연구보고서 2016-021

SW 안전 전문가 자격제도 연구

A Study on the Qualification System of SW Safety Expert

진회승/박태형/박기호/임홍렬/기민관/이승진

2017.04.

SPRi 소프트웨어정책연구소

이 보고서는 2016년도 미래창조과학부 정보통신·방송연구개발사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 미래창조과학부의 공식입장과 다를 수 있습니다.

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

SW 안전 전문가 자격제도 연구

2. 연구 목적 및 필요성

본 연구는 최근 다양한 산업과의 융합으로 인해 소프트웨어 안전의 중요도가 크게 부각됨에 따라, 소프트웨어 안전에 관련된 국제 표준에 부합하는 소프트웨어 안전 전문가 자격제도를 제안함을 목적으로 수행되었다. 최근 소프트웨어와 다양한 산업영역 간의 융합으로, 소프트웨어 역할의 중요성이 부각되고 있다. 특히 무인 자동차, 드론, IoT 및 의료용 기기 등과 같은 다양한 영역에서 사람에게 서비스하는 시스템이 증가하여, 그 시스템을 통제하는 소프트웨어 역할 및 소프트웨어 안전의 중요성이 크게 증가하고 있다. 소프트웨어 안전 수요에 부응하기 위해 소프트웨어 안전 관련 핵심 역량을 갖춘 인력 확보가 매우 중요한 이슈로 대두되고 있다. 적합한 인력 배양을 위한 방편으로 소프트웨어 안전 전문가 국가기술자격에 대한 면밀한 검토가 필요한 것으로 판단되어 본 연구를 수행하였다.

3. 연구의 구성

본 연구는 총 5장으로 구성되어 있다.

제 1장에서는 서론으로 소프트웨어 안전 전문가 가격제도 연구의 배경, 필요성, 연구의 목적 및 본 연구를 수행한 연구 수행 방법을 제시하였다.

제 2장에서는 소프트웨어 안전의 개념 및 중요성을 제시하고, 소프트웨어 안전을 보장하기 위해 제정된 국내외 소프트웨어 안전 확보 체계 및 국제 표준에 대하여 살펴보았다. 이를 기반으로 소프트웨어 안전 전문가 자격의 필요성을 제시하였다.

제 3장에서는 국내 및 해외 주요국의 소프트웨어 관련 전문가 자격제도에 대하여 분석하였다. 이를 위하여 국가기술자격 관련 선행 연구에 대한 조사를 수행하였다. 국내 소프트웨어 관련 자격 관련해서는 국가기술자격, 국가공인민간자격, 비공인자격에 대하여 조사, 분석을 수행하였다. 특히 소프트웨어 안전과 연관도가 높은 정보보안 관련 자격제도에 대하여 면밀한 분석을 수행하였다. 이와 더불어 소프트웨어 안전 관련 해외 주요국의 안전 전문가 자격제도에 대한 조사를 수행하였다.

제 4장에서는 본 과제의 목표인 소프트웨어 안전 관련 국제 인증에 부합하는 소프트

웨어 안전 전문가 자격제도 모델을 제시하였다. 이를 위하여 전문가 자격에서 요구되는 핵심 역량을 도출하고, 이를 기반으로 필기 및 실기 응시 과목, 평가 실시 형태 등 자격 제도의 세부 모델을 제안하였으며, 제시한 자격제도의 정착을 위한 교육 모델 및 효과적인 유지를 위한 다양한 정책적 지원 방안 등을 제시하였다.

마지막으로 제 5장은 결론으로써 진행한 연구에 대한 요약, 시사점 및 향후 연구 방향을 제시하였다.

4. 연구 내용 및 결과

본 연구는 국제 안전 표준에 부합하는 소프트웨어 안전 전문가 자격 검정 제도에 대한 설계를 수행하기 위해, 국제 안전 표준의 상위 도메인인 IEC 61508을 중심으로 개발 계획, 설계 방안, 테스트 전략, 제품 관리 전략 등 다양한 관점에서 필요한 소프트웨어 안전 활동을 우선적으로 검토하였다. 또한, 최근 소프트웨어의 중요도가 커지고 있고 이에 대한 안전성이 부각되고 있는, 자동차(ISO 26262), 항공(DO-178B/C), 철도(EN 50128) 부문에 대한 국제 표준을 분석함으로써, 각 산업 별로 특별하게 요구하고 있는 소프트웨어 안전 확보를 위한 활동과 기술적 요구사항을 기존에 발간된 문헌 검토를 중심으로 수행하였다.

이와 더불어, 기존에 시행되고 있는 소프트웨어 관련 자격 제도에 대한 상세한 검토를, 국가 자격제도 법령, 연구 보고서, 학술 논문 등에 기반을 두어 조사, 분석을 통하여 수행하였다. 국제 안전 인증 표준에 대한 조사 결과를 고려하여, 기존 자격 제도에서 국제 안전 인증 표준에 부합하는 소프트웨어 안전 전문가 자격제도 설계를 위하여 보완해야할 점과 새롭게 도입이 필요한 사항을 도출하였다.

미국 및 유럽과 같은 선진국에서 시행하고 있는 소프트웨어 안전 관련 전문 인력 확보를 위한 자격 검정 사례를, 해외 인증기관과 교육 기관의 인증 사례에서 조사하였다. 본 연구에서 제시하고자 하는 국제 표준에 부합하는 자격 검정 제도에 반영하고, 제시한 자격 검정제도의 활성화를 위한 방안을 제시하였다.

이러한 조사, 분석을 통하여 본 연구에서는 소프트웨어 안전 전문가 자격제도의 모델을 구성하였으며, 도출한 자세한 자격모델은 1) 국제안전표준과의 연계방법, 2) 산업현장의 역량 수요 반영방안, 3) 자격제도 정착을 위한 교육 모델, 4) 자격제도의 세부모델, 5)자격제도의 유지 방안 등에 대해서 제시하였다.

본 연구의 결과인 소프트웨어 안전 전문가 자격 모델은 다음과 같은 내용 및 특성을 갖도록 설계하였다.

1) 소프트웨어 안전의 핵심 역량을 추출하기 위해, NCS(국가직무능력표준)와 해외의 국제 안전 표준에 대한 조사를 기반으로 소프트웨어 안전 전문가가 보유해야 할 핵심역량을 도출하여 자격제도 모델에 반영하였다.

