적 배경을 정리한다. 시험, 평가, 인증이 무엇이며, 어떻게 유기적으로 연결되는지 등에 대한 개론적 수준에서 논의하고자 한다.

제3장에서는 미국을 비롯한 해외 주요국의 시험, 평가, 인증 체계의 현황을 검토하여, 국내 환경과의 비교분석의 근거를 마련하고 시사점을 도출한다.

제4장은 국내 현황분석으로서 , SW공학센터, TTA, KTL 등 국내 주요 시험, 평가, 인증 기관의 조직, 인력, 업무 현황 등을 검토 분석하여, 제 Ⅲ 장에서 논의된 해외 주요국의 현황

과 비교 분석한다.

제5장에서는 제 Ⅲ 장 및 제 Ⅳ 장의 시사점 및 문제점을 중심으로 SW안전을 확보하기 위한 시험, 평가, 인증 체계의 개선방안을 제시한다. 이와 함께, 본 연구를 수행함에 있어 논의된 연구의 한계점과 향후 연구방향을 기술하고자 한다.

제6장은 결론으로서, 연구의 요약, 연구의 한계점, 향후 연구 방향 등에 대해 논의한다.

4. 연구 방법

본 연구는 국내의 SW안전 관련 시험, 평가, 인증 체계에 대한 개선방안을 도출하는 목적을 달성하기 위해서 먼저, 기본적으로는 문헌연구를 중심으로, 시험, 평가, 인증 등에 대한 개요와 해외 주요국 및 국내 체계에 대한 조사를 수행한다. 국내외의 정책문서, 정책보고서, 연구보고서, 학술논문 등이 주된 대상이다.

둘째, 국내 SW안전 전문가 및 전담기관의 담당자와의 인터뷰 등을 통해 연구보고서의 적실성을 제고한다. 인터뷰 및 자문회의 등을 수행하고, 이를 반영함으로써 문헌 중심의 연구가 가지는 문제점을 제거하고자 한다.

제2장 SW안전 확보를 위한 시험·평가 체계

제1절 소프트웨어 시험(Testing)·평가 개요

1. 소프트웨어 테스팅

전자, 자동차 등 국내 주력 산업 전반에서 디지털 컨버전스 현상이 확연하게 진행되고 있다. 이에 따라, 과거 하드웨어 서킷, 마이콤 등에 의해서 구현되던 임베디드 시스템들이 높아진 복잡도로 인하여 임베디드 소프트웨어로 대체 개발되는 현상이 확산되고 있다. 결과적으로 임베디드 소프트웨어의 품질 향상을 위한 테스팅에 대한 필요가 크게 증가하고 있다.[2)]

소프트웨어 품질 관리에 이용되고 있는 다양한 기법들 중에서 가장 널리 이용되고 있는 기법은 소프트웨어 테스팅이다. 소프트웨어 테스팅은 과거에는 소프트웨어 개발자의 책임 하에 수행되었으나, 현재 많은 소프트웨어 개발업체에서는 테스팅 업무를 별도의 소프트웨어 품질관리팀에 위임하고 있다. 따라서 소프트웨어 개발 조직과 소프트웨어 품질관리 조직의 생산성 제고 문제는 매우 중요한 이슈로 등장하고 있다.[3)]

소프트웨어 테스팅은 소프트웨어 결함을 찾아내고 개선하는 일련의 절차를 통해 소프트웨어 품질을 확보하는 가장 대표적인 방법 중의 하나로 알려져 있다. 이전의 소프트웨어 테스팅은 응용 프로그램 또는 시스템이 정상적으로 잘 동작하는지, 성능, 안전성, 사용자 인터페이스 등이 요구사항을 만족하는지를 확인하기 위해 결함을 확인하기 위해 결함을 발견하는 활동으로 정의되어 개발 이후에 수행하는 하나의 업무활동에 지나지 않았다. 하지만 최근에는 소프트웨어 개발 초기단계부터 사용자의 요구사항에 맞는지 확인하고 정상적으로 동작하는지 검증하는 과정을 거치면서 결함을 발견하고 수정하며, 발견된 결함을 기반으로 프로젝트 또는 제품의 리스크에 대한 수치적 데이터를 의사결정권자에게 전달하는 일련의 프로세스 전체를 의미하는 것으로 그 개념이 확장되고 있다. 즉, 소프트웨어 테스팅 활동은 소프트웨어 개발 수명주기 전반에 걸쳐 시스템 또는 명세의 결함을 발견하는 모든 일련의 활동들을 포함하고 있다.[4)]

---

2) 배현섭·윤광식·오승욱, 임베디드 소프트웨어 테스팅 이슈 및 현황, COMMUNICATIONS OF THE KOREA INFORMATION SCIENCE SOCIETY, 24(8), 2006.8

3) 정창신·정순기, 소프트웨어 자동 테스팅 도구의 발전 로드맵 분석, 한국컴퓨터정보학회논문지, 9(1), 2004.3

소프트웨어 품질 특성 중 신뢰도 보장을 위해서 효율적인 품질측정을 위한 테스트 방안이 요구되고 있다. 이는 소프트웨어 유형별 주요 품질 특성을 알고, 그 품질 특성을 확인할 수 있는 구체적인 테스트 방법을 안다면, 무엇을 어떻게 테스트해야 하는지 파악하고 쉽게 접근할 수 있다.[5)]

먼저, 다양한 종류, 다양한 도메인의 소프트웨어들의 분류가 나오고 각각 어떤 품질 속성이 최우선적으로 보장되어야 하는가를 알아야 한다. 둘째, 특성 품질 속성을 검증하기 위해 어떤 테스트 활동을 수행할 것인가에 대한 구체적인 전략 기법, 테스트 활동 지침에 대한 정보가 필요하다. 즉, '소프트웨어-품질속성' 혹은 '품질속성-검증기법'에 대한 정보를 알 수 있다면 특정 소프트웨어에 대한 품질을 확인하고자 할 때 해당 소프트웨어에 있어서 가장 중요한 품질 속성과 그 속성들을 검증하기 위한 테스트 방법들을 도출하여 이를 기반으로 구체적인 테스트 활동을 수행할 수 있게 된다.[6)]

2. 소프트웨어 품질 평가

국내에서도 IT 융합산업이 늘고 있는 가운데 소프트웨어의 품질과 성능에 대한 시험평가가 핵심요소로 떠오르고 있다. 그러나 하드웨어의 경우는 공인시험 인증기관 운영이 활발하게 이루어지고 있는 반면에, 소프트웨어에 대해서는 GS 품질인증을 제외하면 정보보호 분야에만 한정되어 있는 실정이다. 따라서 산업용 소프트웨어 제품의 국제 표준적합성 구현은 필수적인 요구사항이 되고 있으며, 특히 임베디드 소프트웨어 분야에서 국제표준을 활용한 시험 평가는 글로벌 시장 진입에 필수 요건이 되고 있다. 그러나 산업 현장에서는 국제 표준을 어떻게 활용해서 시험 평가를 진행해야 하는지 등에 대한 방법이 명확하지 않아서 적용이 어려운 실정이다.[7)]

소프트웨어 품질 평가는 고품질의 소프트웨어를 생산하기 위한 하나의 방법이다. 이러한 소프트웨어 제품의 품질 평가시 가장 중요한 요소는 평가에 있어서 객관성이 보장되어야 한다는 것과 정량적으로 측정하여 관리할 수 있어야 한다는 것이다. 따라서, 소프트웨어의 품질을 측정하고, 평가하기 위해서는 소프트웨어 생명주기 단계별로 품

4) 차순일, 소프트웨어 테스팅 산업 현황과 전망, 정보과학회지, 28(11), 2010.11
5) 박정인·최진탁, 소프트웨어 신뢰성 테스트를 위한 평가 척도, 융복합지식학회논문지, 1(1), 2013.1
6) 강명묵·구태완·백종문, 소프트웨어 결함 발견 및 제거 노력 기반 신뢰성 추정 모델, 정보과학회논문지:소프트웨어 및 응용, 37(7), 2010.7
7) 노경현·이금석·이민재, ISO 25000과 IOS 29119를 활용한 임베디드 소프트웨어 시험평가 방법에 관한 연구, 한국정보과학회 제16회 한국 소프트웨어공학 학술대회 논문집, 16(1), 2014.2

질평가 체계를 확립하고 이러한 체계에 적용할 수 있는 평가 점검표의 개발이 필수적이다.[8)]

최근 들어 ISO/IEC 9126을 기반으로 하여 소프트웨어 품질 특정을 위한 구체적인 방법들이 많이 개발되었다. 정보통신산업진흥원(NIPA)의 '소프트웨어 기술성 평가 기준 해설서'나, 한국정보통신기술협회(TTA)의 '웹기반 소프트웨어 품질평가 지침'에 구체적인 품질 측정 방법들이 제시되어 있다. 이들은 ISO/IEC 9126 및 ISO/IEC 12119 기반의 심사기준인 평가모듈을 근간으로 하여 국내에 맞게 바꾸었다.[9)]

8) 조재규·이승종, 소프트웨어 품질향상을 위한 품질평가 모델에 관한 연구, 한국정보과학회 학술발표논문집, 30(1B), 2003.4
9) 박정인·최진탁, 소프트웨어 신뢰성 테스트를 위한 평가 척도, 융복합지식학회논문지, 1(1), 2013.1

제2절 소프트웨어 시험·평가 기준으로서의 국제 표준[10)]

1. 소프트웨어 품질 관련 국제 표준

1) ISO/IEC 9126

ISO/IEC 9126은 2001년에 만들어진 소프트웨어 제품 품질에 대한 국제표준으로서 소프트웨어 제품이 갖는 품질 특성에 대하여 6가지로 정의하고 있다. 6가지 품질 특성은 다시 27개의 부특성으로 나누어 정의하고 있다.

<표 2-1> ISO/IEC 9126의 6가지 품질 특성 정의

품질 특성	정의
기능성 (functionality)	특정 조건에서, 문서화된 요구사항과 니즈에 대해 제품에서 구현된 기능을 제공하는 제품의 역량
신뢰성 (reliability)	특정 조건에서, 제품이 성능을 유지할 수 있는 역량
사용성 (usability)	특정 조건에서, 사용자가 제품을 이해하고, 배우고, 즐길 수 있는 역량
효율성 (efficiency)	특정 조건에서, 적정 자원을 사용하면서 요구된성능을 내는 역량
유지보수성 (maintainability)	환경, 요구사항, 기능에 따라 개선·적용·변경을 할 수 있는 역량
이식성 (portability)	환경의 변화에 맞게 쉽게 바뀌어 지는 역량

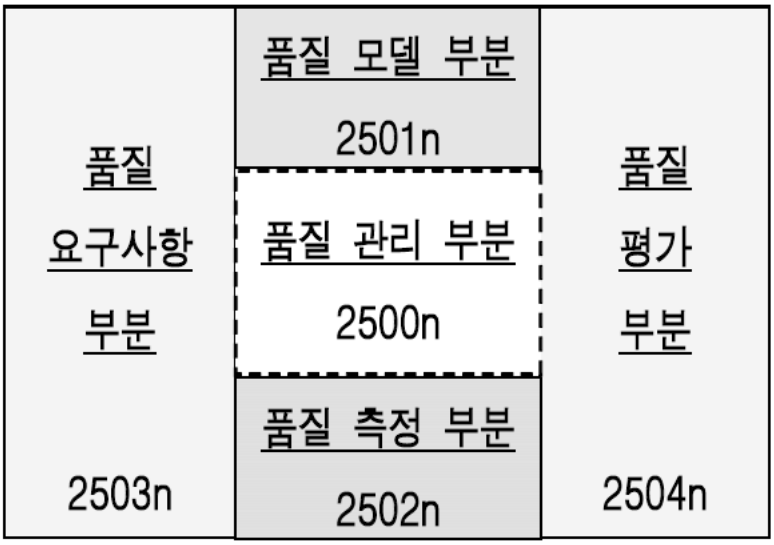
자료 : 윤형진·최진영 (2015) 인용

2) ISO/IEC 25000 시리즈

ISO/IEC 25000 시리즈는 SQuaRE(Software Quality Requirements and Evaluation)fk 불리며, 소프트웨어 제품의 품질 관리, 품질 모델, 품질 요구명세, 품질 측정 및 품질 평가 등을 다루는 다섯 개 부분으로 이루어져 있다.

10) 윤형진·최진영, 소프트웨어 제품과 프로세스 관점에서 국제표준과 비교를 통한 테스팅 프론티어 역량평가 모델 개선 방안, 정보과학회: 컴퓨팅의 실제 논문지, 21(2), 2015.2, pp. 116-118에서 관련 표준 내용을 그대로 인용함

[그림 2-1] SQuaRE 표준 시리즈 구조



자료 : 노경현·이금석·이민재 (2014) 인용

ISO 2500n 품질관리 부분에서는 SQuaRE 구조 모델, 용어, 참조 모델들, 소프트웨어 제품 요구사항 명세 및 평가 관리를 담당하는 기능을 지원하는데 필요한 사항 및 평가를 제공한다. 품질 측정 부분은 측정 참조 모델 및 지침, 품질 측정 요소, 소프트웨어의 내부 및 외부와 사용 품질 측정 지침을 제공한다. 품질 요구사항 부분에서는 품질 요구사항을 개발하기 위한 프로세스에 대한 지침을 제공한다. 품질평가 부분에서는 평가 참조 모델, 평가모듈, 평가 프로세스에 대한 지침을 제공한다.[11)]

11) 노경현·이금석·이민재, ISO 25000과 ISO 29119를 활용한 임베디드 소프트웨어 시험평가 방법에 관한 연구, 한국정보과학회 제16회 한국 소프트웨어공학 학술대회 논문집, 16(1), 2014.2

3) ISO/IEC 25010

ISO/IEC 25010는 2011년에 만들어진 시스템과 소프트웨어 제품에 대한 국제표준으로서, 시스템 및 소스트웨어 제품이 갖는 품질 특성에 대하여 8가지로 구분하고 있다. 8가지 품질 특성은 31개의 부특성을 포함하여 정의하고 있다.

<표 2-2> ISO/IEC 25010의 8가지 품질 특성 정의

품질 특성	정의
기능적합성 (functional suitability)	제품 혹은 시스템이 명시된 조건에서 사용될 경우, 명시되거나 암시된 요구를 충족시키는 기능을 제공하는 정도
수행효율성 (performance efficiency)	규정된 조건 하에 사용된 자원의 크기에 대한 상대적 성능
호환성 (compatibility)	같은 하드웨어 혹은 소프트웨어 환경을 공유하는 동안 기타 제품, 시스템 혹은 구성요소를 교환할 수 있고, 또는 요구된 기능을 구성할 수 있는 정도
유용성 (usability)	제품 및 시스템이 명시된 사용 환경에서 유효성, 효율성 및 만족의 명시된 목적을 달성하는 명시된 사용에 인해 사용될 수 있는 정도
신뢰성 (reliability)	시스템, 제품, 혹은 구성요소가 시간이 명시된 기간에 대해 명시된 조건 하에서 명시된 기능을 구성하는 정도
보안 (security)	제품 또는 시스템의 유형과 인증 수준에 따라 사람 및 다른 제품/시스템이 적절한 데이터 접근을 가지기 위해서 해당 제품 또는 시스템이 데이터를 보호하는 정도
유지관리성 (maintainability)	제품 또는 시스템이 유지관리의 의도에 따라 변경되는 효과성 및 효율성의 정도
이동성 (portability)	시스템, 제품 또는 구성요소가 특정 하드웨어, 소프트웨어 또는 다른 운영 및 사용환경 등이 다른 하드웨어, 소프트웨어 및 환경으로 전환될 수 있는 효과성과 효율성의 정도

자료 : 윤형진·최진영 (2015)에서 인용, 수정

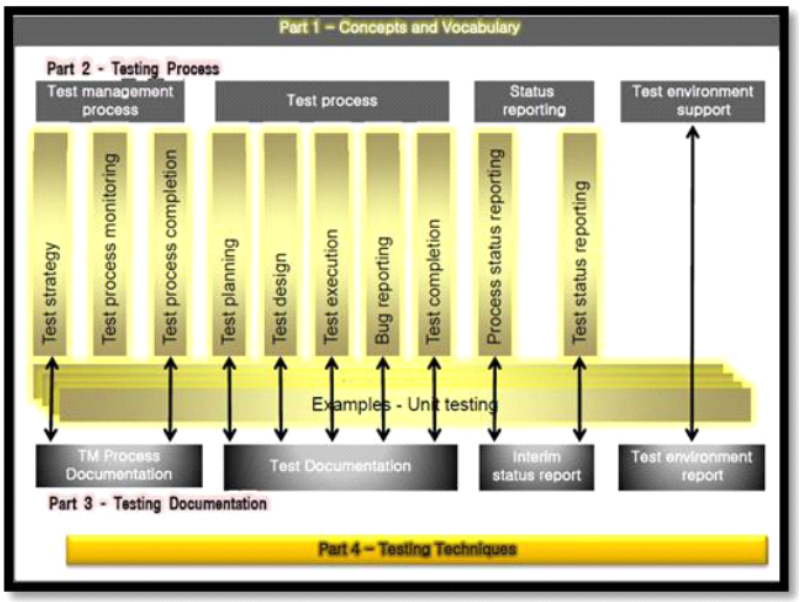
4) ISO/IEC 29119 시리즈

ISO/IEC 29119 시리즈는 소프트웨어 시험 절차 및 관련 산출물 등을 규정한 소프트웨어 시험 평가에 대한 국제 표준으로 소프트웨어 개발 전체 수명주기에 대한 시험 프로세스가 정의되었다. ISO/IEC 29119는 기존의 BSI, IEEE 국가 표준과 산업계의 시험 평가 표준인ISTQB(International Software Testing Qualifications Board)와 혼재하는 것을 해결하기 위해 기존 표준을 대체하고 통합되었다.[12)]

12) 노경현·이금석·이민재, ISO 25000과 ISO 29119를 활용한 임베디드 소프트웨어 시험평가 방법에 관한 연구, 한국정보과학회 제16회 한국 소프트웨어공학 학술대회 논문집, 16(1), 2014.2

Part 1 Concepts and Vocabulary에는 소프트웨어 시험 평가의 원리와 시험 평가 프로세스의 개요, 사용되는 용어가 포함된다. Part 2 Testing Process에는 소프트웨어 수명주기 프로세스 표준(ISO/IEC 12207)을 기준으로 시험평가 절차가 정의되어 있으며, 시험 평가에 필요한 추가적인 가이드가 정의되어 있다. Part 3 Testing Documentation에는 시험 평가에서 작성되는 표준 문서 템플릿이 정의되어 있다. Part 4 Testing Techniques는 시험 평가에 사용되는 시험 기법들이 정의되어 있으며 명세 기반 시험 설계 기법, 구조 기반 시험 설계 기법, 경험 기반 시험 기법 등이 포함된다.

[그림 2-2] ISO/IEC 29119 구성

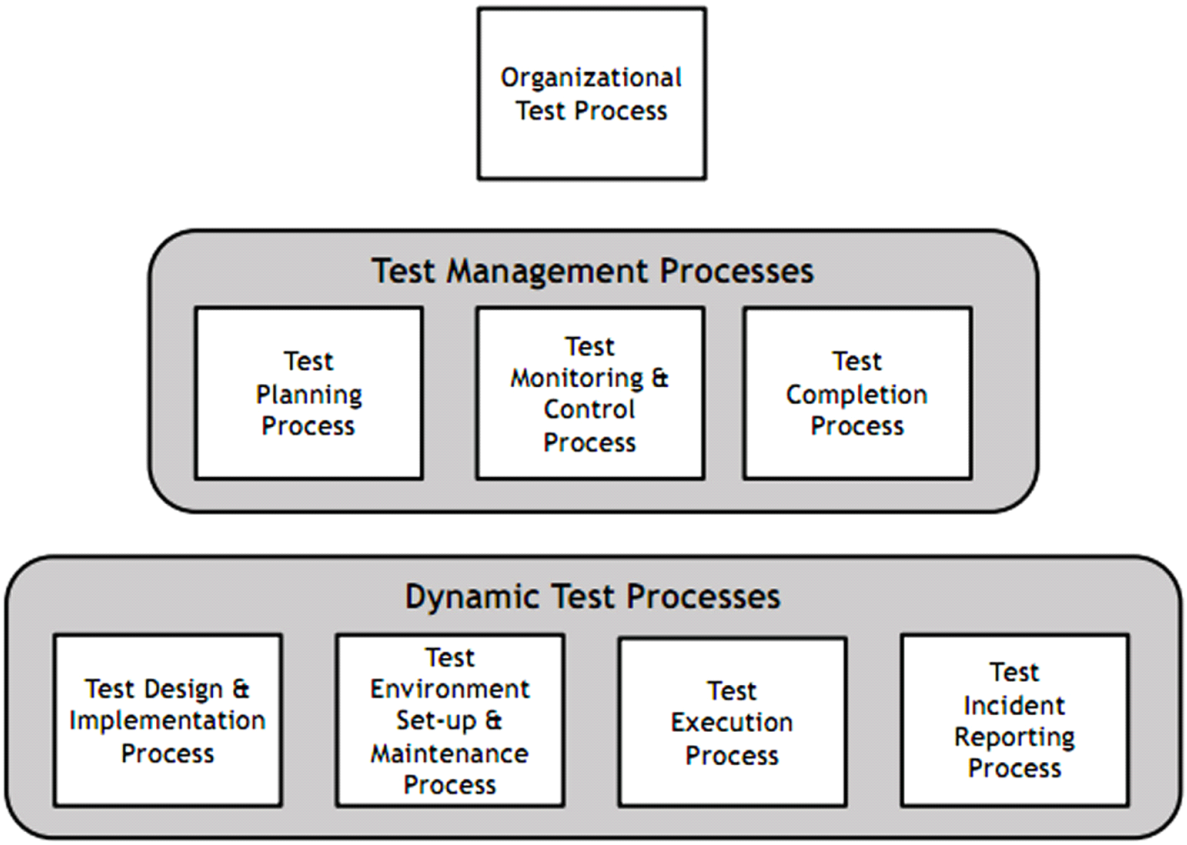


자료 : 노경현·이금석·이민재 (2014)에서 인용

특히, ISO/IEC 29119 part 2는 2013년 만들어진 소프트웨어 테스트 프로세스에 대한 국제표준이다.

테스트 프로세스를 정의하고 있는 part 2에서는 크게 테스트 프로세스 그룹을 '조직적 테스트 프로세스 그룹', '테스트 관리 프로세스 그룹', '동적 테스트 프로세스 그룹' 3개로 구분하고 있다. 그룹의 하위 개념으로 프로세스를 8개로 구분하며, 프로세스의 하위 개념으로 활동(activity)를 두고 33개로 정의하고 있다.

[그림 2-3] ISO/IEC/IEEE 29119 테스트 프로세스 그룹



자료 : ISO/IEC/IEEE 29119

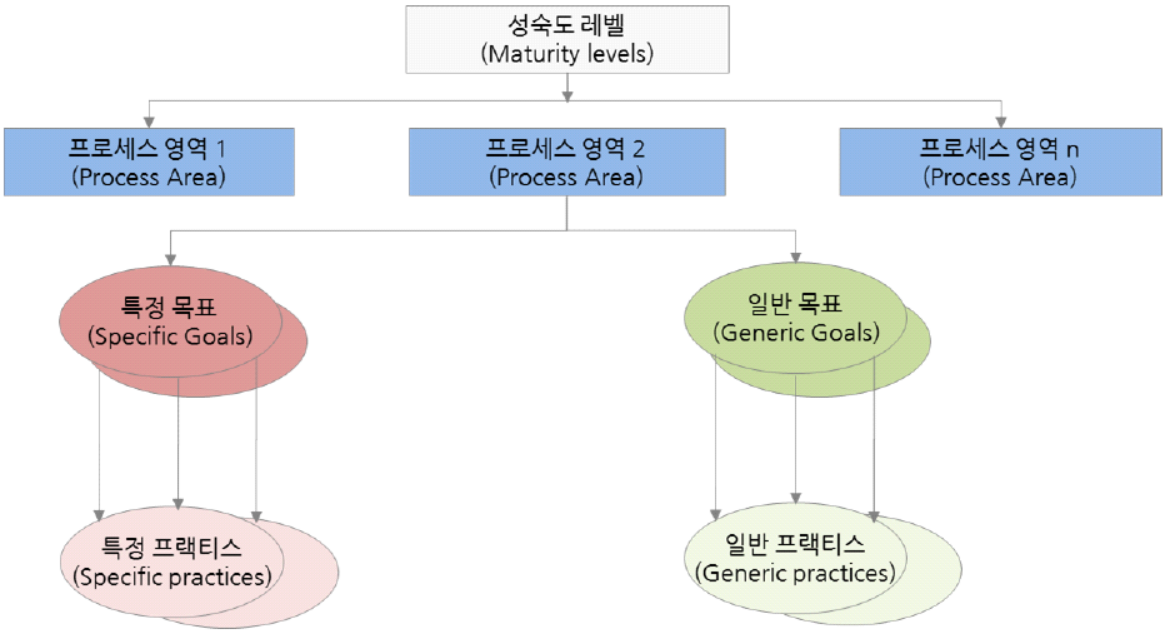
5) TMMi(Test Maturity Model integration)[13]

TMMi는 2008년 SW 테스팅 조직의 성숙도를 평가하고 프로세스를 개선하기 위한 목적으로 비영리 법인인 TMMi 재단에서 개발하였으며, 테스트 조직의 성숙도를 5단계로 평가한다.

TMMi는 각 성숙도 레벨별로 프로세스 영역이 있으며, 하위에 각 프로세스 영역별로 특정 목표와 일반 목표가 정의되어 있다.

13) TMMi는 테스팅 조직에 대한 성숙도 평가모델이지만, 조직의 성숙도가 소프트웨어의 품질을 개선하는 데 기여한다는 측면에서 이 절에서 다루기로 한다.

[그림 2-4] TMMi의 구조



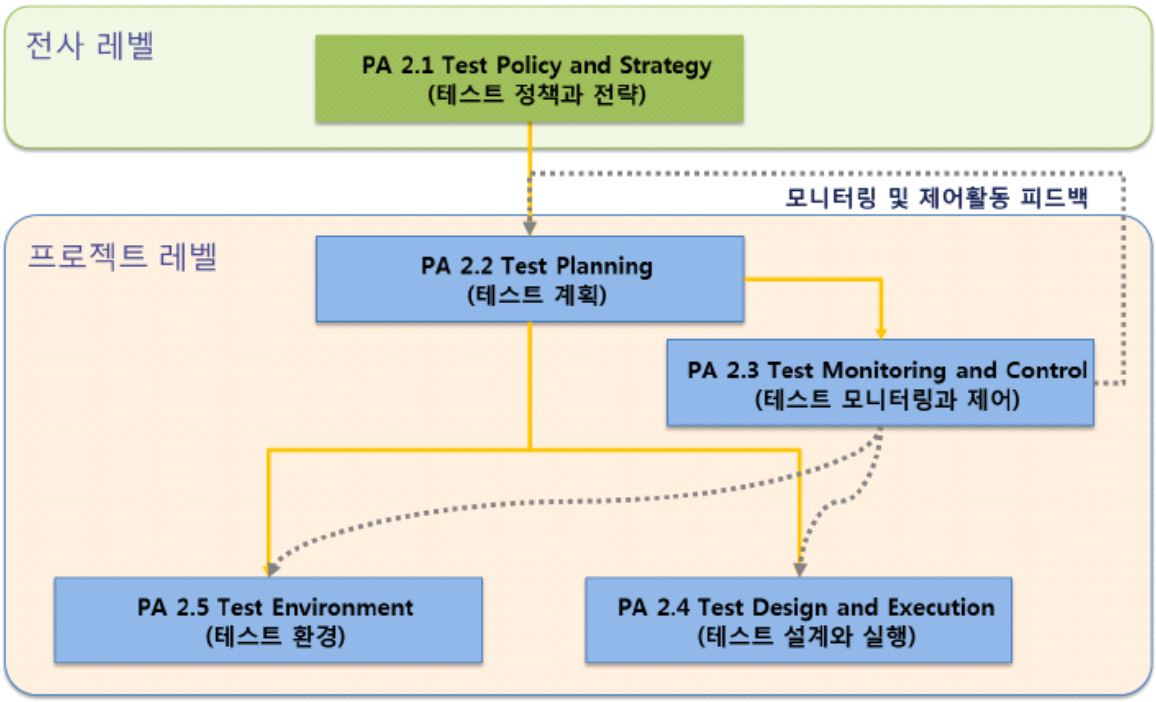
자료 : NIPA·STA (2014)에서 인용

TMMi 레벨 달성이 쉽지 않은 이유는 가장 낮은 프로세스 영역(PA)의 점수가 레벨 달성 여부를 결정하기 때문이다. 따라서 인증 취득을 위해서는 전 프로세스 영역(PA)에 걸쳐 고르게 내재화가 되어야만 가능하다.[14]

예를 들어, TMMi 레벨 2는 아래 그림과 같이 전사 레벨 프로세스와 프로젝트 레벨 프로세스로 구성되며, 5개의 프로세스 영역(PA)이 있다.

14) NIPA·STA, 2013 지역SW융합사업 우수기업 컨설팅 사례집, 2014.5

[그림 2-5] TMMi 레벨 2 프로세스 영역(PA)



자료 : NIPA·STA (2014)에서 인용

2. 소프트웨어 안전 확보를 위한 국제 표준

1) IEC 61508

2000년 국제기구인 IEC(International Electrotechnical Commission)는 IEC 61508을 제정하여 전기/전자/프로그램 가능한 전자 시스템에 대한 기능안전을 명시하였으며 지난 2010년 개정되었다. IEC 61508은 기능안전의 대표적인 표준으로서, 전자기기, 원자력, 의료기기, 프로세스 산업, 자동차 등으로 구분되는 다양한 기능안전 표준의 중추적인 역할을 수행하고 있다.[15)]

IEC 61508(2010)에서는 안전수명주기를 통하여 시스템의 개념단계에서 구현, 양산, 관리, 폐기에 이르기까지의 전사적 과정을 명시하고 있다. 안전제어시스템은 개발부터 운영환경 및 다양한 상황에서 잠재된 위험원을 도출하고 위험원을 허용할 수 있는 수준까지 감소시키고자 한다. 이처럼 위험원을 도출하고 감소시키기 위한 다양한 기법들이 개발 및 발전되고 있으며, 도출된 요구사항을 바탕으로 이에 적합한 안전제어시스

15) 김성규·김용수, 기능안전을 위한 IEC 61508의 안전수명주기에 관한 연구, 신뢰성응용연구, 14(1), 2014.3

템이 설계되었는가를 하드웨어 및 소프트웨어 나아가 시스템 수준에서의 평가가 이뤄지게 된다.[16)]

IEC 61508은 Part 0부터 Part 7까지 총 8개로 구성되어 있다.

<표 2-3> IEC 61508의 구성

구분	구성
Part 0	기능안전성과 IEC 61508
Part 1	일반 요구사항
Part 2	전기/전자/프로그램 가능한 전자장치 안전 관련 시스템의 요구사항
Part 3	소프트웨어 요구사항
Part 4	정의와 약어
Part 5	안전무결성 수준 결정 방법의 예
Part 6	IEC 61508의 Part 2와 Part 3의 적용 지침
Part 7	기법과 수단의 개요

자료 : 김성규·김용수 (2014)에서 인용

Part 0 '기능안전성과 IEC 61508' 에는 기능안전에 대한 일반적인 개념으 ㄹ정의하고 각 Part의 개요 및 구성에 관하여 명시되어 있다.

Part 1 '일반 요구사항' 은 안전 수명주기에 따른 목적, 적용범위, 입력 및 산출물을 명시함으로써, 기능안전을 위한 전체 프레임워크를 정의하고 있다.

Part 2 '전기/전자/프로그램 가능한 전자장치 안전 관련 시스템의 요구사항' 에는 안전제어시스템에 요구되는 안전 요구사항을 결정하기 위한 다양한 기법의 적용 및 SIL의 등급화에 관한 내용이 수록되어 있다.

Part 3 '소프트웨어 요구사항' 에서는 안전제어시스템을 개발함에 있어 하드웨어가 아닌 소프트웨어에 적용되는 안전기능과 SIL에 대하여 명시되어 있다.

Part 4 '정의와 약어' 에는 IEC 61508dp 사용되는 용어에 대한 정의 및 설명을 다루고 있다.

Part 5 '안전무결성수준 결정 방법의 예' 에서는 리스크와 안전무결성의 개념에 대한 설명과 함께 두 개념간의 관계를 명시하고, 안전무결성을 결정할 수 있는 다양한 방법론들에 관하여 예시를 들어 소개하고 있다.

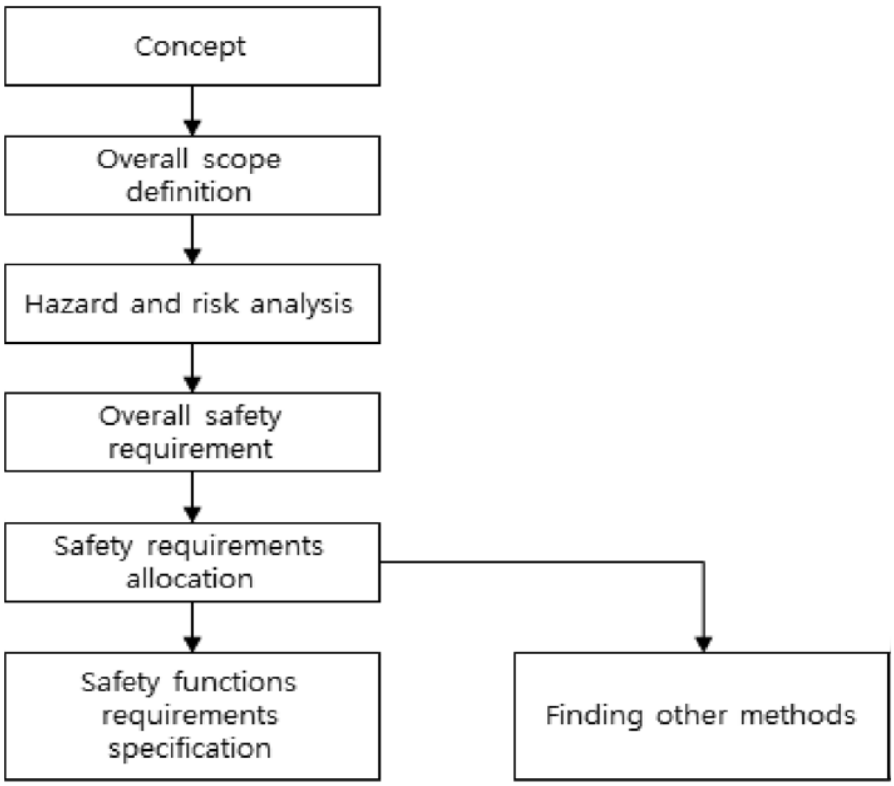
16) 김성규·김용수, 기능안전을 위한 IEC 61508의 안전수명주기에 관한 연구, 신뢰성응용연구, 14(1), 2014.3

Part 6 ‘IEC 61508 Part 2와 Part 3의 적용 지침’ 에서는 Part 2와 Part 3 적용의 기능적 단계와 두 가지 작동모드 하에서의 하드웨어 고장 확률 평가 기법, 진단 범위 및 안전 고장비율 계산 예, 그리고 소프트웨어 안전무결성에 관하여 명시하고 있다.

Part 7 ‘기법과 수단의 개요’ 에는 Part 2 및 Part 3과 관련된 다양한 안전기법에 관한 설명을 제공함으로써, 하드웨어 우발 고장에 대한 제어, 시스템 고장의 회피, 소프트웨어 안전무결성 달성을 위한 기법 및 방법 등이 명시되어 있다.

IEC 61508의 안전기능 도출 과정은 6단계로 이루어져 있으며, 시스템 개념정의에서부터 출발하여 위험분석을 통한 안전 요구사항 도출을 도출하고, 최종적으로 안전기능 요구사항을 도출하게 된다.

[그림 2-6] IEC 61508의 안전기능 요구사항 도출 과정



자료 : IEC 61508(Functional safety of electrical/electronic/programmable electronic safety-related systems) part1, 1998

이 과정은 기능안전성 표준의 핵심적인 과정이라 할 수 있는데, 이후에 정의된 안전 요구사항을 구현하는 과정은 여기에서 도출된 안전기능 요구사항에 따라 달라지게 되는 것이다.[17]

17) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지,

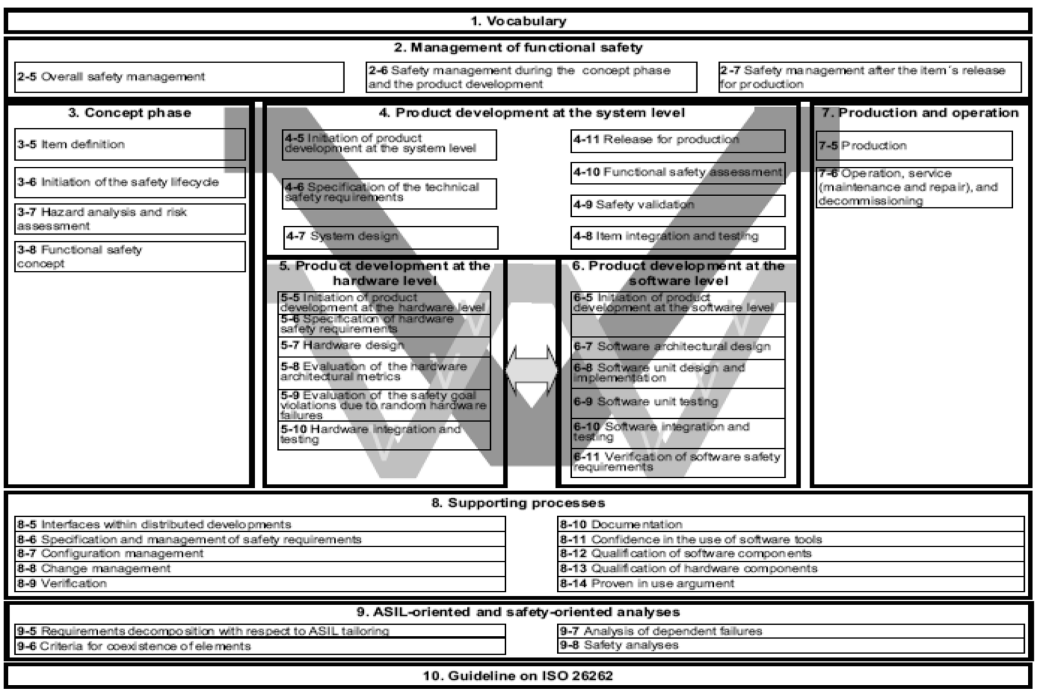
2) ISO 26262 : 자동차 분야 국제 표준

ISO 26262는 IEC 61508을 바탕으로 자동차 분야의 적용을 위해 2011년 11월에 발표된 표준이다. 자동차 ECU의 오작동으로 인한 사고 및 인명손실을 최소화 하는 것이 목적이다.

ISO 26262는 명세, 설계, 구현, 통합, 검증, 인증에 이르는 개발 전 단계에서 최신 개발 방법 및 테스트 방법을 적용하도록 하고 있으며, 기능안전 규격을 준수하기 위한 각 단계에서의 요구사항을 정의한다.