2) 소프트웨어 안전 전문가 자격을, 안전한 소프트웨어를 개발하기 위하여 요구되는 전문가의 역할 및 각 역할 수행을 위하여 요구되는 핵심 역량 등을 기반으로 분류하였다. 소프트웨어 안전 전문 개발자, 안전 전문 설계자, 안전 전문 테스터, 소프트웨어 안전 관리자의 4가지 종류의 자격을 가지도록 설계하였다.

3) 제안한 자격제도의 질적 관리를 위하여, 실무적인 평가를 수행할 수 있는 실기검정 (코딩, 테스팅 등) 등의 평가 항목 신설을 제안하였고, 이와 더불어 재검정 제도를 도입함으로써 지속적인 학습과 개발을 장려하도록 하는 모델을 마련하였다.

4) 산업현장의 역량 수요 반영방안으로, 소프트웨어 안전 협의체를 구성하여 정부부처 및 기관과 기업체, 교육기관 및 연구기관의 협의를 통하여 소프트웨어 안전 관련 역량 수요를 도출하고 보완하는 체계를 갖도록 하였다.

5) 자격제도의 활용 및 활성화를 위해, 대학 등 교육기관과의 연계를 통하여 소프트웨어 안전에 대한 인식 제고를 추진하고, 교육기관에서 관련 과목을 이수한 경우, 과정이수 및 검정에서 일부 과목의 면제 등의 혜택을 부여함으로써 자격제도와 교육기관과의 연계성을 갖도록 하였다.

5. 정책적 활용 내용

본 연구의 결과물은 제4차 산업혁명 시대에 소프트웨어 안전 확보를 위한 전문가 양성 정책 수립에 있어 기초자료로 활용할 수 있다.

자격제도의 질적 관리와 자격제도의 정착 방안을 마련하여 제시한 국제 인증에 부합하는 소프트웨어 안전 전문가 자격제도 모델은 재직자 중심의 소프트웨어 안전 자격증 설계 정책수립에 활용할 수 있다.

6. 기대효과

본 연구는 소프트웨어 안전 기술에 대한 역량과 지식을 갖춘 고급 인력에 대한 확보와 그를 위한 제도적인 장치의 정비에 기여할 것으로 기대한다.

소프트웨어 안전 전문가 자격제도 신설은 소프트웨어 안전 분야에 대한 인식과 기술력 제고에 기반을 마련하고, 사회 전반에 소프트웨어 안전의 중요성을 인식시키며, 궁극적으로 국가 안전에 밑거름이 될 것이다.

SUMMARY

Recently, the software safety becomes more important as the convergence of software and other industries increases. The role of software is more critical and can make severe problem because the software controls various system like a self driving car, drone, IoT device and medical devices. These trends require much more qualified experts about software safety area and the qualification system for them. This study is performed based on this background to design a “Qualification System of Software Safety Expert“ for securing the qualified SW safety expert.

We performed following analysis to present the qualification system of software safety expert. First, we analyzed the international safety standards such as IEC61508 and domain specific international safety standards like ISO26262. Various qualification systems to secure and support the software safety experts in overseas countries are also investigated. This investigation includes the education program and certification mechanism of TUV, ESC, HCRQ. The domestic qualification systems related the software are also examined such as information processing, embedded and information security qualification system. Especially, the qualification system about the information security is throughly analyzed to devise the qualification system for the software safety. We provide the qualification system for software safety expert with the consideration about the international safety standards based on the analysis.

The qualification system for software safety expert proposed in is designed to qualify the expert level in the software safety filed. In order to make the suitable level for the qualification system of high level software safety expert, we focused on the safety related subject rather than basic and general information processing subjects. The proposed “Qualification System of Software Safety Experts“ presents various aspects of the qualification system and has following characteristics.

1) To define the required capabilities of the software safety expert to be tested by the proposed qualification system, we analyze safety related international standards and various existing education and certification systems of major overseas countries, and reflect these analysis results on the proposed qualification system.

2) The proposed qualification system is designed to have four kinds of qualification about the software safety experts. Those are software safety developer, designer, tester and software safety manager. Those are defined based on the role of experts required to develop safe software and the core competencies required to perform each role.

3) We present the detailed model of the qualification system as well. Those are the method of test to have both written and coding test, the subjects and categories of the capability to be tested in the subject. The test process like the scores required to pass the test and the time duration for the written and coding test. The re-qualification model with the 3 year effective period is proposed to encourage the continuous study and development of the software safety technique for the qualified personnel and maintain the level of expertise of the qualified software safety expert.

4) In order to reflect the demand of the industry to the qualification system, we propose a software safety related consortium that is constructed with the government, related industry leading companies, and educational organization. This consortium can provide the feedback about the qualification system and recent industrial trends to be reflected in the test.

5) To utilize and activate the proposed qualification system, we propose a model to promote awareness of software safety through educational institutions such as universities.

CONTENTS

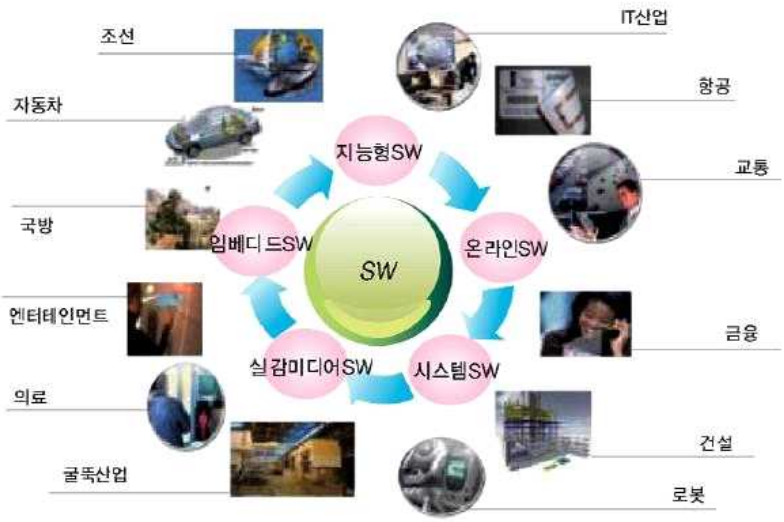
제1장 서 론

제1절 개요

1. 연구의 배경 및 필요성

소프트웨어 산업은 대표적인 지식산업이다. 그와 동시에 개인과 기업 및 정부까지, 각 경제주체의 지식 창출과 활용과 파급에 있어 핵심적인 역할을 수행하는 차세대 지식 정보화 시대의 근간이다. 다른 산업과 비교했을 때, 소프트웨어 산업은 연구개발과 지적 노동량이 월등히 높은 특징을 갖는 지식 집약적인 고부가가치 산업이라 정의할 수 있다.