세부적으로는 시스템 레벨, 하드웨어 레벨, 소프트웨어 레벨에서 각 요구사항들이 정의되어 있다. 이는 제품 개념 단계에서부터 폐기까지 전 수명주기에 걸쳐서 전자장치의 고장으로 인한 자동차의 안전성을 저해할 수 있는 위험을 체계적으로 분석하고, 그 위험에 대처하는 수단이 효과적임을 보장해야 하는 것으로서 시스템공학, 하드웨어, 소프트웨어 공학, 신뢰성 공학 안전성 분석 및 프로세스 능력이 모두 요구된다.[18)]

[그림 2-7] ISO 26262의 구성



자료 : 장승연 (2015)에서 인용

30(2), 2012.2

18) 장승연, 안전소프트웨어를 위한 소프트웨어 테스팅 관점에서의 차량기능안전 표준(ISO 26262) 적용방안 논의, 정보과학회지, 33(7), 2015.7

ISO 26262는 총 10의 Part로 구성되어 있다.[19)]

Part1 Vocabulary 파트는 표준에서 사용되는 용어, 정의, 그리고 약어를 설명하고 있으며, 총 142개의 용어 및 정의와 53개의 약 어로 구성되어 있다.

Part2 Management of functional safety는 기능안전 관리를 위한 요구사항을 정의한 파트로 기능안전에 관련된 개발활동을 계획, 조정, 그리고 추적하는 요건에 대해 기술하고 있다.

Part 3 Concept phase는 아이템 정의를 기반으로 위험원 분석 및 리스크 평가를 통해 ASIL 수준을 판정하며, 안전 목표와 안전 메커니즘을 정의 하는 파트이다. ASIL은 대상 시스템이 달성하고자 하는 기능 안전성의 수준을 나타내는 것으로 최저 등급인 ASIL A부터 최고 등급인 ASIL D 총 4개의 등급으로 구성되어 있다. ASIL 등급이 높다는 것은 해당 시스템이 사고가 날 경우 그 피해가 심각할 수 있다는 것을 의미한다. ASIL은 심각도, 노출확률, 제어 가능성의 추정치를 통하여 결정한다. QM(Quality Management) 등급은 ISO26262를 준수하기 위한 별다른 요구사항은 없다는 것을 의미하지만 기본적인 IST/TS 16949와 같은 품질경영 시스템을 준수해야 한다.

<표 2-4> ISO 26262 ASIL 결정 기준표

Potential severity	Probability of exposure	Controllability		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

자료 : 장승연 (2015)에서 인용

19) 정은기, 권혁무, 이민구, 김동준, 홍성훈, 자동차 기능안전 ISO26262와 대응방안, Korean Soc Qual Manage, 41, 2013

Part4 Product development at the system level는 제품 개발 단계 중 시스템 수준에서의 개발을 명시한다. 시스템 수준의 개발은 기본적으로 V모델을 따른다.

Part5 Product development at the hardware level은 하드웨어 수준의 제품 개발을 기술하며, 시스템 설계 명세를 기반으로 하여 시스템의 하드웨어 개발이 이루어진다. 이 또한 시스템 내부에서 다시 V모델을 따르며 개발, 통합, 검증에 대한 요구사항을 포함한다.

Part6 Product development at the software level은 소프트웨어 수준의 제품개발 또한 V 모델을 따르며 개발, 통합 검증에 대한 요구사항을 정의하고 있다.

Part7 Production and operation는 제품의 생산, 운영, 서비스, 그리고 폐기를 위한 요구사항을 포함한다.

Part8 Supporting processes는 안전 요구사항의 명세 및 경영, 형상관리, 변경 관리, 검증, 문서화, 소프트웨어 도구 사용에 대한 신뢰, 사용증명 논거/주장 등에 대한 요구사항을 정의하고 있다.

Part9 Automotive Safety Integrity Level (ASIL) - oriented and safety-oriented analyses는 ASIL과 안전에 기반한 분석을 위한 요구사항을 기술하고 있다.

Part10 Guideline on IOS26262는 주요 개념, 안전 케이스, ASIL 분해 등 ISO26262의 이해에 도움이 되는 정보를 기술하고 있다.

3) DO-178B : 항공분야 국제 표준

DO-178B(Software considerations in airbone systems and equipment certification: 항공 시스템 및 장비 인증의 소프트웨어 고려사항)는 1992년에 제정된 표준으로 항공분야에서 소프트웨어 기능안전성 표준으로 널리 알려진 표준이다. 그러나 이 표준 역시 엄밀하게는 기능 안전성이라는 개념을 가지고 있지는 않다.[20]

DO-178B는 시스템을 위험등급에 따라 5가지로 구분하여 개발하도록 정의하고 있다. 레벨 A부터 레벨 D까지는 소프트웨어의 오작동이 발생했을 때, 유발할 수 있는 장애의 등급을 나누어 소프트웨어 등급을 정하고 있는데, 특히, 레벨 E는 항공기의 운항이나 파일럿의 임무에 영향을 미치지 않는 소프트웨어로 본 표준의 대상이 아님을 명시하고 있다.[21]

---

20) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2), 2012.2

<표 2-5> DO-178B의 소프트웨어 등급

소프트웨어 등급 (Software level)	설명
Level A	Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a catastrophic failure condition for the aircraft.
Level B	Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a hazardous/severe-major failure condition for the aircraft.
Level C	Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a major failure condition for the aircraft.
Level D	Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a minor failure condition for the aircraft.
Level E	Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system with no effect on aircraft operational capability or pilot workload. Once software has been confirmed as level E by the certification authority, **no further guidelines of this document apply**

자료 : 강해달 (2012)에서 인용

한편 DO-178B에서는 장애(failure condition)에 대한 등급을 정의하고 있다.

<표 2-6> DO-178B에서 정의하는 장애등급

장애등급 (Failure Condition Categorization)	설명
Catastrophic	Failure conditions which would prevent continued safe flight and landing
Hazardous /Severe-Major	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operation conditions to the extent that there would be: (1) a large reduction in safety margins or functional capabilities (2) physical distress or higher workload such that the flight crew could not be relied on to perform their tasks a accurately or completely or (3) adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.
Major	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.
Minor	Failure conditions which would not significantly reduce aircraft safety, and which would involve crew actions that are well within their capabilities.
No Effect	Failure conditions which do not affect the operational capability of the aircraft or increase crew workload.

자료 : 강해달 (2012)에서 인용

21) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2), 2012.2

앞의 표에서, ‘Catastrophic’ 등급은 항공기 자체가 추락할 수 있는 장애, ‘Hazardous/Servere-Major’ 등급은 항공기의 기능이나 항공승무원의 임무에 심각한 피해를 주거나 탑승자 일부에게 생명을 위협하는 부상을 입힐 수 있는 장애, ‘Major’ 등급은 항공기의 기능이나 항공승무원의 임무에 주요한 피해를 주거나 탑승자에게 부상을 입힐 수 있는 장애, ‘Minor’ 등급은 항공기나 승무원에게 그 자신의 능력범위 안에서 해결할 수 있을 정도의 피해를 주는 장애를 말한다.[22)]

DO-178B에는 소프트웨어 테스팅과 관련하여 커버리지(Coverage)라는 정량화된 조건을 명시하고 있다. 이는 소프트웨어 테스팅의 완숙도를 정량적으로 측정하는 지표로써 이후 다른 표준에서도 사용하도록 영향을 주었다고 할 수 있다. DO-178B에서 제시하는 커버리지는 두 가지 종류가 있는데, 하나는 요구사항 커버리지(Requirement Coverage)이며, 나머지는 구조적 커버리지(Structural Coverage)이다.

<표 2-7> DO-178B의 소프트웨어 테스팅 커버리지의 등급별 적용

번호	Objective		적용 SW 등급			
	설명	해당목차	A	B	C	D
1	Test coverage of high-level requirements is achieved	6.4.4.1	●	○	○	○
2	Test coverage of low-level requirements is achieved	6.4.4.1	●	○	○	
3	Test coverage of software structure(modified condition/decision) is achieved	6.4.4.2	●	○		
4	Test coverage of software structure(decision coverage) is achieved	6.4.4.2a 6.4.4.2b	●	●		
5	Test coverage of software structure(statement coverage) is achieved	6.4.4.2a 6.4.4.2b	●	●	○	
6	Test coverage of software structure(data coupling and control coupling) is achieved	6.4.4.2c	●	●	○	
범례	● : The objective should be satisfied with independence, ○ : The objective should be satisfied.					

자료 : 강해달 (2012)에서 인용

요구사항 커버리지는 상위요구사항과 하위요구사항 커버리지를 별도로 적용하는 것을 알 수 있다. 또한 구조적 커버리지도 문장 커버리지, 결정 커버리지, MC/DC 커버리지 등으로 별도로 정의하여 소프트웨어 등급별로 사용하고 있다는 것을 알 수 있다. 이중 현재 커버리지 측정을 자동화할 수 있도록 도구가 개발된 것은 구조적 커버리지 중에서도 코드 커버리지라고 할 수 있는 문장 커버리지, 결정 커버리지, MC/DC 커버

22) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2), 2012.2

리지이다. DO-178B는 이와 같이 소프트웨어 개발 프로세스 단계별 검증프로세스를 명시하고, 프로세스에 Objective라는 구성요소를 추가하여 소프트웨어 등급별 프로세스 테일러링을 정립하였으며, 테스트 커버리지라는 정량적인 수치를 제시하였다는 데 의의가 있다고 할 수 있다.[23)]

4) IEC 62304 : 의료분야 국제 표준

IEC 62304(Medical device software-Software life cycle process)는 2006년도에 제정된 표준으로 제목에서도 알 수 있듯이 '기능안전성' 이라는 개념을 포함하고 있지 않다. 따라서, 엄밀하게는 기능안전성 표준이라고 말하는 것이 무리가 있다. 그러나, 의료기기(Medical Device)는 기본적으로 의료서비스를 받는 환자나 의료서비스 종사자들에게 안전해야 한다는 생각을 전제하고 있고, 각 국가별로 안전에 대한 엄격한 규제와 기준을 가지고 있어서 기능안전성 표준을 이야기할 때 빠지지 않고 등장한다.[24)]

특히, 소프트웨어 개발 프로세스 이전에 요구사항을 정의한 표준(IEC 60601)이 별도로 정의되어있고, IEC 61508을 참조하여 도출해낸 의료기기에 대한 안전요구 사항을 미리 분석해서 명시하고 있다는 점에서 기능안전성 표준으로 분류되고 있기도 하다. 그러나, 의료기기 고유의 기능에서 기능안전성 요구사항을 도출해 내는 과정은 본 표준에 포함되지 않았다는 것은 표준에서 정의하고 있는 개발프로세스를 보면 확연하게 알 수 있다.[25)]

앞선 언급처럼, IEC 62304에서는 안전기능 요구사항을 도출하는 과정이 포함되어 있지는 않으나, 소프트웨어의 위험등급을 나누고, 위험등급에 따라 개발프로세스의 세부적인 사항들을 바꾸는 방법으로 소프트웨어의 안전성을 확보하고자 하였다.

---

23) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2), 2012.2
24) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2), 2012.2
25) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2), 2012.2

<표 2-8> IEC 62304에서 정의하는 소프트웨어의 위험등급

안전등급 (Software safety classification)	설명
Class A	No injury or damage to health is possible
Class B	Non-SERIOUS INJURY is possible
Class C	Death or SERIOUS INJURY is possible

자료 : 강해달 (2012)에서 인용

IEC 62304는 이와 같이 안전이 필요한 소프트웨어의 위험등급을 구분하고 이에 따른 소프트웨어 개발 프로세스를 정의했다는 측면에서 소프트웨어의 안전성을 확보하는 표준으로 참고할 만 하지만, 적극적으로 안전기능 요구사항을 도출하고 이를 구현하기 위한 구체적인 방법을 제시하는 데에는 한계가 있다고 할 수 있다.[26]

26) 강해달, 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2), 2012.2

제3절 SW안전성 확보 기술[27)]

1. 소프트웨어 테스팅 기술

본 절에서는 소프트웨어 테스팅 기술에 대해서 설명한다. 다양한 소프트웨어 테스팅 기술 중에서도 특히 중요한 것으로 판단되는 논리 기반 테스팅(logic-based testing) 기법과 최신 기법의 하나인 Concolic testing 기법에 대해서 자세히 설명한다.

1) Logic-based 테스팅

(1) 필요성

Logical predicate는 참/거짓을 판별할 수 있는 문장을 의미하는데, 특히 소프트웨어의 동작을 결정하는 조건(Condition)이 Logical predicate으로 구성되어있기 때문에 이것을 테스트 하는 것은 매우 중요하다. 예를 들어 시스템을 모델링하기 위하여 유한 상태 기계 방식을 사용한다면, 각 상태 사이의 전이 조건(Transition condition)이 모두 Logical predicate에 해당한다. 따라서 Logic-based 테스트를 수행한다는 것은 전체 시스템의 동작을 테스트한다는 의미를 가질 수 있다.

(2) Logic-based 테스팅 기준

Logical predicate을 테스트하기 위해서 효과적인 테스트 케이스 생성 기준이 필요한데, 다양한 Logic criteria가 이러한 테스트 조건을 한다. 예를 들어 Clause criteria의 경우, predicate 내의 각 Clause들이 참/거짓 값을 갖도록 테스트 해야만 만족되는 것으로 정의된다. 그러나 단순히 개별적인 Clause가 참/거짓 값을 가지는 것으로는 부족하며, 여러 Clause에 해당하는 값의 조합을 모두 고려해야 모든 경우를 테스트했다고 볼 수 있다. Combinatorial criteria는 각 Clause의 참/거짓 값의 모든 조합의 경우를 테스트하는 조건인데, 따라서 Clause 개수를 n개라 할 때 총 2^n개의 테스트 케이스가 필요하다. Combinatorial criteria가 강력하다는 사실은 분명하지만, 확장성에서 큰 문제가 있기 때문에 실질적으로는 거의 사용되지 않는다.

---

27) 이 절의 내용은 지은경, 소프트웨어 안전 확보를 위한 기술 분석 보고서, SPRi 내부자료, 2015.12를 발췌·요약함

최근의 연구 결과[28]에 따르면 Minimal-MUMCUT라는 Criteria을 사용하면 Fault hierarchy 그림의 9가지 DNF 오류들을 모두 잡을 수 있다는 것이 알려져 있다. 단, 그보다 더 복잡한 오류에 대해서는 보증할 수 없다. 예를 들면 하나의 Predicate에 대하여 ENF 오류가 가해지고 이어서 TNF 오류가 가해질 경우 ENF나 TNF 오류 하나만 가해지는 경우에 비해 훨씬 복잡한 문제가 된다. 그러나 실제 항공기 소프트웨어에 쓰이는 프로그램을 분석해 본 결과, Minimal-MUMCUT을 이용하여 99% 이상의 Logical 오류를 잡아낼 수 있다는 것을 실험적으로 증명하기도 하였다.

2) Concolic 테스팅

(1) 기본 개념

일반적으로 하나의 소프트웨어는 주어진 입력에 따라서 매우 다양한 행동(behavior)을 보인다. 그것은 프로그램 내부에 있는 분기(branch)와 반복(loop) 때문인데, 이러한 부분들이 소프트웨어의 테스트를 어렵게 만들기도 한다. 소프트웨어의 모든 부분을 효과적으로 테스트하기 위해서는 다양한 테스트 케이스가 필요하지만, 이전까지의 테스트 케이스만으로 제대로 테스트 하려면 어떤 새로운 테스트 케이스를 만들어야 할지 쉽게 알 수 없다. 이러한 문제를 해결하는데 Concolic testing 기법이 매우 효과적이다. Concrete와 Symbolic의 합성어인 Concolic은 두 어원대로 Concrete과 Symbolic 수행의 장점을 하나로 합친 것이다. Concolic testing은 크게 두 부분으로 나뉜다. 먼저 Concrete 값을 이용해서 프로그램을 수행하는 도중에 분기 혹은 반복문을 지나면서 얻어지는 Symbolic 조건문을 저장해두어야 한다. 기존 Concrete 값으로는 더 이상 프로그램 수행이 불가능 할 때 모아두었던 Symbolic 조건을 풀어서 새로운 Concrete 값을 생성하고, 지나오지 않았던 새로운 방향으로 프로그램을 실행해 갈 수 있게 된다.

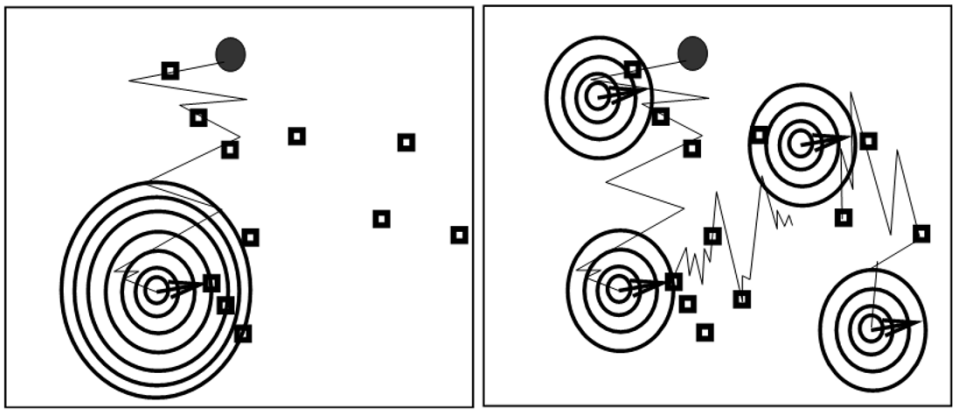
(2) Hybrid concolic 테스팅

일반적인 Concolic testing 기법은 Symbolic 조건을 풀어낼 수 없는 경우 종료하게 된다. 그런데 적지 않은 경우에 그러한 복잡한 Symbolic 조건이 프로그램 상에 많이 포함되어 있는데, 그럴 경우 프로그램 전반에 대한 테스트가 실질적으로 불가능하다고

28) Kaminski, Garrett, and Paul Ammann. "Reducing logic test set size while preserving fault detection." Software Testing, Verification and Reliability 21.3 (2011): 155-193.

볼 수 있다. 이러한 문제점을 해결하기 위하여 제안된 것이 바로 Random testing 그리고 Concolic testing을 합쳐낸 하이브리드 기법이다.[29)]

[그림 2-8] (a) 기존 Concolic testing (b) 하이브리드 Concolic testing



그림에서 검은색으로 가득 찬 원은 테스트 시작점을 의미하며, 작은 정사각형들은 각각 프로그램에서의 분기/반복문을 의미한다. 방사형 원이 퍼져나가는 것이 Concolic testing을 이용하여 주변을 탐색해 나가는 과정을 의미하며, 이때 더 많은 정사각형을 건드릴수록 더 많은 프로그램의 부분들을 테스트했다고 볼 수 있다. 시작점에서 방사형 원의 중심까지 가는 부분은 Random run이라 불리는데, 임의의 값을 찾아가는 과정이다. 그림의 (a) 부분에서 볼 수 있듯이 기존의 Concolic testing은 방사형 원이 한번만 퍼져가다 끝나는 반면, 그림의 (b) 부분의 하이브리드 기법에서는 매번 더 이상 주변 탐색이 불가능한 경우 새로운 탐색 출발점을 찾아 Random run을 수행하게 된다. 따라서 상대적으로 더 많은 정사각형을 건드릴 수 있고, 결국 프로그램의 더 많은 부분을 효과적으로 테스트하게 된다.

2. 소프트웨어 안전성 분석 기술

1) 소프트웨어 안전성 분석 개요

본 절은 이장수 외 논문[30)]의 내용을 기반으로 안전성 분석 기술에 대해 설명한다.

29) Majumdar, Rupak, and Koushik Sen. "Hybrid concolic testing." Software Engineering, 2007. ICSE 2007. 29th International Conference on. IEEE, 2007.
30) 이장수, 이동아, “소프트웨어 기반의 안전 필수 시스템을 위한 안전성 분석 기법.” 정보과학회지 33권 7호, pp.41-46, 2015.

안전성 분석(safety analysis)[31]은 시스템이 만족해야 할 안전성을 만족하는지 확인하는 활동으로서, 안전 필수 시스템 개발 시 반드시 수행하는 활동 중에 하나이다. 시스템의 안전성을 분석하기 위한 다양한 기법들이 존재하며, 시스템의 성격과 개발 단계에 따라 분석 기법들을 선택적으로 적용해야 한다. 대표적으로 FTA (Fault tree analysis), FMEA (Failure modes and effects analysis), HAZOP (Hazard and operability analysis)과 같은 분석 기법들이 개발되어 널리 사용되고 있다. 이러한 기법이 개발해 사용한 초기에는 하드웨어 위주의 시스템이 대부분이었다. 하지만 안전 필수 시스템에 소프트웨어가 도입되고 그 비중이 점점 커짐에 따라서 시스템의 성격도 달라졌으며, 이와 함께 시스템의 안전성을 분석하는 안전성 분석 기법도 발달해 왔다.

소프트웨어는 하드웨어와 달리 논리적인 계산으로 기능을 구현하기 때문에, 마모에 의해서 소프트웨어 기능이 바뀌거나 소멸되지 않는다. 또한 소프트웨어는 적은 비용으로 복제가 가능하기 때문에 하드웨어에 비해 재사용하기 쉽고, 기능의 구조가 코드 안에 숨어있기 때문에 소프트웨어 자체만으로 그 기능을 파악하기 어렵다. 이러한 소프트웨어만의 특징으로 인해 하드웨어에 적용했던 기존 안전성 분석 기법은 소프트웨어에 적용 가능하도록 개선되거나 새로 개발되었다.

본 절에서는 안전 필수 시스템 개발에 사용되는 여러 안전성 분석 기법에 대하여 소개한다. 다양한 안전 필수 분야에서 발행한 표준에서 언급하는 안전성 분석에 대하여 소개하고 표준의 요건을 만족시킬 수 있는 분석 기법에 대하여 자세히 소개한다. 특히, 기존의 하드웨어 기반 시스템에서 사용하였던 분석 기법을 비롯한, 소프트웨어 기반의 시스템을 대상으로 안전성 분석을 수행할 수 있는 기법에 대하여 다룬다.

2) 소프트웨어 안전성 분석 기법의 특징

안전성 분석 기법은 분석 목적, 분석 절차, 분석 시기와 같은 다양한 특징을 가진다. 안전성 분석의 목적은 크게 세 가지(위험 식별, 위험 영향 분석, 위험 원인 분석)가 있고, 분석 기법에 따라 한 가지 이상의 목적을 달성할 수 있기 때문에 목적에 따라 기법 선택이 달라진다. 또한 분석의 절차와 방향과 같은 분석 수행의 특징도 기법마다 서로 다르며, 시스템 개발 단계의 특정 시점에 적용할 수 있도록 개발된 기법도 존재한다[32].

---

31) 위험성 분석(Hazard analysis)도 시스템의 안전성을 확보하기 위한 분석 활동이다. 본 보고에서는 위험성 분석과 안전성 분석을 통칭하여 안전성 분석이라 한다.

32) Clifton A. Ericson, II, “Hazard Analysis Techniques for System Safety”, Wiley, 2005.

대표적인 안전성 분석 기법의 특징은 위험과 위험의 원인을 도출하는 방법에 있다. 이 중 귀납적인 안전성 분석 방식은 주어진 데이터를 활용해 결론을 도출하는 방식으로, 위험 식별 활동에 사용된다. 예를 들어 열차의 선로 구조에 대한 정보를 분석해, 선로의 구조가 틀어지면 열차 탈선과 같은 위험을 밝혀낼 수 있다. 이와 대조적인 연역적 분석 방법은 전제로부터 결론을 도출해내는 추론 방식을 말한다. 연역적인 안전성 분석 방식은 결론을 뒷받침하는 명확한 증거를 제시하는 방식으로, 위험의 원인을 분석하는 활동에 적합하다. 예를 들어 열차 탈선의 원인을 밝혀내고, 해당 원인이 열차 탈선을 일으킬 수 있음을 증명하는 방식이다.

귀납적・연역적 분석 방식과 유사한 상향식(Bottom-up)・하향식(Top-down) 기법은 안전성 분석을 수행할 때 시스템을 바라보는 관점에 따라 나뉜다. 상향식 분석은 시스템의 낮은 관점으로부터 높은 관점으로 분석하고, 하향식은 상향식과 반대의 방향으로 분석을 수행한다. 예를 들면 자동차의 안전성을 분석하고자 할 때, 상향식은 센서나 모터(하위)에서 발생하는 원인으로 인한 자동차(상위)에서 발생하는 결과를 분석하는 반면, 하향식은 자동차의 특정 상황(상위)의 원인을 센서나 모터와 같은 요소들(하위)에서 찾아내는 방식이다. 귀납적・연역적 방식과 상・하향식 방식은 완전히 일치하는 개념은 아니지만, 일반적으로 귀납적 분석은 하향식으로 진행되고 연역적 분석은 상향식으로 진행된다.

안전성 분석의 결과는 정성적(qualitative) 결과와 정량적(quantitative) 결과로 나눌 수 있다. 정성적 결과는 수치화 되지 않지만 일반적으로 정량적 결과보다 도출하기 쉽고 비용이 적게 든다. 정량적 결과는 수치화된 결과를 보여준다. 정성적 결과에 비해 정교하고 객관적이지만 결과 도출이 어렵고 복잡하다.

안전성 분석 기법은 위 특징뿐만 아니라 분석 시기(개발 초기, 설계 단계, 구현 단계 등), 분석가의 전문성 요구 정도와 같은 특징에 따라 사용 시기, 적용 대상, 분석 범위 등이 결정된다는 특징도 있다.

3) 소프트웨어 안전성 분석 기법

(1) Preliminary hazard analysis (PHA) & Software Safety Assessment (SWSA)

PHA는 위험 식별과 원인, 영향 등을 밝혀낼 수 있는 안전성 분석 기법으로 널리 사용된다. 밝혀낸 위험과 원인 등을 제거하기 위한 목적으로 분석을 수행하며, 분석의 결과는 정성적으로 표현되는 기법이다. PHA는 일반적으로 시스템의 초기 개발 단계에

수행되며, 시스템의 초기 설계 정보를 바탕으로 분석을 수행한다.

PHA 수행은 일반적으로 워크시트(Worksheet)를 이용해 수행한다. 워크시트를 이용한 안전성 분석은 체계적으로 수행이 가능하고, 다른 기법들에 비해 빠르고 쉽게 수행이 가능한 장점이 있다. 또한 분석 전문가뿐만 아니라 개발자도 이해하기 쉽다.

PHA는 시스템 레벨에서 수행되는 분석 방법이기 때문에 소프트웨어를 포함하여 분석이 가능하다. 하지만 소프트웨어 자체만을 대상으로 수행하기에는 적합하지 않다. 소프트웨어의 안전성 분석을 위한 기법 중 PHA와 유사한 기법으로는 SWSA가 있다. SWSA는 소프트웨어 개발의 초기 단계에서 수행하는 기법으로, PHA와 마찬가지로 워크시트 작성을 통해 분석을 수행한다.

(2) Fault tree analysis (FTA)

FTA는 다양한 산업 분야에서 널리 사용되는 안전성 분석 기법으로서, 대표적인 연역적 분석 방법 중 하나이다. 분석하고자 하는 결과(위험 또는 고장)를 최상위에 놓고 그 원인을 하위로 연결해 가면서 분석을 수행 한다. 둘 이상의 원인이 존재할 경우, 원인과 결과를 AND나 OR와 같은 논리 게이트로 연결하여 결과 발생 조건을 생성한다. 분석을 통해 밝혀낸 원인이 더 이상 분석이 불가능한 원인이 될 때까지 분석을 수행하게 된다.

FTA는 전형적인 연역적 분석 방법이면서 하향식으로 시스템의 위험을 분석한다. 분석하는 대상인 최상위의 결과는 대상 시스템의 상위 개념에서 나타날 수 있는 위험 상황이나 고장을 의미하고, 원인은 시스템을 구성하는 요소들의 결함을 의미한다. 분석 결과는 수학적 표현 방식인 고장 확률과 같은 정량적 결과일수도 있고, 자연어로 원인을 표현한 정성적 결과일 수도 있다. 시스템 개발 단계에 구애 없이 다양한 시점에 사용 가능하며, 분석의 범위도 수행 시 결정이 가능하다. 단 분석의 범위가 너무 넓을 경우 분석 수행이 불가능할 정도로 규모가 커질 수 있고, 분석가의 시스템에 대한 높은 이해도를 바탕으로 분석을 수행하게 된다.

SFTA (Software FTA)는 일반적인 FTA와는 많은 차이를 가진다. 소프트웨어의 결과(출력)에 대한 역방향 분석(Backward analysis)을 통해서 특정 출력을 생성할 수 있는 입력 조합을 찾는 분석을 수행한다. 소프트웨어 개발 초기단계에는 적용할 수 없으며, 상세 설계 이상의 개발 단계 이후에 적용이 가능하다. 소프트웨어에 반복문이 존재할 경우 분석이 무한히 진행될 수 있으며, 원인은 확률이 아닌 명확한 입력 조합으로 표

현된다.

(3) Failure mode and effects analysis (FMEA)

FMEA는 서브시스템이나 컴포넌트의 잠재적인 고장 유형이 시스템에 미치는 영향을 분석하는 기법이다. 시스템의 특정 부분이 일으키는 고장 유형(Failure mode)이 전체 시스템의 신뢰도나 안전성에 영향을 미칠 수 있는지 확인하는 방법으로서, 원인으로부터 결과를 도출하는 귀납적 추론 방법을 이용한 분석을 수행한다. FMEA는 PHA와 유사하게 워크시트 작성을 통해 이루어지지만, PHA 적용 시기보다 늦은 설계가 완성된 단계에서 수행할 수 있는 기법이다.

Software FMEA (SFMEA)는 FMEA를 소프트웨어에 적용 가능하도록 보완된 안전성 분석 기법이다. FMEA의 고장 유형은 소프트웨어의 데이터나 이벤트로 대체되어 SFMEA를 수행한다. 특정 데이터 유형이나 이벤트가 소프트웨어에 미칠 수 있는 영향을 분석하는 기법이다.

(4) Hazard and operability analysis (HAZOP)

HAZOP은 위험을 찾아내고 분석할 수 있는 기법으로, 안전성 분석에 널리 사용되는 기법 중 하나이다. 이 분석 기법은 시스템의 기능이나 요건과 같은 매개변수(Parameter)와 HAZOP에서 제공하는 가이드 워드(Guide words)를 조합하여 예상치 못한 시스템의 행위를 도출하고, 도출된 행위가 시스템의 안전에 어떤 영향을 줄 수 있는지 분석한다. FMEA와 마찬가지로 귀납적 추론 방식에 기반하며 워크시트 작성을 통해 분석을 수행하지만, 위험 식별에 보다 유용하게 사용된다.

HAZOP은 소프트웨어에 대한 분석도 포함하여 수행 가능하다. 소프트웨어에 대한 HAZOP을 수행할 경우에는 소프트웨어의 명령(Instruction)과 가이드 워드를 조합하여 소프트웨어의 예상치 못한 동작을 도출할 수 있다. 소프트웨어 특징을 반영한 타이밍 가이드워드가 추가될 수 있다.

(5) System theoretic process analysis (STPA)

STPA는 STAMP (System theoretic accident modeling and process)을 기반으로 하는 모델의 안전성 분석을 위해 개발된 기법이다[33]. STAMP는 시스템의 사고와 위험이 시

스템의 특정 부분의 고장이나 실패로부터 발생하는 것이 아니라, 시스템 요소간의 상호작용의 부적절한 행위에 의해 발생한다고 전제한다. 즉, 시스템의 각 요소가 이상 없이 동작한다 하더라도 요소간의 상호작용이 시스템의 안전성을 위협할 수 있다. STAMP의 시스템 요소는 하드웨어와 소프트웨어를 비롯한 사람이나 조직까지 포함하는 포괄적인 개념으로 사용된다.

STPA를 수행하기 위해서는 시스템의 사고와 위험이 정의되어 있어야 하고, 시스템을 STAMP를 기반으로 하는 Control Structure로 모델링 할 수 있어야 한다. Control Structure는 시스템을 개념적인 요소들과 요소간의 상호작용(Control, Feedback)으로 표현한다. STPA는 Control Structure에 나타난 컨트롤을 4 가지 위험한 상황으로 분석한다. 4 가지 위험 상황은 컨트롤의 부재, 부적절한 컨트롤, 컨트롤 타이밍과 컨트롤의 지속시간을 의미하며, 4 가지로 분석된 컨트롤을 Unsafe control action (UCA)이라고 한다.

33) Nancy G. Leveson, “Engineering a Safer World: Systems Thinking Applied to Safety”, MIT Press, 2011.

제3장 해외 주요국의 SW안전성 확보 체계

이 장에서는 해외 주요국의 소프트웨어 안전성 확보를 위한 표준, 시험 및 평가, 인증 조직에 대해 살펴보겠다. 소프트웨어 안전 표준 및 표준의 적용 방법이 나라별, 도메인별로 다르게 지정되어 있어 표준, 시험 및 평가, 인증조직을 도메인별로 기술하였다. 특정 도메인에서는 소프트웨어 안전을 위한 표준 및 기술이 성숙되어 있는 반면, 다른 도메인에서는 아직 소프트웨어 안전에 대한 개념조차 제대로 정립되지 않는 경우도 있다. 소프트웨어 안전 체계를 구현함에 있어 성숙된 도메인에서 정의된 체계를 전 도메인에 도입하여, 소프트웨어 안전을 높이는 노력이 필요하리라고 본다.

제1절 표준

소프트웨어 안전 표준은 나라별, 도메인별로 표준이 다르게 지정되어 있으며, 적용 방식도 다르다. 소프트웨어 안전을 보장하기 위한 표준은 IEC 61508[34]을 근간으로 소프트웨어 안전이 필요한 각 산업 군별로 산업 특성을 고려한 소프트웨어 안전 표준을 제정한 경우와 특정 도메인 자체적으로 안전 표준을 제정한 경우가 있다.

소프트웨어 안전에 대한 적용 방식도 국가에서 법률로 정하여 강제하는 방식과 강제적이 아닌 자율적으로 소프트웨어 안전을 지키도록 하나 사고 후 강력한 처벌 규정으로 안전성을 강화하는 경우가 있다.

자동차, 철도, 원자력, 기계 산업의 경우 IEC 61508을 기초로 각 도메인에 맞는 표준을 작성하였다. 항공 산업의 경우 DO-178을 만들어 항공 산업의 기준으로 활용하고 있으며 유럽과 미국 표준으로 사용하고 있다. 의료기기 소프트웨어는 IEC 62304 표준을 적용하고 있다.

- IEC 61508 : 7개의 파트로 구성(SW 요구사항은 파트 3)되어 있으며, 소프트웨어 개발의 전체 안전성 생명주기를 포함. 소프트웨어 안전성 요구사항 수집, 설계 및 개발, 테스트, 통합, 안전성 확인, 수정 검증, 평가의 과정을 포함

34) IEC 61508(전기/전자/프로그램 가능한 전자 안전 관리 시스템의 기능 안전)은 산업에 적용되는 규칙의 국제표준이다.

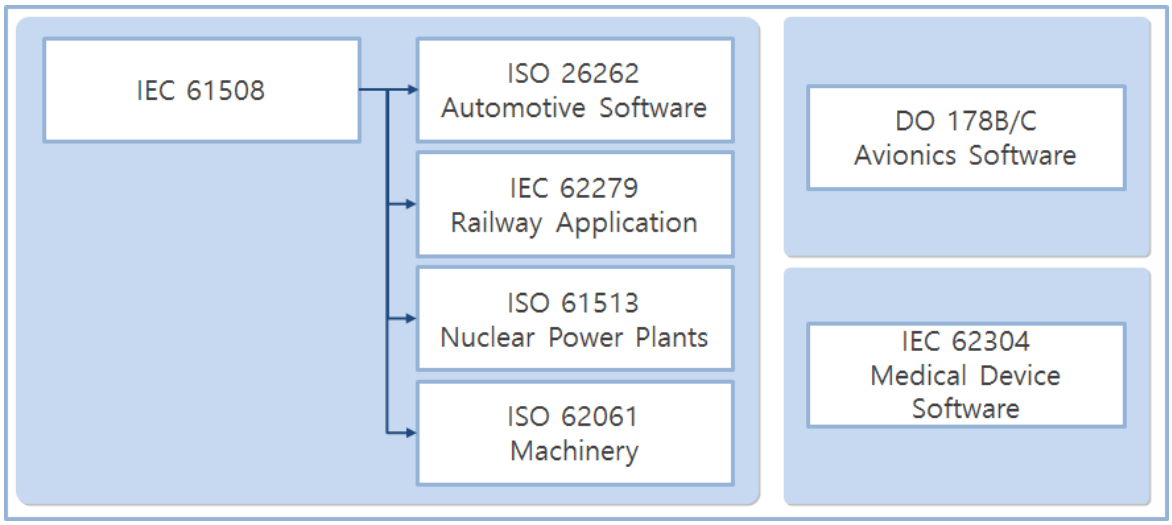
- 자동차 (ISO 26262) : 자동차 전기/전자 시스템 안전(Functional Safety)에 대한 소프트웨어 표준

- 철도 (IEC 62279 / EN 50128) : 커뮤니케이션, 시그널링 및 처리시스템에 대한 철도 제어 및 보호를 위한 소프트웨어 개발 포함, 관련 하드웨어 표준과 연관

- 원자력 (ISO 61513) : 원자력발전소의 안전에 중요한 시스템의 장치와 제어에 대한 요구사항 및 권고사항을 제공

- 항공 (DO-178B/C) : RTCA와 EUROCAE에 의해 개발된 항공기 시스템에서 사용되는 안전 필수 소프트웨어의 안전성을 취급하는 개발 가이드로, 미국 연방 항공국(FAA)이 항공기 소프트웨어 인증을 위한 용도로 사용할 것을 인정하여 항공기 소프트웨어 표준으로 인정

[그림 3-1] 소프트웨어 안전관련 국제표준 관계도



자료 : SPRi (2015)에서 인용

나라별로 적용하는 표준이나 적용 방식이 달라 도메인별(자동차, 항공, 철도), 주요 국가별(미국, 유럽) 표준에 대해 기술하였다.

1. 자동차 부문

IEC 61508에서 파생된 자동차 소프트웨어 안전 표준인 ISO 26262가 있으며, 미국, 유럽 전역과 일본은 각 다라의 형편에 맞게 다른 형태로 적용하고 있다.

1) 소프트웨어 안전 관련 주요 표준

(1) ISO 26262 (자동차 기능안전성 국제 표준)

ISO 26262는 3.5톤 이하의 차량에 적용되는 기능 안전성(Functional Safety) 표준이며 (소프트웨어 부분은 Part 6), 기능 안전 표준인 IEC 61508에서 자동차 부문 전기, 전자 시스템의 오류로 인한 사고방지를 위해 자동차 및 자동차 부품에 맞게 작성되었다. 초판은 2011년 11월에 발표되었고, 2018년 1월 2차 버전이 나올 예정이다. 2차 버전은 모터사이클과 3.5톤 이상의 차량이 포함되고, 전기차와 차량 보안에 대한 내용이 많이 언급되고 있다.

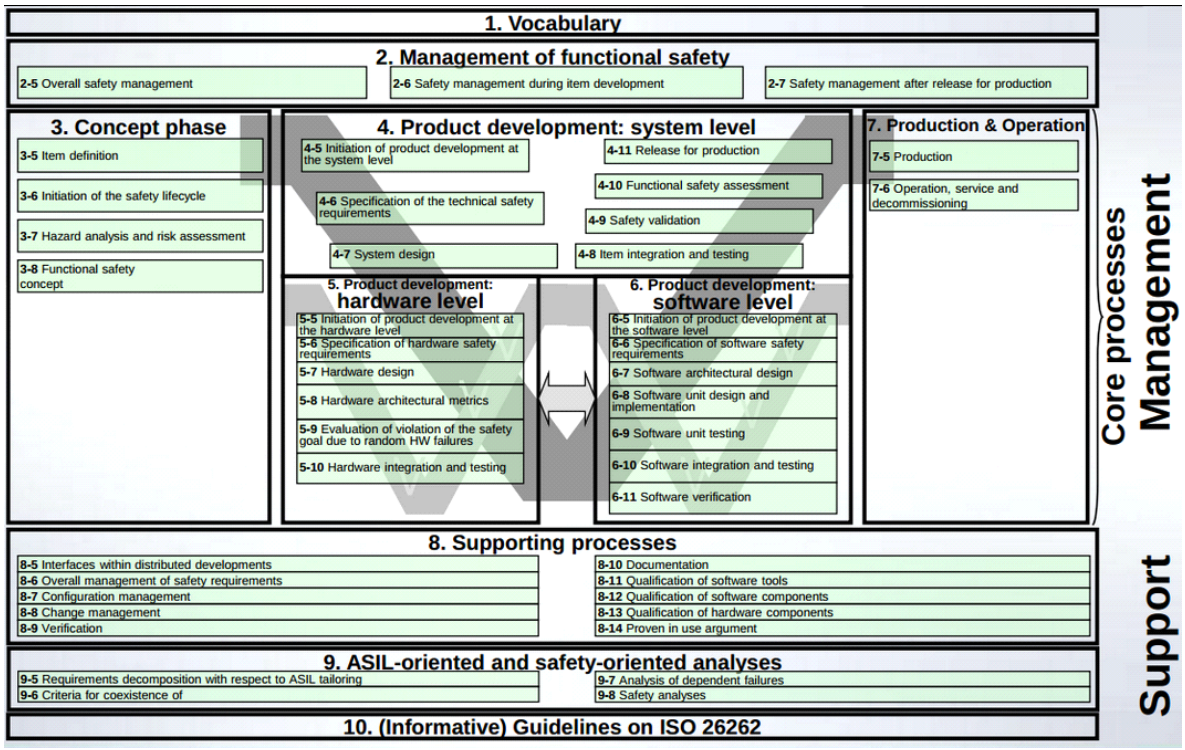
ISO 26262는 자동차에 탑재되는 전기/전자 시스템의 오류로 인한 사고방지를 위해 ISO에서 제정한 자동차 기능 안전 표준으로서, 위험을 초래하는 운전 상황의 위험을 수치화하고 소프트웨어적 또는 하드웨어적인 문제를 감지/제어하거나 이들의 영향을 최소화하기 위한 안전 조치에 대하여 정의한 것이며, 충분 또는 수용가능한 수준의 안전을 달성하기 위하여 위해도 분석(Hazard Analysis) 및 리스크 평가(Risk Assessment)를 통해서 ASIL(Automotive Safety Integrity Levels)을 각 기능에 대해 정의한다.

ISO 26262는 차량 개발 프로세스 기획, 설계, 구현, 통합, 검증, 인증, 생산 전 단계에서 전기/전자 시스템의 오작동에 의해 발생할 수 있는 위험 인자를 식별하고 관리하여 차량 안전성 즉 기능 안전을 확보하는데 그 목적을 두고 있다. 시스템 개발 시 요구되는 안전 관련 활동으로는, 아이템 정의(Item Definition), 위해도 분석(Hazard Analysis) 및 리스크평가(Risk Assessment), 기능 안전 개념(Functional Safety Concept), 기술 안전 개념(Technical Safety Concept), 시스템/하드웨어/소프트웨어 개발(System / Hardware / Software Development), 안전 분석(Safety Analysis)이 있다. [35]

ISO 26262는 기본적으로 ISO 61508과 동일한 'V' 모델을 따르고 있지만 HW와 SW 구성 요소를 모두 고려한 시스템 수준에서 독립적인 제품 개발 단계를 통해 시스템을 설계한 후 HW와 SW 개발이 독립적으로 병행 될 수 있는 구조로 구성되어있다.

35) 위키백과, ISO 26262, https://en.wikipedia.org/wiki/ISO_26262 (2015.12 최종 수정), 국내 소프트웨어 안전 산업동향 조사에서 재인용, 2015.08

[그림 3-2] ISO 26262 Structure



자료: Dr. Qi Van Eikema Hommes (2012); SPRi (2015)에서 재인용, 2015.08

ISO 26262는 총 10개의 파트로 구성되어 있으며, 개발 초기부터 생산, 폐기에 이르는 전체 생명주기에서의 안전 관련 요구사항을 제시한다. ISO 26262 구성 파트별 세부 사항은 다음과 같다.

〈표 3-1〉 ISO 26262 구성 파트별 세부 사항

파트	구성	세부설명
1	용어	관련 용어 정리
2	기능 안전성 관리	기능 안전성에 관련된 개발 활동을 계획, 조정, 추적하는 요건을 정의하며 안전 문화와 같은 조직 차원에서 갖추어야 할 것 에서부터 품목 개발, 생산 이후에 걸친 전반적인 안전성 관리 요구사항을 정의함
3	구상 관리	개발 품목 정의를 기반으로 해저드 분석 및 위험 심사를 통해 자동차 안전 무결성 레벨을 판정 하며, 안전 목표와 안전 메커니즘을 정의함
4	제품 개발 : 시스템 레벨	시스템 수준에서의 개발은 기본적으로 V모델을 따르며 기술적 요구사항과 시스템 디자인, 그리고 테스트 프로세스가 통합의 왼쪽부분에 오고, 검증, 확인과 심사가 오른쪽 부분에 위치함. 전기전자 시스템외의 타 기술로 구현된 안전메커니즘을 확인(Validation), 외부 수단으로 구현된 안전 개념의 효과 확인, 사람의 통제성 및 작동작업에 대한 전제 등을 검증하는 것을 포함 함
5	제품 개발: HW 레벨	시스템 설계명세를 기반으로 하여 아이템의 하드웨어 개발이 이루어지는데, V모델의 개념에 따른 하드웨어의 개발, 통합, 검증 등에 대한 요구사항을 정의함
6	제품 개발: SW 레벨	SW 수준의 개발에 대해 V모델의 개념에 따라 개발, 통합, 검증 등에 대한 요구사항을 정의함
7	생산 및 운용	품목 생산을 위한 계획, 샘플 생산, 양산, 서비스 등에 관한 요구사항을 정의함
8	지원 프로세스	안전 요구사항 관리, 명세 방법, 형상/변경 관리, 검증, 문서화, 지원 도구 자격 검증, 재사용 SW 자격 검증, HW 자격검증, 실제 사용을 통해 입증된 안전성 등에 대한 요구사항 정의함
9	자동차 안전 무결성 레벨 및 안전 중심의 분석	안전 요구사항 자동차 안전 무결성 레벨을 분해하는 방법, 안전 관련 구성요소 사이 공존의 조건인 상호 간섭 정도, 위험 분석 방법 등을 기술함
10	가이드라인	주요 개념, 안전케이스, 자동차 안전 무결성 레벨 분해 등 ISO 26262 이해에 도움이 되는 정보 기술

자료 : 권기현 (2012)에서 인용

(2) AUTOSAR (AUTomotive Open System Architecture,자동차 전장 SW 플랫폼 규격)

개방형 자동차 표준 소프트웨어 구조(architecture)로서, 자동차 전기전자 시스템 구조(E/E architecture)의 표준화를 위해 제조사(OEM), 개발사(Tier 1), 툴 개발사들에 의해 개발되었다. ISO 26262에 비해 HW와 SW의 명확한 분리를 통하여, SW의 재사용성, 확장성 등을 향상시켜, 복잡한 SW를 빠르고 신뢰성 있게 개발하는데 실질적인 도움을 주는 표준이라고 할 수 있다.

중요한 시스템 함수(또는 기능) 표준화, 응용 소프트웨어 인터페이스 영역 간 경계 표준화, 가용성/보안/소프트웨어 갱신을 위한 미래 차량 요구조건을 만족 등이 목표이다. AUTOSAR 프로젝트에서 전기전자 시스템 구조를 디자인 모델로부터 만드는 데 사용할 수 있는 방법론을 개발하였다. 이 접근 방식은 4단계(입력 서술, 시스템 설정, ECU 설정, 실행 가능한 소프트웨어 생성)로 이루어져 있다.[36)]

(3) MISRA-C

ISO 26262 전에는 안전 관련 자동차 시스템을 위한 소프트웨어의 개발은 주로 자동차 산업 소프트웨어 신뢰성 협회(MISRA)의 가이드라인이 적용되었다. MISRA C는 MISRA(Motor Industry Software Reliability Association)에서 개발한 자동차 산업에 사용되는 임베디드 소프트웨어의 코드 안전성, 호환성, 신뢰성 향상을 위한 C 프로그래밍 언어에 대한 개발 가이드라인이다.(C++의 경우 MISRA C++가 있다) MISRA-C를 만족하기 위한 수많은 소프트웨어 툴이 존재하지만 어떠한 도구도 MISRA-C를 100% 만족할 수는 없다. 그 이유는, MISRA-C의 규정에서는 반드시 사람이 해야만 하는 내용이 포함되어 있기 때문이다.[37)]

MISRA C는 자동차 산업을 위해 개발되었지만, 우주/항공, 의료장비, 국방, 철도 등의 다양한 산업에서 활용되고 있다. MISRA C:2012의 경우 총 143개 규칙과 16개의 지침으로 구성되어 있다. ISO 26262와 MISRA C의 차이점은, MISRA C가 코딩 표준인데 반하여 ISO 26262는 차량용 전기/전자 시스템의 오류에 대해 회피 또는 제어하기 위한 방법과 조치를 정의한 것이다.[38)]

---

36) 위키백과, AUTOSAR, https://ko.wikipedia.org/wiki/AUTOSAR, 2015.9 최종 수정
37) 위키백과, https://ko.wikipedia.org/wiki/Misra_c, 2015.08 최종 수정
38) 위키백과, Misra C, (2015). https://ko.wikipedia.org/wiki/Misra_c (2015-8 방문), 국내 소프트웨어 안전 산업동향 조사에서 재인용, 2015.08 최종 수정

2) 주요 국가별 표준

미국과 유럽은 제조물 책임법이라는 간접조항에 따라 안전 표준 준수를 강제하지 않는다는 공통점이 있고 자동차 판매 승인 방식에서 사후 관리와 형식승인이라는 차이점이 있다. 미국의 경우 제조사 자체 인증에 의해 인증이 가능하나, 유럽의 경우는 법규에 의한 국가형식승인이 필요하다. 일본은 ISO 26262를 사정에 맞게 적용하였다.

(1) 미국

자동차 산업에서 소프트웨어 안전에 대한 표준은 명확히 정의되어 있지 않고, FMVSS(Federal Motor Vehicle Safety Standards) 라는 표준으로 자동차, 자동차 안전관련 부품 및 시스템에 대한 설계, 제작, 성능 및 내구성 요구사항에 대해 정의하고 있다. FMVSS는 미국 교통국(Department of Transportation, 도로교통안전청) 산하 NHTSA(National Highway Traffic Safety Administration)가 지정, 관리한다. 충돌회피, 내충격성, 충돌 후 생존가능성, 기타 규정의 네 개 의 항목으로 나누어져 각 항목에 관련된 세부적인 규격을 또한 포함하고 있다. 브레이크 시스템, 제어 시스템 관련, 연료시스템, 오토바이 헬멧, 안전벨트 부품, 운전자 충돌보호, 브레이크 호스, 램프, 반사장치 관련 장비, Air 브레이크 시스템 등과 관련된 품목을 다룬다. 참고로 캐나다는 Canada Motor Vehicle Safety Standards (CMVSS)라는 FMVSS를 일부 차용한 표준을 가지고 있다. [39]

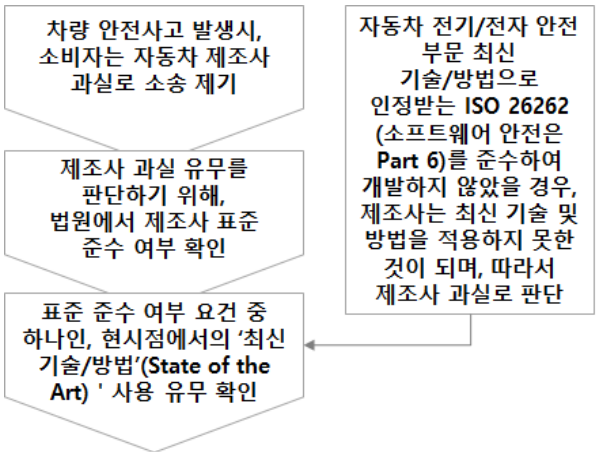
미국의 안전 표준 준수는 명확한 법률에 근거한 강제적인 준수보다는 자체 승인 후 사후 관리와 제조물 책임법에 따른 자동차 제조사들의 자발적인 준수가 핵심이다. 즉, 미국에서 제조사의 자발적 준수를 유도하는 방법은 미국 내에서 판매되는 자동차 안전 준수 관련 법/제도 부분에 따른 미국 연방 도로교통안전청 (NHTSA)에서 수행하는 자국 내 판매 자동차의 안전 표준 준수 여부 확인 활동이 있고, 제조물 책임법 (Products Liability Law)에 따라, 자동차 제조사가 사고 발생 시 예상되는 소송에 대비하여 자동차 소프트웨어를 포함한 자동차의 설계, 테스트, 제조를 ISO26262 안전 표준에 따라 수행하게 하는 방법이 있다.[40]

제조물 책임법은 자동차 제조사로 하여금 자동차 및 자동차 부품에 대한 안전 표준

39) 위키백과, Federal Motor Vehicle Safety Standards,
https://en.wikipedia.org/wiki/Federal_Motor_Vehicle_Safety_Standards, 2016.1 최종 수정
http://www.nhtsa.gov/cars/rules/import/FMVSS/
40) 국내 소프트웨어 안전 산업동향 조사, 2015.08 인용

을 따르게 하는 간접적 조항이다. 제조물책임법은 제조되어 시장에 유통된 상품(제조물)의 결함으로 인하여 그 상품의 이용자 또는 제3자(=소비자)의 생명, 신체나 재산에 손해가 발생한 경우에 제조자 등 제조물의 생산, 판매과정에 관여한 자의 과실 유무에 관계없이(=무과실) 제조자 등이 그러한 손해에 대하여 책임을 지도록 하는 법을 말한다.[41] 자동차 사고 발생시, 소비자는 자동차 제조사에 대하여 제조물책임법에 근거하여 소송을 제기할 수 있다. 이 경우, 자동차 안전에 대한 문제는 제조사의 과실로 인정되는데, 연방 규정에서 규정된 표준의 준수 여부가 안전에 대한 제조사의 책임 준수 여부로 검토된다. 즉, 연방 규정에서 규정된 표준대로 제품을 제작하지 않았을 경우, 설계를 적정하게 하지 못한 것이며(설계 결함), 제조사의 과실로 판단된다. 설계 결함에 대한 최신 기술이라는 용어는 자동차 제작 시에 자동차의 설계 결함이 있었는지를 판단하는 주요 기준 중의 하나로서 법정에서 자주 사용되고 있다. 즉, 자동차 제작 시에 최신 기술 및 방법을 사용하지 않았을 경우, 제조사가 자동차 제조 시 상당한 노력을 하지 않았다는 증거가 되며, 따라서 제조사의 과실이 있다는 의미이다. 즉, 현재 시점의 최신 기술인 글로벌 설계 표준인 ISO 26262를 준수하여 개발해야 한다는 사항이 제조사에 자연적 의무사항이 된다.[42]

[그림 3-3] 제조물 책임법과 소프트웨어 안전표준 적용



자료 : SPRi (2015)에서 인용

41) 위키피디아, 제조물책임법, https://ko.wikipedia.org/wiki/%EC%A0%9C%EC%A1%B0%EB%AC%BC%EC%B1%85%EC%9E%84%EB%B2%95, 2015.12 최종수정

42) Canis, Bill. and Richard K. Lattanzio, (2014). "U.S. and EU Motor Vehicle Standards: Issues for Transatlantic Trade Negotiations". pp.8., "Federal Motor Vehicle Safety Standards", 『Wikipedia』, https://en.wikipedia.org/wiki/Federal_Motor_Vehicle_Safety_Standards (2016.1 최종 수정), 국내 소프트웨어 안전 산업동향 조사에서 재인용, 2015.08

(2) 유럽

유럽의 경우도 미국과 유사하게 소프트웨어 안전에 대한 표준 준수 의무는 명확하게 법률로 명시되어 있지 않지만, 자동차 / 자동차 시스템 / 자동차 부품 수준에서 안전을 준수해야 한다는 안전 요구 사항은 지정하고 있다.

소프트웨어 안전 표준 준수는 명확한 법률에 근거한 강제적인 준수보다는 자동차 및 자동차 부품 승인 및 제조물 책임법 법률 적용에 따른 자동차 제조사들의 자발적인 준수가 핵심이다. 유럽의 경우도 미국의 경우와 비슷하게 안전관련 법/제도 준수를 유도하는 활동도 크게 2가지로 볼 수 있는데, 첫째가 자동차 및 부품의 대한 형식승인이고 두 번째가 제조물 책임법에 의한 것이라 볼 수 있다. 유럽 내에서 판매되는 자동차는 판매 전 안전 준수 관련 형식승인(Type Approval)을 통해 철저한 검사를 시행하여 EEC 법규 또는 UNECE (UN Economic Commission for Europe, 국제연합 유럽경제위원회) 법규(58 협정)[43]에 따른 인가를 받은 후 다시 각국 법규의 인증을 받은 다음, 판매가 가능하다. 제조물 책임법은 미국의 적용 방법과 유사하다.[44]

58협정의 경우는 독일의 주도하에 통일기술기준의 제정 및 국가 간 승인의 상호인정을 위해 채택된 협정으로 미국을 제외한 42개국이 참여하고 있다. 미국이 참여하지 않은 이유는 미국은 정부차원의 인증시스템이 없어 승인의 상호인정 의무를 이행할 수 없다고 판단하여 반대하였다. 제조물 책임법의 경우 제조사가 최신 기술 및 방법을 사용하여 자동차를 설계하고 제조해야 제조자 과실을 면책할 수 있어, 국제 표준인 ISO 26262를 준수하는 이유가 된다.

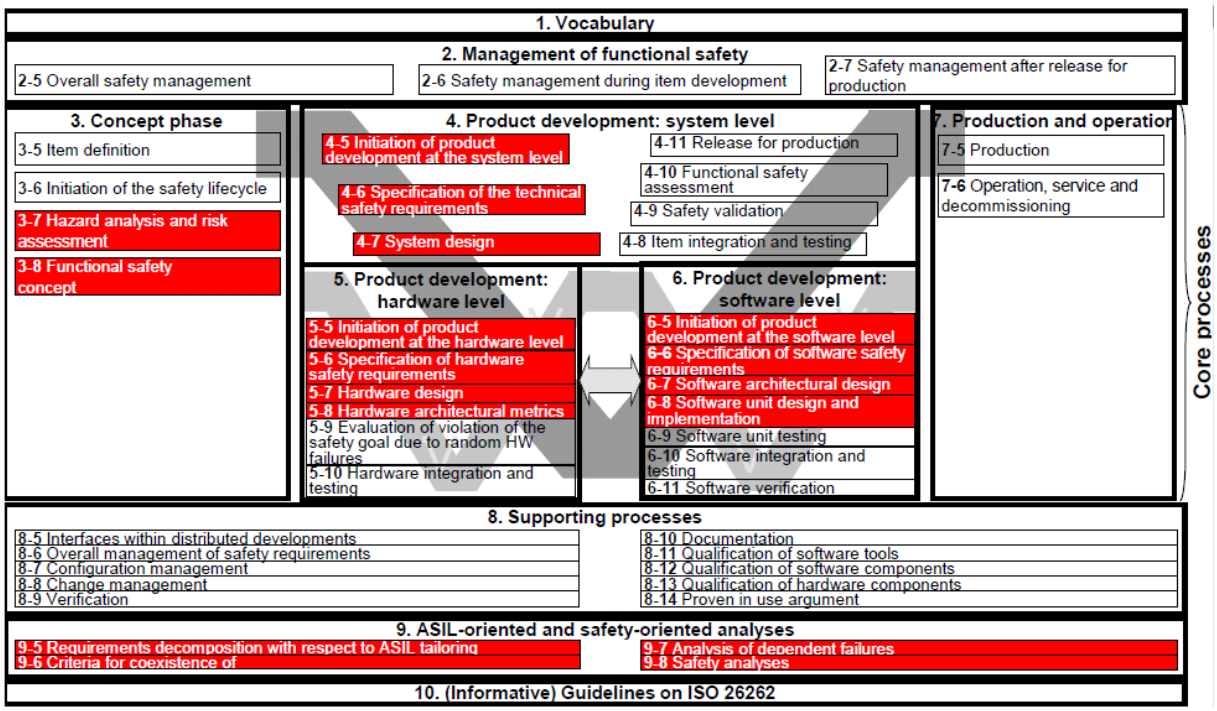
유럽의 통일법규는 국제연합 유럽경제위원회(ECE)에서 정한 ECE 규정과 경제공동체(EEC)에서 제정한 EEC 법규의 두 형태가 있고 또 각국별로 국가형식승인(NTA, National Type Approval)이 있다. ECE 규정은 협정서에 비준한 국가에만 적용되고 법규가 자발적이기 때문에 관계국에 강제력이 없고 자국의 법규에 일치시킨 가맹국에만 상호자동승인제도로 통용되고 있다. 이에 반해 EEC 법규는 회원국에 대하여 강제력을 갖고 있어 이 규정에 의한 형식승인을 회원국 주무당국이 인정한 차량은 모두 공동시장 내에서 판매가 가능하다. 모든 자동차관계 유럽법규는 형식승인(Type Approval)에 기초하고 있다. 즉, 유럽의 인증제도는 북미의 자기인증과는 달리 국가 승인기관이나

43) UN Vehicle Regulations - 1958 Agreement ,
http://www.unece.org/trans/main/wp29/wp29regs1-20.html
44) SPRi, 소프트웨어 안전 산업동향 조사, 2015.8 인용

국가가 지정한 인증기관에게 판매전에 철저한 검사를 시행하고 인증을 요청하는 사전 인증제도이다. 먼저 EEC/ECE 법규에 따른 인가를 받은 후 다시 각국 법규의 인증을 받아야 한다. 이 제도는 제조업자로 하여금 생산일치성과 판매된 각 차량에 대하여 법규와 일치한다는 것을 확인하는 증명서를 발행하도록 강제되어 있다. 주요법규내용은 형식승인(Type Approval), 제품책임(Product Liability), 정기검사제도(Periodic Inspection), 배출가스규제(Emissions), 연비(Fuel Consumption), 엔진력(Engine Power)등이 있다. [45]

ISO 26262의 경우 별도의 규정으로 구별하여 구현되지 않고, 자동차의 전기/전자 부품 또는 시스템 제작 시 준수해야 하는 표준으로 내용이 포함되어 활용되어 적용되고 있다. 소프트웨어부분의 ISO 26262의 구현을 위한 가이드라인을 SAFE(Safe Automotive soFtware architEcture)에서 제공하고 있다.[46] 가이드라인의 범위는 다음과 같다.

[그림 3-4] ISO 26262 관련 SAFE 가이드라인 범위



자료 : ITEA(2013)에서 인용

45) 최인정, 자동차 법규, http://dwcij.com.ne.kr/study/study_app2.htm, (2015-8 방문), 국내 소프트웨어 안전 산업동향 조사에서 재인용, 2015.08
46) Safe Automotive soFtware architEcture, http://www.safe-project.eu/

SAFE는 소프트웨어 개발자에게 AUTOSAR 요구사항에 부합하는 ISO26262 구현 방식을 제공하고, 안전하고 재사용이 가능한 소프트웨어 테스트 방안을 조기에 제공한다.

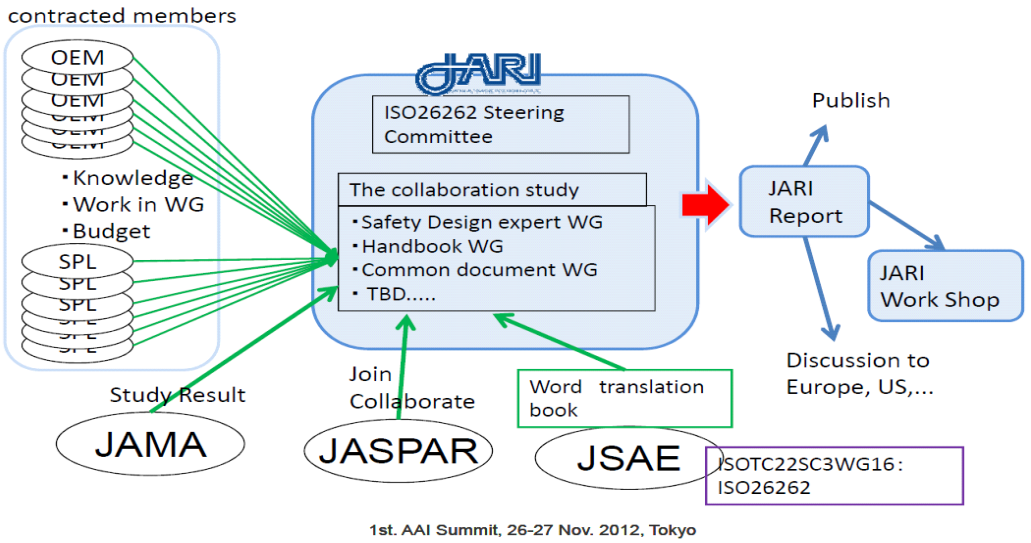
(3) 일본

일본의 경우 정부 연구 기관과 자동차 및 부품 업체가 ISO 26262을 도입하면서, 발생한 주요 이슈에 대한 연구 및 적용을 통해 표준에 대한 가이드 및 활용 제작에 대한 많은 활동이 있었다.

JARI(Japan Automobile Research Institute: 일본 자동차 연구기관)는 2005년도부터 ISO 26262에 대한 연구 활동을 시작했으며, JSAE WG(Automotive Engineers of Japan Work Group)과 ISO 26262에 대한 연구를 지속하였다. 그 후 JARI에서는 JAMA(Japan Automobile Manufacturers Association: 일본 자동차 제조사 협회)와 2008년까지 ISO 26262에 대한 연구, 특히 ASIL에 대한 연구를 계속하였고, 2009년 JARI가 주요 부품 업체를 대상으로 ISO 26262를 업무 프로세스에 적용하는데 따른 문제점을 조사하여 문제점 해결의 노력을 하였다. 도출된 문제점으로 회사 별로 ASIL 등급을 제정하는 의사 결정 프로세스의 상이, 전반적인 ISO 26262 및 관련 안내서 상용화에 대한 번역 어려움, 안전 관리 기술 레벨 문제, 안전 담당자들의 교육 등에 대한 문제가 도출되었다. 이 같은 문제를 해결하기 위해서 JAMA는 OEM 업체, JSAE는 ISO 26262 번역 및 가이드 제작, JASPAR(Japan Automotive Software Platform and Architecture)는 자동차 소프트웨어를, 그리고 JAPIA(Japan Auto Parts Industries Association)는 공급자를 담당하는 조직을 만들었다. 2011년 3월에는 JARI가 OEM 및 공급 업체를 회원으로 하는 ISO 26262 운영위원회를 조직하였고, JAMA, JSAE, JASPAR가 참관자로 참여하였다.[47)]

47) Ryuji Osuga (2012):, SPRi, 소프트웨어 안전 산업동향 조사, 2015.8 재인용

[그림 3-5] 일본의 ISO 26262 협력 시스템 및 회원사



Total: 26 companies 1 April, 2012

Manufacturer members	Supplier members	
TOYOTA	AISIN	DENSO
NISSAN	ADVICS	NISSIN
HONDA	CALSONIC KANSEI	Hitachi Automotive Systems
SUZUKI	KEIHIN	MITSUBISHI ELECTRIC
SUBARU	JTEKT	AISIN AW
MAZDA	SHOWA	TOSHIBA
MITSUBISHI	SUMITOMO ELECTRIC	Panasonic
DAIHATSU	YAZAKI CORPORATION	KYB
YAMAHA	NSK	

자료: Ryuji Osuga (2012); SPRi (2015)에서 재인용

JARI는 ISO 26262 표준을 충족하기 위한 프로세스 적용방안과 문서 제작에 대한 가이드를 제공하고, 공통으로 사용 가능한 문서를 제공하여 기업에게 도움을 주었다. 이는 모든 표준을 적용하기 위해서 기본적으로 제공하여야 하는 서비스이며, 프로세스를 어느 정도 구체화하고, 기술을 공통화 하느냐에 따라 기업에 도움을 주는 정도가 다르다.

또한 일본은 정부/기업간의 협력을 통해 정부의 자동차 기술기준 및 인증시스템의 세계적인 조화를 지원하기 위해 JASIC (Japan Automotive Standards Internationalization Center, 일본자동차기준인증국제화연구센터)을 설립하고, 국제표준에 부합하도록 적극적으로 대비하고 있다.

이처럼 일본은 정부 연구기관, 완성차, 자동차 부품업체, 소프트웨어 업체 등이 연합

하여, ISO 26262를 실질적으로 적용하는데 노력했으며, 일본 정부 연구 기관은 기업의 업무 부담을 줄이기 위한 표준의 해석, 프로세스 적용 방안, 문서 제작 가이드 등을 제공하는 등의 역할을 하였다.

2. 항공 부문

항공 부문의 소프트웨어 안전은 자동운전과 결부되어 상당히 상세한 표준으로 발전하였으며 특히 항공이 발달한 미국의 정부 기관에서 여러 가지 표준을 적용하고 있었다. 항공기는 그 용도별로 우주항공용도, 국방용도, 그리고 민간상용으로 구분될 수 있으며 각각의 표준이 용도에 맞게 발전하였다. 여기에서는 NASA(National Aeronautics and Space Administration, 미국우주항공국)와 FAA(Federal Aviation Administration, 미국연방항공청)에서 적용하는 소프트웨어 안전 표준과 군사 표준 규격에 대하여 설명하였다.

1) 소프트웨어 안전 표준

(1) NASA의 SW 안전 표준 (NASA-STD-8719.13C)

NASA에 의해 제작되거나 납품하는 소프트웨어에 대해 안전을 보장하기 위한 표준으로, NASA SW Safety Guidebook (NASA-GB-8719.13)은 소프트웨어 안전을 구현하는데 필요한 정보를 제공한다. 소프트웨어 안전에 대한 요구사항은 프로세스와 기술적인 사항으로 나뉘며, 이 표준은 프로세스적인 요구사항(소프트웨어 안전을 보장하기 위해 수행하여 하는 것)을 포함하고 있으며, 기술적인 요구사항을 일부 포함하고 있다. 또한 NASA Software Engineering 요구사항(NPR 7150.2)에서 최소한의 기술적 안전 요구사항을 포함하고 있다.[48)]

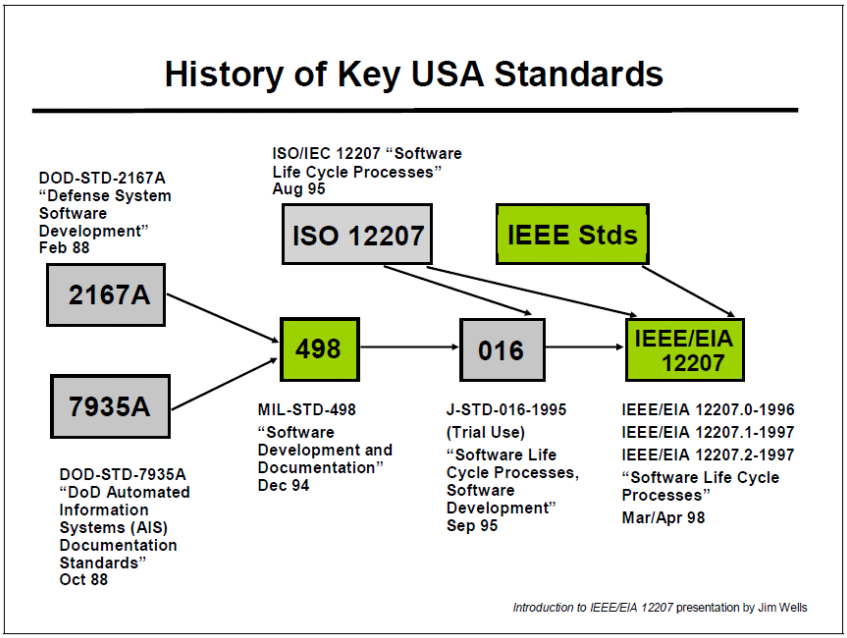
(2) DO-178B / EUROCAE ED-12B

미국 FAA에서 사용하는 표준으로, 유럽에서 사용하는 표준의 명칭(EUROCAE ED-12B)은 다르나, 동일한 내용을 포함하고 있다. 여기서는 DO-178B아고 통일하여 서술하겠다. DO-178B (항공기 시스템과 장비 인증에 관한 소프트웨어 고려사항)는 미

48) NASA Technical Standard, Software Safety Standard, NASA-STD-8719.13C, 2013.7

국의 RTCA(Radio Technical Commission for Aeronautics)와 유럽의 EUROCAE(European Organisation for Civil Aviation Equipment)에서 공동 작업한 소프트웨어 개발 표준이다. 이 표준은 RTCA와 EUROCAE가 개발 후, 이를 미국 연방 항공국(FAA, Federal Aviation Administration)이 민간 항공기 소프트웨어 인증을 위한 용도로 사용할 것을 인정하여 현재 상용 항공기 소프트웨어를 위한 일반적인 표준 인증으로 자리 잡았다. [49]

[그림 3-6] 미국 표준 역사



자료 : Stacy Nelson (2003)에서 인용

(3) MIL-STD 498 (국방 표준)

MIL-STD-498 (Military-Standard-498)은 미국의 군사 표준규격이었으며, "소프트웨어 개발과 문서화 요건을 수립"하기 위한 목적으로 만들어졌다. 이 표준 규격은 1994년 11월 8일 공표되었으며, 기존의 표준규격인 DOD-STD-2167A, DOD-STD-7935A, 그리고 DOD-STD-1703을 대체하여 적용되었다. 그리고 상용 표준이 만들어지는 동안 2년 동안 잠정적인 표준으로 적용되었다. 이 표준규격은 1998년 5월 27일 J-STD-016과 IEEE 12207로 대체되어 효력을 상실했다. 한국을 포함하여 미국이 아닌 다른 나라에서는 여전히 이 표준 규격을 따르는 경우가 있는데, 그 이유는 새로운 표준규격에 비해

49) 위키백과, https://ko.wikipedia.org/wiki/DO-178B, 2015.2 최종 수정

MIL-STD-498이 자유롭게 공개되어 있어, 더욱 익숙하고 이익을 가져다준다고 판단되었기 때문이다.[50]

2) 주요 국가별 표준

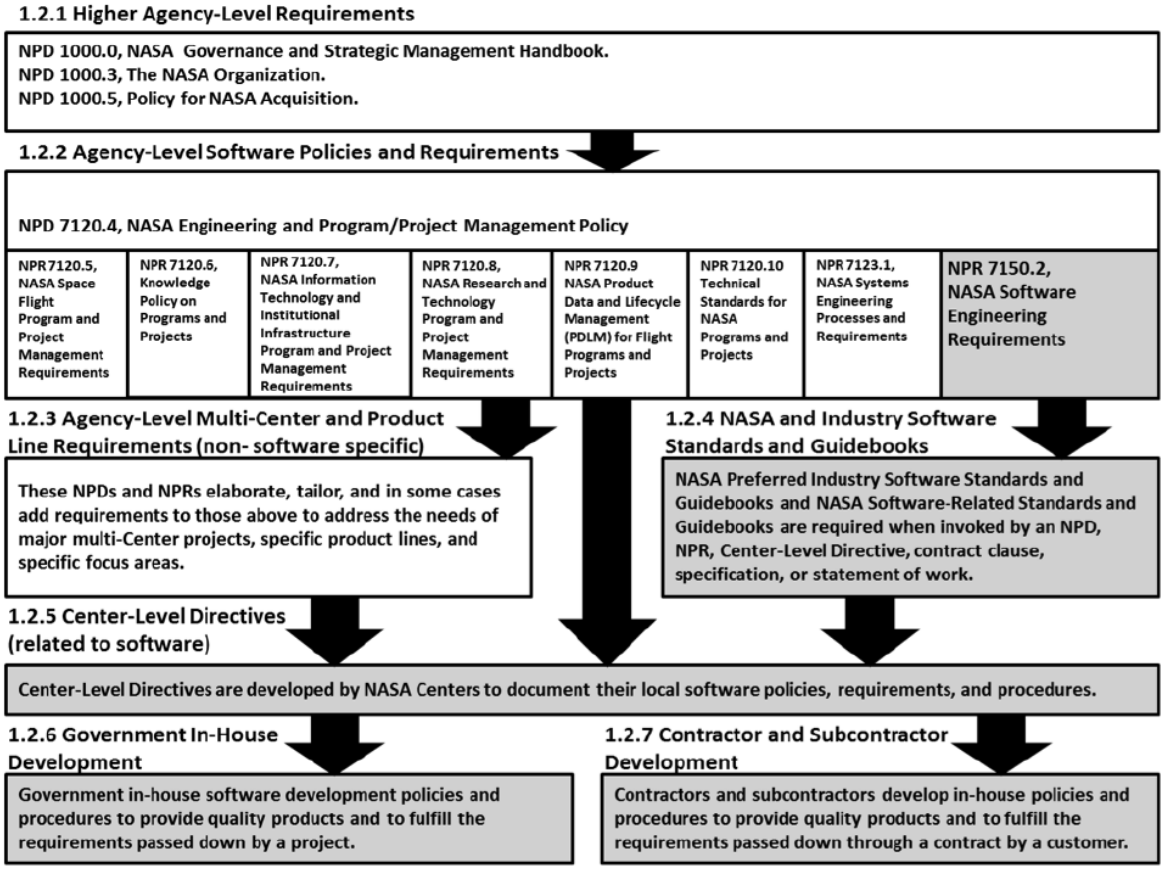
(1) 미국

NASA의 소프트웨어 개발 표준은 NASA Software Engineering 요구사항(NPR 7150.2)로 소프트웨어 안전 기술에 대한 최소한의 요구사항을 포함하고 있다. NASA의 소프트웨어 개발을 위한 체계는 다음과 같다.

NASA Policy Directive (NPD) 1000.0, 즉 NASA 거버넌스와 전략적인 경영 핸드북에 포함된 거버넌스 모델에 맞춰, NASA Software Engineering 요구사항(NPR 7150.2)에서 소프트웨어 획득, 개발, 유지보수, 폐기, 운영 및 관리에 관한 요구사항을 설정하였으며, NASA의 NPR은 NASA Policy Directive (NPD) 7120.4의 구현하기 위한 방법으로서 사용된다. NPD 7120.4는 소프트웨어 생성, 획득, 관리에 대한 NASA의 상위 정책이다. 소프트웨어 품질과 요구사항을 만족하기 위한 하위 체계로 센터 레벨, in-house 개발 및 외주 개발의 관리 방안을 마련하고 있다. 이러한 체계는 다음 [SW 관리 문서 관계도 그림]에서 확인된다.

50) 위키백과, MIL-STD-498, https://ko.wikipedia.org/wiki/MIL-STD-498, 2013.11 최종 수정

[그림 3-7] SW 관리 문서 관계도



자료 :NASA Software Engineering Requirements(NPR 7150.2), 2014.

표준을 수행하기 위한 주최로서 Acquirer(획득자 또는 구매자) 조직과 Provider(제공자 또는 개발자) 조직이 있다. Acquirer(획득자 또는 구매자) 조직은 제공받거나 구매한 소프트웨어에 대하여 소프트웨어의 안전성을 높인 프로그램을 구현하고 이를 위한 충분한 자원을 제공해야 하는 책임이 있으며, Provider(제공자 또는 개발자) 조직 또한 제공하거나 개발하는 소프트웨어에 대해서 안전 프로그램을 구현하고 이를 위한 충분한 자원을 투입해야 하는 책임이 있다. 51)

민간항공기 감항인증인 DO-178B는 다음과 같은 문서를 참고할 수 있다.