[그림 1-1] 소프트웨어와 산업 영역간의 융복합



자료: 중소기업청 (2012), 중소기업통합기술로드맵

소프트웨어는 그림 1과 같이, 교통, 의료, 금융 등 대부분의 산업에 적용되어 사용되고 있으며, 최근에는 자동차, 선박, 철도 등의 장비가 첨단화되고 기능이 복잡해지면서 소프트웨어와의 밀접도가 지속적으로 증대되고 있다. 결과적으로, 소프트웨어는 산업간 융합의 근간을 이루는 핵심 열쇠로서, 향후 산업과 기술 간의 융합 현상이 더욱 늘어날수록 소프트웨어의 적용 범위는 지속적으로 확대될 것으로 예상되고 있다.[1)]

1) 조병선, 조상섭 (2014), 소프트웨어의 산업의 특징 및 구조변화에 대한 분석, 전자통신동향분석 제 29권 제 2호, 한국전자통신연구원(ETRI)

한편, 최근 주요 산업별로 소프트웨어 비중이 갈수록 증가하고 있으며, 일례로 자동차의 경우 2020년에는 전체 자동차 개발 비용 중 소프트웨어 개발 비중이 54%가 넘을 것으로 전망되고 있다.[2] 소프트웨어가 다양한 산업분야와 융합되고 있고, 최근 관심이 집중되고 있는 IoT (Internet of Things) 기술의 발전에 따라, 대부분의 국가 기반시설뿐만 아니라 대단위 산업분야 및 개인의 일상생활에 이르기까지 소프트웨어에 의해 구동되는 새로운 변혁의 시대에 진입하고 있다. 이와 같이 다양한 기기에 핵심 기능이 소프트웨어로 구현됨에 따라 소프트웨어의 안전은 그 중요성이 더욱 증가하고 있다. 기존의 시스템에서 일반적인 소프트웨어 품질 저하에 따른 고장 (failure) 등은 사용자의 불편을 유발하는 정도 수준의 문제로 인식되었으나, 최근 소프트웨어에 의한 제어가 도입되어 사용되고 있는 원자력, 자율주행차, 항공우주, 의료, 로봇 등의 다양한 시스템의 경우 인간 생명에 대한 위험으로부터 최악의 경우 국가 존립 기반에도 심각한 문제를 발생시킬 수 있는 요소로 변화되었다. 최근에 발생한 소프트웨어 안전 관련 사고들은 소프트웨어의 오류가 인간의 안전에 얼마나 큰 영향을 미치는 가를 확인해주었으며, 그 주요 사례는 다음과 같다.

1991년, 걸프전에서 패트리어트 미사일 방어 시스템에서 발생한 시간 계산 오류, 2014년에 도요타 급발진 사고 등은 많은 인명의 희생을 일으키는 사고를 유발하였다. 특히 도요타사의 캠리 급발진 사고는, 캠리의 전자식 연료분사 제어장치(엔진 스로틀 컨트롤 시스템, ETCS)의 소프트웨어 결함이 급발진을 일으켰다고 지적되고 있다. 특히 ETCS에 내장된 소프트웨어에 문제가 생겼을 때 이를 대응하거나 해결해주는 방어수단(fail safes) 장치도 정상적으로 작동하지 않았음을 지적하여, 소프트웨어 안전 관리상에 문제로 인하여 발생한 사고였음을 알 수 있었다.[3]

결과적으로, 최근의 소프트웨어 산업은 다양한 산업과 융합됨에 따라, 소프트웨어의 안전성 확보가 보다 핵심적인 문제로 대두되게 되었다. 이러한 소프트웨어 안전 요구에 대한 중요성 증대에 따라, 미국과 유럽을 비롯한 선진국들은 안전성 확보를 위한 국제 표준을 제정하고, 이러한 표준을 준수하도록 하는 다양한 정책적 수단을 마련하여 시행하고 있는 추세이다. 이에 비하여 국내의 경우 아직 안전에 대한 인식 자체가 미흡하고, 이에 대응할 수 있는 역량을 갖춘 인력 확보와 그에 대한 국가적 지원 및 법 제도의 구축이 미흡한 실정이다.

이와 같이 소프트웨어 및 소프트웨어 안전의 중요성 증대와 소프트웨어 안전 관련 핵심 역량을 갖춘 인력 확보가 중요해짐에 따라, 이에 적합한 인력 배양과 검증을 위한 방편으로 소프트웨어 안전 전문가 국가기술자격에 대한 검토가 필요한 것으로 판단된다.

---

2) 이근상 (2015), IoT 산업의 키, 소프트웨어 안전, JBTP 이슈앤테크, vol 49
3) 도요타 자동차 급발진 사고 사례, http://www.etnews.com/20140320000188

또한 본 연구소에서 시행한 소프트웨어 안전 교육을 위한 수요 조사에 의하면 정부 주도의 소프트웨어 안전 교육과정 개설 시 선호하는 운영방식에 대해서는 선택 교육보다는 소프트웨어 안전 전문가 자격증과 연계된 교육을 선호해 소프트웨어 안전 분야 재직자들의 안전 전문가 자격증의 대한 수요를 간접적으로 추출하였다. 소프트웨어 안전 교육을 위한 수요 조사에서 시급성에 따라 산업 도메인별로 국제 수준에 준하는 소프트웨어 안전과 관련된 법규 및 자격인증을 강화가 필요하다는 결론을 도출하였다.

2. 연구의 목적

앞서 언급한 바와 같이, 최근 소프트웨어와 다양한 산업영역간의 융합으로 인해, 소프트웨어 역할의 중요성이 부각되고 있으며, 무인 자동차, 드론, IoT 및 의료용 기기 등과 같은 다양한 영역에서 사람에게 서비스하는 시스템이 증가함에 따라, 그 시스템을 통제하는 소프트웨어 안전의 중요성이 무엇보다도 중요한 개념으로 부각되고 있다.