- DO-248B : DO-178B에 적용되는 베스트 프랙티스 설명 문서

- DO-278 : 지상 시설, 비행용이 아닌 CNS/ATM (communications, navigation, and surveillance/air traffic management) 시스템에 대한 소프트웨어 표준 문서

51) NASA Technical Standard, Software Safety Standard, NASA-STD-8719.13C, 2013.7

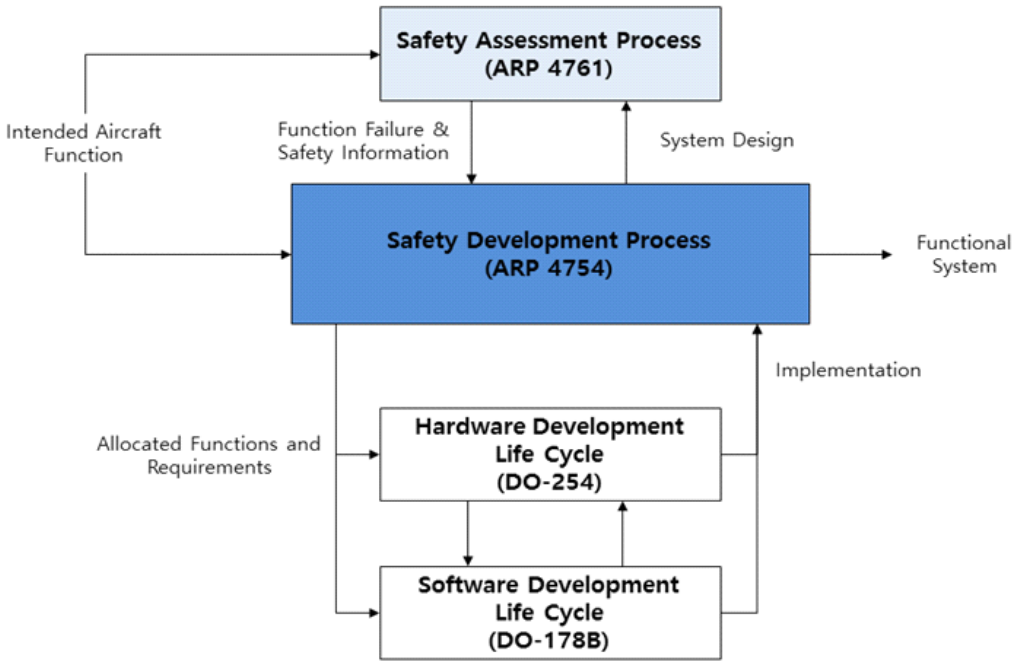
- DO-254 : DO-178B와 동일하나, 하드웨어에 적용되는 표준 문서

DO-178B와 관련하여 SAE International[52]에서 작성한 ARP (Aerospace Recommended Practice) 4761과 ARP4754가 있으며, 이들은 FAA의 14 CFR 25.1309 (항공기의 장비, 시스템과 설치 규정)와 유럽의 CS-25.1309의 규정 준수 여부를 입증하는데 사용된다.

- ARP4761 : 항공기의 안전 평가 절차 수행 가이드

- ARP4754 : 항공기 시스템 개발 프로세스 가이드

[그림 3-8] DO-178B관련 문서 관계



자료: RTCA DO-178B Process visual Summary.
https://upload.wikimedia.org/wikipedia/commons/4/4f/DO-178B_Process_Visual_Summary_Rev_A.pdf, 정영철, 국내 소프트웨어 안전 산업동향 조사, 2015.08에서 재인용

(2) 유럽

유럽은 미국과 유사한 체계와 표준을 적용하고 있는데, 미국의 FAA에 대응되는, EASA, JAA 또는 CAA 기관에서 JAR 또는 CS 규정을 적용하고 있다. 다음은 미국과

52) SAE International은 항공우주, 자동차 및 상용차 업계에서 종사하는 128,000명 이상의 엔지니어와 관련 기술 전문가로 구성된 글로벌 협회. SAE International은 평생 교육과 임의 표준 개발 부문에 주력

유럽의 항공 표준의 대응관계를 표시한 것이다.[53]

<표 3-2> 미국과 유럽의 소프트웨어 안전 표준

구분	미국	유럽
기구	FAA	EASA, JAA, CAA
규정	FAR	JAR, CS
항공시스템의 소프트웨어 안전	DO-178B	ED-12B
항공시스템의 하드웨어 안전	DO-254	ED-80
베스트 프랙티스	DO-248B	ED-94B
지상 시설 시스템에 대한 소프트웨어	DO-278	ED-109

- EASA (European Aviation Safety Agency, 유럽항공안전기구)
- JAA (Joint Aviation Authorities, 유럽항공연합)
- CAA (Civil Aviation Authority, 민간항공기구)
- JAR (Joint Aviation Requirements)
- CS (Certification Specifications)

3. 철도 부문

미국은 화물 및 저속 수송을 목적으로 AREMA에서 제정한 AREMA 2011 C&S Manual을 사실상 표준으로 적용하고, 유럽연합은 승객 및 고속 수송을 목적으로 유럽연합에서는 EN 50128을 적용하고 있다.

1) 표준

(1) AREMA C&S Manual (미국)

AREMA(American Railway Engineering and Maintenance of Way Association)에서 제정한 'The AREMA Communications and Signals Manual of Recommended Practices' (이하 AREMA C&S Manual)는 전기/전자/소프트웨어 안전 표준(De-facto Standard)으로

53) SPRi, 소프트웨어 안전 산업동향 조사, 2015.8

미국 및 캐나다 철도 산업에서 인정받고 있다. 2011년에 개정된 AREMA 2011 C&S Manual의 소프트웨어 및 시스템 안전 관련 주요 항목을 살펴보면, Section 17 품질보장 부분에 안전표준을 포함하고 있다. Section 17.3 안전 보장 관련 부문은 'Part 17.3.1 전기전자/소프트웨어 기반 장비에 대한 안전 보증 권고 프로그램', 'Part 17.3.3 핵심 전기전자/소프트웨어 기반 장비에 대한 하드웨어 분석 실무권장지침', 'Part 17.3.5 핵심 전기전자/소프트웨어 기반 장비에 대한 위험 식별 및 관리를 위한 권장 절차'가 있다. [54]

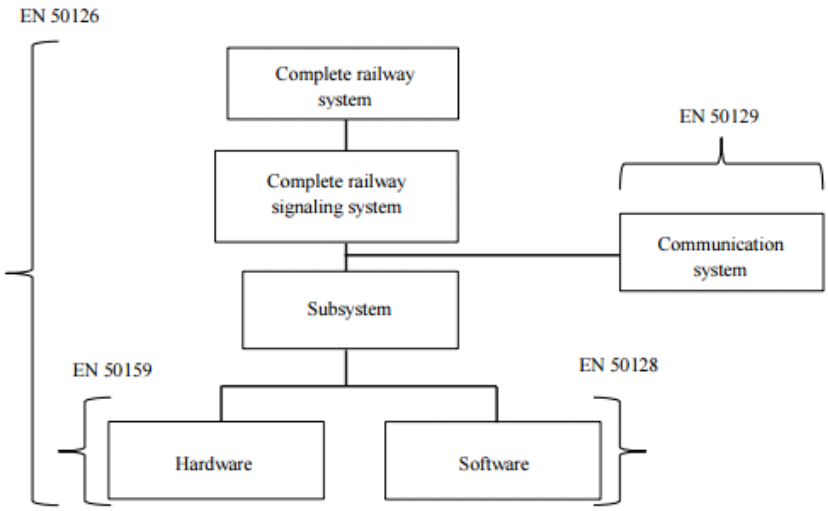
(2) EN50128 / IEC 62279 (유럽)

EN 50128는 철도 산업에 관련된 유럽의 안전 관련 소프트웨어 표준으로, 안전한 소프트웨어 개발을 위한 방법론, 원리, 방법 등을 규정하고 있다. 현재버전은 2012년 3월 발표되었다. 주요 원칙으로는 하향식 디자인 방법(Top-Down Design Method), 모듈성(Modularity), 개발 단계 별 검증(Verification after each development step), 명확한 문서화(Clear documentation), 검증가능한 문서(Verifiable Document), 해당 기기에서의 소프트웨어 확인 테스트(Test the software on the target hardware: Validation)가 있다. 주요 구성요소는 소프트웨어 보증 수준(Software Assurance levels), 소프트웨어 개발 프로세스(Software Development Process), 크로스프로세스 요구사항(Cross-Process Requirements), 기법 및 방법(Technique and Measures)이 있다. EN 50128을 기반으로 한 국제 표준으로 IEC 62279가 있으며, 서로의 내용은 동일하며 EC 50128의 경우 CENELEC(European Committee for electrotechnical standard)에서, IEC 62279는 IEC에서 관장한다.[55]

관련 표준으로 철도 전체시스템 관련 EN 50126, 하드웨어와 신호체계 관련 EN 50129가 있다. 각 표준간의 관계는 아래 그림과 같다.

54) AREMA, https://www.arema.org/publications/cs/index.aspx/
55) 위키피디아, EN_50128, https://de.wikipedia.org/wiki/EN_50128, 2015.9 최종 수정
CENELEC, http://www.cenelec.eu/

[그림 3-9] 철도 시스템 관련 표준



자료 : Jean-Louis Boulanger, Cenelec 50128 and IEC 62279 Standards, 2015, book

유럽과 미국 표준을 비교해 보면, 아래와 같다.

- 유럽 표준은 다른 안전 표준과 비슷하게 초기 설계부터 개발, 테스트, 생산까지 안전 시스템 라이프사이클 전반에 걸친 품질과 안전관리 강조
- 유럽 및 미국 표준 모두 시스템의 안전 등급 설정을 요구하고 있으나, 유럽의 경우 IEC 61508과 비슷한 안전 등급 정의 사용(Safety Integrity Levels 0-4)
- 미국 표준은 FRA(Federal Railroad Administration) 규정을 만족하기 위해 Design Diversity and Self checking, Checked Redundancy, N-Version Programming, Numerical Assurance, Intrinsic Fail Safe Design 등의 개념을 도입하고 있음.
- 위험 유형(Hazard Classifications), 위해도 분석(Hazard Analysis), FTA(Fault Tree Analysis), 고장 모드 및 영향분석(Failure Modes and Effects Analysis) 등의 활동은 두 표준 모두 포함 [56)]

지금까지 자동차, 항공, 철도 도메인의 표준에 대해 살펴보았으며, 각 도메인별, 국가별로 한 개 이상의 표준을 가지고 있었다. 앞으로 각 표준에 대한 도메인별 국가별 시험 및 평가, 인증에 대해 살펴보기로 하겠다.

56) James B. Balliet(2011). pp 20, SPRi, 소프트웨어 안전 산업동향 조사, 2015.8 인용

제2절 시험 및 평가

본 절에서는 소프트웨어 안전성에 대한 시험 및 평가에 대해 기술하기 전에 산업 도메인에서 제품 안전성 시험 및 평가에 대해 기술하고, 소프트웨어 부분에 대해 설명하도록 하겠다. 소프트웨어 안전 표준이 도메인별로 상이하게 정해서, 소프트웨어 안전 시험 및 평가 기준 자체가 다르고, 전체적으로 산업 도메인의 제품 안전성이 보장되어야 소프트웨어 안전이 보장된다고 볼 수 있다.

1. 개요

안전 표준에서는 SIL(Safety integrity level)을 기능 안전에 의해 위험 감소 레벨로 정의하고, 각 디바이스는 안전 요구사항에 의해 정해진 SIL을 만족해야 하는 테스트를 거친다. 각 SIL을 사용하는 표준은 IEC 61508 과 관련된 IEC 61511 (Safety instrumented systems for the process industry sector), IEC 61513 (nuclear industry), IEC 62061 (safety of machinery), EN 50128 (railway applications – software for railway control and protection), EN 50402 (fixed gas-detection systems), ISO 26262 (automotive industry) 등이 있다.

도메인 간 SIL의 관계는 다음과 같다.

<표 3-3> 도메인간 SIL 관계

도메인	도메인 SIL				
Automotive (ISO 26262)	QM	ASIL-A	ASIL - B/C	ASIL-D	
General (IEC-61508)	(SIL-0)	SIL -1	SIL -2	SIL -3	SIL -4
Aviation (DO-178/254)	DAL-E	DAL-D	DAL-C	DAL-B	DAL-A
Railway (CENELEC 50126/128/129)	(SIL-0)	SIL -1	SIL -2	SIL -3	SIL -4

자료 : ASIL, https://en.wikipedia.org/wiki/Automotive_Safety_Integrity_Level, 2015년 10월
DAL (Design Assurance Levels)

이러한 SIL은 디바이스 기능 안전성에 대해 검사하며, 하드웨어와 소프트웨어를 분리하지는 않지만, 소프트웨어에 대해서는 특히 복잡한 소프트웨어에 대해서는 검사하기가 쉽지 않은 단점을 가지고 있다.

2. 자동차 부분

자동차 소프트웨어 안전성 평가는 기능안전성평가의 부분으로 소프트웨어는 자동차 부품으로 간주하여, 통합적으로 시험 및 평가를 수행한다.

<표 3-4> 각국의 자동차 안전도 평가제도

구분	미국	유럽	일본
주관	교통부 NHTSA (도로교통안전청)	EU집행위원회 영국환경교통지역성 스웨덴 운수성 자동차클럽 등	국토교통성 자동차사고대책기구 (NASVA, National Agency for Automotive Safety & Victim's Aid)
평가방법	고정벽정면충돌 (56km/h) 63도 측면충돌 (62km/h) 주행전복(80km/h)	40%부분정면충돌 (64km/h) 90도 측면충돌 (50km/h) 기둥 측면충돌 (29km/h) 보행자(40km/h) 좌석(16,24km/h후방충돌)	고정벽정면충돌 (55km/h) 40% 부분정면충돌 (64km/h) 90도 측면충돌 (55km/h) 보행자 (머리) 제동(100km/h) 좌석(16km/h후방충돌)
향후계획	충돌상호 안전성 전복상해 안전성 어린이좌석 안전성	충돌상호 안전성	지주측면 안전성 충돌상호 안전성 보행자안전성(다리)
홈페이지	safercar.gov	euroncap.com	www.nasva.go.jp

자료 : 교통안전공단 홈페이지, http://www.ts2020.kr/html/nsi/rci/CSRNationalEval.do 편집

(1) 미국

Department of Transportation(DOT, 교통부) 산하 NHTSA (National Highway Traffic Safety Administration, 도로교통안전청)는 안전에 대한 표준을 제정하고, 자동차, 자동차 부품, 오토바이 등이 안전 관련 법조항을 만족하도록 규제하고 있으나, 자동차나 자동차 부품에 대한 표준 준수 인증을 자동차 제조사로부터 직접 하지 않고 사후 검사형태로 안전 보장을 시행하고 있다. 자동차 제조사는 자동차 및 자동차 부품에 대해 모든 안전관련 규정을 준수했다는 자체 인증을 테스트 기관에 의해 실시하며, 자체적으로 테스팅 및 리콜에 대한 책임을 지고 있다.[57)]

인증 후 사후 관리로서 OVSC (Office of Vehicle Safety Compliance)는 새로운 자동차 모델이 시장에 출시되고 난 후, 제품의 무작위로 선택하여 자체 테스팅 설비에서 테스팅을 진행하여, 표준(FMVSS, Federal Motor Vehicle Safety Standards) 준수 여부를 확인한다. 이러한 테스트는 소프트웨어에 대한 테스트라기보다 전체 시스템, 즉 자동차 안전에 대한 테스트이다. 현재는 인증을 위해서는 소프트웨어에 대한 테스트는 없다고 볼 수 있으며, 제작사들이 자동차의 안전을 위해 안전 표준을 준수하기 위한 자체 소프트웨어 테스트가 있다고 볼 수 있다.

NHTSA는 미국 NCAP를 시행하며, 운전석과 동반석의 정면 및 앞좌석과 뒷좌석의 측면, 전복 시 안전도를 평가한다. 지난 1978년부터 매년 미국시장에 판매되는 자동차에 대한 충돌안전성을 검증하는 테스트를 실시하고 그 결과를 발표해, 미국은 물론 전 세계 자동차 소비자들의 신차 구매에 큰 영향을 미치고 있다.

사설기관인 IIHS(Insurance Institute for Highway Safety, 고속도로 안전보험협회)에서 시행하는 테스트는 자동차 제조업체에게 자동차 설계에 영향을 미치고, 미국 소비자 구매와 자동차 보험료 산정에 영향을 준다. 테스트 부분은 충돌 시 차량 강성, 충돌회피 및 완화, 아동용 시트 장착이다. IIHS는 정부기관은 아니나, 각종 연구를 통해 도로교통안전청(NHTSA)이 각종 안전장치를 의무화 할 것을 제안하기도 한다.

(2) 유럽

유럽의 경우는 각 부분별(성인 탑승자 보호, 아동 탑승자 보호, 보행자 보호, 안전 지원기술) 평가결과를 5개의 별로 점수를 부과하여 유로 NCAP (European New Car Assessment Program, 유럽 신차 안전성 테스트 프로그램)의 홈페이지에 공개하고 안전

57) NTASA홈페이지, http://www.nhtsa.gov/SPRi, 소프트웨어 안전 산업동향 조사, 2015.8 재인용

에 의한 자동차 선정 기준을 제시한다. 유로 NCAP는 '유로앤캡'이라고도 하며 유럽 전역의 정부 기관, 자동차 단체, 소비자 협회로부터 충돌 안전성의 표준으로 인정받고 있다. 법률적으로 모든 차량이 테스트 받도록 규정되어 있지는 않아, 앞서 표준부문에 기술한 대로 시험 및 평가가 법률적인 강제사항은 아니다. 그러나 자동차 안전도에 대한 평가를 실시하여 해당 차량의 안전성 정보를 공개하여 소비자에게는 보다 안전한 차량에 대한 정보를 제공하여 자동차를 구매 시 소비자의 권익을 향상시킴과 동시에 자동차 제작사로 하여금 보다 안전한 자동차 제작을 유도하고 있다.

(3) 일본

일본도 자동차사고대책기구에서 유럽과 유사한 JNCAP를 수행하고 있으며, 크게 4개 부분(충돌 안전성, 보행자 보호, 안전벨트, 브레이크)에서 테스트를 시행한다. 일본의 경우 보행자 안전이 테스트의 중요 요인이다. 안전벨트 알림 테스트의 경우는 2009년부터 시행하였으며, 표시, 알림시간, 상태 확인 등에서 소프트웨어의 역할이 중요한 부분을 차지한다.

(4) 그 외 지역

그 외의 지역(호주, 남미, ASEAN)에서도 유사한 NCAP를 시행하며, 각 국가에서 실시하는 충돌테스트 평가방법과 종류에서 차이가 있지만, 대부분 정면, 측면, 주행 중 전복에 대해서 테스트를 진행 하고 있으며, 최근 들어 자동차사고의 상당 비중을 차지하는 부분 정면충돌을 실시하는 국가가 증가하고 있다.

(5) 소프트웨어 테스트

위에서는 공인된 국가기관에서 하는 자동차 테스트에 대해 설명했으며, 자동차 안전성을 위해 자동차 제작사에서는 ISO26262에 기초하여 소프트웨어 테스트를 수행한다. 이는 ISO26262의 V모델에 의한 소프트웨어 유닛테스트, 통합테스트, verification 이 포함된다. 소프트웨어 유닛테스트 방법은 다음과 같은 것이 있다.

〈표 3-5〉 소프트웨어 유닛테스트 방법

테스트 방법	테스트 권유 레벨
요구사항 기반 테스트	모든 ASIL
인터페이스 테스트	모든 ASIL
오류 발생 테스트 (Fault injection test)	모든 ASIL 이나, ASIL D는 적극 권유
모델 코드 비교 테스트	모든 ASIL 이나, ASIL C, D는 적극 권유

자료 : Bharat Bhushan Konka, University of Gothenburg, A case study on Software Testing Methods and Tools ,A pre-study on software testing requirements of ISO/DIS 26262, 2011년 7월

통합테스트 방법도 소프트웨어 유닛테스트 방법과 동일하나, 가능하면 자원 사용 테스트(Resource usage test)를 권유하고 있다.

3. 항공 부문

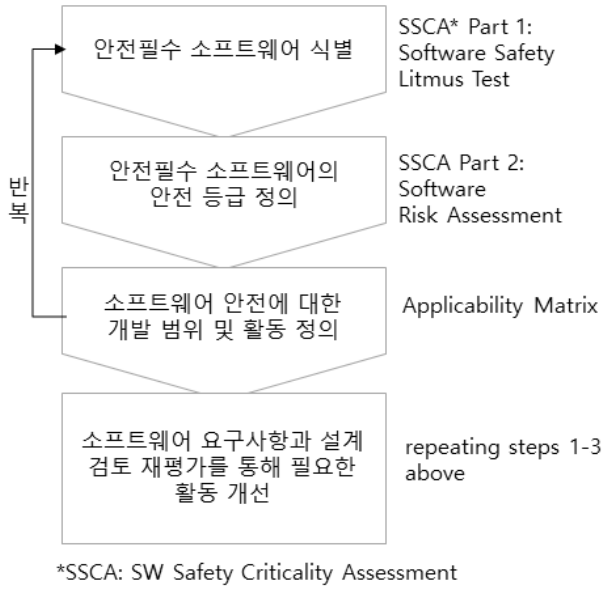
항공은 비교적 소프트웨어 테스트에 대한 프로세스에 대한 중요성이 다른 도메인에 비해 강조되어 있다. 자동차 부분도 소프트웨어 테스트에 대한 프로세스가 상세하고 정교하게 이루어지나, 하드웨어에 소프트웨어에 대한 부분도 많이 속해있어 분리가 어려운 부분도 있다. 항공의 경우는 소프트웨어 중심으로 보다 테스트가 이루어지고 있다. 항공 부문은 미국을 중심으로 기술하도록 하겠다.

(1) 미국

어느 도메인보다 시스템에서 소프트웨어의 중요성을 인지하고 표준에 적용하고 있는 분야이며, 그 사실은 NASA의 표준문서(Software Safety Standard)에서 확인가능하다. 소프트웨어의 테스트 프로세스인 SSCA(Software Safety Criticality Assessment)는 다음과 같다. 테스트를 책임지는 Acquirer and Provider SMA(Safety and Mission Assurance)는, 안전절차나 기술적인 구현에 있어서 평가를 하는 독립적인 조직이고, 소프트웨어 제작과정, 특히 안전에 관련된 개발 과정에서 안전하지 못한 항목이 발생할 경우, 개발 중 또는 소프트웨어를 인수하기 전에 상위 조직에 이슈를 보고하고 해결해야 하는 책임을 가지고 있다. 시스템이 복잡해짐에 따라 소프트웨어의 중요성이 커지고, 시스템의 안전이 중요해 지면, 소프트웨어의 안전 또한 중요해진다. 소프트웨어는 시스템의 하나의 요소로서 평가된다. 이러한 소프트웨어 안전 평가를 위하여 SSCA(Software

Safety Criticality Assessment)는 두 개의 부분으로 나누어져 있다. Part1은 Software Safety Limus Test로 소프트웨어가 안전 검사가 필요한지 여부를 식별하고 Part2는 Software Risk Assessment로 위험의 레벨을 결정한다. 먼저, Acquirer는 SSCA를 통하여 소프트웨어의 안전 위험도를 결정하고 Provider는 소프트웨어 안전위험도에 따라 필요한 안전 테스트 기반 SSCA를 수행한 다음, 프로젝트 개발이 진행됨에 따라 위해도 분석, 조건 및 이벤트에 대해 필요시마다 이를 수행한다. 시스템과 소프트웨어의 개발이 진행되는 동안 Provider는 안전 요건을 만족하는 소프트웨어라는 것을 증명하기 위하여 반복적으로 평가를 수행하며, Acquirer SMA에게 SSCA의 결과 (즉, Software Safety Criticality와 Software Risk Assessment)가 정확하다는 승인을 득해야 한다. Provider는 품질기록(요구사항)으로 승인받은 SSCA를 관리해야 한다.[58)]

[그림 3-10] 소프트웨어 안전 진단 단계



자료 : 정영철, 국내 소프트웨어 안전 산업동향 조사, 2015.08

NASA의 센터 수준의 기관은 NASA의 표준을 사용하여 내부에서 개발한 소프트웨어와 외주한 소프트웨어를 포함하여 NASA에서 사용하는 소프트웨어를 테스트 한다. 기본적인 소프트웨어 레벨(Class A ~ Class H, 예 : Class A - 인간관련 우주 소프트웨어, Class B - 인간과 관련되지 않은 우주 소프트웨어 또는 큰 규모의 항공기 등)은 NASA Software Engineering 요구사항(NPR 7150.2)에 정의되어 있다. 소프트웨어 레벨 정의는 센터마다 약간씩 차이가 발생하기도 하나, 거의 비슷하다. NASA AFRC(NASA Dryden

58) NASA Technical Standard, Software Safety Standard, NASA-STD-8719.13C, 2013.7

RC, 2014년 1월 이름 변경)에서 Class B는 Mission-Critical 소프트웨어를 의미하고 Class A는 Safety-Critical 소프트웨어를 의미한다. Class B 소프트웨어의 장애는 비행체와 비행에는 문제가 없고, 데이터에만 장애가 있고, Class A 소프트웨어의 장애는 항공기와 파일럿을 위험에 빠지게 하므로 Class A 소프트웨어 인증에 필요한 테스팅은 Class B보다 더 엄격한 기준이 적용된다.[59]

민간 항공기 문야의 표준인 RTCA/DO-178B의 경우도 안전 소프트웨어에 대해서 더 철저한 검사와 인증 절차와 방법이 필요하다고 인지하고 있다. 이러한 인증 절차의 결정을 위해 DO-178B는 5단계로 소프트웨어를 구분하였으며, 안전 평가 프로세스(Safety assessment process), 위해도 분석(Hazard analysis)로 단계를 구분한다. [60]

- Level A (Catastrophic) : 항공기 추락의 위험을 갖는 항공기나 부품의 고장 위험 수준
- Level B (Hazardous) : 항공기 성능 또는 안전에 큰 부정적인 요소를 갖거나 물리적인 변형 또는 과도한 업무 부하로 인해 조종사가 비행을 유지할 수 없는 위험 수준, 회피 가능한 방법이 있음
- Level C (Major) : 심각한 수준이지만 위험한 상태는 아님, 예를 들어 승객이 다치는 것보다 불편한 상태)
- Level D (Minor) - 고장 상태가 보이지만 Major 상태보다는 덜한 상태 수준, 예를 들어 승객에게 불편을 초래하거나 조종사나 관제탑 합의에 의해 비행 경로를 변경하는 상태
- Level E (No Effect) : 안전, 비행 조정 또는 조종사 과부하에 영향을 미치지 않은 고장 수준

위와 같은 소프트웨어 레벨에 따라 만족시켜야 할 요건의 수와 독립성 수준이 정해지며, 표준에 따르면 “독립성“이란, 해당 개발 산출물의 개발자와 그 산출물을 검증하는 책임을 가진 사람이 명확히 분리되어 있어야 한다는 의미이다.

---

59) Nelson, Stacy, “Certification Processes for Safety-Critical and Mission-Critical Aerospace Software“. NASA., 2003

60) 위키백과, DO-178, https://ko.wikipedia.org/wiki/DO-178B, 2015년 2월 최종 수정

<표 3-6> 소프트웨어 레벨에 따른 독립성

레벨	고장영향성	만족요건 수	독립성 만족요건 수
A	Catastrophic	66	25
B	Hazardous	65	14
C	Major	58	2
D	Minor	28	2
E	No Effect	0	0

소프트웨어 레벨(A에서 D까지, E의 경우에는 DO-178B 상 요건이 없음)에 따른 목표를 만족시키기 위해서는 프로세스가 필요하다. DO-178B에서 프로세스 자체가 구체적으로 명확히 기술되어 있지 않으며 추상적인 수준으로 기술되어 있고, 이를 구체적인 실제 프로젝트에서 실행하는 방법에 대해서는 각 프로젝트 계획 단계에서 이를 계획하도록 되어 있다. 그러므로 실제 프로젝트에서는 구체적인 프로세스를 만족시킨다기보다는 DO-178B의 각각의 요건(objectives)을 만족시키기 위한 활동들이 진행된다. 그리고 사실 그러한 활동이 계획 단계에서 수행된다.

(2) 소프트웨어 테스트

NASA에서는 안전필요도에 따라 3가지로 테스트 레벨을 분류하고 있다. 소프트웨어 안전필요도는 소프트웨어 위험도와 Hazard 심각성에 따라 구분되는데, 자세한 내용은 NASA Software Safety Guidebook에서 확인 가능하다.

<표 3-7> 소프트웨어 안전필요도에 따른 테스트

테스트	안전필요도		
	MIN	MOD	FULL
통합 테스트	R	HR	M
기능 테스트	M	M	M
소프트웨어 안전테스트	M	M	M
Test Coverage 분석	R	HR	M

자료 : NASA Software Safety Guidebook, NASA-GB-8713.13, 2004년 3월, R :권장, HR : 적극권장, M : 의무

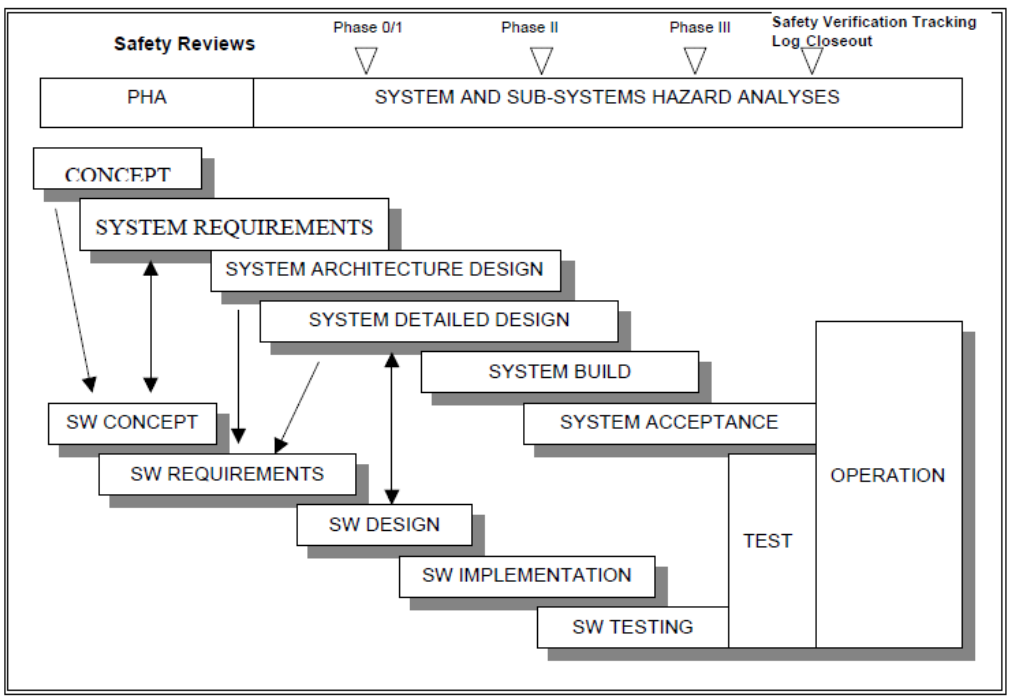
NASA에서 Test Coverage 분석을 위해 사용가능하다고 NASA Software Safety Guidebook에 기술한 툴은 다음과 같다.

- C++ Test and Jtest, Parasoft, http://www.parasoft.com/

- CodeTEST, Metrowerks, http://www.metrowerks.com/
- Code Warrior Analysis Tools, Metrowerks, http://www.metrowerks.com/
- Cantata, IPL (for C code), http://www.iplbath.com/products/tools/pt200.shtml
- C-Cover, Bullseye Win32 and Unix; C and C++
- XPEDITER, Compuware Win32; C, C++, Java and Visual Basic (VB)
- PureCoverage, Rational Win32 and Unix; C, C++, Java and VB
- TestWorks, Software Research Win32 and Unix; C, C++, and Java
- LiveCoverage, Paterson Technology Win32; C, C++, and VB
- DACSTM-Object Coverage, DDC-I Inc Ada; Qualified for FAA verification
- CoverageScope, Real-Time Innovations VxWorks
- GCOV, GNU Linux; C and C++

소프트웨어 테스트는 시스템 테스트와 별개로 이루어지며, 시스템과 소프트웨어가 각각 개발되고 테스트 된 후 통합테스트가 이루가 진다.

[그림 3-11] 안전, 시스템, 소프트웨어 타임라인



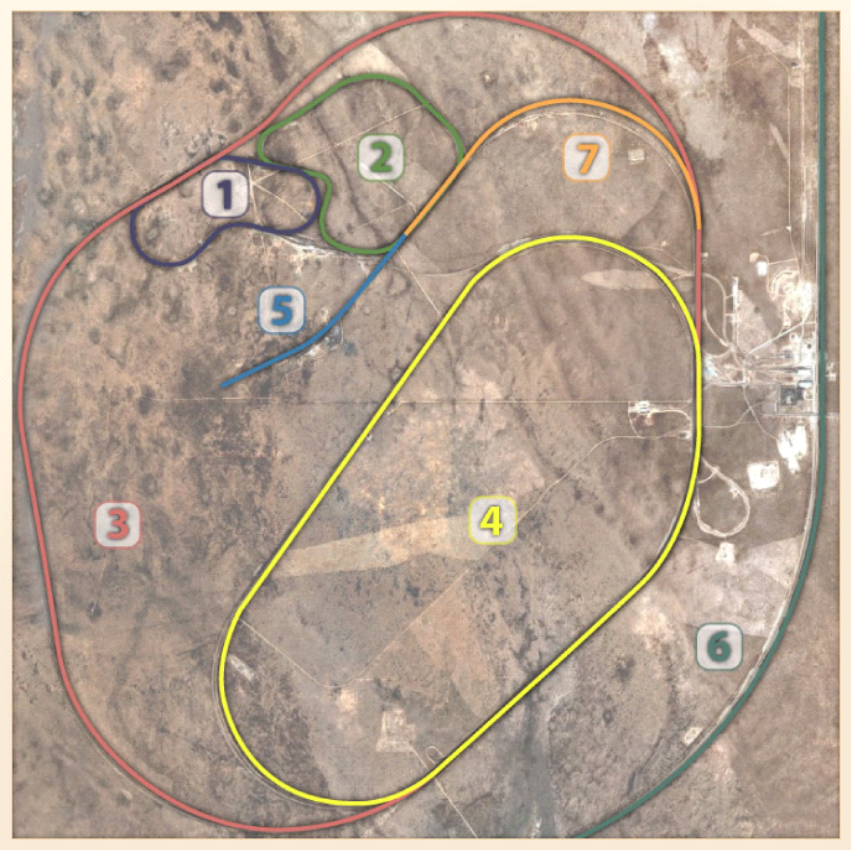
자료 : NASA Software Safety Guidebook, NASA-GB-8713.13,

4. 철도 부분

(1) 미국

미국의 경우 TTCI(교통기술센터, Transportation Technology Center, Inc.)에서 안전성 검사를 시행하는데, 테스트를 위해 48마일의 테스트 트랙을 설치하고 있다.

[그림 3-12] FAST - Facility for Accelerated Service Testing



자료 : TTCI(교통기술센터, Transportation Technology Center, Inc.) 홈페이지

7개의 트랙은 테스트를 위한 다른 기능을 가지고 있으며, 특히 2. WRM(Wheel Rail Mechanism), 6. PTT(Precision Test Track)는 안전에 대한 테스트 구역이다.

(2) 소프트웨어 테스트

SIL에 대해 권장되는 소프트웨어 테스트는 다음과 같다.

<표 3-8> SIL에 따른 소프트웨어 테스트

테스트	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
정적 분석		HR	HR	HR	HR
동적 분석 및 유닛테스트		HR	HR	HR	HR
코드 test coverage	R	HR	HR	HR	HR
블랙박스 테스트	HR	HR	HR	M	M
인터페이스 테스트	HR	HR	HR	HR	HR

자료 : Parasoft White Paper, Satisfying EN 50128 Requirements with Parasoft c/c++ test. achieving Functional Safety of Railway Software, R :권장, HR : 적극권장, M : 의무

각 도메인별로 살펴본바와 같이 SIL을 만족하기 위한 소프트웨어 테스트 범위나 방법은 정해져 있지 않고, 정부기관, 표준 제정 기관, 정부기관이 위탁한 테스트, 인증업체에서 권장하는 가이드 수준으로 제공하고 있다. 그러나 SIL을 만족하기 위한 테스트 결과는 인증에 사용하고 있으며, 테스트에 대한 공인된 각종 Tool이 지원되고 있다. 그리고 사고 시는 제작업체에게 안전책임 의무를 지우게 된다.

인증기관과 인증 프로세스에 대해서는 다음절에 살펴보기로 한다.

제3절 인증 조직 및 프로세스

인증 조직은 국가에서 자국 내 판매하는 제품에 대한 안전 표준 준수 여부 확인 조직이 있고, 수출하거나 수입하는 제품에 대한 표준 준수여부를 확인해 주는 글로벌 인증기관이 존재하고 있다. 이 절에서는 먼저 글로벌 인증기관에 대해 기술하고, 도메인별, 국가별 인증기관 및 인증 프로세스에 대해 기술하도록 하겠다.

1. 글로벌 인증기관

TIC (Testing, Inspection and Certification)을 수행하는 기관으로서 SGS, Bureau Veritas, Intertek, Dekra, DNV GL 등의 글로벌 기업이 존재한다. 이러한 기업들은 주로 유럽을 중심으로 활동하면서 매출 기준 실적으로 최소 5%에서 최대 22%까지 성장세를 나타내고 있다. 이는 소프트웨어 안전에 대한 관심이 지속적으로 증가하는 것이라 볼 수 있으며, 앞으로도 지속되리라 본다.

(1) SGS

SGS는 소프트웨어 안전과 관련된 국제표준 IEC 61508, ISO 26262를 적용하여 자동차, 화학물질, 에너지 ,파이낸스 등 산업영역에서 테스팅, 컨설팅, 인증 및 교육 서비스 등을 제공하고 있다.

SGS의 기능 안전 전문가들은 구성품 및 제품과 관련한 국제표준을 준수하는 안전 프로세스 개발을 지원한다. SGS는 TUV와 단일 단위의 기능 안전팀을 운영하는데, 이것은 기능 안전 공인 기관으로서, 제품이나 시스템의 안전성 확인, 제품안전에 대한 법적 증명 인증서 발행 및 관련 표준 요구사항에 대한 컨설팅을 제공한다. 또한, 신규 표준 작성 과정에 참여하여, ISO 26262와 관련된 ISO그룹 TC22/SC3/WG16나 IEC61508과 GK914 같은 많은 표준위원회에서 활동하고 있다.[61]

(2) Bureau Veritas

1828년 설립된 Bureau Veritas는 6만명 이상의 직원, 1,400지사를 보유한 글로벌 기

61) SGS 홈페이지 , http://www.sgsgroup.kr/, http://www.sgs.com/

업이다. 서비스 분야는 검사, 인증, 컨설팅 등이며, 인증분야는 IEC61508관련 SIL인증(Safety Integrity Level), ASME인증(American Society of Mechanical Engineers) , IRIS 인증 (international Railway Industry Standard), ISO9001 (품질인증) 등이 있다. 62)

최근에 진행하고 있는 것으로는 첫째, 임베디드 소프트웨어의 테스팅과 위험평가에 관한 가이드이다. 현대에 들어와서 임베디드 소프트웨어는 항공기, 자동차, 가전, 헬스케어 기기, 선박까지 제조된 제품의 하드웨어에 점점 더 많이 비율이 증가하여 사용되고 있는데, 임베디드 소프트웨어는 하드웨어와 통합되어 있어 성능과 실패 위험이 어느 부분에서 나타났는지 평가하기 어렵다. 그래서 프랑스 공공연구기관인 CEA LIST와 함께 화이트박스 테스트에 기초한 임베디드 소프트웨어에 대한 인증 가이드라인을 발표할 계획이다. 화이트박스 테스트는 소프트웨어 테스트 방법의 하나로 여기서는 하드웨어와 소프트웨어를 포함한 제품 사양에 대한 임베디드 소프트웨어의 안전성과 성능을 테스트하고 중대한 위험을 평가할 것이다.

두 번째는 철도 수송의 안전성에 대하여 전 프로젝트 동안 위험관리를 위한 10가지 황금률을 제시하는 국제 가이드를 출판했다.63)

(3) Intertek

1896년 미국에서 설립된 Intertek도 38천명이상의 직원을 데리고, 안전에 관한 테스트 및 검사, 인증, 교육 등을 수행한다. 국제공인시험 및 인증기관 Intertek은 다양한 첨단 시험장비와 시험평가 기술력을 기반으로 UL/IEC/ISO인증, 고장분석, 환경시험, 내구시험, 구조물시험, 성능평가, 신뢰성컨설팅 등을 제공하고 있다. 특히 Automotive / Aerospace / Military 관련 시험 인증 서비스를 하고 있다.

Intertek의 주요 기능 안전 관련 활동으로는, IEC 61508 표준에 기초한 온라인 가스 분석 시스템 (Online Gas Analyzer Systems) 분야의 프로세스 모니터링 서비스 시스템 설치 서비스와 전기차 관련 기능안전성 검증 활동이 있다. 온라인 가스 분석 시스템은 설계, 제작, 설치, 주입, 시작 및 운영의 전 주기 서비스와 프로젝트 관리, 기존 시스템의 변경, 문제 해결, 국내/국제 산업 특화된 표준에 대한 컨설팅 및 모니터링 시스템 설치 등의 서비스를 제공하며, 전기차 분야에서는 배터리 시스템의 안전성 검증, 실패 제어 및 ETL / CB / E-Mark 등의 인증 획득 및 ISO 26262 기반의 기능안전 테스팅

62) Bureau Veritas 홈페이지, http://www.bureauveritas.com/
63) Bureau Veritas. (2014). “Annual Report & Activity Report“ , 정영철, 국내 소프트웨어 안전 산업동향 조사, 2015.08에서 재인용

서비스를 수행한다.[64]

- ETL : ETL은 미국 연방정부 및 각 주 정부, 각 시 당국에서 안전시험 서비스의 포괄적인 제공을 허가받은 UL 인증마크와 동등한 자격임

- UL : 전기기기, 기계류, 건축 자재 등 1400여개 대상 품목에 대하여 안전 검사를 실사하는 비강제 인증제도. 그러나 미국의 개별 주법에서 의무화하는 한편 소비자의 인지도가 높아 실제로는 강제성을 보이고 있음

- CB : 전기전자 제품의 안전과 전자파에 대한 국제인증 제도로서 전 세계.43개국의 회권국간 중복시험 없이 해당국가의 인증을 획득할 수 있는 국제적 상호 인정제도

- E-MARK : EU 자동차분야의 형식승인제도로서 강제규격에 해당되며, 자동차 시장 유통 전에 EU 회원국 중 한 회원국으로부터 반드시 형식승인을 받아야 하는 강제검사제도임

(4) Dekra

DEKRA는 독일인증기관으로 기능 안전 서비스 활동으로, 테스트 장비에 필요한 기능 안전 및 안전표준에 준하는 안전 무결성 레벨 (SIL)을 결정하기 위한 위험 평가 및 전체 제품 제작과정을 포함하는 평가 계획을 작성하는 것이 있다. 이러한 활동은 하드웨어 및 소프트웨어 안전 요구사항 검토, 설계 프로세스, 검증 테스팅, 문서 및 기술 파일 제작을 포함한다. 또한 기능안전에 대한 국제표준인 IEC 61508을 기본으로 하며, 의료장치 부문의 IEC 62304, 프로세스 산업부문의 IEC 61511, 자동차 부분의 ISO 26262 등 각 제품에 대한 표준의 기능 안전성을 평가하고 수행한다.[65]

Dekra는 CENELEC, IEC 등의 기관 표준화에 참여하고, 테스팅 전문가들과 정규적으로 만나 기술교환을 한다.

(5) DNV GL

DNV GL은 기술적 평가, 연구, 자문 및 위험관리 분야에서 전문성을 가진 국제적인 인증기관이며 선급협회로서, 2013년 9월에 이 분야의 선도기업인 노르웨이의 DNV (Det Norske Veritas)와 독일의 GL(Germanischer Lloyd)의 합병으로 설립되었다.

64) InterTek 홈페이지, http://intertek.co.kr/, SPRi, 소프트웨어 안전 산업동향 조사, 2015.8 인용
65) Dekra, http://www.dekra-certification.com/en/industry , 정영철, 국내 소프트웨어 안전 산업동향 조사, 2015.08에서 재인용

DNV GL는 주요 서비스를 하고 있는 해양, 석유, 에너지 분야의 고객에게 다음과 같은 비즈니스 과제를 고객들이 안고 있다고 분석했다. 해양, 석유, 에너지 산업 분야는 산업적 특성에 따라 특히 안전하고 사고율이 낮은 운영 요구에 따라 점차 안전 소프트웨어의 의존성이 증가하게 되었고, 하드웨어가 소프트웨어의 통합 또한 빠르게 진행되고 있다고 판단되었다.

선박, 석유 및 가스 산업에서 복잡한 시스템의 제어기능은 하드웨어적인 방법에서 복잡한 소프트웨어 포함되어있는 임베디드 시스템으로 변경되어, 현대의 모든 on-board 선박, 해양 설비 및 석유가스 시설들이 임베디드 소프트웨어에 의존하게 되었다. 또한 규제와 안전에 대한 요구사항은 점점 늘어나게 됨에 따라, 기업은 소프트웨어를 검증하고 확인하고 통합하는 과제 (안전이 보장된 품질보증활동 수행 : 안전요인 식별, 프로세스 관리, 실패 원인 식별, 요구사항과 변경사항 관리 등)를 해결해야 하는 숙제를 안게 되었다. 기업 과제에 대하여 DNV GL은 임베디드 소프트웨어 산업의 경험과 사례를 바탕으로, 맞춤화된 사례와 표준 및 방법론을 제공하고 있다.[66]

<표 3-9> 주요 TIC 업체 제공 서비스 및 주요 활동

기관	활동
SGS	- IEC 61508, ISO 26262 인증 - 자동차, 화학, 에너지 산업 활동 - SGS/TUV 기능안전팀 운영 - 표준위원회 활동 (ISO, IEC 61508 등)
Bureau Veritas	- 자동차 분야의 기능안전 평가 - 철도분야 인증 - 임베디드 SW에 인증 가이드 진행 - 철도 수송 안전성 관련 가이드
Intertek	- IEC61508 - 온라인 가스분석시스템, ISO 26262 기반 전기차 기능안정성 검증 - 표준화 참여(CENELEC, IEC)
DEKRA	- IEC61508 - 의료, 프로세스, 자동차 기능 안전성 평가
DNV GL	- 해상부분 인증 기관 - 임베디드 SW 관련 안전성 검증, 평가, 기술개선

자료 : 정영철, 국내 소프트웨어 안전 산업동향 조사, 2015.08 편집

66) DNV GL, https://en.wikipedia.org/wiki/DNV_GL, 2015년 10월 최종 수정, 정영철, 국내 소프트웨어 안전 산업동향 조사, 2015.08에서 재인용

글로벌 TIC 업체들은 여러 산업 분야의 테스팅, 컨설팅, 인증 및 교육 서비스를 제공하는 동시에 표준기관의 표준 제작에 참여하고 있으며, 전문가 그룹과도 교육하여 기술력을 높여가고 있다.

2. 자동차 부분

(1) 미국

미국은 교통국(Department of Transportation) 산하 NHTSA(National Highway Traffic Safety Administration)에서 자동차 제조사에 FMVSS(Federal Motor Vehicle Safety Standards)를 준수하게 하고, 도난 방지, 연료 효율 등에 대한 규정 제정 및 시험 평가를 수행한다.[67] NHTSA는 1970년 고속도로안전법(the Highway Safety Act)에 의해 설립되었으며, 자동차 및 자동차 장비에 대한 안전 성능 표준을 설정하고 적용하며, 주 및 지방 정부에 보조금을 통해 효과적인 지역 고속도로 안전 프로그램을 수행한다. NHTSA는 자동차 및 자동차 부품이 안전 관련 법조항을 만족하도록 규제하고 있으나, 자동차나 자동차 부품에 대한 표준 준수 인증을 수행하지 않으며, 제조사가 자체인증을 수행한다.

제조사 자체인증 후 관리 측면에서, NHTSA 내의 ODI(Office of Defect Investigation)에서 표준 준수여부를 확인하여 표준을 만족하지 못할 경우 자동차 제조사에 리콜을 권고하거나 리콜을 강제화할 수 있으며, 심할 경우 벌금을 부과하기도 한다.

독립, 비영리 단체로 고속도로 안전보험협회 IIHS(Insurance Institute for Highway Safety)가 있으며, 미국 자동차 보험 시장의 80%를 대표하는 세 가지 주요 보험 협회에 의해 1959 년에 설립되었다.[68] 매년 자체 기준에 맞춘 테스트를 통해 차량의 안전 등급을 매기고 가장 안전한 차량을 선정한다. 안전등급은 부문별로 Good / Acceptable / Marginal / Poor(우수/ 양호/ 미흡/ 열등)로 매겨지는데, 미국에 판매하고자 하는 모든 차량 제조사가 이 연구소의 기준을 맞추기 위해 설계를 개선하고 있다.

(2) 유럽

유럽의 인증제도는 북미의 자기인증(Self-Certification)과는 달리 판매전에 EU나 국가에 의해 공인된 인증기관에 의해 철저한 검사를 시행하는 사전인증제도

67) NHTSA(National Highway Traffic Safety Administration), http://www.nhtsa.gov/
68) IIHS(Insurance Institute for Highway Safety), http://www.iihs.org/iihs

(Pre-Certfication System)로 먼저 EEC/ECE 법규에 따른 인가를 받은 후 다시 각국 법규의 인증을 받아야 한다. EU 가맹국 대부분이 국가 기관 또는 사설 기관이 형식승인(e-Mark)을 수행하고 있다.[69]

e-Mark는 EU 자동차분야 승인제도로서 유럽연합 시장에 제품을 판매하기 전에 EU 회원국(독일, 프랑스, 이탈리아, 네델란드 등 15개국)으로부터 반드시 형식승인을 받아야 하는 강제검사제도이다. 1970년 2월 EU집행위는 최초로 자동차분야 EU 형식승인 제도를 도입, 시행하였으며 1992년 8월 70/156/EEC지침을 수정 보완한 'EC Whole Vehicle Type-Approval' 92/53/EEC 지침을 도입, 1993년 1월부터 한 회원국에서 형식승인을 받은 자동차는 다른 회원국의 형식승인을 받지 않고도 15개 회원국내에서 유통될 수 있도록 하였다. ECE (유럽 공동체) 및 EU(European Union)는 ECE R-10.02 와 Directive 95/54/EC (72/245/EEC를 개정)에 따라 1996년 1월 1일부터 차량은 강제로 적용하고 전장품은 자율 적용하여 오다가 2002년 10월 1일부터는 전장품도 강제로 적용하고 있다.[70]

각국의 인증기관으로는 영국의 경우 VCA(Vehicle Certification Agency), 독일의 경우 Kraftfahrt-Bundesamt (KBA, Federal Motor Transport Authority) 등이 있다. 추가적으로, ECWVTA(Whole Vehicle Type Approval)라는 형식승인 제도가 있는데, 이 제도의 경우 한번 형식승인을 받을 경우, EU 가맹국별 추가적인 형식승인을 받을 필요가 없다. 2015년 6월 현재 총 38개의 인증기관이 있으며, 그 중 한 개의 인증기관을 선택해 인증을 득해야 한다.[71]

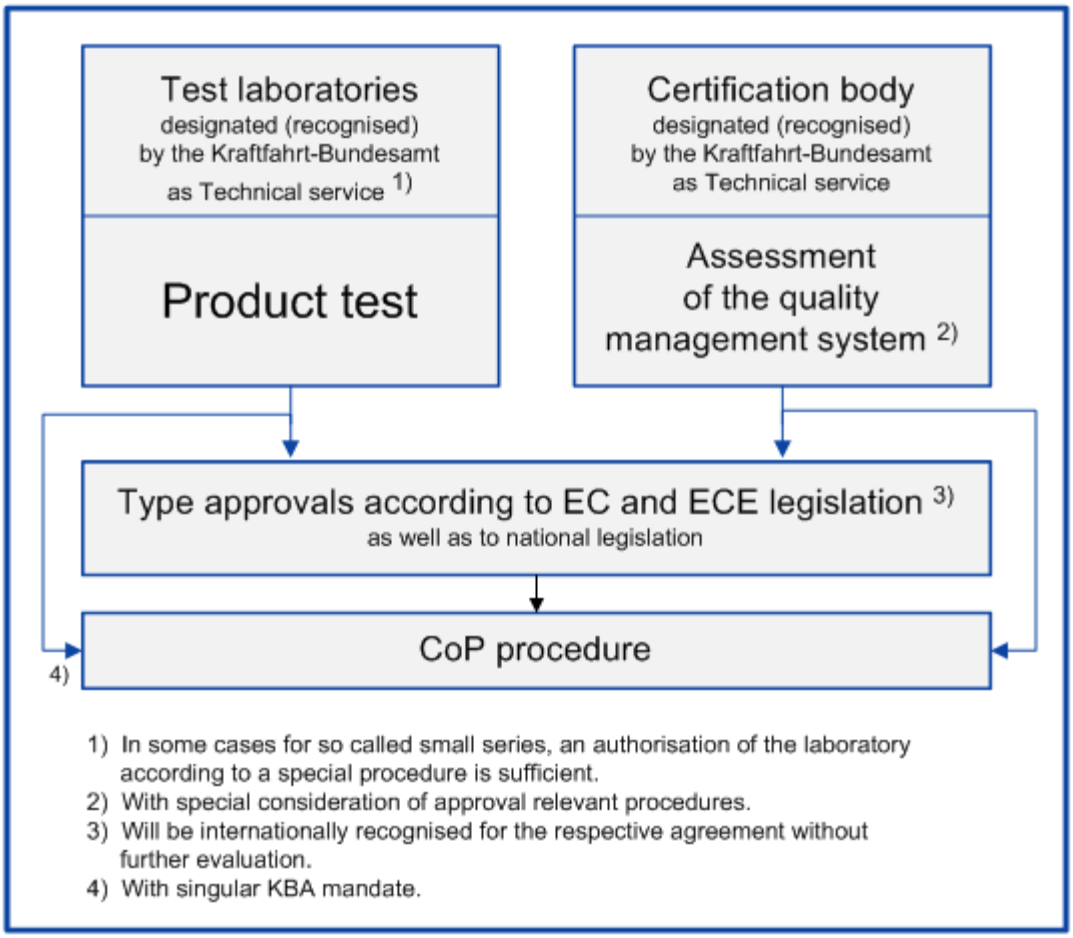
VCA는 영국 정부의 교통부 산하의 인증기관으로서 자동차 및 시스템, 부품에 대한 국제적인 공인 시험 및 인증 서비스를 제공하고 있으며, 자동차 산업 분야에서 30년 이상의 경험을 가진 기관이다. ISO 26262, IEC 61508과 같은 기능안전에 대한 전문 자문 및 인증 서비스를 제공하고 있으며, 경영 시스템 인증 서비스 기관으로 ISO 9001, ISO/TS 16949, ISO 14001, OHSAS 18001과 같은 Management System Certification 서비스 제공하고 있다.[72]

KBA (Federal Motor Transport Authority) 는 자동차 및 부품을 인증, 자동차 테스트

69) SPRi, 소프트웨어 안전 산업동향 조사, 2015.8 인용
70) 한국산업기술시험원, 해외인증정보시스템,
http://certinfo.or.kr/viewWiki.do?wikiGroupNo=64
71) Technical harmonisation in the EU, National type-approval authorities,
http://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/eu/index_en.htm
72) Vehicle Type Approval, http://www.dft.gov.uk/vca/

센터 모니터, 기술 서비스, 자동차 및 부품 리콜, 자동차 및 운전자 등록 및 등록 정보 제공(독일 한정), 등록 및 사고 통계 데이터 제공 등의 서비스를 제공하고 있다. 테스트 및 인증 과정은 다음과 같다.[73)]

[그림 3-13] 인증을 위한 기술서비스



자료 : Kraftfahrt-Bundesamt, Federal Motor Transport Authority, http://www.kba.de/EN/Fahrzeugtechnik_en/Typgenehmigung_en/Benennung_Technischer_Dienste_en/benennung_technischer_dienste_node_en.html

- Test laboratories (시험 기관) : 시험을 수행하고 감독하며, KBA의 형식승인 절차 / COP 제품 검사에 대한 시험 보고서를 작성합니다. 평가는 EN ISO / IEC 17025 및 / 또는 EN ISO / IEC 17020에 기초하여 수행된다.

- Certification Bodies (인증 기관) :

품질 경영 시스템의 요구 사항에 부합되는 정도를 평가하고 KBA의 형식승인 절차 /

73) Kraftfahrt-Bundesamt, Federal Motor Transport Authority, http://www.kba.de/EN/Home/home_node.html

COP (Conformity of Production) 시스템 평가를 위한 증명을 작성한다. 평가는 EN ISO / IEC 17021 표준을 기준으로 한다.

Test laboratories 의 제품 테스트와 Certification Bodies의 인증을 거친 후 EC/ECE 의 형식승인(Type Approvals)을 득한다. 독인의 경우, CoP(Conformity of Production) 과정이 추가된다.

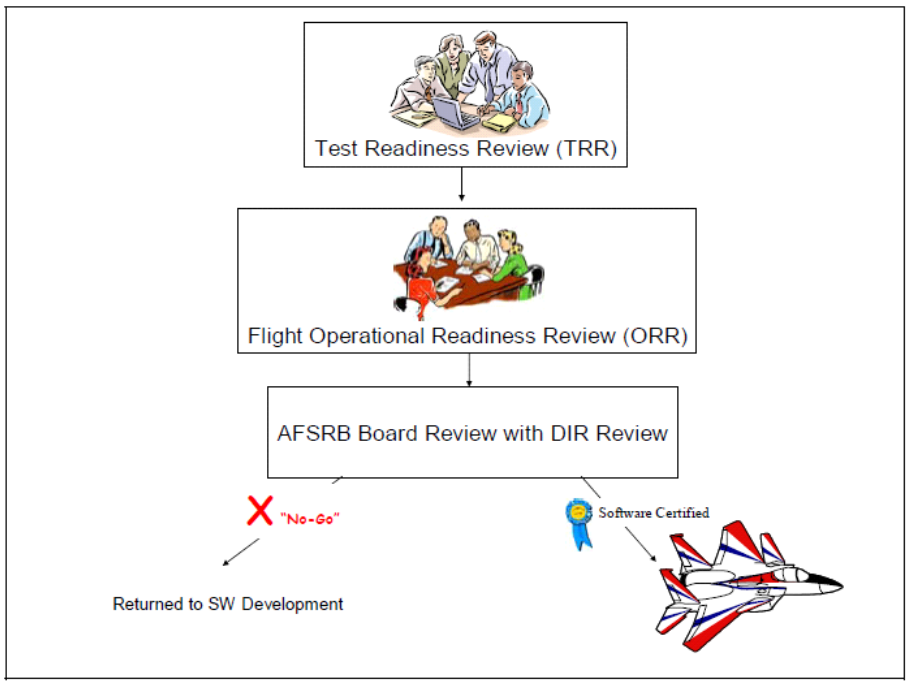
3. 항공부문

(1) 미국

NASA에서 사용하는 Safety-Critical 소프트웨어에 대하여 NASA 표준을 사용하여 인증하는 기관은 센터 수준 기관인 AFRC (Armstrong Flight Research Center), ARC (Ames Research Center), JPL (Jet Propulsion Lab) 등이다.

여기서는 AFRC의 인증 과정에 대해 기술하겠다. 인증과정은 Dryden Handbook Code X (Airworthiness and Flight Safety Review, Independent Review, Mission Success Review, Technical Brief and Mini-Tech Brief Guidelines), Dryden Flight Research Center Policy(Airworthiness and Flight Safety Review Process/ Flight Operational Readiness Review (ORR) and Operational Readiness Review Panel (ORRP))에 기술되어 있다. 이 문서들은 프로세스 언제, 어떻게 진행하는지 자세히 설명하고 있다. 소프트웨어가 인증을 위해서 내부 프로젝트 팀에 의해 Test Readiness Review (TRR)를 거친다. 내부 검사 과정을 마치면 프로젝트에 참여하지 않은 기술자 (Operational Readiness Review Panel, ORRP)들의 검사를 거친다. ORRP의 검사를 Flight Operational Readiness Review (ORR)라고 하며, 검사 후에는 Chair of the AFSRB(Airworthiness Flight Safety Review Board)에게 검사를 받는다. AFSRB는 “go” 또는 “no-go” 결정을 내릴 수 있다.

[그림 3-14] Class A 소프트웨어의 AFRC의 인증 과정



자료 : Stacy Nelson, Certification Processes for Safety-Critical and Mission-Critical Aerospace Software, 2003

DO-178B (항공기 시스템과 장비 인증에 관한 소프트웨어 고려사항)는 항공기 시스템과 장비의 소프트웨어 부분이 감항성(airworthiness) 인증 요구사항의 준수 여부를 검증하는 소프트웨어 개발 표준으로 FAA가 민간 항공기 소프트웨어 인증을 위한 용도로 사용할 것을 승인했다. FAA는 1993년 1월에 AC[74] 20-115B (Radio Technical Commission for Aeronautic, 최신 AC 20-115C[75], Airborne Software Assurance, 2013년 7월 발표 이후 취소)를 발표하여, 전자 설비 또는 시스템을 사용하는 항공기에 대하여 TSO (Federal Aviation Administration technical standard order), TC (형식승인, type certification) 또는 STC (supplemental type certification)를 위한 요청에 대해서 규제 준수를 증명하기 위한 방법으로 DO-178B를 사용할 수 있으나. DO-178B가 항공기 소프트웨어에 대한 FAA 승인을 확인받는 유일한 수단은 아니라고 명시하였다

DO-178B 표준 인증은 일반적으로 FAA에서 그 권한을 위임받은 DER (Designated Engineering Representative)이 항공기 제조사 내에 고용되어 인증 절차를 수행한다.

74) AC : 통지 사항, Advisory Circulars
75) FAA 홈페이지 , AC 20-115C, https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1021710

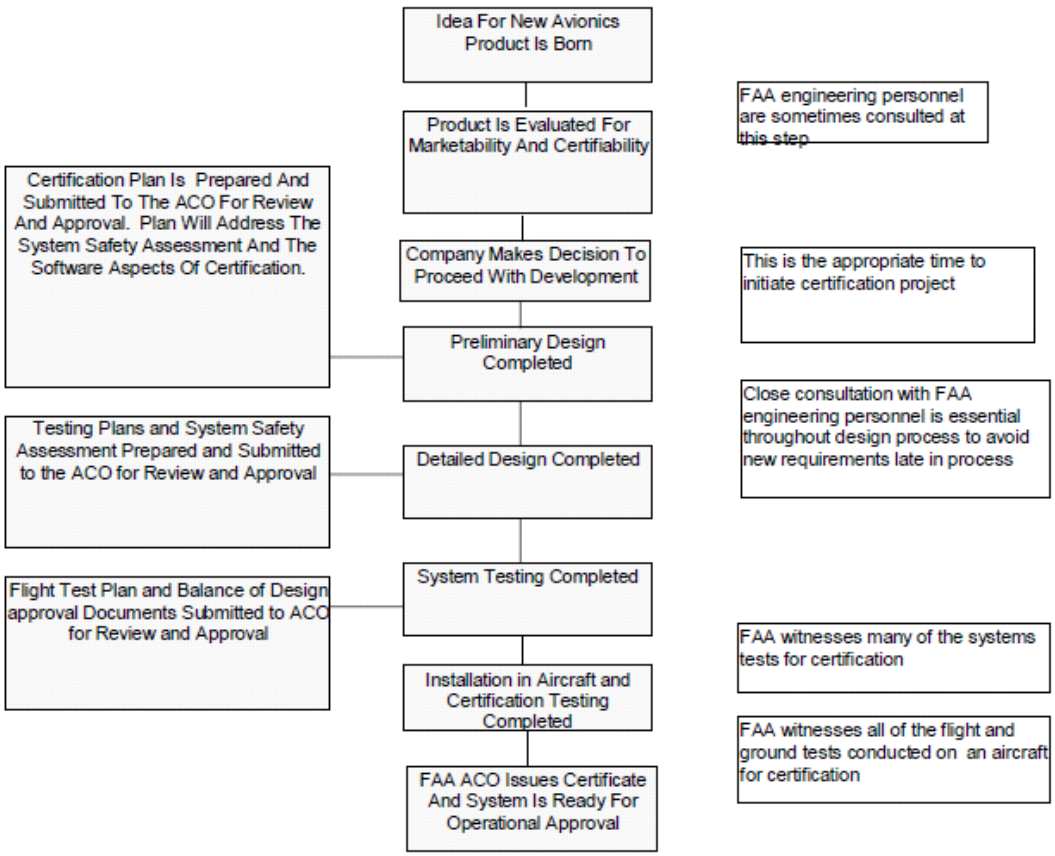
인증절차는 다음과 같다.

- 인증요청자는 CA(certification authority)에 인증하고자 하는 제품의 인증 기준을 확인한다.

- Plan for Software Aspects of Certification (PSAC) 제작한다. PSAC는 시스템 개요, 소프트웨어 개요(특히 안전관련 사항, resource sharing, redundancy, multiple-version dissimilar software, fault tolerance and timing/scheduling strategies) 소프트웨어 안전 등급, 소프트웨어 개발 계획과 데이터 등을 포함한다.

- CA는 PSAC를 확인하고 인증 기준에 부합한지 평가하고 인증한다. [76]

[그림 3-15] FAA 인증 프로세스



자료 : Stacy Nelson, Certification Processes for Safety-Critical and Mission-Critical Aerospace Software, 2003

76) Stacy Nelson, Certification Processes for Safety-Critical and Mission-Critical Aerospace Software, 2003

(2) 유럽

유럽의 민간항공기 인증기관은 EASA (European Aviation Safety Agency, 유럽항공안전기구), JAA (Joint Aviation Authorities, 유럽항공연합), CAA (Civil Aviation Authority, 민간항공기구) 등이 있으며, JAR (Joint Aviation Requirements), CS (Certification Specifications) 규정에 의해 미국과 유사한 체계를 적용하고 있다. EU 국가를 위한 인증기관은 EASA이며, CAA는 개별국가를 위한 인증기관이다. 특히 CAA는 영국을 위한 인증기관 용어로 쓰이며, FAA는 미국을 위한 CAA이다. JAA의 경우는 인증기관이라기보다는 인증기관 연합으로, 인증 규정에 대한 책임을 가지고 있다. 2002년 EASA가 설립된 이후 JAA의 업무가 EASA로 이전 되었다. 2009년 이후 JAA는 해체되었으며, JAA TO(Joint Aviation Authorities Training Organization)로서 현재는 교육을 제공하고 있다.

4. 철도 부문

(1) 미국

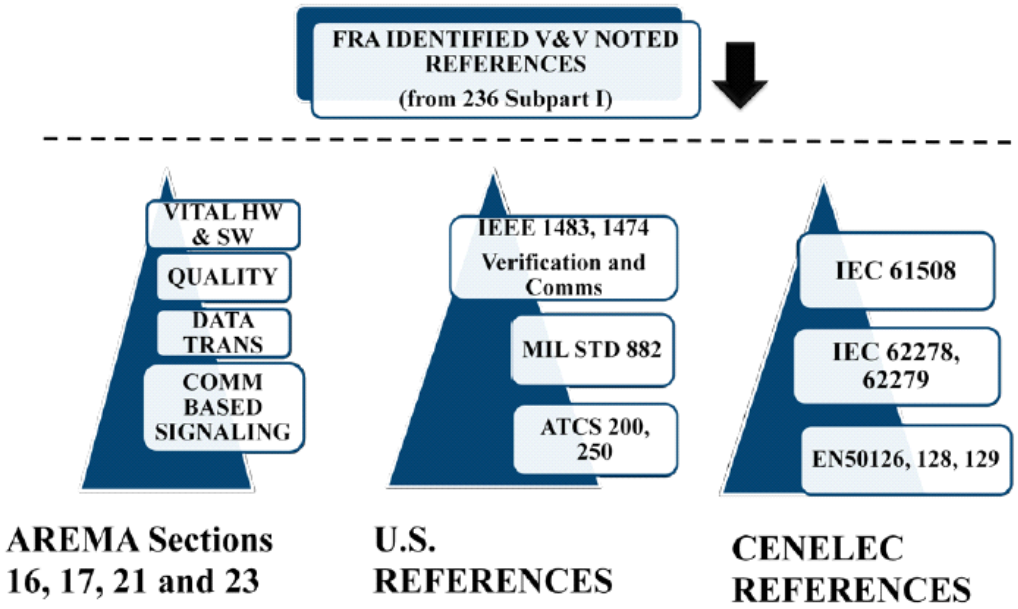
미국은 철도차량 및 용품 안전인증이 자동차의 경우와 같이 국가가 관여하지 않는 자율인증의 형태이다. 그러나 연방법령의 안전기준 준수여부에 대한 사후 관리·감독 시 증빙자료를 요청할 수 있어 실질적으로는 이를 충족하기 위한 안전인증이 실시되고 있다.

미 연방철도국(Federal Railroad Administration: FRA)은 2005년 6월 49 CFR Part 236 Subpart H: 프로세스 기반의 시그널 및 철도 통제 시스템 개발 표준과 2010년 1월 49 CFR Part 236 Subpart I: PTC(Positive Train Control System) 발표했다. 이 규정들은 철도 자체만이 아니라, 고용자들의 안전에도 중요성에도 관심이 있으며, 안전 시스템의 안전 개발 방법, 변경, 테스팅, 운영 방법 등을 포함하고 있다. 그러나 안전 인증 획득을 위한 안전 집행 기관, 공급자 프로세스 등을 정해 놓지는 않았다. 즉, 철도 사업자들은 FRA 규정을 만족하면 자신의 프로세스, 절차, 분석 방법과 문서를 통해 인증을 받을 수 있다.

FRA 규정에는 철도 사업자들이 인증 획득을 위한 CFR Part 236 Subpart H에 포함되어 있는 제품 및 시스템 안전 계획(Product & System Safety Plans) 수립 시 활용 가능한 검증 및 확인(V&V) 표준들이 열거되어 있는데, 여기에는 AREMA(Sections 16,17,21, 23)를 포함한 미국 표준뿐만 아니라 유럽 표준(CENELEC, EN50126, 128,129)도 포함되

어 있다. [77]

[그림 3-16] 검증 및 확인(V&V) 활동 시 인정되는 주요 표준들



자료: James B. Balliet. Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance . 2011

FRA 규정에 나타난 표준으로 AREMA, IEEE1483, 1474, IEC61508 등이 안전 인증 표준으로 사용될 수 있다.

승인기관으로 AAR은 철도운송회사들을 포함한 북미 철도산업 종사업체들의 협의체로서, 미국 철도차량 및 용품의 자율인증을 관할함과 동시에 연방철도국(FRA)과 관리·감독 및 정책·규제 측면에서 긴밀하게 협력한다. 인증절차는 철도차량 및 용품 제작자가 AAR(미국철도협회,Association of American Railroads)에 인증을 신청하고 AAR 산하기관인 TTCI(교통기술센터, Transportation Technology Center, Inc.)는 자체 검사기준에 의거하여 검사를 수행한다. AAR은 검사를 통과한 철도차량 및 용품을 승인하고 사후 관리·감독을 수행한다.[78]

77) James B. Balliet. Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance . 2011 , 정영철, 국내 소프트웨어 안전 산업동향 조사, 2015.08에서 재인용

78) FRA, https://www.fra.dot.gov/Page/P0397, AAR (Association of American Railroads), https://www.aar.org/, TTCI, http://www.aar.com/,
해외인증정보시스템. AAR. http://certinfo.or.kr/viewCert.do?certNo=3. 한국산업기술시험원

(2) 유럽

유럽연합 철도차량 및 용품 안전인증체계는 자국 내 안전기준 적합여부를 검사하는 국내운영성 인증과 상이한 규격 및 기술기준을 보유한 유럽연합 가맹국 간 통행 시 운영성을 검증하는 상호운영성(Interoperability)인증 (TSI)으로 구분되어, 각 경우에 따라 구성요소 및 승인 절차의 차이점이 존재한다. 유럽연합의 철도차량 및 용품 안전인증은 독립적인 전문기관이 제품의 상호운영성・국내운영성 검사기준 준수여부를 검증한다. 국가가 설립한 독립기관은 전문기관의 검사결과를 바탕으로 철도차량 및 용품을 승인하여 판매를 허가하고 해당 제품형식이 일정한 규격을 유지하는지 여부를 관리・감독한다. 승인절차는 철도차량 및 용품 제작자의 신청에 의하여 전문기관에서 검사를 수행하고 그 결과를 NSA(유럽연합 가맹국 철도안전 주무부처,National Safety Authority)에 보고하면, NSA는 검사결과를 바탕으로 승인여부를 결정하고, 승인 완료된 제품은 등록 후 ERA(유럽철도국, European Railway Agency)에 보고된다.

EN 50128는 철도차량 및 용품의 상호운영성(Interoperability)인증 (TSI)에 소프트웨어 표준으로 되어 있어서, 관련 사업자들은 TSI의 요구사항 준수에 대하여 평가를 받고 철도 인증을 받아야 하므로 EN 50128 표준은 법으로 적용된다. 유럽 연합에서 규정한 지침 및 TSI가 유럽 연합 회원국에 적용되는 방법을 독일의 경우를 예로 들면, 독일은 독일 교통부 산하 독립 조직으로 독일연방철도국 (Eisenbahn-Bundesamt: EBA)[79]이 유럽연합지침(Directive 2004/49/EC) 및 TSI에 따라 안전 규정을 제정하고 안전 인증을 수행한다. 소프트웨어 안전 표준에 대해서는, 철도 건설 및 운영 규정(Die Eisenbahn-Bau- und Betriebsordnung: EBO)에 철도차량용 안전 관련 소프트웨어 개발 시에 철도 안전 표준인 EN 50128을 준수하도록 규정하고 있다.[80]

결론적으로 인증을 위해서 정부기관, 표준 제정기관, 테스트 기관, 인증기관 등이 관여하고 있다. 테스트 기관 및 정부가 위임한 인증기관은 글로벌 업체가 수행하는 경우가 있으며, 그 성장속도가 빠르게 증가하고 있다. 소프트웨어 안전 제고 및 안전 산업 활성화를 위해서는 표준 제정기관 활동에 참여하여 표준 제정에 기여하고, 테스트 기관 및 인증기관으로서 기술력을 높이는 활동이 필요하리라 본다. 그리고 도메인별로 나누어진 표준 및 가이드를 비교/분석하여, 소프트웨어 안전 제고 및 안전성 확보 체계 마련에 기반으로 사용해야 할 것이다. 물론 이러한 활동은 정부기관 및 연구소에서도 수행해야 하겠지만, 테스트 및 인증 업체에 위임하여, 국내 테스트 및 인증 산업 활성화에도 기여해야 하겠다.

79) EBA, 독일연방철도국, http://www.eba.bund.de/EN/Home/homepage_node.html
80) SPRi, 소프트웨어 안전 산업동향 조사, 2015.8

제4장 국내 SW안전 확보 체계 현황

제1절 개요

국내 소프트웨어 안전성 관련 시험, 평가, 인증 전문 기관 현황은 기본적으로는 산업별로 구분되어진다.

소프트웨어 안전성 국제 표준 준수 및 대응의 미비로 국내 소프트웨어 안전성 보장 수준은 낮은 상태이다. 원자력, 자동차, 의료, 국방, 항공 등의 소프트웨어 안전성 보장을 위한 국제 표준은 독일, 프랑스, 미국 등의 선진국에서 주도하고 있으며, 소프트웨어 안전 관련 산업 또한 활발하다. 기술의 우위에 있는 선진국들은 안전성 국제 표준을 지원하는 도구 등의 판매와 국제 인증을 위한 안전 컨설팅 활동을 통해 많은 이익을 올리고 있다.

따라서 국내 소프트웨어 안전성 경쟁력 확보를 위해서는 소프트웨어 안전을 위한 도구 개발 둥 관리 기술 개말 및 시의성 있는 국제 표준의 대응이 필요하다.

국제 표준 활동에 적극 참여함으로써, 국제 표준 기술에 대한 대응력을 높임과 동시에 현재의 표준을 구체적으로 분석하여 이에 대응할 수 있는 소프트웨어 기술 개발이 필요하다.

현재 소프트웨어 안전성 국제 표준은 관련 산업이 지속적으로 발전하고 기술개발이 이루어짐에 따라 계속해서 많은 수정 보완 작업이 요구되고 있다. 또한 산업 분야별로도 신규 표준 제정 예정 분야가 많이 있으므로 국내도 이에 적극 참여하여 국내 자체 기술력을 확보해야 한다.

소프트웨어 개발 프로세스 상에서 SW 품질・안전・신뢰성을 높이기 위해서는 관련 도구를 활용하는 게 필수적이다.

소프트웨어 가 안전하게 개발될 수 있도록 지원하는 기능을 가진 케이스 도구들(대표적으로 SCADE suite, AUTOSAR 등)은 핵심 기술이 공개되어 있지 않으며 수억 원의 라이센스 비용이 든다.

장기적인 관점에서 소프트웨어 안전성 평가 도구 개발 기술을 국산화 하여, 고가의 해외 도구 사용 라이센스 비용 및 기술 이전 비용을 절감해야 할 것이다.

소프트웨어 개발 측면으로는 우선 하나의 기술로 모든 유형의 버그를 찾아내는건 불

가능하기 때문에, 정형 검증・테스팅・정적 분석 등 다양한 방법이 동원되어야 한다.

소프트웨어 개발 전체 프로세스에서 안전성을 보장하는 소프트웨어 안전 공학 연구를 꾸준히 하고, 소프트웨어 생명 주기 별 안정성 활동 지침 개발이 필요하다.

안전성 확보를 위한 소프트웨어 공학 기법, 특히 요구공학 기업은 점점 복자해져가는 시스템과 다른 신뢰성 평가 지표들을 통합적으로 고려할 수 있도록 개선하는 연구가 필요하다.

System of System의 위험을 평가하기 위한 방법이 필요하며, V&V(Verification & Validation) 단계에서는 개발된 소프트웨어 시스템이 실제 요구사항을 만족하고 있는지 기능적 레벨에서 확인할 수 있는 모델과 프로세스가 요구된다.

관련 기관은 아래 표와 같다.

<표 4-1> 소프트웨어 안전 관련 기관

	자동차	철도	항공/우주	원자력	국방
정부기관	국토교통부	국토교통부	국토교통부	미래부/원안위 / 산업부	방위사업청
유관기관	교통안전공단	철도기술연구원	한국항공우주연구원	한국원자력연구원 원자력안전기술원	국방기술품질원,
역할	자동차 안전평가	철도 시험 인증	항공우주안전 인증	원자력 SW 안전지원	군수품의 품질보증

제2절 국내 안전 관련 기관

각 기관의 개요 및 주요기능은 아래와 같다.

1. 한국산업기술시험원 (KTL)

한국산업기술시험원은 시험평가기술 지원을 통한 산업기술향상을 위해 2006년 11월 설립된 대한민국 산업통상자원부 산하 기관이다. 주로 제품의 성능 및 안전성에 대한 품질인증과 산업현장측정표준 유지 및 지원, 그리고 시험평가기술의 개발 등을 통해 제조기업의 기술수준과 경쟁력을 높이는 것을 목표로 선진국 시험인증기관과의 교류, 협력을 통해 국제적인 기능과 역할을 강화하고 있다.