이러한 산업의 변화에 따라, 각 주요 선진국들에서는 국제 안전 표준 제정에 적극적으로 참여하고 있으며, 소프트웨어 안전 표준을 통해 소프트웨어 안전 산업의 진입장벽을 높임으로서 각 기업 및 국가의 이익을 반영하고자 하는 노력을 경주하고 있다. 또한 소프트웨어 안전에 대한 전문 능력을 갖춘 인력 확보와 교육 체계, 그리고 국가적 지원 체계 및 관련 자격 검정 제도를 구축하여 시행하고 있다. 이에 비하여 국내의 경우에는 소프트웨어의 안전의 개념과 이의 중요성에 대한 인식이 매우 낮을 뿐만 아니라, 국가적 지원 체계가 미흡하다. 소프트웨어 안전 역량 강화 및 검증을 위한 소프트웨어 안전 관련 자격 검정 제도가 미비한 상태로, 소프트웨어 안전에 많은 관심을 가지고 관련 산업 육성 등에 노력을 경주하고 있는 해외에 비하여 많이 뒤쳐져 있는 현실이다.

이러한 점을 고려하여 본 연구에서는 소프트웨어 관련 자격 제도 및 소프트웨어 안전 관련 자격제도를 중심으로 기존 국가 자격제도의 현황 및 문제점을 살펴보고, 기능안전 관련 국제 안전 표준을 다양한 산업 분야에 대하여 검토함으로써, 국제안전표준을 고려한 소프트웨어 안전 전문가 자격제도의 모델을 제안하고자 한다. 이와 더불어 제안한 소프트웨어 안전 전문가 자격제도의 꾸준한 유지 발전을 위한 국가 지원 체계 등 정책적 지원 방안들을 제시하고자 한다.

제2절 연구의 구성 및 방법

1. 연구의 구성

본 연구는 총 5장으로 구성되어 있다.

제 1장에서는 서론으로 소프트웨어 안전 전문가 가격제도 연구의 배경, 필요성, 연구의 목적 및 본 연구를 수행한 연구 수행 방법을 제시한다.

제 2장에서는 소프트웨어 안전의 개념 및 중요성을 제시하고, 소프트웨어 안전을 보장하기 위해 제정된 국내외 소프트웨어 안전 확보 체계 및 국제 표준에 대하여 살펴본다. 이를 기반으로 소프트웨어 안전 전문가 자격의 필요성을 제시한다.

제 3장에서는 국내 및 해외 주요국의 소프트웨어 관련 전문가 자격제도에 대하여 분석하였다. 이를 위하여 국가기술자격 관련 선행 연구에 대한 조사를 수행하였다. 국내 소프트웨어 관련 자격 관련해서는 국가기술자격, 국가공인민간자격, 비공인자격에 대하여 조사, 분석을 수행하였다. 특히 소프트웨어 안전과 연관도가 높은 정보보안 관련 자격제도에 대하여 면밀한 분석을 수행하였다. 이와 더불어 소프트웨어 안전 관련 해외 주요국의 안전 전문가 자격제도에 대한 조사를 수행하였으며, TUV, ESC, HCRQ 등 인증, 교육 기관의 프로그램을 위주로 조사하였다.

제 4장에서는 본 과제의 목표인 소프트웨어 안전 관련 국제 인증에 부합하는 소프트웨어 안전 전문가 자격제도 모델을 제시하였다. 이를 위하여 전문가 자격에서 요구되는 핵심 역량을 도출하고, 이를 기반으로 필기 및 실기 응시 과목, 평가 실시 형태 등 자격 제도의 세부 모델을 제안하였으며, 제시한 자격제도의 정착을 위한 교육 모델 및 효과적인 유지를 위한 다양한 정책적 지원 방안 등을 제시하였다.

마지막으로 제 5장은 결론으로써 진행한 연구에 대한 요약, 시사점 및 향후 연구 방향을 제시한다.

2. 연구 방법

본 연구에서 제시하고자 하는 국제 표준에 부합하는 자격 검정 제도에 대한 설계를 위해, 국제 안전 표준의 상위 도메인인 IEC 61508을 중심으로 개발 계획, 설계 방안, 테스트 전략,

제품 관리 전략 등 다양한 관점에서 필요한 소프트웨어 안전 활동을 검토하였다. 또한, 최근 소프트웨어의 중요도가 커지고 있고 이에 대한 안전성이 부각되고 있는, 자동차(ISO 26262), 항공(DO-178B/C), 철도(EN 50128) 부문에 대한 국제 표준을 분석함으로써, 각 산업별로 특별하게 요구하고 있는 소프트웨어 안전성 확보를 위한 활동과 기술적 요구사항을 기존에 발간된 문헌 검토를 중심으로 수행하였다.

이와 더불어, 기존에 시행되고 있는 소프트웨어 관련 자격 제도에 대한 상세한 검토를 진행하였다. 이는 국가 자격제도 법령, 연구 보고서, 학술 논문 등에 기반을 두어 조사, 분석을 수행하는 방식으로 진행되었으며, 앞서 제시한 국제 안전 인증 표준에 대한 조사 결과를 함께 고려하여, 기존 자격 제도에 추가하여 국제 안전 인증 표준에 부합하는 소프트웨어 안전 전문가 자격제도 설계를 위하여 보완해야할 점과 새로운 도입이 필요한 점을 도출하였다.

마지막으로, 미국 및 유럽 등 선진국에서 소프트웨어 안전에 대한 전문 인력 확보를 위해 시행하고 있는 자격 검정 사례를, 해외 인증기관과 교육 기관의 웹페이지 및 자료를 활용하여 조사하여, 본 보고서에서 제시하고자 하는 국제 표준에 부합하는 자격 검정 제도에 반영하고, 제시한 자격 검정제도의 활성화를 위한 방안을 제시한다.