[그림 4－1] 한국산업기술시험원 조직도

자료: 한국산업기술시험원 홈페이지

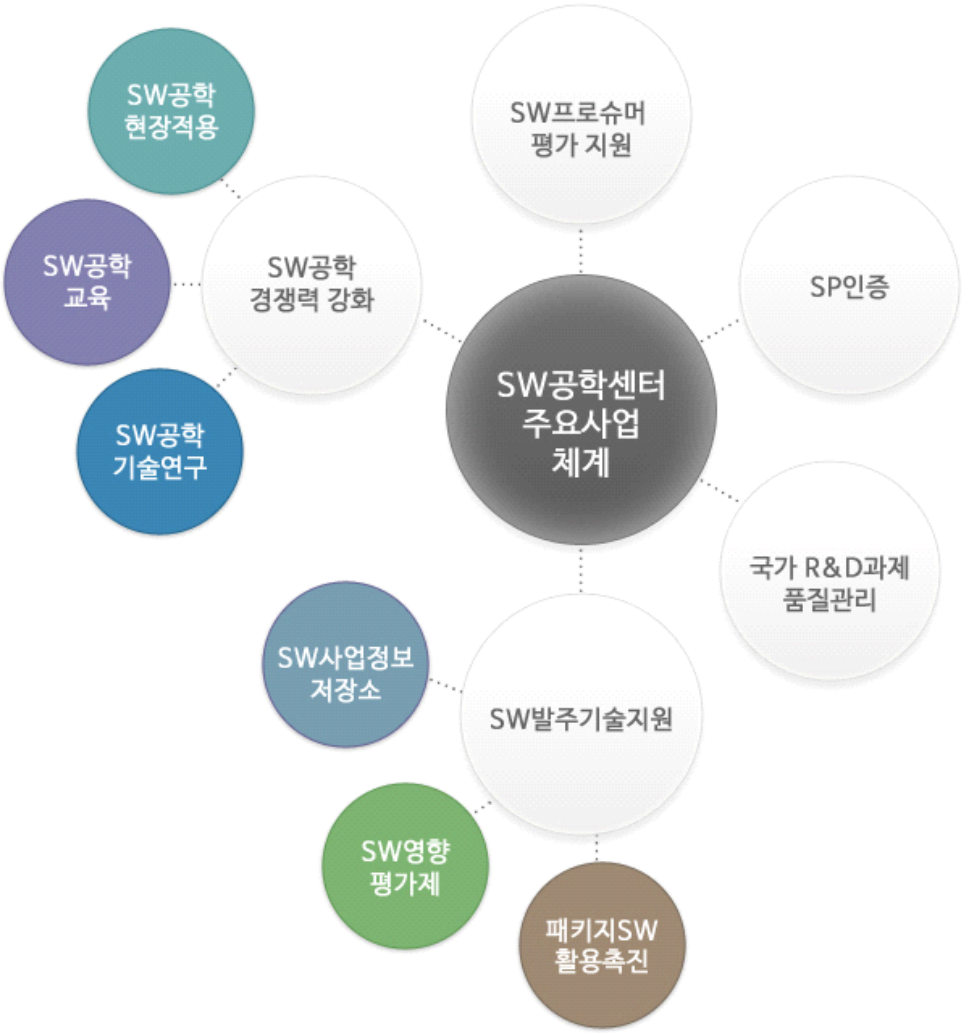
2. 소프트웨어공학센터 (SW 공학센터)

소프트웨어공학센터는 SW품질을 향상시키기 위해 산업에 필요한 SW공학 기술을 연구하고, 중소 SW기업의 SW품질 개선, 현장적용 지원, SW공학기술 적용 성과 및 관련 기술자료 등을 제공한다. 또한 SW개발 사업의 성공을 위하여 문제점을 사전에 예측하고 SW품질과 생산성 제고, 제품결함을 예방 할 수 있도록 SW공학 컨설팅을 제공하고, 국가 주요 SW R&D과제에 대한 품질관리 업무도 수행한다. 더불어 SW품질과 생산성, 비용 등을 체계적으로 추적 평가하기 위한 SW사업정보 저장소를 운영한다.

[그림 4-2] 소프트웨어 공학센터 조직

자료: 소프트웨어 공학센터 홈페이지

[그림 4－3] 소프트웨어 공학센터 주요사업



자료: 소프트웨어 공학센터 홈페이지

3. 한국정보통신기술협회 (TTA)

정보통신 분야의 새로운 표준을 발굴, 제정하고 ICT표준 제품에 대한 국제적 수준의 시험 및 인증 서비스를 원스톱으로 제공하는 민간 자율의 ICT 표준화 및 시험인증 기관이다.

기술 연구 단체로 정보통신분야의 표준화 활동 및 표준 제품의 시험인증을 위해 만들어진 단체이다.

[그림 4-4] 한국정보통신기술협회 조직

자료: 한국정보통신기술협회 홈페이지

4. 한국철도기술연구원 (KRRI)

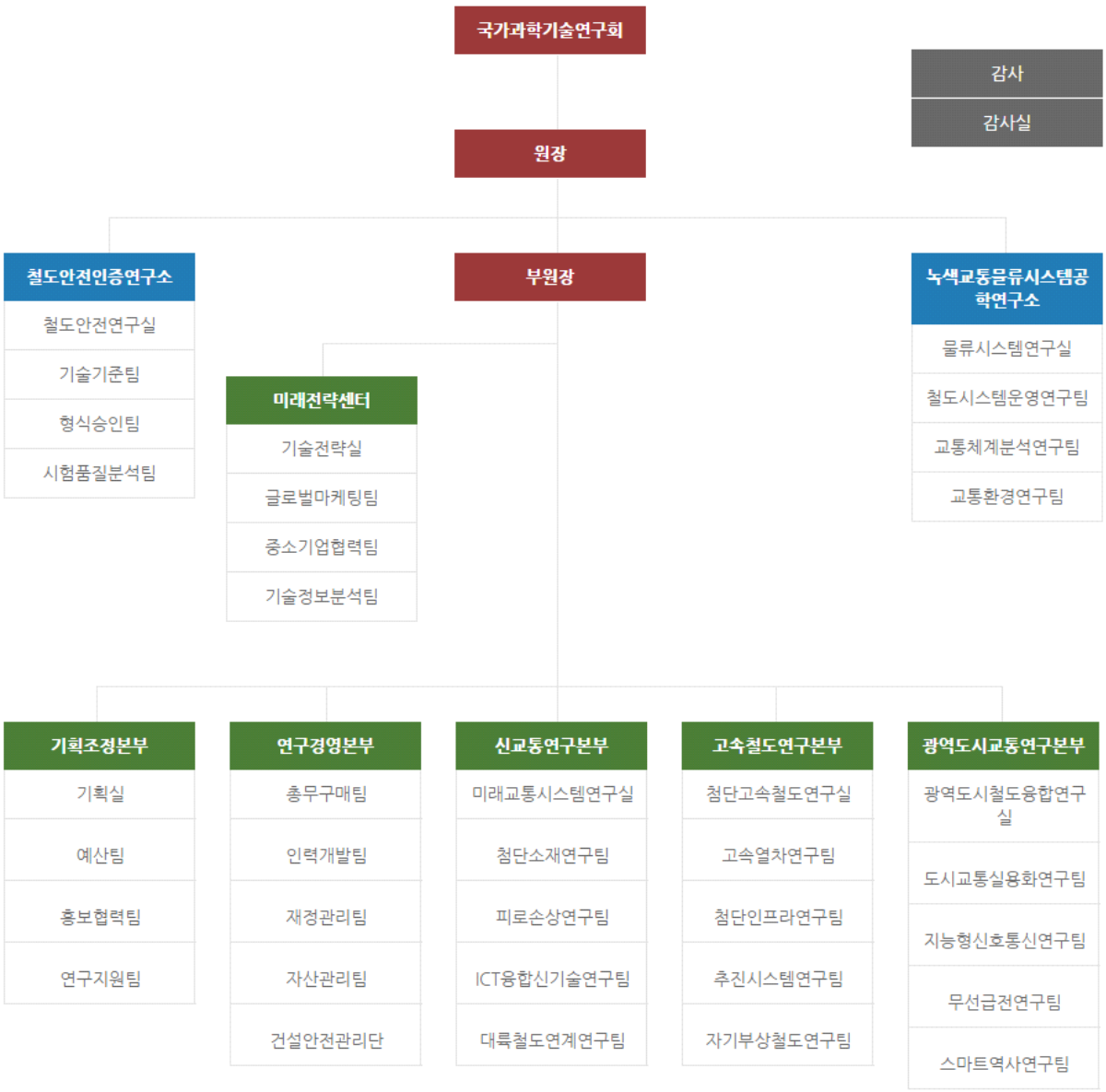
한국철도기술연구원은 철도분야의 기술개발 및 정책연구를 위해 설립된 기관으로 철도안전인증연구소에서 철도시스템 안전 확보를 위해 필요한 관련 법규 및 국내외 표준을 기반으로 공정한 시험 및 검사를 수행한다.

o 주요기능 및 역할은 아래와 같다.

- 고속철도, 일반철도, 도시철도 및 경량전철시스템 연구개발
- 차세대 대중교통시스템 연구개발
- 철도안전, 표준화, 철도정책 및 물류기술 연구개발
- 남북철도 및 대륙철도 연계기술 연구개발
- 철도, 대중교통, 물류 등 공공교통시스템 핵심원천기술 연구개발
- 중소·중견기업 등 관련 산업계 협력·지원 및 기술사업화 등

주요 연구사업으로는 고속철도 R&D, 도시·광역교통 R&D, 철도안전 R&D, 철도물류 R&D, 미래핵심기술 R&D 가 있다.

[그림 4－5] 한국철도기술연구원 조직



자료: 한국철도기술연구원 홈페이지

5. 교통안전공단 - 자동차안전연구원

교통사고에 의한 사회적 손실 절감, 소비자보호에 의한 국민의 권익 보호, 국내자동차관련 산업의 기술정보 지원, 정부의 자동차관련 정책 및 기술 지원의 목적으로 설립되었다.

주로 자동차 HW와 관련된 시험을 시행한다.

시험은 충돌시험, 충격시험, 도로안전시설성능시험, 소음/전파시험, 성능시험, 동화시계시험, 주행시험, 미래차시험과 자기인증/리콜, 자동차안전도평가를 수행한다.

[그림 4－6] 자동차안전연구원 조직

자료: 교통안전공단 홈페이지

6. 자동차부품연구원 (KATECH)

국내 자동차부품업계의 자생력 확보와 산업육성을 위해 정부와 업체가 힘을 모아 설립하였으며, 연구개발, 시험인증, 교육 및 정보제공 등 다양한 지원을 수행하고 있다.

o 주요역활

- 전략적 핵심 기술 개발 : 원천기술 개발, 고객중심 기술 개발, 부품업체 공통 에로 및 취약기술 개발
- 국가자동차산업 기술 기획 : 산업융합원천기술개발 사업 기획, 그린카 산업 육성 기획, 지능형 자동차사업 육성 기획, 신개념 1인용 운송수단 기획
- 신뢰성 평가 및 기술 교육 : 중소기업 200여개 사 설계 기술, 10년 10만마일 보증을 위한 부품 신뢰성 체계 구축
- 지역특화기술 개발 : 대구 지능형 자동차 사업, 전북 상용차 사업, 광주 클린디젤 자동차 사업, 울산 전기자동차 사업

o 주요기능

- 연구개발 / 기술지도
- 신뢰성 인증 / 고장 분석
- 부품 / 성능시험
- 기술교육 / 인력양성
- 연구시험 / 시설제공

[그림 4-7] 자동차부품연구원 조직

자료: 자동차부품연구원 홈페이지

7. 한국항공우주연구원 (KARI)

항공우주과학기술영역의 새로운 탐구, 기술선도, 개발 및 보급을 통하여 국민경제의 건전한 발전과 국민생활의 향상에 기여를 목적으로 설립되었다.

주요 연구로는

- 항공기·인공위성·우주발사체의 종합시스템 및 핵심기술 연구개발
- 국가항공우주개발 정책수립 지원, 항공우주 기술정보의 유통 및 보급·확산
- 시험평가시설의 산·학·연 공동 활용, 중소·중견기업 등 관련 산업계 협력·지원 및 기술사업화
- 정부, 민간, 법인, 단체 등과 연구개발협력 및 기술용역 수탁·위탁, 주요 임무 분야의 전문인력 양성

등이 있다.

[그림 4-8] 한국항공우주연구원 조직도

자료: 항국항공우주연구원 홈페이지

8. 한국원자력연구원 (KAERI)

대한민국 최초의 원자력 연구 기관으로 원자로의 연구 및 개발, 방사성 동위원소의 생산 및 핵기술자의 양성을 주요 업무로 하고 있다.

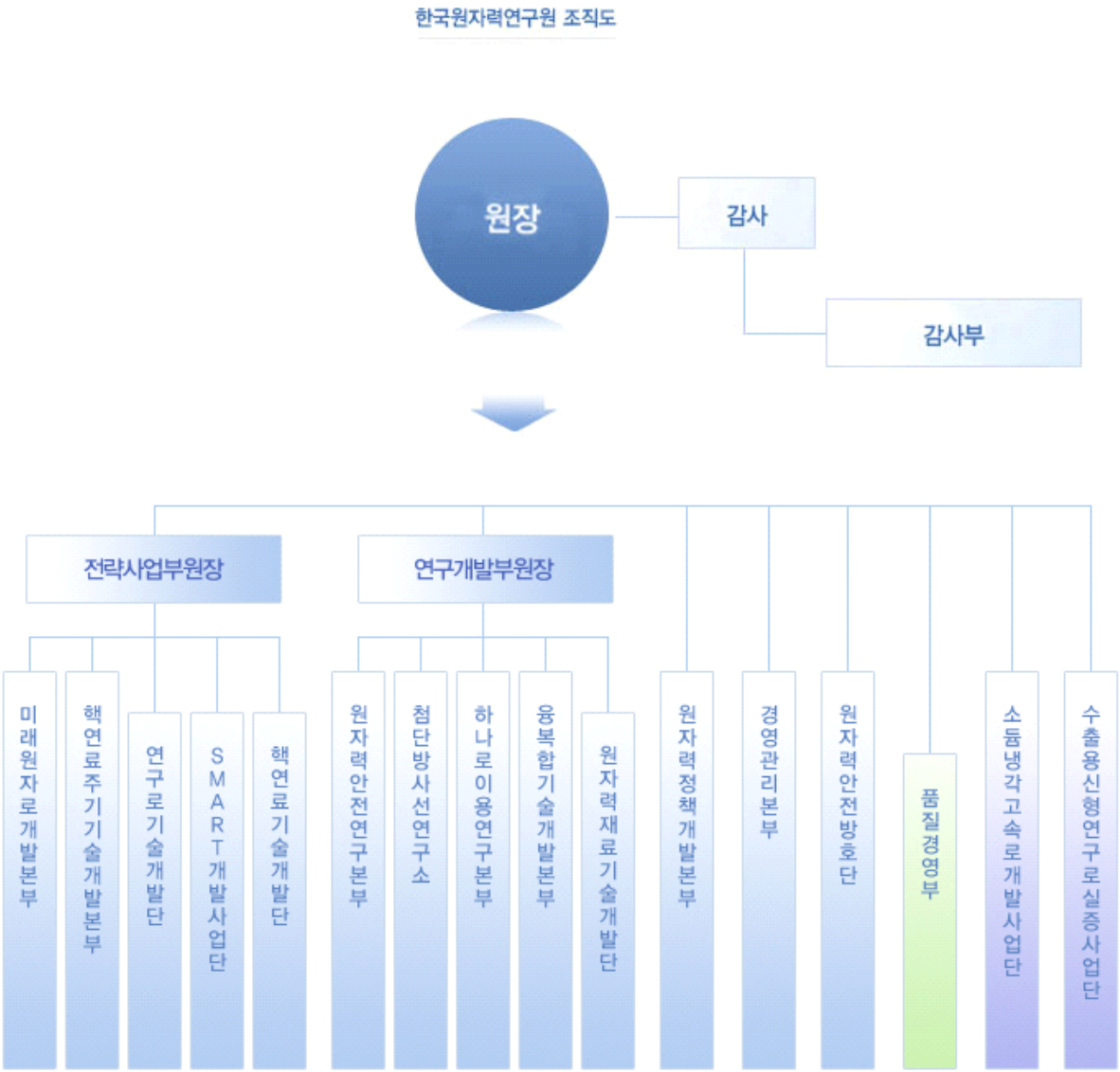
한국 원자력 연구원에서는 원자력의 평화적 이용이라는 설립 취지에 따라 방사선의 산업적 이용, 동위원소 생산, 미래 원자력에너지 연구, 방사선의 의학적 이용, 원자력 정책연구 등의 연구업무를 수행하며 연구로인 하나로를 운영하고 있다.

o 주요 기능은 아래와 같다.

- 원자로 핵연료주기 연구개발 및 원자력이용 신에너지기술 연구개발
- 방사선 응용과학 연구개발
- 의학, 농업, 공업, 식품, 생명과학 등 RT 관련 연구
- 원자력 기초기반기술 연구
- 가속기, 양자광학, 연구로 이용기술 등
- 원자력 정책연구 및 원자력기술정보의 수집
- 원자력 관련 대형연구시설 개발, 운영
- 원자력설비 및 환경 안전성연구 개발 등

- 연구분야 중 원자력안전연구
- 열수력 안전 연구
- 종합안전평가
- 환경안전연구
- 원자력 재료 기술
- 중대사고 중수로 안전연구

[그림 4－9] 한국원자력연구원 조직도



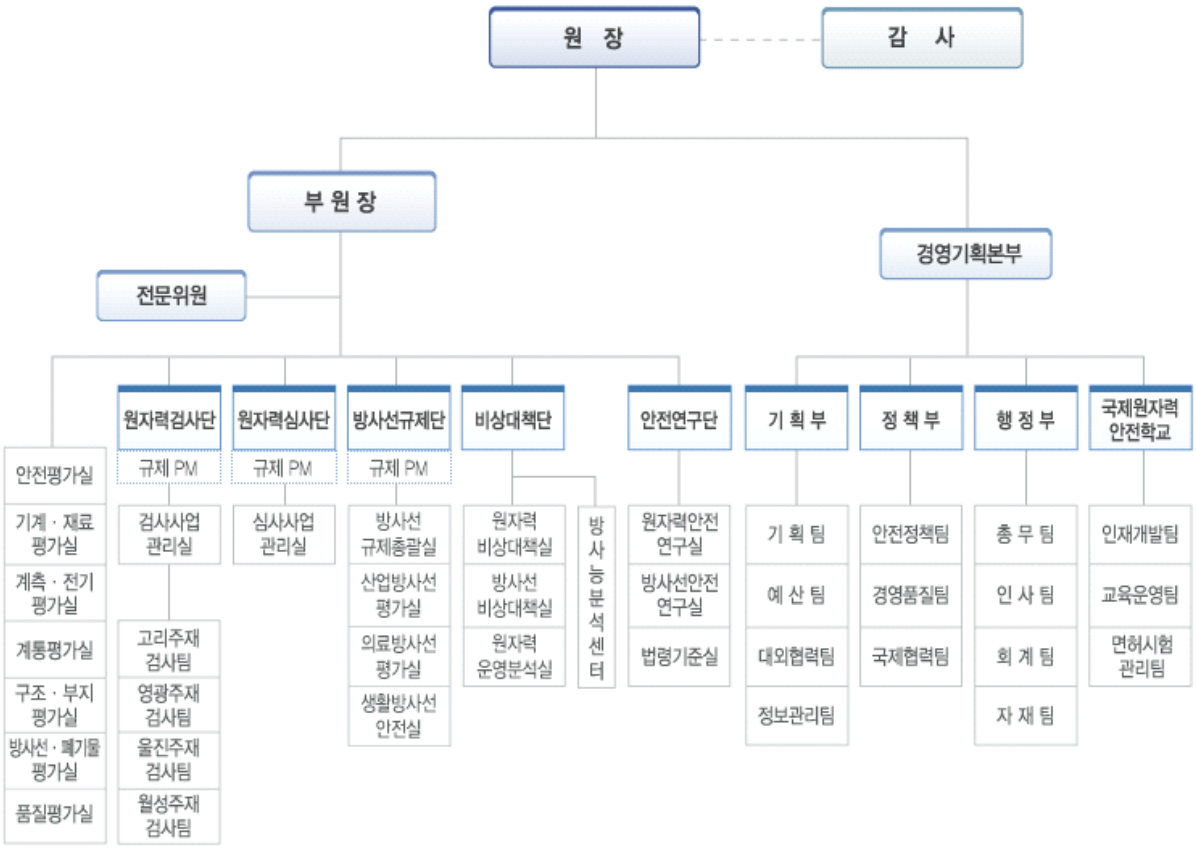
자료: 한국원자력연구원 홈페이지

9. 한국원자력안전기술원 (KINS)

우리나라 원자력과 방사선의 생산과 이용에 따른 방사선 재해로부터 국민의 건강과 국토환경을 보전하기 위해 설립된 원자력안전규제전문기관이다.

원자력발전소의 경우 부지적합성 및 설계·건설·운영의 안전성, 환경영향 들을 종합적으로 평가·심사하고 있으며 원자력 시설에 대해 건설에서부터 운영에서 폐기에 이르기까지 허가된 사항의 이행여부를 점검·확인하고 우리나라 실정에 적합한 각종 안전기준을 개발하여 국내원자력시설규제에 적용하고 있다. 또한 방사성동위원소 및 방사선발생장치의 사용허가심사, 시설·운반·포장 등에 대한 검사 원자력안전규제기술 연구 및 개발, 자격면허시험관리 등의 업무를 수행중이다.

[그림 4－10] 한국원자력안전기술원 조직도



자료: 한국원자력안전기술원 홈페이지

10. 국방기술품질원 (DTAQ)

국방기술품질원은 우수 군수품 획들을 위해 품질보증 및 품질경영 업무를 수행하고, 국방과학기술의 조사·분석·평가 및 정보관리를 체계적으로 수행하고 있다. 국방품질경영과 국방기술기획 활동을 통해 우리나라의 국방체제를 미래 안보환경에 발맞추어 발전시키고, 군이 추구하는 첨단 정보화과학군 건설에도 핵심적인 역할을 수행중이다.

아울러 국방 예산절감을 위해 방위력 개선사업 분석 및 지원, 국방연구개발사업 평가 업무를 담당하고 있으며, 국내 방위산업 제품의 수출경쟁력을 강화하기 위한 국산화개발 사업, 국방마크 인증제도 운영, 국제품질보증협력 등 다양한 업무를 수행하고 있다.

[그림 4-11] 국방기술품질원 조직도

자료: 국방기술품질원 홈페이지

제3절 분야별 시험·평가·인증 현황

1. 일반 분야

일부 분야를 제외하고는 각 분야별 국제 표준을 따르는 상황이다. 주요산업별로 국제 표준이 존재하는 경우 공공차원에서 별도의 새로운 표준을 만들 필요는 없다고 판단된다. 하지만 국제 표준이 없는 특정 시스템(예. 정보시스템 중 관제시스템)의 경우, 관련 표준 등을 활용하여 어느 정도의 표준과 가이드가 필요하다.

최근 국내에서도 주요 산업 도메인별로 국제 표준을 도입하여 적용하려는 노력이 진행 중이다. 학계/국가기관 이나 산업도메인별 선도 업체를 중심으로 소프트웨어 안전 표준이 국내 장착 될 수 있도록 국제 표준의 국내 현황을 반영한 상세 수행 가이드 제정 등의 노력이 필요하다.

국내의 경우 여러 분야 중 국내 공공기관 납품 소프트웨어의 경우 소프트웨어산업 진흥법에 근거하여 소프트웨어산업 발전의 기반을 조성하고 국산 소프트웨어 품질 경쟁력 강화를 위해 품질인(GS 인증) 제도를 시행하고 있다.

소프트웨어 산업 진흥법 제13조에 의거, 공공기관에 납품하는 소프트웨어를 대상으로 GS인증제도를 운영 중이다. 2001년부터 제도를 시행하였으며 ISO/IEC 9126,25051 등 국제 표준에 근거하여 품질특성별 결함을 확인하고 인증을 부여한다. 현재 인증기관은 한국정보통신기술협회(2000년)와 한국산업기술시험원(2008년) 이다. 인증 과정에서 품질 평가모델을 기반으로 제품의 기능성, 사용성, 신뢰성, 효율성, 상호운용성, 표준적합성, 성능 등을 평가하고, 발견된 결함에 대해서는 업체가 수정 후 재평가가 가능하다. 이러한 과정을 통해 소프트웨어 제품의 품질 향상을 유도한다.

GS인증 획득 시 조달청 제3자 단가계약 체결, 우선구매 제도, 성능보험 제도 등의 제도 혜택을 받을 수 있으며, 제품에 대한 신뢰도 향상 및 국내외 시장 개척 등의 효과를 얻을 수 있다.

1) 한국정보통신기술협회 - 소프트웨어시험인증연구소

(1) 확인 및 검증(Verification & Validation) 시험

o 개요

소프트웨어의 기능, 성능, 보안성, 안전성 등에 대해 신청업체(기관)의 요구사항에 따라 시험 후 시험결과서를 제공한다.

o 시험 대상

- 패키지, 모바일, 임베디드, 컴포넌트, 게임, GIS, e-Biz, e-Learning, 주문형(SI) SW, 운영체제, 디지털콘텐츠, 보안용 SW, 웹관리 도구, SW개발도구, 유틸리티, 홈네트워크, 스토리지, 바이오메트릭스, 교육용SW 등 소프트웨어 전 분야

o 시험 방법

- 시험신청기관의 요구사항에 따른 기능 및 성능 시험
- 과제계획서를 기반으로한 시험항목 도출 및 시험

o 시험 수행

- 시험 수행 : TTA는 시험대상 제품을 수령하여 신청기관과 합의한 요구사항에 기반하여 시험을 수행
- 과제 검증 시험 수행 : TTA는 시험대상 제품을 수령하여 과제계획서를 기반으로 시험항목을 도출하여 시험을 수행

o 시험 절차

[그림 4-12] TTA 확인·검증 시험 업무 절차

자료: 한국정보통신기술협회 홈페이지

(2) 시스템안전성 진단 및 컨설팅

o 개요

국가기간시설, 정보통신기반시설 등 국민 안전과 관련된 시스템 및 소프트웨어의 안전성 진단과 컨설팅을 통해 국민 안전 확보 및 재난 예방에 기여한다.

o 진단 및 컨설팅 대상

- 철도, 항공, 에너지 등 국민 안전과 관련된 시설에서 사용되는 시스템 및 소프트웨어
- 열차, 항공 등의 통합관제시스템
- 댐, 수자원관리시스템
- 재난전파경보시스템 등

IEC 61508, ISO/IEC 9126 등 시스템 안전 및 소프트웨어 품질에 관한 국제표준을 기반으로 안전성 진단을 수행한다.

- 시스템 위험, 품질, 시스템 구조 등의 측면에서 안전성 진단 및 개선방안 컨설팅
- 시스템 위험원 분석 및 안전기능 진단
- 소스코드 품질 및 기능 동작 정확성 진단
- 운영 및 유지보수 품질 진단
- 시스템 구조, 성능 및 장애 대비 안전성 진단 등

(3) GS시험・인증 (1등급)

o 개요

- 소프트웨어산업진흥법 제13조에 의거한 소프트웨어의 품질 인증

o 시험 대상

- 패키지, 모바일, 임베디드, 컴포넌트, 게임, GIS, e-Biz, e-Learning, 주문형(SI) SW, 운영체제, 디지털콘텐츠, 보안용SW, 웹관리 도구, SW개발도구, 유틸리티, 홈네트워크, 스토리지, 바이오 메트릭스, 교육용SW 등 소프트웨어 전 분야

[그림 4－13] GS 시험・평가 대상

자료: 한국정보통신기술협회 홈페이지

o 시험방법

- ISO/IEC 9126, 25041, 25051 국제표준에 근거한 품질평가 모델을 기반으로 기능성, 사용성, 이식성, 효율성, 신뢰성, 유지보수성에 등에 대한 시험
- 결함 발견 시 결함리포트 및 보완 기회 제공 후 회귀시험
- SW유형별 테스트케이스 개발 및 적용
- 제품의 품질을 종합적으로 평가한 시험결과서 제공

[그림 4－14] GS 시험·평가 항목

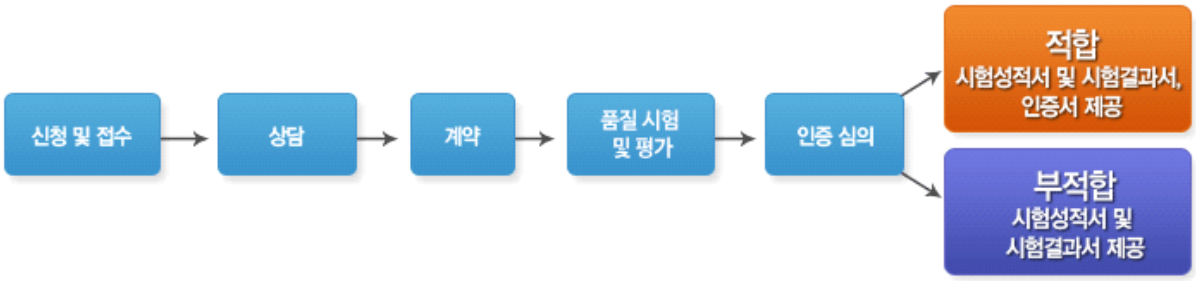
자료: 한국정보통신기술협회 홈페이지

o 시험 절차

TTA는 시험환경(HW, SW) 구축 및 제품 설치 후 계약 내용에 따라 시험을 수행한다. 시험환경 구축 및 제품 설치 시, 시험신청기관에게 지원을 요청할 수 있다.

- 제품 분석 및 설계
- 결함 보고
- 회귀시험
- 현장심사

[그림 4－15] GS 시험·평가 절차



자료: 한국정보통신기술협회 홈페이지

(4) GS시험·인증 (2등급)

o 개요

- 소프트웨어산업진흥법 제13조에 의거한 소프트웨어의 품질 인증
- 행정업무용 SW 선정제도가 GS인증 제도로 통합됨에 따라 기존 행정업무용 SW 적합성 시험이 GS인증 2등급으로 대체되어 제공
- 1등급이 2등급 보다 높은 인증의 등급

o 시험 대상

- 패키지, 모바일, 임베디드, 컴포넌트, 게임, GIS, e-Biz, e-Learning, 주문형(SI) SW, 운영체제, 디지털콘텐츠, 보안용SW, 웹관리 도구, SW개발도구, 유틸리티, 홈네트워크, 스토리지, 바이오 메트릭스, 교육용SW 등 소프트웨어 전 분야

o 시험 방법

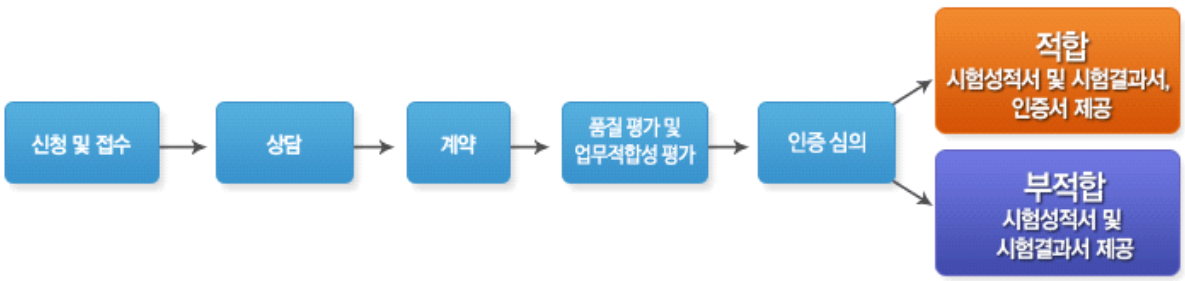
- 품질 시험: ISO/IEC 9126, 25051 국제표준을 기반으로 기능성, 사용성, 이식성, 효율성, 신뢰성, 유지보수성에 대한 SW품질시험
- 업무적합성 평가: 시험신청기관의 유지보수 및 운용지원, 교육훈련 지원, 업체신뢰성, 행정업무적합성에 대한 평가

o 시험 절차

TTA는 시험환경(HW, SW) 구축 및 제품 설치 후 계약 내용에 따라 시험을 수행한다. 시험환경 구축 및 제품 설치 시, 시험신청기관에게 지원을 요청할 수 있다.

- 제품 분석 및 설계
- 결함 보고
- 회귀시험
- 현장심사

[그림 4－16] GS(2등급) 시험·평가 절차



자료: 한국정보통신기술협회 홈페이지

2) 한국산업기술시험원

한국산업기술시험원은 전기전자분야, 정보통신분야, 레이저분야/배터리분야, 원자력기기분야, 신뢰성분야, 방폭분야, 에너지효율분야, 환경분야, 의료기기/용품분야, 소프트웨어분야, 기계설비분야, 재료분아, 기계류부품분야, 일반실험 총 15분야의 시험을 진행한다.

이 중 소프트웨어 신뢰성 관련 시험분야인 소프트웨어분야는 일반소프트웨어시험, 소프트웨어V&V 두 가지가 존재한다.

품질평가 분야는 유통업체납품 제품품질평가, 조달물품 전문기관 검사, 조달품적합시험, 고객의뢰 품질평가 총 4가지가 있으며, 소프트웨어 평가는 존재하지 않는다.

(1) 일반소프트웨어시험

o 소프트웨어 제품의 성능, 신뢰성 및 품질을 객관적으로 확인하기 위한 시험 평가

o 소프트웨어 제품의 성능, 신뢰성 및 품질을 객관적으로 시험, 평가하여 성적서 발행 및 ISO/IEC 17025에 의해 공인된 성적서를 발행하는 경우

o 시험 수험 목록

- 소프트웨어 성능시험
- 소프트웨어 품질시험
- 소프트웨어 신뢰성시험
- 소프트웨어 공인시험

[그림 4-17] 일반소프트웨어시험 업무 절차

자료: 한국산업기술시험원 홈페이지

o 대상품목

일반소프트웨어 분야 : 패키지, 임베디드, 시스템 소프트웨어 등 소프트웨어의 전분야

(2) 소프트웨어 V&V

소프트웨어 V&V(Verification & Validation)는 소프트웨어의 안전성, 신뢰성 및 품질을 확보하기 위한 Verification과 Validation을 말하며, 안전과 생명을 다루는 원자력 발전, 의료 철도, 플랜트산업 분야 등에 필요하다.

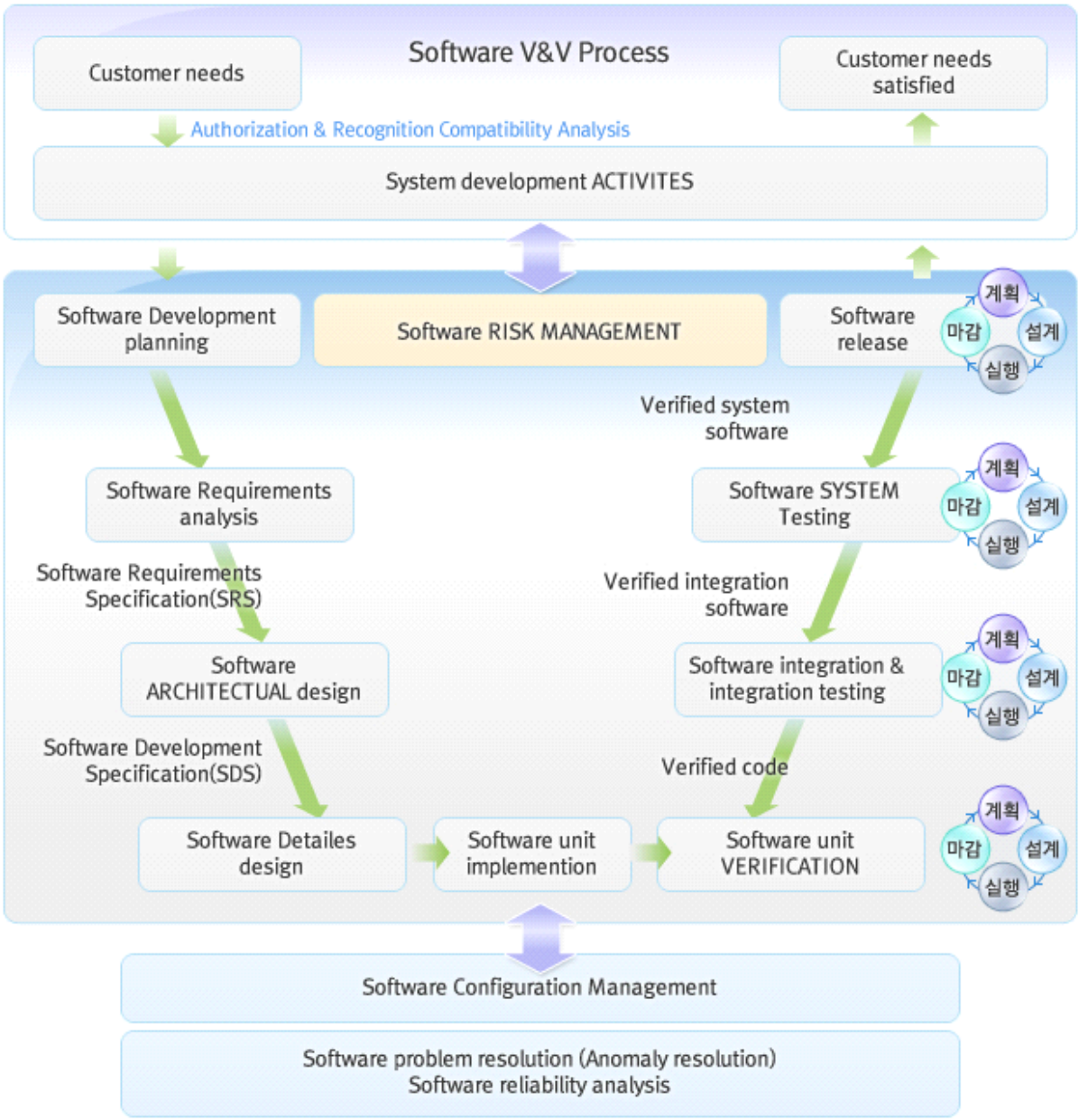
소프트웨어 V&V는 ‘특정 요구사항이 충족되었음을 객관적인 증거의 제공을 통하여 확인’하는 Verification과 ‘사용자의 요구 및 사용 목적에 일치함을 객관적으로 입증’하는 Validation을 말한다.

다음과 같은 소프트웨어 Life cycle 전반에 걸쳐 수행한다.

o 시험 수험 목록

- 소프트웨어 개발계획
- 소프트웨어 요구사항 분석
- 소프트웨어 아키텍쳐 설계
- 소프트웨어 (기본, 상세)설계
- 소프트웨어 구현(코딩)
- 단위, 통합, 시스템, 인수 테스팅
- 설치 및 점검, 운영
- 유지보수 및 재사용
- 형상관리, 결함관리
- 리스크 분석 등

[그림 4－18] 소프트웨어 V&V



자료: 한국산업기술시험원 홈페이지

[그림 4－19] 소프트웨어 V&V 업무 절차

자료: 한국산업기술시험원 홈페이지

o 대상품목

- 발전소 분야 : 원자력, 화력 등 발전소에 사용되는 소프트웨어
- 의료기기 분야 : 의료 통합시스템 및 의료기기에 사용되는 소프트웨어
- 철도 분야 : 철도차량 및 철도시스템에 사용되는 소프트웨어
- 산업플랜트 분야 : 산업현장, 플랜트등에 사용되는 소프트웨어

한국산업기술시험원에서 국내인증 분야는 K마크인증, 전기용품안전인증, 전자파적합등록/인증, 승강기인증, 방폭인증, 공산품안전인증, CC인증, GS인증, 신재생에너지인증, 친환경제품인증, 에너지효율인증, KS인증, KAS인증, 정보통신기기인증, 신뢰성평가인증 이렇게 총 15개 분야의 인증을 수행하고 있다.

이 중 소프트웨어와 관련된 품질 인증은 GS인증이다.

(3) GS인증

o 개요

o 관련법령

소프트웨어산업진흥법 제13조, 동법시행령 제9조, 10조 및 동법 시행규칙 제4조, 제6조

o 인증대상 제품

모든 분야에 대한 소프트웨어를 대상으로 함. (미래창조과학부 고시 제 2013-142호의 제3조)

다만 다음 각호의 경우에는 그 대상에서 제외한다.

1. 기술성 및 경제적 가치가 미흡한 단순기능 소프트웨어
2. 독자적인 환경에서만 운영되는 범용성이 없는 소프트웨어
3. 게임산업진흥에관한법률 제2조 1호, 1의2호에 따른 사행성 소프트웨어 4. 건전한 기업활동을 저해하는 위해성 소프트웨어

o 인증기준 및 방법

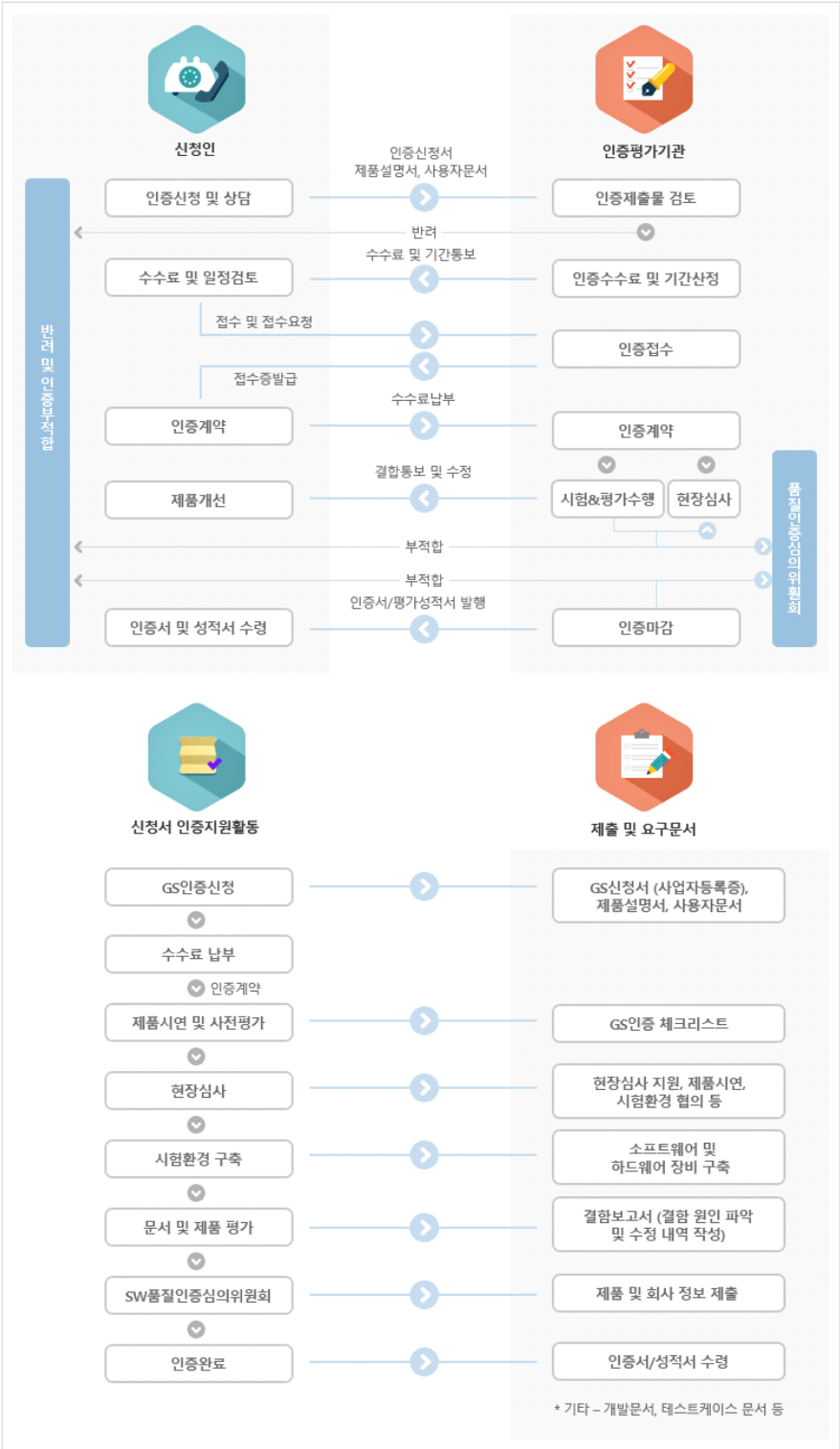
- ISO/IEC 25051 소프트웨어 제품 품질 요구사항 및 평가

- ISO/IEC 9126-2 소프트웨어 품질특성평가
- ISO/IEC 14598 소프트웨어 제품 품질측정 프로세스

[그림 4－20] 인증기준

자료: 한국산업기술시험원 홈페이지

[그림 4-21] GS평가/인증 프로세스



자료: 한국산업기술시험원 홈페이지

o GS인증지원 혜택

- 중소기업청 성능인증 신청 대상 가능 및 성능인증 적합성검사 면제(중소기업청, 2005.07.01)
- 조달청 “다수공급자 계약 적격성 평가 " 제외(조달청고시 2012-35, 2012.08.24)
- 조달청 우수 제품 등록 시 가점(조달청고시 2011-14, 2011.10.27)
- GS인증제품 우선구매 지원
- 중기청, GS이증제품 우선구매지원(중소기업제품 구매촉진 및 판로지원에 관한 법률 제2조)
- GS인증 획득 제품 우선구매 및 성능보험제도 도입(중기청 고시 2010-29, 2010.09.02)
- 전자정부 기술제안서(RFP) 기술평가 시 가산점 부여(행안부 고시 2009-40, 2009.08.28)
- 병역특례지정 업체 지정 심사시 가산점 부여 등(2005.07.01)
- 신SW상품대상 수상작 GS인증 의무화

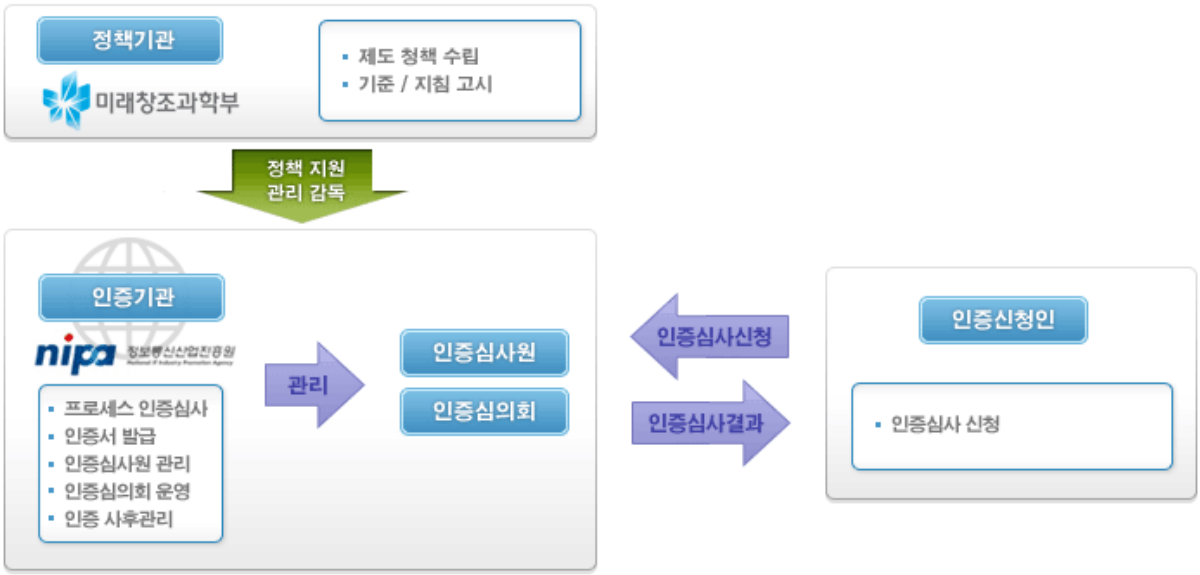
3) 소프트웨어 공학센터

(1) SP인증 (SW프로세스 품질인증)

o 개요

SW프로세스 품질인증(‘SP인증’)제도는 SW산업진흥법 제23조에 근거하여 국내SW기업의 SW사업 수행능력을 강화하고 SW사업의 부실방지를 목적으로 기업의 SW개발 단계별 작업절차 및 산출물 관리 역량 등을 분석하여 SW개발 프로세스 역량수준을 평가·인증하는 제도이다.

[그림 4－22] 소프트웨어 프로세스 품질인증 체계도



자료: 소프트웨어 공학센터 홈페이지

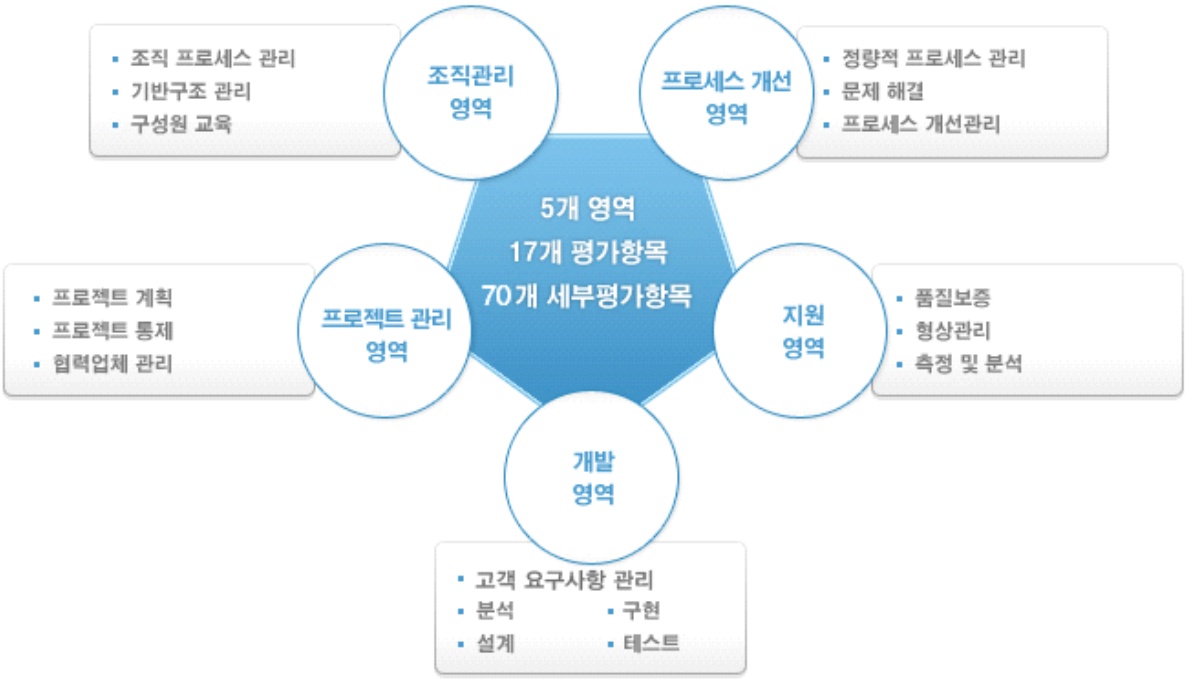
o 인증기준 및 등급

- 소프트웨어프로세스 품질인증 기준이란?

「소프트웨어프로세스 품질인증 기준」이란 소프트웨어 기업 및 개발 조직의 소프트웨어 프로세스 품질역량 수준을 심사할 때 활용하는 기준을 의미한다. 소프트웨어프로세스 품질인증 기준은 조직의 프로젝트 수행역량 강화를 위해 필요한 핵심 활동을 제시하고 있으며. 조직은 인증기준에서 제시하고 있는 핵심 활동의 수행을 통하여 프로세스 역량수준을 효과적으로 개선할 수 있다.

소프트웨어프로세스 품질인증 기준은 5개 영역, 17개 평가항목, 70개 세부평가항목으로 구성되어 있다.

[그림 4-23] 소프트웨어 프로세스 품질인증 기준의 구성



자료: 소프트웨어 공학센터 홈페이지

- 소프트웨어프로세스 품질인증 등급이란?

「소프트웨어프로세스 품질인증 등급」이란 인증신청 조직의 품질역량 수준을 심사한 결과를 의미하며, 해당 조직의 품질역량을 프로젝트에서 조직 차원으로 유도하기 위한 계층 구조로 되어 있다.

※ 인증등급은 2개 등급(2등급, 3등급)만 유효 수준을 효과적으로 개선할 수 있다.

[그림 4－24] 소프트웨어 프로세스 품질인증 등급

자료: 소프트웨어 공학센터 홈페이지

<표 4-2> 인증 등급 내용

인증 등급	내용
1등급	프로젝트의 성공 여부와 관계없이 특정 프로젝트를 수행할 수 있는 수준이나, 프로젝트 수행을 위한 기본적인 활동들이 안정적으로 수행되지 못해 품질, 비용, 납기 측면에서 기대되는 목표를 충족시키지 못할 확률이 높은 상태로 프로젝트 수행을 위한 프로세스 역량 개선이 필요한 수준
2등급	개별 프로젝트를 수행하기 위해 필요한 프로젝트 차원의 프로세스가 수립되고, 이를 기반으로 프로젝트를 통제하여 성공적으로 프로젝트를 수행할 수 있는 역량 수준
3등급	조직의 프로세스 체계를 정의하고 정량적인 데이터 관리를 통해 조직 차원의 프로세스를 개선하고 발생되는 문제의 근본 원인을 해결함으로써 일관된 품질수준의 프로젝트 수행이 가능하며, 지속적으로 프로세스를 개선할 수 있는 역량 수준

[그림 4－25] 소프트웨어 프로세스 품질인증 절차

자료: 소프트웨어 공학센터 홈페이지

o 사전진단 서비스

SP 인증획득에 관심 있는 기업을 대상으로 인증심사 준비내용 등을 진단하여 인증심사 준비를 효율적으로 할 수 있도록 지원한다.

원내소속 ‘SP 인증심사원 ’ 이 신청기업을 방문하여 인증제도 , 심사절차 설명 등 상담 서비스 한다.

2. 철도

철도시스템은 소프트웨어 오류와 같은 고장이 발생할 경우 인명 피해뿐만 아니라 사회·경제적으로 큰 문제가 발생할 수 있는 Safety-Critical System이다.

국내 철도제어시스템 분야도 도시철도, 고속철도 등이 상용화됨에 따라 소프트웨어에 기반을 둔 디지털 제어 시스템을 다수 적용하고 있는 추세이다. 또한 국제 규격에 의한 철도제어시스템 소프트웨어 안전성 검증이 요구되고 있는 상황이다.

하지만 국내 철도 분야는 이런 소프트웨어 기반 시스템의 신뢰성·품질·안전 확보를 위한 개발 기술 과 완성된 소프트웨어의 검증을 위한 체계가 미흡한 실정이다. 기계, 전기 전자식 철도제어시스템은 경험적, 물리적으로 안정성 확보가 가능하였으나 컴퓨터 및 소프트웨어를 이용한 철도제어시스템은 고장 원인을 찾고 안전성 평가 하기 어렵다.

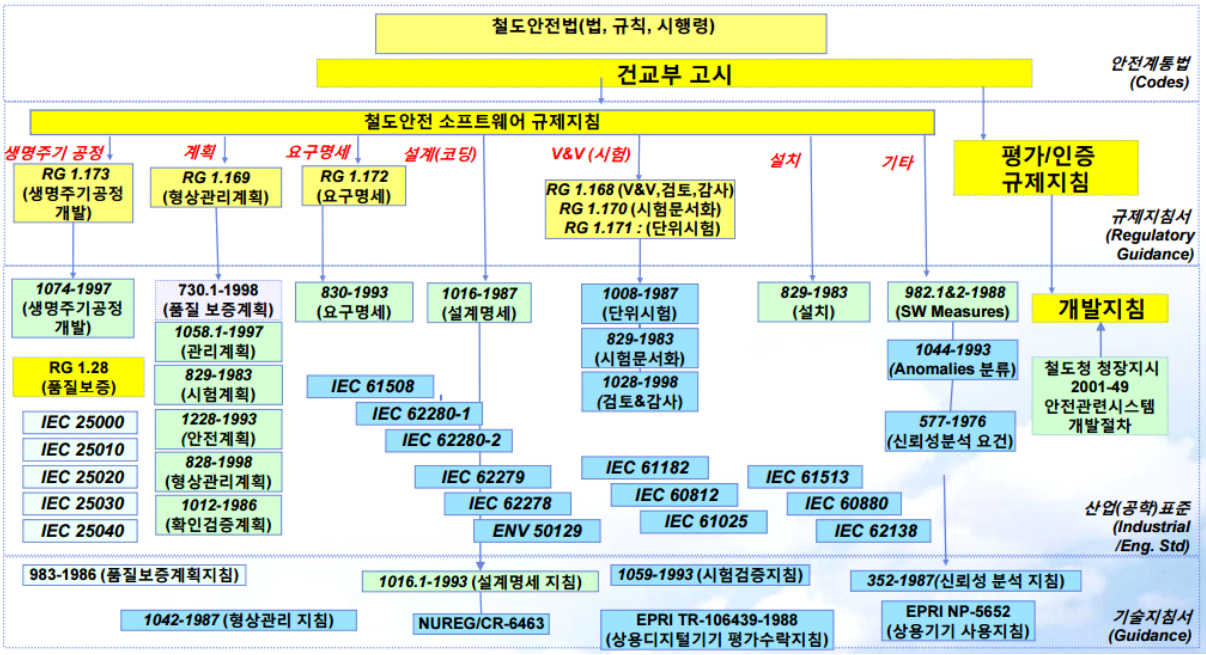
고 신뢰도 철도소프트웨어 안전기준 프로세스 확립을 위해서는 전체 프로세스를 구성하는 각 단계에서 사용되는 고 신뢴 소프트웨어 세부 기술들을 철도 산업에 알맞게 적용하고 수정하는 작업이 필수적이다. 현재까지 국내에서 적용된 기술들은 대부분 단편적으로 적용되고 있으면, 이러한 기술들만으로는 전반적인 신뢰성 및 안전성 향상을 기대하기 힘들다. 따라서 전반적인 개발 및 검증, 검사 체계를 확립하는 작업이 우선적으로 요구된다.

〈표 4-3〉 철도 소프트웨어 안전 기준 체계

철도 안전법	(법률) 철도 안전을 확보하기 위하여 필요한 사항을 규정하고 철도 안전관리체계를 확립함으로써 공공복리의 증진에 기여함을 목적으로 한다.
철도 안전법 시행령	(대통령령) 철도안전법에서 위임된 사항과 그 시행에 관하여 필요한 사항을 규정한다.
철도 안전법 시행규칙	(건설교통부령) 철도안전법 및 동법시행령에서 위임된 사항과 그 시행에 관하여 필요한 사항을 규정한다.
건설교통부 고시	(건교부고시) 기술적으로 특정한 규제요건과 규제지침을 규정한다.
안전기준체계 (산업표준, 상세기준) 기술 지침서	(표준 및 지침) 부품이나 장비의 설계, 테스트, 검증, 안전성/신뢰성 분석 등 기술적으로 구체적인 기준을 표준으로 규정하고 그 적용 및 해석을 위한 기술적 지침을 제공한다.

자료 :『안전 소프트웨어 국제표준 현황』, 이장수 한국원자력연구원 재구성

[그림 4－26] 자동차 기능안전 구성



자료 :『안전 소프트웨어 국제표준 현황』, 이장수 한국원자력연구원

1) 한국철도기술연구원

(1) KOLAS 공인 및 일반시험

한국철도기술연구원은 국제적으로 인정된 ISO 9001, ISO/IEC 17025 기준에 적합한 국제공인 시험기관으로서 2000년부터 KOLAS 공인시험기관으로 지정되어 역학(차량 및 시설), 전기, 화학분야의 다양한 시험항목을 인정받아 국제수준의 공인시험업무를 수행하고 있다.

o 시험 구분

- KOLAS 공인시험

KOLAS 공인시험은 KOLAS 인정기구로부터 인정받은 항목 또는 품목에 대하여 품질시스템과 절차서에 따라 수행하는 시험이다.

* KOLAS(Korea Laboratory Accreditation Scheme, 한국인정기구)

- 일반시험

일반시험은 일반철도용품의 품질을 확인하기 위해 수행하는 시험이다.

o 시험 분야

(2) 형식승인업무

한국철도기술연구원은 2014년 3월부터 철도안전법 제77조 제2항 및 동법 시행령 제63조 제2항에 의거 형식승인검사기관으로 지정되어 철도차량 및 용품의 형식승인, 제작자승인, 철도차량의 완성검사를 수행한다.

o 개요

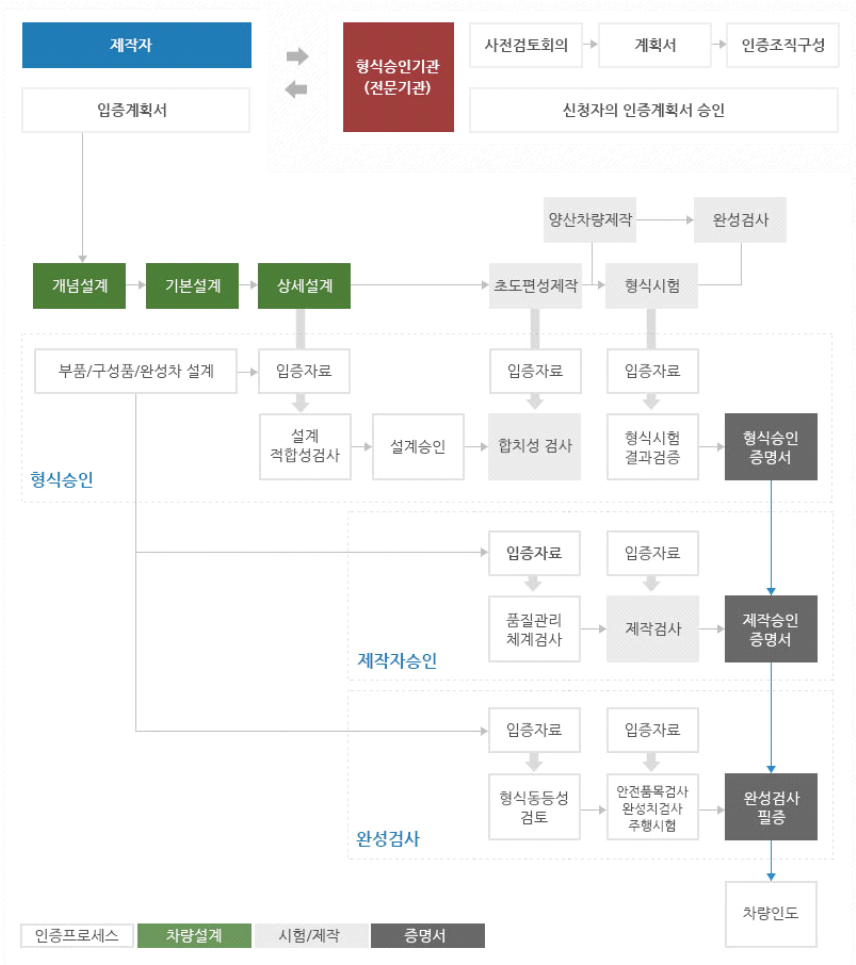
국내에서의 운행을 목적으로 제작·수입되는 철도차량과 용품은 철도안전법, 시행령, 시행규칙에 의거 형식승인을 받아야 하며, 설계단계에서의 형식승인, 제작단계에서의 제작사승인, 완성단계에서의 완성검사로 구분 한다.

o 관련 법규

o 업무 범위


설계단계
▪ 차량/용품 형식승인
- 설계 적합성 검사
- 합치성 검사
- 형식시험
제작단계
▪ 제작자
- 제작자 주도의 품질관리
▪ 검사기관
- 차량용품 제작자 승인(품질관리체계의 적합성 검사, 제작검사)
완성단계
▪ 완성검사(철도차량)
- 완성차량검사(안전품목검사, 완성차량 검사)
- 주행시험(예비주행 및 시운전 시험)
사후관리
- 안전 및 품질확인, 점검 제재수단 강화

o 절차


제작자
입증계획서
형식승인기관 (전문기관)
사전검토회의
계획서
인증조직구성
신청자의 인증계획서 승인
양산차량제작
완성검사
개념설계
기본설계
상세설계
초도편성제작
형식시험
부품/구성품/완성차 설계
입증자료
입증자료
입증자료
설계 적합성검사
설계승인
합치성 검사
형식시험 결과검증
형식승인 증명서
형식승인
입증자료
입증자료
품질관리 체계검사
제작검사
제작승인 증명서
제작자승인
입증자료
입증자료
형식동등성 검토
안전품목검사 완성치검사 주행시험
완성검사 필증
완성검사
차량인도
인증프로세스
차량설계
시험/제작
증명서

(3) 제품 인증

제품이 규정된 요구사항에 적합함을 입증하는 평가 제공 및 제3자(인증기관)가 증명하는 것이다. 소비자, 규제당국, 업계 및 기타 이해당사자들에게 제품에 대한 신뢰를 제공하는 적합성평가 활동을 수행한다.

국가적, 지역적, 국제적 차원에서 제품의 무역, 시장접근, 공정경쟁 및 소비자의 수용 촉진 한다.

o 법적 근거

- 국가표준기본법 제21조(적합성평가체제의 구축)
- 국가기술표준원고시(제2014-800호) 제품인증기관 인정 및 사후관리 등에 관한 요령

o 국제 표준

- SO/IEC 17000 Conformity assessment
- Vocabulary and general principles
- ISO/IEC 17065 Conformity assessment
- Requirements for bodies certifying products, processes and services
- ISO/IEC 17067 Conformity assessment
- Fundamentals of product certification and guidelines for product certification schemes
- 국제인정기구협의(IAF)에서 정한 국제 표준 또는 가이드 등

o 인증 범위

인증분야 (한국표준산업분류(KSIC))

	대분류		중분류		소분류		세부 분류	
C 제조업	31	기타 운송장비 제조업	312	철도장비 제조업	3120	철도장비 제조업	31201	기관차 및 기타 철도차량 제조업
							31202	철도차량 관련 부품 및 관련 장치 물 제조업체

o 인증 대상 : 철도 용품

o 인증 유형 : (ISO/IEC 17067)

유형	대상	인증 활동
Type 1a	하나 또는 그 이상의 제품 샘플	▪ I 선택(계획, 준비, 요구사항, 샘플링 포함) ▪ II 시험·검사 등을 통한 특성 결정 ▪ III 검토 ▪ IV 인증 결정 ▪ V 인증서 발행
Type 1b	제품의 전체 배취(Batch)	▪ I 선택(계획, 준비, 요구사항, 샘플링 포함) ▪ II 시험·검사를 통한 특성 결정 ▪ III 검토(평가) ▪ IV 인증 결정 ▪ V 인증서 발행

o 인증 기준

- IEC 62425 Railway applications
- Communication, signalling and processing systems
- Safety related electronic systems for signalling
- IEC 62278 Railway applications
- Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
- IEC 62279 Railway applications
- Communication, signalling and processing systems
- Safety related electronic systems for signalling
- IEC 62280 Railway applications
- Communication, signalling and processing systems
- Safety related communication in transmission systems

3. 원자력

원전 안전에 중요한 보호, 제어, 감시 시스템 등이 기존의 아날로그 방식에서 디지털 방식으로 전환됨에 따라 소프트웨어의 안전성 확보가 원전 계측제어의 핵심으로 부상한 가운데, 이번 회의를 통해 IAEA 회원국 간 기술 정보 교류 및 IAEA 원전 안전 소프트웨어 지침 개정에 대한 논의가 이뤄진다.

국내의 경우, 영광 3,4호기의 일부 안전관련 계측제어계통을 디지털-기반계통으로 설계되었다. 이후 울진 3,4호기와 영광 5,6호기의 일부 제어기능을 PCS기반의 디지털 설비로 채택하는 등 점차 디지털 기반 제어 적용이 증가하고 있다. 따라서 차세대 원전의 경우에는 주요 안전관련 계측제어계통설계에 소프트웨어를 기반으로 하는 디지털 기술이 응용되고 있다.

원자로 안전계통에서 문제가 발생할 경우, 그로인해 발생할 경제적, 산업적 파장은 막대하다. 따라서 원자로 제어를 위한 기능을 소프트웨어로 구현할 경우, 그 소프트웨어가 허용 가능한 개발 계획에 따라 개발되었는지, 수명 주기는 어떠한지, 결과물은 어떤 식으로 구현되었는지 반드시 검증하여야 한다. 이를 위해 소프트웨어 개발 단계에서 국제표준, 개발 규정 및 개발 지침에 의한 체계적인 품질관리가 필수적이다.

디지털 계측제어계통 소프트웨어 설계 및 검증과 관련된 규제기술개발을 위한 주요 법규, 규제 지침에 관련된 내용은 다음과 같다.

o 교육과학기술부, 원자로시설 등의 기술기준에 관한 규칙

제1조(목적) : 이 기준은 「원자로시설 등의 기술기준에 관한 규칙」 제67조 제2항의 규정에 의한 품질보증에 관한 세부요건을 정함을 목적으로 한다.

제2조(적용범위) : 이 기준은 「원자력법」 제11조 제2항・제21조 제2항・제33조 제2항 및 제43조 제3항의 규정에 의한 발전용원자로설치자・발전용원자로운영자・연구용원자로설치자・연구용원자로운영자 및 핵연료주기사업자(이하 “원자력관계사업자”라 한다)가 작성・제출하는 품질보증계획에 대하여 적용한다.

제3조(세부요건) : 「원자로시설 등의 기술기준에 관한 규칙」 제68조 내지 제85조에 대한 세부요건은 사업의 단계별로 다음 각 호와 같이 적용한다.

1. 발전용원자로 건설 : 「교육과학기술부고시 제2008-14호(전력산업기술기준의원자

로시설 기술기준 적용에 관한 지침 고시)」로 적용을 고시한 전력산업기술기준(KEPIC)의 원자력품질보증기준(QAP) 또는 이와 동등한 기준

2. 발전용원자로 운영 : 「교육과학기술부고시 제2008-14호(전력산업기술기준의 원자로시설 기술기준 적용에 관한 지침 고시)」로 적용을 고시한 전력산업기술기준(KEPIC)의 원자력품질보증기준(QAP) 또는 이와 동등한 기준 및 ANSI/ANS3.2 Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plants, 1994 Edition
3. 연구용원자로의 건설 및 운영 : ANSI/ANS 15.8 Quality Assurance Program Requirements for Research Reactors, 1995 Edition

제4조(적용방법) : 이 기준의 적용방법은 「교육과학기술부고시 제2008-14호(전력산업기술기준의 원자로시설 기술기준 적용에 관한 지침 고시)」제4조와 같다.

1) 한국원자력연구원

한국원자력연구원은 차세대원자로개발, 선진핵연료개발, 핵연료주기기술개발, 연구용원자로 '하나로', 원자력산업기술개발, 방사선융합기술개발, 원자력안전연구, 미래형신기술개발, 원자력정책등의 업무를 수행중이다.

이 중 원자력안전연구 부분에서 소프트웨어 안전 관련 업무를 수행중이다. 안전해석 코드 개발 및 응용, 계통 및 기기의 실증실험, 원전 내부검사용 로봇시스템 개발 등 원자력 시설의 안전 확보를 위한 연구를 진행한다.

계측제어 및 안전성평가를 위해 경보원인 추적 시스템, 원전디지털 안정등급 제어기기, 터빈사이클 이용 성능분석진단 프로그램 개발, 통합 경보진단운전지원시스템, 가상 중대사고 모의 및 훈련도우미 개발, 국내 고유 신뢰도 데이터베이스, 디지털 계측제어 리스크 분석 기술, 사용 후 핵연료 운반 및 저장시설 확률론적 운영안전성 평가 연구 등이 있다.

디지털 계측제어 리스크 분석 기술을 살펴보면 소프트웨어의 신뢰도를 측정하기 위한 기술들을 다루고 있다.

o 디지털 고유 특성별 신뢰도 평가 방법론 개발

- 고장검출범위 정량화 기법 개발
- SW 신뢰도 평가를 위한 BBN 모델 개발
- 디지털 기기 신뢰도 비교 분석
- 안전필수 통신망 신뢰도 평가 기법 개발
- 조건부 인간오류 분석 기법 개발
- 디지털 기기 공통원인고장 평가 방법론

o 디지털 안전계통 상세 신뢰도 분석 모델 개발

- DPPS (디지털 발전소 보호계통)
- DESFAS (디지털 공학적 안전설비 작동계통)
- ESF-CCS (공공적안전설비 기기제어계통)

o 디지털 위험도 영향 평가 모델 개발

- 디지털 안전계통의 원전 위험도 영향 평가 모델 개발
- 디지털 I&C PSA 모델 연계 및 통합 기술 개발

4. 의료

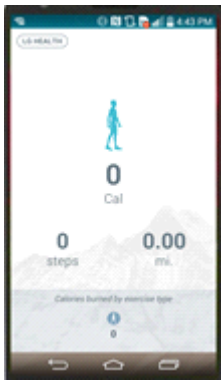
의료기기 소프트웨어는 의료기기의 성능을 발휘하기 위한 핵심 부분이다. 사람을 대상으로 사용하는 기기의 특성상 소프트웨어의 사소한 변경이나 오류가 심각한 결과를 초래할 수 있다.

현대 의료기기는 환자측정데이터는 수집・저장・관리・분석・전송 등의 기능을 하므로 보완상 안전관리 강화 필요성이 커지고 있다. 최근 IT 기술 발전으로 웨어러블 기기등 다양한 형태의 의료기기가 나오고 있어, 의료기기 소프트웨어 안전이 중요하다.

의료기기 소프트웨어란 의료기기에 해당하는 목적으로 사용하기 위해 개발된 소프트웨어 시스템으로 독립형 소프트웨어와 내장형 소프트웨어, 모바일 의료 앱 등을 말한다.

- 독립형 소프트웨어: 소프트웨어 그 자체로서 의료기기의 사용목적에 부합하는 기능을 가지며, 범용 컴퓨터와 동등 환경에서 운영되는 의료기기 소프트웨어
- 내장형 소프트웨어: 별도의 의료기기 시스템에 내장되어 운영되는 소프트웨어

[그림 4－27] 독립형 소프트웨어의 예



자료 : 식품의약품안전처 식품의약품안전평가원 의료기기심사부 『의료기기 소프트웨어 허가・심사 가이드라인』

[그림 4－28] 내장형 소프트웨어의 예

자료 : 식품의약품안전처 식품의약품안전평가원 의료기기심사부 『의료기기 소프트웨어 허가·심사 가이드라인』

국내는 『의료기기의 전기기계적 안전에 관한 공통기준 규격』에 따라 등급별 적용 중이다. 등급별 적용시기는 4등급(15년 1월 1일), 3등급(15년 7월 1일), 2등급(16년 1월 1일), 1등급(16년 7월 1일)이다

국제 표준인 IEC-60601-1 3rd 의무적용시기는 미국(14년 1월 1일), EU 및 캐나나(12년 6월), 일본(17년 6월) 이다.

o 국내 의료기기 소프트웨어 안전 가이드

- 의료용 소프트웨어 심사 가이드라인, 식품의약품안전청 의료기기본부
- 의료용 소프트웨어 특성평가 가이드라인, 식품의약품안전청 의료기기본부
- 의료기기 소프트웨어 밸리데이션 가이드라인(Guidelines for Software Validation of Medical devices), 식품의약품안전청 의료기기본부 의료기기 품질팀

<표 4-4> 현행 의료기기 소프트웨어 관련 기술문서 작성 및 첨부자료

모양 및 구조	소프트웨어에 대한 구조 또는 알고리즘, 주요기능 등
원자재	소프트웨어의 모델명 또는 명칭, 버전, 운영환경 등
사용방법	프로그램의 주요기능을 확인할 수 있는 화면 사진을 포함한 그 기능에 대한 사용방법
시험규격	소프트웨어의 주요기능을 확인할 수 있는 시험규격
첨부자료	- 모델명 또는 명칭, 버전, 운영환경, 구조 등 확인자료(소프트웨어 요구사항명세서, 개발명세서, 사용자설명서, 제품안내서 등) - 성능에 관한 자료 : 검증 및 유효성 확인 자료

자료: 『의료기기 소프트웨어 안전관리』, 식품의약품안전처

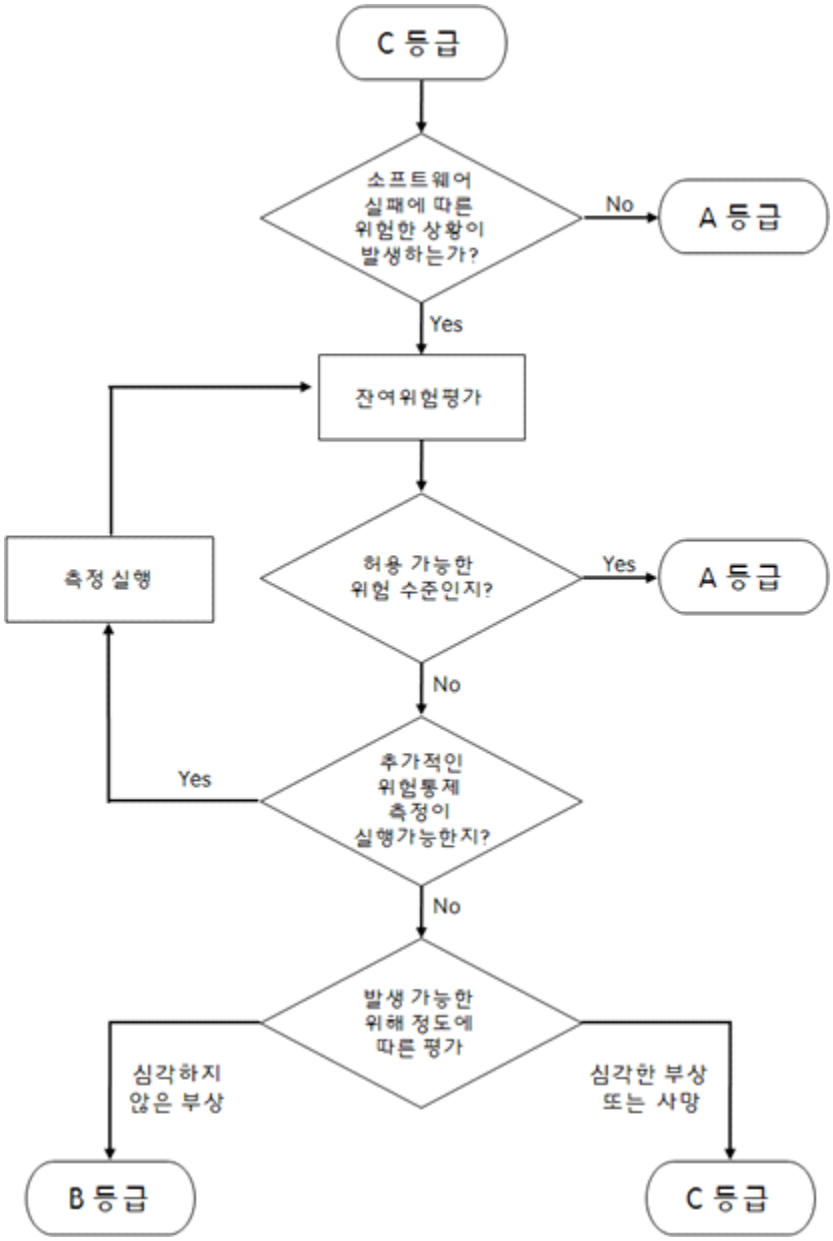
o 의료기기 소프트웨어 심사의 적용 범위

- 내장형 소프트웨어(예: 초음파영상진단장치 등) 및 모바일 의료용 앱을 포함하여 소프트웨어 자체가 의료기기인 독립형 소프트웨어(예: 의료영상전송장치소프트웨어 등)에 적용
- 또한, 의료기기 내에서 사용되는 상용소프트웨어(SOUP, Software of Unknown Provenance)를 포함
- 단, 별도 표시기능이나 사용자 화면 없이 의료기기 제어를 수행하는 펌웨어 수준의 소프트웨어, 의료기기 제조 및 개발을 위해 사용되는 소프트웨어, 구매 및 관리 프로그램 등 의료기기 품질관리를 위해 사용되는 소프트웨어는 본가이드라인의 적용범위에서 제외

의료기기 소프트웨어의 고장, 설계 결함 또는 사용 시 발생할 수 있는 잠재적 결함으로부터 환자, 사용자 또는 기타 사람에게 영향을 끼칠 수 있는 위해(harm)의 정도에 따라 소프트웨어의 안전성 등급을 결정한다.