제2장 소프트웨어의 안전 전문가 자격제도 설계의 이론적 배경

제1절 소프트웨어 안전의 중요성 및 국내외 관련 현황

1. 소프트웨어 안전의 중요성

주지하는 바와 같이 소프트웨어 적용 산업군의 급격한 확장 및 안전 관련 기간 시설 등에의 적용에 따라 소프트웨어 안전에 관한 요구는 크게 증가하고 있다. 이와 관련하여 IEC (국제전기기술위원회, International Electrotechnical Commission)에서는 모든 산업에 기본적인 기능안전 표준을 목적으로 IEC 61508을 제시하였다. 또한 자동차 분야(ISO 26262), 항공분야(DO-178B/C), 철도 분야(EN 50128)등과 같은 도메인별 소프트웨어 안전 관련 기능 안전에 대한 국제 표준이 제정되어 기능 안전을 확보하기 위한 노력이 진행되고 있다. 소프트웨어 안전 선진국에서는 자동차, 항공, 철도 관련 개발, 테스트, 인증 등의 시스템을 갖추고 안전 필수 시스템의 안전 보장을 위한 활동을 하며, 신기술 분야인 자율주행차, 드론 등의 안전관련 법 제정, 안전가이드 개발을 진행하고 있다.

국내에는 아직 소프트웨어 안전에 대한 개념과 인식이 부족한 상태이며, 이에 따라 소프트웨어 안전에 대한 법령, 가이드라인 등의 제도적인 기반 역시 미비한 상황에 있다. 이로 인하여 도메인별로 안전성 보장과 사고 예방을 위한 위험요소 분석 등에 대한 연구 활동 역시 저조하며, 안전 필수 시스템 개발 시에 소프트웨어 위험 분석과 설계, 개발 단계의 안전 활동이 부족하며, 테스트, 인증 등에 미비하게 안전 활동을 하고 있는 실정이다.

이러한 문제는 소프트웨어 안전에서 가장 중요한 요인 중의 하나인 사고 예방이라는 측면에서 볼 때 예방 실패 가능성을 높이게 되고, 그 결과로 앞에서 살펴본 사례에서와 같이 막대한 사회경제적 피해나 인명 피해를 유발하는 결과를 초래할 수 있는 위험에 노출되게 된다. 최근에는 이러한 점을 개선하고자, 소프트웨어 안전에 대한 인식 및 문제점 등에 대한 조사 등이 수행되고 있으며, 이를 위한 해결 방안에 대한 연구 등이 수행되고 있다. [4]

4) SPRI (2015), 소프트웨어 안전 산업동향 조사.

2. 소프트웨어 안전 확보를 위한 기술 역량 강화의 필요성

미국과 유럽 주요국 등의 소프트웨어 안전 선진국은 자동차, 의료, 원자력, 항공 등의 소프트웨어 안전 보장을 위한 국제 표준을 주도하고 있으며, 소프트웨어 안전 관련 산업과 이에 대한 체계 확보 노력도 활발히 진행하고 있다. 이에 따라 표준 개발 초기부터 관련 기술 및 관련 지식을 축적한 선진 기업들은 국제 표준을 준수하는 설계 도구 등의 판매와, 국제 인증에 부합하는 시스템 및 소프트웨어 설계를 위한 컨설팅 활동을 통해 많은 이익을 창출하고 있다.

반면에, 국내의 경우 국제 안전 표준 준수 및 대응의 미비로 국내 소프트웨어 안전 보장 수준은 낮은 상태이며, 이를 지원하기 위한 국가적 지원 체계와 인력 확보를 위한 방안 또한 미흡한 상황이다. 현재의 시장 현황으로 판단하면 매년 16% 정도의 연평균 성장률을 갖는 고성장 산업임에도 불구하고, 아직까지 제대로 된 산업으로 인정받지 못하고 있는 실정이다. 관련 기업들은 법제도의 미비, 표준/절차/가이드의 부재, 해당 전문 인력 육성 시스템의 결여 등으로, 해당 산업 발전에 큰 어려움을 겪고 있는 실정이다.

이에 따라 법/제도 체제의 정비, 표준/절차/가이드의 제정, 인력 양성 및 이를 위한 교육 체계의 구축 등 다양한 측면에서의 소프트웨어 안전 관련 지원 방안이 요구되며, 이를 통하여 소프트웨어 안전 관련 기술 역량 강화가 매우 중요하다.

특히, 소프트웨어 안전 교육 측면에서 국내에서는 체계적인 교육 전략과 교육 기관이 미비하여, 소프트웨어 안전 기술이 필요한 기업들이 기술 역량 강화에 어려움을 토로하고 있다. 이에 본 연구소에서는 소프트웨어 안전 교육을 위한 수요 조사와 커리큘럼 작성에 관한 연구를 수행하였다. 소프트웨어 안전 수요 조사 결과, 소프트웨어 안전 인식이 부족하다는 사실을 다시 확인하였으며, 현재는 시스템 중심의 안전 교육이 이루어지고 있다는 사실을 발견하였다. 소프트웨어 안전 교육은 체계적이지 않고, 소프트웨어 안전 표준을 중심으로 산발적으로 일어나고 있었다.

소프트웨어 안전 재직자 전문가 가격제도에 소프트웨어 안전 교육을 연계하여, 실질적이고 효과적인 역량 유지를 위한 소프트웨어 안전 재직자 전문가 가격제도의 제안이 필요하며, 지속적으로 교육과 연계한 자격제도 운영이 필요하다.

제2절 국내외의 소프트웨어 안전 확보 체계 현황 및 국제표준

1. IEC 61508

국제기구인 IEC(International Electrotechnical Commission)는 IEC 61508을 제정하였다. IEC 61508은 전기/전자/프로그램 가능한 전자 시스템에 대한 기능안전을 명시하였으며, 2000년에 제정되어, 2010년 개정되어 현재에 이르고 있다. IEC 61508은 기능 안전(functional safety)의 대표 표준이다. 그림 1과 같이, 전자기기, 원자력, 의료기기, 공정 산업, 자동차 등으로 구분되는 다양한 산업별 기능 안전 표준의 중추역할을 수행하고 있다.[5)]

[그림 2-1] 기능 안전을 명시한 산업 분야별 국제 표준

2010년 개정된 IEC 61508 에서는 안전수명주기를 통해서, 시스템의 개념단계부터 구현-양산-관리-폐기에 이르는 전사적 과정을 명시하고 있다. 안전 제어시스템을 통하여 개발, 운영 환경 및 다양한 상황에서 잠재되어 있을 수 있는 위험원인을 도출하고, 해당 위험원을 허용할 수 있는 수준까지 감소시키고자 하며, 이처럼 위험원인을 도출하고 감소시키기 위한 다양한 기법들이 개발/발전되고 있으며, 도출된 요구사항을 바탕으로 하여 적합한 안전 제어시스템이 설계되었는가를 하드웨어 및 소프트웨어, 그리고 이들을 통합한 시스템 수준에서의 평가가 수행되게 된다.