안전성 등급은 A등급(부상이나 신체적 피해가 발생할 가능성이 없음), B등급(심각하지 않은 부상(경상)이 발생할 가능성이 있음, C등급(심각한 부상 또는 사망이 발생할 가능성이 있음) 으로 나뉜다.

[그림 4－29] 의료기기 소프트웨어 안전성 등급판단 절차



자료 : 식품의약품안전처 식품의약품안전평가원 의료기기심사부 『의료기기 소프트웨어 허가·심사 가이드라인』

5. 자동차

자동차에서 전장품과 소프트웨어 비중이 높아지면서 소프트웨어 설계와 기능 안전 확보가 중요한 문제로 떠올랐다. 엔진이나 제동장치를 직접 제어하는 전자제어장치(ECU)에서 소프트웨어 오류가 발생한다면 치명적인 사고로 이어질 수 있다. 특히 하이브리드카 같은 최신 기능을 탑재한 차량일 경우, 일반 차량보다 소프트웨어 비중이 더욱 많으므로 이런 오류에 대한 위험성은 점점 더 커질 것이다.

자동차는 다른 분야와는 다르게 민간 영역이라는 특수성이 있어 소프트웨어안전에 대한 기능안전성 평가들은 주로 민간 사업자 주도하에 진행된다.

자동차 및 자동차 부품을 생산·판매 하는 민간사업자들은 해외 판매를 위해서 자연스럽게 안전 인증 작업을 해야만 하는 상황이다.

최근 유럽 및 여러 다른 국가에 자동차 및 자동차 부품 수출·판매 하기 위해서는 해당 국가의 기준에 따른 안전 승인이 필수적이다. 유럽의 경우 개별 국가가 아닌 유럽 전체를 통용하는 인증 시스템이 있다.

국내의 경우 최근까지 이러한 인증 및 인증을 위한 컨설팅 작업에 대한 노하우가 부족해 외국 안전 컬설팅 업체에 의존하고 있었다.

그러나 2015년 산업통산자원부 국가기술표준원은 ‘국가기간산업 기능안전 컨소시업’ 협약식을 개최하였고 한국산업기술시험원, 한국철도기술연구원, 자동차부품연구원 등이 참여하여 자동차 및 철도의 기능 안전 기업지원 서비스를 제공하기로 하였다.

이를 통해 그간 글로벌 인증기관이 장악하고 있는 기능안전분야 시험 평가를 국내기관이 수행해 시험평가 비용절감, 기술유출방지, 국내기업 수출지원 등의 효과를 볼 수 있게 되었다.

1) 한국산업기술시험원

한국산업기술시험은 ISO 26262제정 Working Group 한국 대표 기관으로 IT/소프트웨어 시험·평가·인증사업(Test·Evaluation & Certification for IT/Software) 으로 아래와 같은 업무를 수행 중이다.

(1) 기능 안전성 (Functional Safety)

o 관련 표준

- IEC 61508 Ed.2.0: Functional Safety of electrical/electronic/programmable electronic safety - relate systems

o 적용 분야 : 프로세스(공장, Oil, Gas), 기계류, 원자력 발전소, 수송 시스템

o 대상 시스템 : 안전 기능을 수행하는 전기/전자/프로그래밍 가능한 전자 시스템

o 목적 : 인명 피해, 환경 피해, 산업 재산에 대한 불합리한 수준의 리스크 제거

o 적용 단계 : 전 라이프사이클 단계에 적용 (설계/시험/구축/운용/패기)

o 제공서비스

- 기능안전 인증 획득 지원
- 기능안전 R&D 프로세스 구축 지원
- 교육 (In-house 교육 포함)
- 기능안전요건 만족을 위한 소프트웨어 시험 서비스 (KOLAS 국제 공인 성적서 발행)
- 시스템 구조 평가 (Safe Failure Fraction, Hardware Fault Tolerance 분석 등)

(2) 자동차 기능 안전성 (Road Vehicle - Functional Safety)

o 관련표준

- ISO 26262: 2011 Road Vehicles - Functional Safety

[그림 4－30] 자동차 기능안전 구성

자료: 한국산업기술시험원 홈페이지

o 제공 서비스

- 자동차 기능안전 (Road Vehicle - Functional Safety) 컨설팅
- 기능안전 프로세스 구축 지원 (OEM side, Supplier side)
- Automotive SPICE와 연계 구축 지원
- 기능안전 교육 (In-house 교육 및 정규 교육)
- 엔진구동 / 샤시 / 전장 분야 전자 제어기의 개발 지원 (기능안정성 분야)
- 자동차 기능안전 심사 (Audit), 3자 평가 (Assessment)
- 기능안전 요건 만족을 위한 Software 시험 서비스 (국제 공인 성적서 발행)
- Hardware Architecture 평가 (Hardware Architecture Metrics, PMHF 등) 서비스
- Hazard Analysis and Risk Assessment 서비스

2) 자동차부품연구원

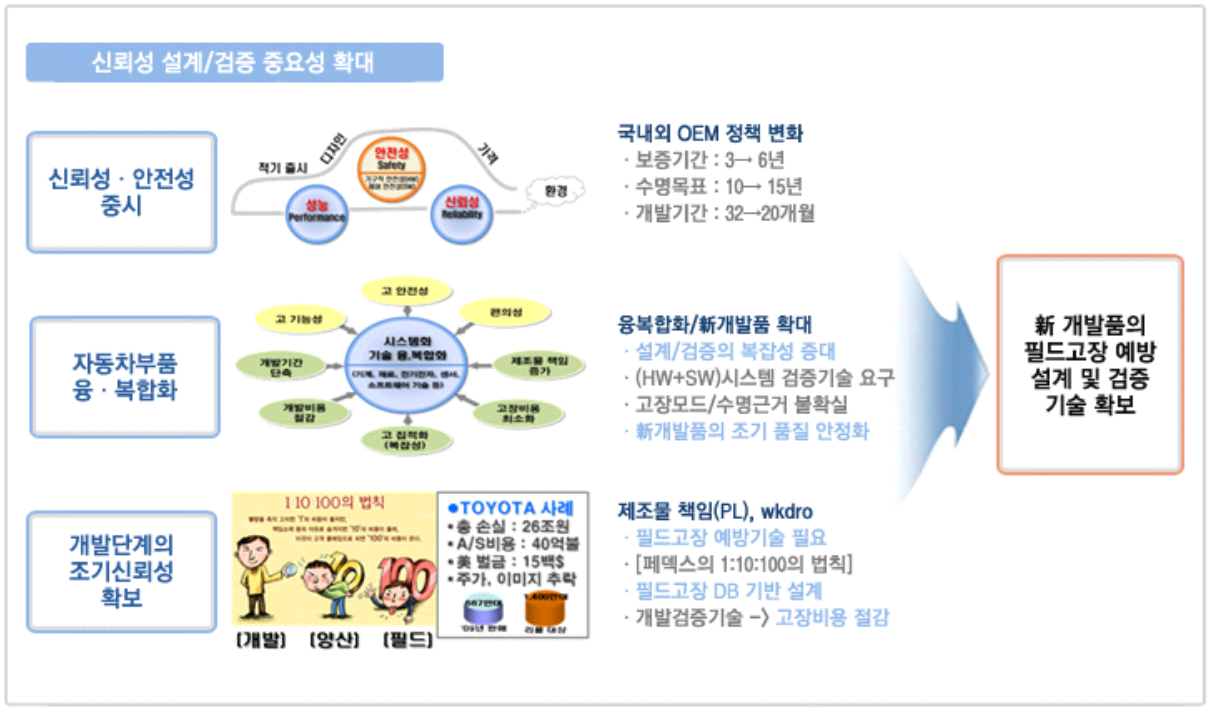
자동차 부품연구원은 크게 7개의 연구 본부(그린파워 시스템 연구본부, 자동차 융합 부품 기술 연구본부, 스마트 자동차 기술 연구본부, 지능형 차체 섀시 연구본부, 자동차 친환경 신소재 기술 연구 본부, 자동차 소재 융합 시스템 연구본부)로 구성되어 있고, 이 중 신뢰성 연구본부에서 자동차 분야의 신뢰성 평가인증, 전자파 시험 등 공인 시험기관 업무 수행과 차량의 극한기술 연구, 융합시스템 연구를 통한 안전기술 개발 업무 등을 수행한다.

신뢰성 연구본부의 신뢰성연구센터는 산업통상자원부가 지정한 국내 유일의 자동차 부품 분야의 전문 신뢰성 연구센터로서, 자동차 분야에서 요구되는 총체적인 신뢰성 기술지원은 물론, 연구개발 단계에서의 신뢰성 기술접목을 통해 자동차 부품의 신뢰성 문제해결 및 신뢰성 향상을 위한 연구를 하고 있다.

센터 주요 업무로는 수명예측 및 가속시험법 개발, 가속스트레스 시험, 필드 고장재현 및 고장메커니즘 분석, 실차기반 환경/내구 신뢰성 평가 기술개발, 그린카부품 신뢰성 평가 등이다.

자동차 부품의 융·복합화로 인한 신뢰성 설계/검증의 중요성이 커지고 있고, HW+SW시스템 검증기술 요구 되어있다. 이에 신 개발품의 필드고장 예방설계 및 검증 기술 확보에 관한 연구를 진행 중이다.

[그림 4-31] 신 개발품의 필드 고장 예방설계 및 검증기술 연구



자료: 자동차부품연구원 홈페이지

또한 자동차부품 연구시험장비 공동이용고객지원시스템을 개설하여 자동차 부품의 시험분석을 진행 중이다.

시험분석분야는 측정, 소음/진동/ 환경시험, 부식시험, 전지전자, 부품시험, 전자파, 기기분석, 연비 및 배출가스, 엔진출력, 주행시험, 냉각 및 공조시험, 타이어효율등급, CNG부품시험, 블랙박스성능시험 이 있고, 이 중 소프트웨어 안전 분야 시험은 주로 전기전자 분야에서 이루어진다.

전기전자 분야는 총 41개의 항목을 시험한다. 대부분 전기전자 제어 부품들의 수명, 성능 위주의 시험을 하고 소프트웨어 특화 시험분야로는 자동차 기능안전 소프트웨어 검증' 항목이 있다.

제4절 소결

소프트웨어 안전 확보를 위한 안전 작업들은 국방, 항공, 원자력 등 일부 영역에서 주로 적용되어 왔고, 일반 기업은 이에 대한 비용 지출을 많이 하지 않는 경우가 많았다. 하지만 자동차, 전자기기 등 현재 나오고 있는 대다수의 제품에 소프트웨어가 탑재되고 있어 소프트웨어 안전 확보를 위한 활동이 중요하게 되었다.

소프트웨어 안전을 위한 활동을 발 빠르게 추진하고 있는 선진국에 비해, 국내의 소프트웨어 안전 산업은 아직 초기 단계이다. 외국계 선진 업체들이 국내 시험・인증 시장의 25%를 차지하고 있다. 이렇듯 국내 시험・인증을 외국계 업체에게 의지하다보면 고비용적인 측면은 차치하더라도, 시험・인증을 위해서는 국내 제품 소프트웨어를 외국 업체에게 공개해야 되기 때문에, 국내 기술 유출에 대한 걱정이 앞서는 것도 사실이다.

국내 소프트웨어 안전 관련 업체들은 현재까지 주로 저부가가치 서비스인 제품 개발 최종단계에 이루어지는 품질 중심의 테스팅 및 컨설팅을 주로 하고 있다. 따라서 고부가 가치 서비스인 제품 개발 초기 단계부터 이루어지는 안전 분석, 설계 컨설팅 및 인증으로의 작업 전환이 필요하다. 『국내 소프트웨어 안전(Safety) 산업동향 조사』에 따르면 국내 업계에서 생각하는 해외 선진사와의 가장 큰 차이는 다양한 산업별로 보유하고 있는 레퍼런스라고 나타났다. 따라서 국내 업체가 각 산업군별로 안전 수행 작업을 하여 관련 레퍼런스를 쌓아 한 단계 발전할 수 있도록 하는 정책적 지원도 필요하겠다.

국내에서 이미 수행하고 있는 소프트웨어 품질 관련 인증들도 현 상황을 반영하여 수정 보완 작업이 필요하다. GS 인증, SP 인증 등은 소프트웨어 안전 특성 반영에는 미흡점이 있다. 기능 안전 관련 국제 표준 내용을 분석하여 품질 및 프로세스에 대한 내용에 소프트웨어 안전 기능 요소를 반영하는 것이 필요하다.

다행히 최근에는 정부가 소프트웨어 안전 시험・인증・평가의 중요성을 깨닫고 일부 분야에서 국내에서 시험・인증의 역할을 강화하고 있다. 자동차, 철도는 국내 시험인증기관들의 컨소시엄을 통해 국내 기업들이 기능안전 관련 서비스를 받을 수 있게 되었다.

소프트웨어 안전 확보가 기업은 제품 품질을 높여 시장 경쟁력을 확보하고, 이는 곧 국가 경쟁력으로 이어져 소프트웨어 중심사회의 실현 기반이 될 것이다.

제5장 문제점 분석 및 개선방안

제1절 소프트웨어 안전성 확보 체계 상의 문제점 및 시사점

1. 안전 개념 확립의 문제

현재 국내는 소프트웨어와 관련된 품질(Quality), 보안(Security), 안전(Safety) 간의 개념이 명확하지 못하다. 특히 소프트웨어 품질, 보안, 안전 사이의 개념 구분이 모호하여, 소프트웨어 안전에 대한 연구 범위 및 정책 방향 설정이 이루어지고 있지 않았다.

해외 사례의 경우, 주요 산업도메인별 소프트웨어 안전에 대한 국제 표준이 존재하여 명확한 개념 및 안전 등급(SIL) 평가도 산업도메인별로 차별화 되어 정의 되어 있었다. 예를 들어, 도메인별로 자동차 분야는 SIL 1,2,3,4 등급으로 구분하고 있으나, 철도 분야는 SSAS 0,1,2,3,4의 5개 등급을 적용하고, 항공 분야는 DO-178B에서 Level A, B, C, D, E로 구분하여 적용하고 있었다.

같은 원자력 분야라고 하더라도, IAEA에서는 Safety System/Safety Related System/Systems not important to safety의 3개 등급을, IEC는 Category A,B,C, Unclassified의 4개 등급으로 구분하고 있었고, 미국은 1E, Non-nuclear safety의 2가지로만 소프트웨어 안전 등급을 정의하고 1E 등급에 규정을 적용하고 있었다.

소프트웨어 안전에 대한 개념이 확립되지 못하는 경우, 국제 표준을 적용하는 데 어려움을 겪을 수밖에 없으며, 이로 인해 글로벌 진출에 있어, 국제적 안전 수준을 충족하지 못해 실패하는 상황이 발생하게 되는 문제가 있다.

2. 관리·감독의 분산과 정보공유의 문제

국내의 경우, 소프트웨어 안전을 시험·평가·인증하는 기관이 상대적으로 분산되어 있다.

각 산업분야 별로 안전점검 기관 및 인허가 담당기관이 달라서 정보공유를 통한 협업이 원활하지 않은 상황이며, 안전 관련 기관 간 해외 수출 지원이나 인증 관련 업무 등에 어려움을 겪고 있다.

또한 담당 부처 및 전담기관의 분산으로 인해 소프트웨어 안전 관련 공통기술의 활용도가 낮아 중복투자 또는 예산 낭비가 발생할 가능성도 존재한다.

3. 소프트웨어 안전 확보 기술 역량의 문제

소프트웨어 안전 확보를 위한 기반 기술이 해외 주요국에 비해 취약하다는 점을 지적할 수 있다.

산업 분야별로 소프트웨어 안전 관련 기능안전성 국제 표준이 존재함에도 불구하고, 여전히 국내 적용에 대한 연구활동이 미흡하다. 특히, 산업별로 안전성 보장 및 사고 예방을 위한 위험요소 및 분석 등에 대한 연구활동이 저조하여 소프트웨어 개발 단계 중 설계 단계에서 안전성이 제대로 반영되지 못한다.

이러한 문제는 소프트웨어 안전사고의 예방이라는 측면에서 접근할 때, 예방 실패 가능성을 높이게 되고, 그 결과로 막대한 사회경제적 피해나 인명 피해를 초래하게 된다.

4. 소프트웨어 안전 전문인력 확보의 문제

국내 소프트웨어 분야 산업 기업의 경우, 업체가 대부분 300억 미만의 중소규모이며, 저부가가치 사업인 제품 테스팅 서비스가 주 매출원(전체 매출의 65%)이었다. 또한, 소프트웨어 안전 관련 사회/산업적인 기반이 미성숙 되어있어, 소프트웨어 안전 관련 적절한 대가를 받지 못하고, 충분한 교육 기회도 제공되지 못하고 있었다. 상기, 세 가지 이유로 인하여, 수준 높은 안전 전문 인력 유입과 전문 인력 육성이 어려워, 전문 인력 부족 문제가 존재하고 있다.

소프트웨어 안전성을 확보하기 위해서는 개발에서부터 시험, 평가, 인증에 이르는 체계적으로 전문인력이 양성되어야 함에도 불구하고, 현재 국내의 경우에는 품질 및 프로세스 중심으로 소프트웨어 공학 교육이 이루어지고 있어, 소프트웨어 안전 전문인력을 양성하기에는 어려움이 있다.

나아가, 소프트웨어 안전 분야에 종사하는 인력의 전문성을 강화하기 위한 교육기관도 없는 실정이어서 체계적인 교육이 이루어지지 못하고, 현장에서 실무경험을 축적하는 수준에 머무르고 있다.

제2절 소프트웨어 안전성 확보를 위한 체계 개선 방향

1. 국제 표준 준수 및 국제 활동 지원 강화

소프트웨어 안전성 관련 국제표준이 존재하고, 각 산업분야 별로 세분화되고 있다. 모표준으로서 IEC 61508을 토대로 국내 실정에 맞는 공통 기준이 마련되어야 한다. 나아가 소관 부처 및 전문기관과의 협력을 통해 산업별 특화된 소프트웨어 안전 기준을 마련하고, 산업별 기존의 안전 관리 규정에 SW안전 기준을 현실적으로 반영할 필요가 있다.

또한 소프트웨어 안전 관련 국제표준에 대응하고, 국내 적용을 위해서 관련 국제 회의 및 기구 등에 적극 참여할 수 있도록 지원체계를 강화할 필요가 있다. 이는 글로벌 경쟁력 강화에도 큰 기여를 하는 문제이기도 하다.

따라서 현재, 국내의 국제표준화 활동 지원사 업이나 국가 표준기술력 향상 사업 등 국제 표준화 기반 강화와 전문가 양성 등을 목표로 하는 지원 사업을 보다 확대 지원할 필요가 있다.

2. 소프트웨어 안전성 강화를 위한 법제도의 개선

해외 선진국에서는 주요 산업 도메인별 소프트웨어 안전 표준이 준수 될 수 있도록, 직간접적으로 법/규정을 제정하고, 관리감독 기관에서 감독하고 있다.

철도 부분은 유럽 연합의 경우 EN50128이 준수되어야 한다고 법/규정에 명시되어 있고, 미국의 경우 AREMA C&S Manual이 준수되어야 한다고 법/규정에 직접적으로 명시되어 있다.

자동차의 경우는 자동차 제조물 책임법에서 최신 기술 및 기법을 활용해야 한다는 포괄적인 법/규정을 통해서 점진적으로 업계가 ISO 26262를 준수될 수 있도록 간접적으로 강제화 하고 있다.

법/제도에서 표준 준수 여부를 정부 기관이 관리/감독하거나, 허가 받은 업체가 인증을 수행함으로써, 표준이 준수될 수 있도록 제도화 하고 있다.

국내의 경우에도, 일관된 소프트웨어 안전 관련 정책을 시행하기 위해 소프트웨어 안전법과 같은 기본법을 제정할 필요가 있다. 기본법 제정을 통해 산업군별 소프트웨어 안전성을 확보하는 계기를 마련해야 한다.

또한 산업별 특성을 고려하여, 소관 부처 및 전문기관과의 협력을 통해 기존의 관련 규정 및 지침에 소프트웨어 안전 내용을 반영하여야 한다.

이를 계기로 소프트웨어 개발단계에서부터 시험, 평가, 인증에 이르는 전 단계에 안전성을 제고할 수 있어야 할 것이다.

3. 소프트웨어 안전성 제고를 위한 기술 기반의 강화

안전성 확보기술은 안전 필수 시스템 개발에 필수불가결한 요소이다. 시스템의 종류와 안전 요구 사항에 따라 안전성 분석의 종류와 기법을 결정해 적용하게 된다. 특히, 현대에 개발되는 대부분의 시스템은 제어 기능은 소프트웨어로 구현되기 때문에 소프트웨어의 안전성 분석이나 소프트웨어를 포함하는 전체 시스템의 안전성 분석이 반드시 수행되어야 한다. 안전 필수 분야의 표준이 제시하는 시스템의 안전성 확보를 위한 활동은 해당 시스템을 운영하기 위한 최소한의 요건을 의미한다. 시스템의 보다 높은 안전성을 확보하기 위해서는 표준에서 요구하는 최소한의 요건이 아닌 더 많은 연구와 노력이 필요하다.

따라서, 우선적으로 산업군별 공통 적용 가능한 표준 모델을 개발하고, 이를 기반으로 산업군별 특화 모델을 개발, 보급할 필요가 있다.

소프트웨어 안전성 관련 요구사항 도출 및 관리, 설계, 개발, 테스팅 등의 단계에서 시스템의 안전성을 분석하고, 이에 따른 안전 메커니즘에 대한 설계 및 구현을 위한 체계 및 도구를 개발·지원해야 한다.

한편, 민간의 역량을 강화 하기 위해 소프트웨어 안전 관련 국가 차원의 R&D 지원으 ㄹ통해 해외 의존도가 높은 소프트웨어 안전 확보 기술을 국산화할 필요가 있다. 특히, 인증으로 이어지는 테스팅 및 정적 분석 도구 분야의 지원사업을 강화하고 국내 운용사례 확보를 통해 기술을 고도화해야 할 것이다.

4. 소프트웨어 안전 전문인력의 양성

해외 TIC기업을 살펴보면, 소프트웨어 안전 표준 및 가이드에 계획, 설계, 개발, 구현, 운영, 폐기까지의 전 과정에 대해 검사/테스팅/인증 업무에 대하여 서비스를 제공하며, 고가의 비용을 청구 하고 있다.

전문인력 육성의 경우 선진 TIC 기업은, 1. 일반적인 TIC 교육 또는 기업 특화된 교육을 실시하여 전문 인력을 육성하거나(ex. SGS, Bureau Veritas 등), 한편으로, 2. TIC 밸류체인의 업무 뿐 아니라, 엔지니어링 업체를 인수하여 인력 역량을 보강하고 있는 기업도 있다.[81)]

국내의 경우, 전문 인력 확보를 위해서는 소프트웨어 안전 관련 사회/산업적인 기반 성숙이 선행되어 소프트웨어 안전 산업에 대한 인식 제고, 소프트웨어 안전 서비스에 대한 대가의 현실화, 국내 TIC업체의 고부가가치 서비스로의 전환 등이 이루어지고, 이를 통해 수준 높은 전문인력이 유입 또는 육성되는 선순환 구조를 마련해야 한다.

대학 및 대학원 등 제도권 교육을 통해 신규인력을 양성하여 시장에 공급함과 동시에 재직자를 위한 소프트웨어 안전 전문 교육프로그램을 개설하여 전문역량을 강화시키는 것도 중요하다. 이와 연계하여 소프트웨어 안전분야에 국가자격제도를 도입하고, 신뢰성 있는 전문가로의 위상 강화도 고려해 볼 필요가 있다.

5. 소프트웨어 안전 인식제고를 위한 정보공유 활동의 강화

소프트웨어 안전 관련 신기술, 위험요인, 대응방안 등의 정보 공유를 위한 협의체를 구성하고 활성화 될 수 있도록 지원할 필요가 있다. 안전과 관련된 문제는 결국 안전에 대한 인식제고에서 출발하는 것이기 때문에, 소프트웨어 개발 기업, 안전 컨설팅 기업, 전담기관 담당자, 발주 담당자 등의 인식제고에 많은 노력을 기울여야 한다.

이를 위해서 정기적으로 소프트웨어 안전 관련 컨퍼런스나 세미나를 개최하여 산업계, 학계, 정부 등의 적극적인 참여를 유도할 필요가 있다.

금융, 교육, 국방, 정보통신 분야에서 이미 구축되어 있는 정보공유분석센터(ISAC)처럼 인허가를 관장하는 전담기관 간의 정보공유 체계를 강화하고, 공통기술, 사고사례, 문제해결 사례 등을 적극 공유해야 한다. 나아가 소프트웨어 안전사고 대응 모범사례집 발간을 통해 역량 강화와 인식을 제고하는 노력도 필요하다.

81) 예를 들면, Mistras는 석유가스 산업의 Carmegen Engineering 인수, Applus+ RTD는 엔지니어링 서비스를 제공하는 Kiefner and Associates 인수, DNV의 석유가스 재생 엔지니어링 부문 조직 등

제6장 결 론

본 연구는 소프트웨어의 안전성 확보를 통해 국가 전반의 안전성을 높이고자 하는 방향성을 가지고, 소프트웨어 안전성 확보 체계, 즉 시험, 평가, 인증 관련 국내외 현황을 중심으로 개선 방향을 제안하고자 수행되었다.

최근 국내에서 발생한 대형 사고사례에서 알 수 있듯이, 여전히 사고발생의 주요 원인으로 안전불감증이 지적되고 있으며, 자동화 된 일련의 시스템의 문제 보다도 사람의 문제가 더 크게 작용하는 경향이 있다.

이러한 근본적인 이유와 함께 국내 소프트웨어 안전 분야는 해외 주요 선진국에 비해 낮게 형성되어 있어서, 여전히 산업분야로 확대·성장하기에는 어려움이 있어 보인다. 그러나 우리의 상황과는 달리 해외 주요국은 소프트웨어 안전 부문에 대해 매우 활발하게 논의하고 있으며, 시험, 평가, 인증 분야가 주요한 산업의 하나로 인식되고 있다.

국내의 경우, 소프트웨어 안전에 대한 명확한 개념이 정립되어 있지 못할 뿐만 아니라, 이를 정학하기 위한 제도적인 기반마저 미흡한 실정이다. 사회경제적인 인지도 또한 낮아, 수준 높은 전문 인력 유입이 어려우며, 소프트웨어 안전이 소프트웨어 개발의 부수적 활동으로 인식되기도 한다. 나아가 소프트웨어 안전 분야에 종사하는 기업의 수익성 및 매출이 낮아 대부분 영세성을 벗어나지 못하고 있다.

국내 소프트웨어 안전성을 제고하기 위한 기반을 조성하고 국내의 소프트웨어 안전 분야 종사기업들의 경쟁력을 강화하기 위해 법·제도적인 기반을 구축하는 일이 시급하다고 판단된다.

소프트웨어 안전성을 확보하기 위한 시험, 평가, 인증 체계가 보다 효율적이고 유기적으로 구축될 수 있도록 해야 한다. 효율적으로 구축되어야 한다는 것은 소프트웨어 개발자가 혹은 안전을 위한 소프트웨어가 시험, 평가, 인증 받기위해 투입하는 비용과 시간이 과다하지 않고, 신속하게 이루어 질 수 있는 체계여야 한다는 것이다. 또한 유기적이어야 한다는 것은 시험, 평가, 인증 담당 기관이나 조직이 독립성을 확보하면서도 소프트웨어 안전 수요 기업이나 제품을 위해 단절 없이 진행되는 체계여야 한다는 것이다.

소프트웨어 안전분야에서 정책연구에 대한 기반이 부족한 상황에서 본 연구는 해외의 시험, 평가, 인증 등 소프트웨어 안전성 확보 체계에 대한 연구를 통해 개선방안을

제시하였다는 의의를 가진다.

그럼에도 불구하고, 본 연구는 소프트웨어 안전 분야가 시장조사의 불충분, 산업군으로 미분류, 소프트웨어 안전 개념의 미확립, 프로세스 중심의 연구 등 다양한 제약 사항으로 인해, 문헌연구에 국한할 수밖에 없었다는 한계를 가진다.

향후에는 보다 현실 적합한 정책을 도출하기 위해 적실성 있는 소프트웨어 안전 시장 조사·연구를 강화할 필요가 있겠다.

참 고 문 헌

국내 문헌

NIPA·STA (2014), 2013 지역SW융합사업 우수기업 컨설팅 사례집

강명묵·구태완·백종문 (2010), 소프트웨어 결함 발견 및 제거 노력 기반 신뢰성 추정 모델, 정보과학회논문지:소프트웨어 및 응용, 37(7)

강해달 (2012), 소프트웨어 테스팅 관점에서 본 소프트웨어 기능안전성 표준 비교, 정보과학회지, 30(2)

국토해양부 한국건설교통기술평가원 (2008),『철도소프트웨어 안전기준 및 체계 구축 연구보고서』,

권기현(2012),『고 신뢰 융합SW를 위한 필수 SW공학기술 조사용역』, 정보통신산업진흥원 부설 SW공학센터

김성규·김용수 (2014), 기능안전을 위한 IEC 61508의 안전수명주기에 관한 연구, 신뢰성응용연구, 14(1)

노경현·이금석·이민재 (2014), ISO 25000과 IOS 29119를 활용한 임베디드 소프트웨어 시험평가 방법에 관한 연구, 한국정보과학회 제16회 한국 소프트웨어공학 학술대회 논문집, 16(1)

박정인·최진탁 (2013), 소프트웨어 신뢰성 테스트를 위한 평가 척도, 융복합지식학회논문지, 1(1)

배현섭·윤광식·오승욱 (2006), 임베디드 소프트웨어 테스팅 이슈 및 현황, COMMUNICATIONS OF THE KOREA INFORMATION SCIENCE SOCIETY, 24(8)

소프트웨어정책연구소 (2015),『국내 소프트웨어 안전(Safety) 산업동향 조사』

식품의약품안전처 (2014),『의료기기 소프트웨어 안전관리』,

식품의약품안전처 식품의약품안전평가원 의료기기심사부 (2014)『의료기기 소프트웨어 허가·심사 가이드라인』,

윤광식 (2011),『철도 안전 필수 소프트웨어 테스팅』, 슈어소프트테크(주)

윤형진·최진영 (2015), 소프트웨어 제품과 프로세스 관점에서 국제표준과 비교를 통한 테스팅 프론티어 역량평가 모델 개선 방안, 정보과학회: 컴퓨팅의 실제 논문지, 21(2)

이장수 (2011),『안전 소프트웨어 국제표준 현황』, 한국원자력연구원

이장수·이동아 (2015),“소프트웨어 기반의 안전 필수 시스템을 위한 안전성 분석 기법.” 정보과학회지, 33(7).

장승연 (2015), 안전소프트웨어를 위한 소프트웨어 테스팅 관점에서의 차량기능안전 표준(ISO 26262) 적용방안 논의, 정보과학회지, 33(7)

정영은 (2013),『소프트웨어 품질인증 현황 및 전망』, TTA Journal Vol 149.

정은기·권혁무·이민구·김동준·홍성훈 (2013), 자동차 기능안전 ISO26262와 대응방안, Korean Soc Qual Manage, 41

정창신·정순기 (2004), 소프트웨어 자동 테스팅 도구의 발전 로드맵 분석, 한국컴퓨터정보학회논문지, 9(1)

조재규·이승종 (2003), 소프트웨어 품질향상을 위한 품질평가 모델에 관한 연구, 한국정보과학회 학술발표논문집, 30(1B)

지은경 (2015), 소프트웨어 안전확보를 위한 기술 분석 보고서, SPRi 내부자료

차순일 (2010), 소프트웨어 테스팅 산업 현황과 전망, 정보과학회지, 28(11)

한국방송통신전파진흥원 (2013) ,『IT 융합 산업의 H/W 및 S/W의 안전표준화 기술 동향』, 방송통신기술 이슈&전망 제19호.

한국원자력기술원 (2010), 『POSAFE-Q 이중화 소프트웨어의 설계 및 검증 적합성 평가』
행정자치부 (2010),『국가안전관리기본계획 2010-2014』

해외 문헌

Bharat Bhushan Konka(2011). “A case study on Software Testing Methods and Tools ,A pre-study on software testing requirements of ISO/DIS 26262.”, University of Gothenburg, pp38

Bureau Veritas. (2014). "Annual Report & Activity Report."

Canis, Bill. and Richard K. Lattanzio, (2014). "U.S. and EU Motor Vehicle Standards: Issues for Transatlantic Trade Negotiations." CRS(Congressional Research Service Report), pp.8.

Clifton A. Ericson, II (2005), 「Hazard Analysis Techniques for System Safety」, Wiley.

Dr. Qi Van Eikema Hommes(2012). “ASSESSMENT OF THE ISO 26262 STANDARD, ROAD VEHICLES -FUNCTIONAL SAFETY.” SAE 2012 Government/Industry Meeting

IEC (1998), IEC 61508(Functional safety of electrical/electronic/programmable electronic safety-related systems) part1.

ITEA(2013). “Safe Automotive soFtware architEcture (SAFE).” ITEA (Information Technology for European Advancement)

James B. Balliet(2011). “Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance”, AREMA

Kaminski, Garrett, and Paul Ammann (2011), "Reducing logic test set size while preserving fault detection", *Software Testing, Verification and Reliability* 21(3), pp. 155-193.

Majumdar, Rupak, and Koushik Sen (2007), "Hybrid concolic testing." *Software Engineering*, ICSE 2007. 29th International Conference on. IEEE.

Nancy G. Leveson (2011), 「Engineering a Safer World: Systems Thinking Applied to Safety」, MIT Press.

NASA(2013). “NASA Software Safety Guidebook, NASA-GB-8713.13.”

NASA(2013). “NASA Technical Standard, Software Safety Standard, NASA-STD-8719.13C.”

Nelson, Stacy(2003) "Certification Processes for Safety-Critical and Mission-Critical Aerospace Software.", NASA

Parasoft White Paper(2012). “Satisfying EN 50128 Requirements with Parasoft c/c++ test. achieving Functional Safety of Railway Software.”, Parasoft

Ryuji Osuga(2012). “Functional Safety (ISO26262) activities in Japan.” 1st. Asia Automobile Institute Summit

기타

AAR (Association of American Railroads) 홈페이지. AAR. https://www.aar.org/,

AREMA 홈페이지. AREMA C&S Manual, https://www.arema.org/publications/cs/index.aspx/

Bureau Veritas 홈페이지, http://www.bureauveritas.com/

CENELEC 홈페이지. EN50128. http://www.cenelec.eu/
Dekra 홈페이지. Dekra. http://www.dekra-certification.com/en/industry
EBA. 독일연방철도국. http://www.eba.bund.de/EN/Home/homepage_node.html
EC 홈페이지. Technical harmonisation in the EU, National type-approval authorities. http://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/eu/index_en.htm
FAA 홈페이지, https://www.faa.gov/
FRA 홈페이지. 연방철도국(FRA). https://www.fra.dot.gov/Page/P0397,
IIHS 홈페이지. Insurance Institute for Highway Safety, http://www.iihs.org/iihs
InterTek 홈페이지, http://intertek.co.kr/
KBA 홈페이지. Kraftfahrt-Bundesamt, Federal Motor Transport Authority. http://www.kba.de/EN/Home/home_node.html
NHTSA 홈페이지. FMVSS. http://www.nhtsa.gov/cars/rules/import/FMVSS/
NHTSA 홈페이지. National Highway Traffic Safety Administration, http://www.nhtsa.gov/
SAFE 홈페이지, Safe Automotive soFtware architEcture. http://www.safe-project.eu/
SGS 홈페이지 , http://www.sgsgroup.kr/, http://www.sgs.com/
TTCI, 인증절차. http://www.aar.com/
UNECE 홈페이지. UN Vehicle Regulations - 1958. Agreement. http://www.unece.org/trans/main/wp29/wp29regs1-20.html
VCA 홈페이지. Vehicle Type Approval, http://www.dft.gov.uk/vca/
교통안전공단 - 자동차안전연구원 홈페이지. http://www.ts2020.kr/html/nsi/rci/CSRResearcherGuide_1.do
교통안전공단 홈페이지, 각국의 자동차 안전도 평가제도. http://www.ts2020.kr/html/nsi/rci/CSRNationalEval.do
국방기술품질원 (DTAQ) 홈페이지. www.dtaq.re.kr
소프트웨어공학센터 (SW 공학센터) 홈페이지. www.sw-eng.kr
식품의약품안전처 식품의약품안전평가원 홈페이지. www.mfds.go.kr
위키백과(2013년 최종 수정). MIL-STD-498. https://ko.wikipedia.org/wiki/MIL-STD-498
위키백과(2015년 최종 수정). AUTOSAR. https://ko.wikipedia.org/wiki/AUTOSAR
위키백과(2015년 최종 수정). DO-178B. https://ko.wikipedia.org/wiki/DO-178B
위키백과(2015년 최종 수정). ISO 26262. https://en.wikipedia.org/wiki/ISO_26262
위키백과(2015년 최종 수정). Misra C, (2015). https://ko.wikipedia.org/wiki/Misra_c
위키백과(2016년 최종 수정). FMVSS(Federal Motor Vehicle Safety Standards. https://en.wikipedia.org/wiki/Federal_Motor_Vehicle_Safety_Standards,
위키피디아(2015년 최종 수정). 제조물책임법. https://ko.wikipedia.org/wiki/%EC%A0%9C%EC%A1%B0%EB%AC%BC%EC%B1%85%EC%9E%84%EB%B2%95
위키피디아(2015년 최종 수정). ASIL. https://en.wikipedia.org/wiki/Automotive_Safety_Integrity_Level
위키피디아(2015년 최종 수정). DNV GL. https://en.wikipedia.org/wiki/DNV_GL
위키피디아(2015년 최종 수정). https://de.wikipedia.org/wiki/EN_50128,
자동차부품연구원 (KATECH) 홈페이지. www.katech.re.kr

최인정. 자동차 법규. http://dwcij.com.ne.kr/study/study_app2.htm
한국산업기술시험원 (KTL) 홈페이지. www.ktl.re.kr
한국원자력안전기술원 (KINS) 홈페이지. www.kins.re.kr
한국원자력연구원 (KAERI) 홈페이지. www.kaeri.re.kr
한국정보통신기술협회 (TTA) 홈페이지. www.tta.or.kr
한국철도기술연구원 (KRRI) 홈페이지. www.krri.re.kr
한국항공우주연구원 (KARI) 홈페이지. www.kari.re.kr
해외인증정보시스템 홈페이지. e-Mark, AAR. http://certinfo.or.kr/index.do, 한국산업기술시험원

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.