5) 김성수, 김용수, "기능 안전을 위한 IEC 61508의 안전수명주기에 관한 연구", 신뢰성 응용 연구, 제 14권, 제 1호, pp. 81-91, 2014.

이러한 안전 무결성과 평가의 기준으로 IEC 61508은 SIL(Safety Integrity Level)을 제시하고 있다.[6] SIL은 안전 필수 시스템의 안전 무결성 등급이며 위험원에 따라 요구되는 수준이 결정된 후 위험원은 정성 및 정량적인 기법들을 통하여 평가된다. 이때의 SIL은 네 가지의 등급으로 구분되고 높은 등급을 가질수록 안전 무결성의 엄격함을 요구한다. IEC 61508은 요구된 SIL에 대한 적합 여부를 검증하기 위하여 두 가지 요소를 명시하고 있다. 먼저, 구조적 측도는 시스템의 결함 허용 수준인 HFT(Hardware Fault Tolerance)와 진단 비율인 SSF(Safe Failure Fraction)에 대한 고려를 함으로써, 시스템의 구조적 강건성을 평가하게 된다. 다른 하나의 측도로는 시스템의 고장 확률 부분에서 평가를 수행한다. 시스템의 작동 요구 빈도에 따라서 PFH(Frequency of dangerous Failures per Hour)와 PFD(Probability of dangerous Failure on Demand)로 구분되고 각기 다른 평가기준을 갖게 된다.

IEC 61508은 파트 0부터 파트 7까지 총 8개의 파트로 구성되어 있으며, 각 파트의 내용은 표 1과 같다. 파트 0(기능 안전과 IEC 61508)은 일반적인 기능안전에 대한 개념을 정의하고, 각 파트의 개요 및 구성에 관하여 명시되어 있다. 파트 1(일반 요구사항)은 기능안전을 위한 전체 프레임워크를 정의하고 있으며, 안전 수명 주기에 따른 목적, 적용범위, 입력 및 산출물을 명시한다. 파트 2(전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 요구사항)은 SIL의 등급화에 관한 내용과 안전제어시스템에 요구되는 안전 요구사항을 결정하기 위한 다양한 기법의 적용이 수록되어 있다. 파트 3(소프트웨어 요구사항)은 안전제어시스템을 개발함에 있어 소프트웨어에 적용되는 SIL과 안전기능에 대하여 명시되어 있다. 파트 4(정의와 약어)는 IEC 61508에서 사용되는 용어의 정의와 설명을 다루고 있다. 파트 5(안전 무결성 수준 결정 방법의 예)에서는 위험과 안전 무결성의 대한 개념설명과, 두 개념간의 관계를 명시한다. 안전 무결성을 결정할 수 있는 다양한 방법론들을 예시를 들어 소개되어 있다. 파트 6(IEC 61508 파트 2와 파트 3의 적용 지침) 에서는 진단 범위 및 안전 고장 비율 계산 예, 파트 2와 파트 3 적용의 기능적 단계와 두 가지 작동모드 내에서의 하드웨어 고장 확률의 평가 기법, 소프트웨어 안전 무결성에 대하여 명시되어 있다. 파트 7(기법과 수단의 개요)은 파트 2 및 파트 3와 관련된 다양한 안전 기법에 관한 설명을 제공함으로써, 시스템 고장의 회피, 하드웨어 우발 고장에 대한 제어, 소프트웨어 안전 무결성 달성 기법과 방법에 대하여 명시하고 있다.

소프트웨어 안전을 보장하기 위해서는 모든 부문이 연관되어 있으나, 소프트웨어 안전과 밀접하게 관련된 부문은 파트 3, 파트 6, 파트 7이다.

---

6) 김정환, 김범수, 양재모, 장창봉, 김민섭, 정상용, 고재욱, “SIL (Safety Integrity Level) 선택에 의한 리스크 감소에 관한 연구”, 한국가스학회지, 제 15권, 제 5호, pp. 57-62, 2011.

<표 2-1> IEC 61508의 파트 구성

구분	내용
파트 0	기능안전성과 IEC 61508
파트 1	일반 요구사항
파트 2	전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 요구사항
파트 3	소프트웨어 요구사항
파트 4	정의와 약어
파트 5	안전 무결성수준 결정방법의 예
파트 6	IEC 61508파트 2와 파트 3의 적용 지침
파트 7	기법과 수단의 개요

2. 자동차 부문에서의 안전 확보 체계 및 국제 표준

자동차에서 전장부품과 소프트웨어 비중이 높아지면서 소프트웨어 설계와 기능 안전 확보가 중요한 과제로 부각되고 있다. 소프트웨어 오류가 엔진이나 제동장치를 직접 제어하는 전자제어장치(ECU)에서 발생한다면 치명적인 인사 사고로 이어질 수 있다는 점에서 소프트웨어 안전은 매우 중요한 요소라 할 수 있다. 특히, 커넥티드카와 자율주행차와 같은 최신 기능을 탑재한 차량일 경우, 소프트웨어의 비중은 일반 차량보다 더욱 높음으로 소프트웨어에서 유발되는 시스템 오류에 대한 위험성은 더욱 커지게 된다. [7)]

자동차는 다른 분야와는 다르게 민간 영역이기 때문에 소프트웨어 안전에 대한 기능 안전성 평가들은 주로 민간 기업 주도하에 진행되었다. 자동차 및 자동차 부품을 생산하고 판매하는 관련 기업들은 해외 수출을 위해서 자연스럽게 안전 인증을 받아야만 하는 상황이다. 최근 유럽과 여러 다른 국가에 자동차 및 자동차 부품을 수출하기 위해서는 해당 국가의 기준에 따른 안전 승인이 필수적이다. 유럽의 경우, 개별 국가가 아닌 유럽 전체에서 통용하는 인증 시스템이 존재한다. 하지만, 국내의 경우 최근까지 이러한 인증과 인증을 위한 컨설팅 작업에 대한 노하우가 부족하기 때문에, 관련 서비스를 주로 외국 안전 컨설팅 업체에 의존하고 있는 실정이다.[8)]

자동차 부문에서의 국제 안전 표준 (ISO 26262)은 2011년 11월 15일에 제정되었다. ISO 26262는 자동차에 내장되는 전기/전자 시스템 안전(functional safety)를 위하여, IEC 61508을 근간으로 제정한 표준으로써 주요 자동차 제조업체에 채택되고 있다. 현재 자동차 범위 확장과 새로운 기술 적용을 위해 '18년을 목표로 2nd 버전을 만들고 있다. ISO 26262 제정 전에는 자동차 시스템의 소프트웨어 안전 관련 개발은 주로 자동차 산업 소프트웨어

7) SPRI (2015), 소프트웨어 안전 산업동향 조사.
8) SPRI (2016), 소프트웨어 안전성 확보 체계에 대한 연구.

신뢰성 협회(The Motor Industry Software Reliability Association, MISRA)의 가이드라인이 적용되었다. MISRA C는 MISRA에서 개발한 자동차 산업용 임베디드 시스템 소프트웨어의 코드 안전성, 호환성, 신뢰성 향상을 위한 C 프로그래밍 언어 개발 가이드라인이다.[9)]

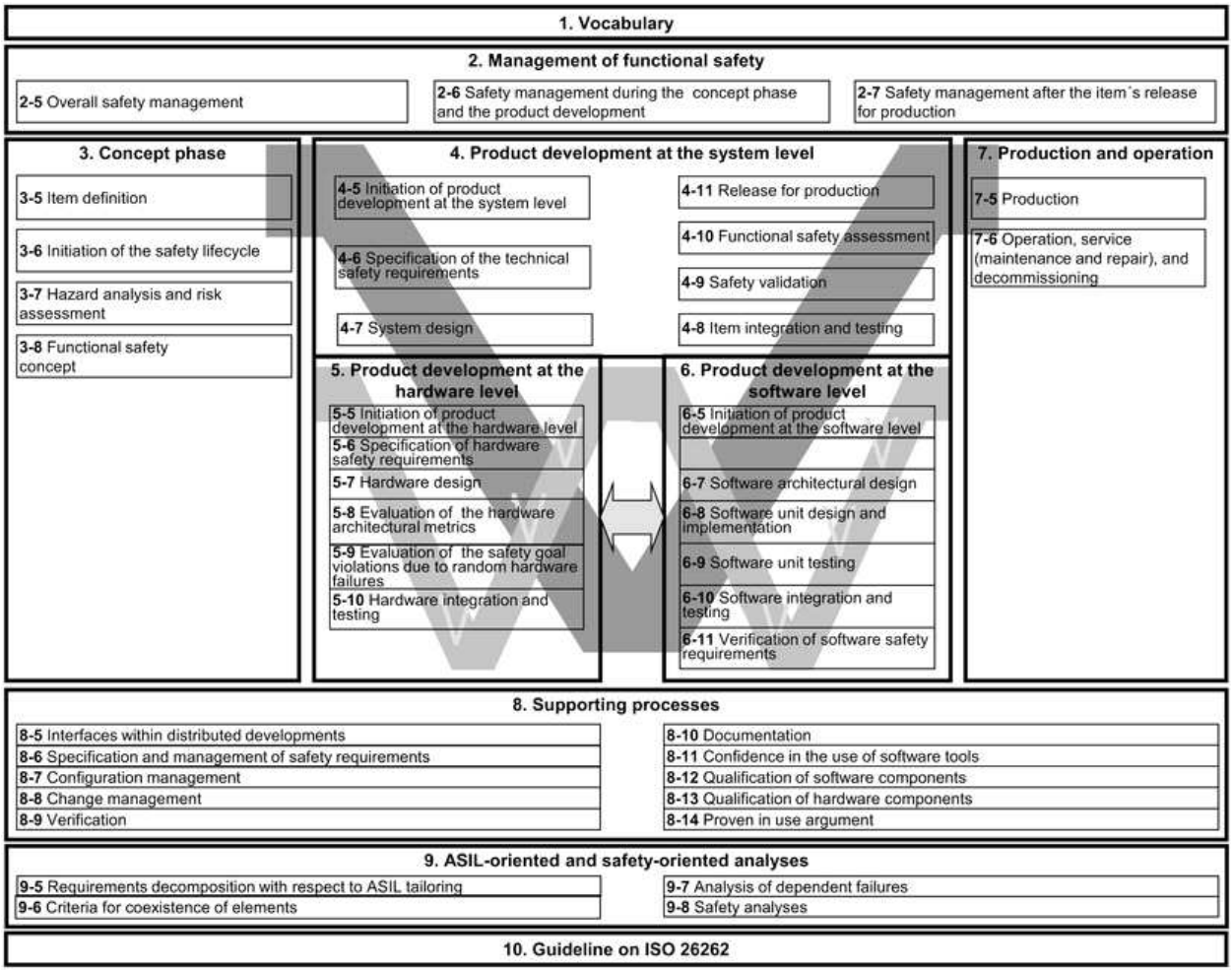
ISO 26262는 차량 개발 프로세서 기획 단계부터 전기/전자 시스템의 오작동에 의해 발생할 수 있는 위험 인자를 식별하고 관리하여 차량 안전성을 확보하는 데 목적을 두고 있다. 시스템 개발 시 요구되는 안전 관련 활동으로, [그림 2-2]과 같이, 아이템 정의(item definition), 헤저드 분석(hazard analysis) 및 리스크 평가(risk assessment), 기능 안전 개념(functional safety concept), 기술 안전 개념(technical safety concept), 시스템/하드웨어/소프트웨어 개발 (system/hardware/software development), 안전 분석(safety analysis)이 있다.[10)11)12)]

[그림 2-2]와 같은 구조와 안전 체계를 갖는 ISO 26262는 표 1과 같이 10개의 파트로 구성되어 있다. 파트 1은 ISO 26262의 용어의 정의가 포함되어 있으며, 파트 2에서는 기능 안전 관리(management of function safety)를 위해 조직 차원에서 가져야할 품목 개발, 생산에 걸쳐 전반적인 안전 관리 요구사항이 기술되어 있다. 파트 3에서는 개발 품목을 정의하고 그를 기반으로 위험 분석 및 리스크 평가를 통한 ASIL(Automotive Safety Integration Level)을 결정하고 안전 목표를 결정한다. 파트 4(제품 개발: 시스템 레벨)에서는 ISO 26262의 V 모델에 따른 시스템 수준의 기술적 요구 사항이 기술되어 있다. 파트 5 (제품개발: 하드웨어 레벨)에서는 시스템 설계 명세를 기반으로 하드웨어 개발, 통합 검증 요구 사항이 기술되어 있으며, 파트 6(제품 개발: 소프트웨어 레벨)에서는 V 모델에 따른 소프트웨어 레벨의 개발, 통합 검증 요구 사항이 명시되어 있다. 파트 7 (생산과 운영)에서는 제품의 생산 계획과 양산, 그리고 출시 이후의 서비스에 관한 요구사항이 기술되어 있으며, 파트 8 (지원 프로세스)에서는 안전 요구사항 명세 및 관리, 형상관리, 변경관리, 검증 요구사항이 기술되어 있다. 마지막으로 파트 9(ASIL-oriented and safety-oriented analysis) 에서는 ASIL 분해 방법과 위험 분석 방법이 기술되어 있고, 파트 10에서는 ISO 26262 주요 개념 및 ASIL 분해 등 고려사항이 명시되어 있다.

---

9) 위키백과 (2015), AUTOSAR, https://ko.wikipedia.org/wiki/AUTOSAR.
10) 채승엽, ISO 26262 해외 가이드라인 쉽게 이해하기, http://www.autoelectronics.co.kr/article/articleView.asp?idx=1416
11) 장승연 (2015), 안전소프트웨어를 위한 소프트웨어 테스팅 관점에서의 차량기능안전 표준(ISO 26262), 적용방안 논의, 정보과학회지, 33(7).
12) 정은기, 권혁무, 이민구, 김동준, 홍성훈 (2013), 자동차 기능안전 ISO26262와 대응방안, Korean Soc Qual Manage, 41.

[그림 2-2] ISO 26262 Structure



자료: ISO, ISO 26262-1:2011(en) (Figure 1 — Overview of ISO 26262)[13]

13) ISO, https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en (2016.12.18.)

<표 2-2> ISO 26262의 각 파트 명 및 내용

구분	내용
파트 1. Vocabulary	표준에서 사용되는 용어, 정의, 그리고 약어를 설명하고 있으며, 총 142개의 용어 및 정의와 53개의 약어로 구성.
파트 2. Management of functional safety	기능 안전 관리를 위한 요구사항을 정의한 파트. 기능안전에 관련된 개발활동을 계획, 조정, 그리고 추적하는 요건에 대해 기술.
파트 3. Concept phase	아이템 정의를 기반으로 위험원인 분석, 리스크 평가를 통해 ASIL 수준을 판정. 안전목표와 메커니즘을 정의하는 파트.
파트 4. Product development: system level	제품 개발 단계 중 시스템 수준에서 개발을 명시. V모델을 따름
파트 5. Product development: Hardware level	하드웨어 수준의 제품개발, V 모델을 따름. 개발과 통합 검증에 대한 요구사항 정의
파트 6. Product development: Hardware level	소프트웨어 수준의 제품개발, V 모델을 따름. 개발과 통합 검증에 대한 요구사항을 정의.
파트 7. Production and operation	제품의 생산과 운영, 서비스, 폐기를 위한 요구사항 포함.
파트 8. Supporting process	안전 요구사항의 명세 및 경영, 변경 관리, 검증, 문서화, 형상관리, 소프트웨어 도구 사용에 대한 신뢰, 사용증명 논거/주장 등에 대한 요구 사항을 정의.
파트 9. ASIL oriented and safety-oriented analysis	ASIL과 안전에 기반한 분석을 위한 요구사항을 기술.
파트 10. Guidelines on ISO 26262	주요 개념과 안전 케이스, ASIL 분해 등. ISO 26262의 이해에 도움이 되는 정보를 기술.

ISO 26262와 관련된 국제 인증기관은 미국, 유럽을 중심으로 위치하고 있다. 미국은 미국 교통국(Department of Transportation) 산하의 NHTSA(National Highway Traffic Safety Administration, 고속도로교통안전청)에서 자동차 제조사에게 FMVSS(Federal Motor Vehicle Safety Standards)를 준수하게 하며, 도난 방지, 연비 등에 대한 규정 제정 및 시험 평가를 수행한다. NHTSA는 고속도로안전법(the Highway Safety Act)에 의해 1970년에 설립되었다. 자동차 및 자동차 장비에 대한 안전 성능 표준을 설정 및 적용하며, 주(state) 혹은 지방 정부의 보조금을 통하여 지역 고속도로 안전 프로그램을 수행한다. NHTSA는 자동차와 자동

차의 부품이 안전 관련법 조항을 충족하도록 규제하고 있으나, 제조사가 자체 인증을 수행하며, 자동차나 자동차 부품에 대한 표준 준수 인증을 수행하지는 않는다.

유럽의 인증제도는 북미의 자기인증(Self-Certification)과는 다르다. 유럽의 인증제도는 판매 전에 EU나 해당국가에서 공인한 인증기관에 의하여 철저한 검사를 시행하는 사전인증제도 (Pre-Certification System)이다. 먼저 EEC/ECE[14] 법규에 따른 인가를 받은 다음, 다시 각국 법규에 따른 인증을 받아야 한다. EU 가맹국 대부분은 국가기관 또는 사설기관이 형식승인인 e-Mark를 수행하고 있다.

일본도 자동차사고대책기구에서 유럽과 유사한 JNCAP(Japan New Car Assessment Program)를 수행하고 있으며, 충돌 안전성/보행자 보호/안전벨트/브레이크 4개 부분에서 테스트를 시행한다. 일본의 경우 보행자의 안전 또한 테스트의 중요 요소이다. 안전벨트 알림 테스트는 2009년부터 시행하였으며, 표시, 알림 시간, 상태 확인 등에서 소프트웨어의 역할이 중요한 부분을 차지한다. 그 외의 지역인 호주, 남미, ASEAN[15] 에서도 유사한 NCAP를 시행한다. 각 국가에서 실시하는 충돌테스트는 평가방법과 종류에서 차이가 있다. 하지만 대부분 정면, 측면, 주행 중 전복에 대해서 테스트를 진행한다. 최근에는 자동차사고의 상당 비중을 차지하는 부분 정면충돌을 실시하는 국가가 증가하고 있다.[16][17]

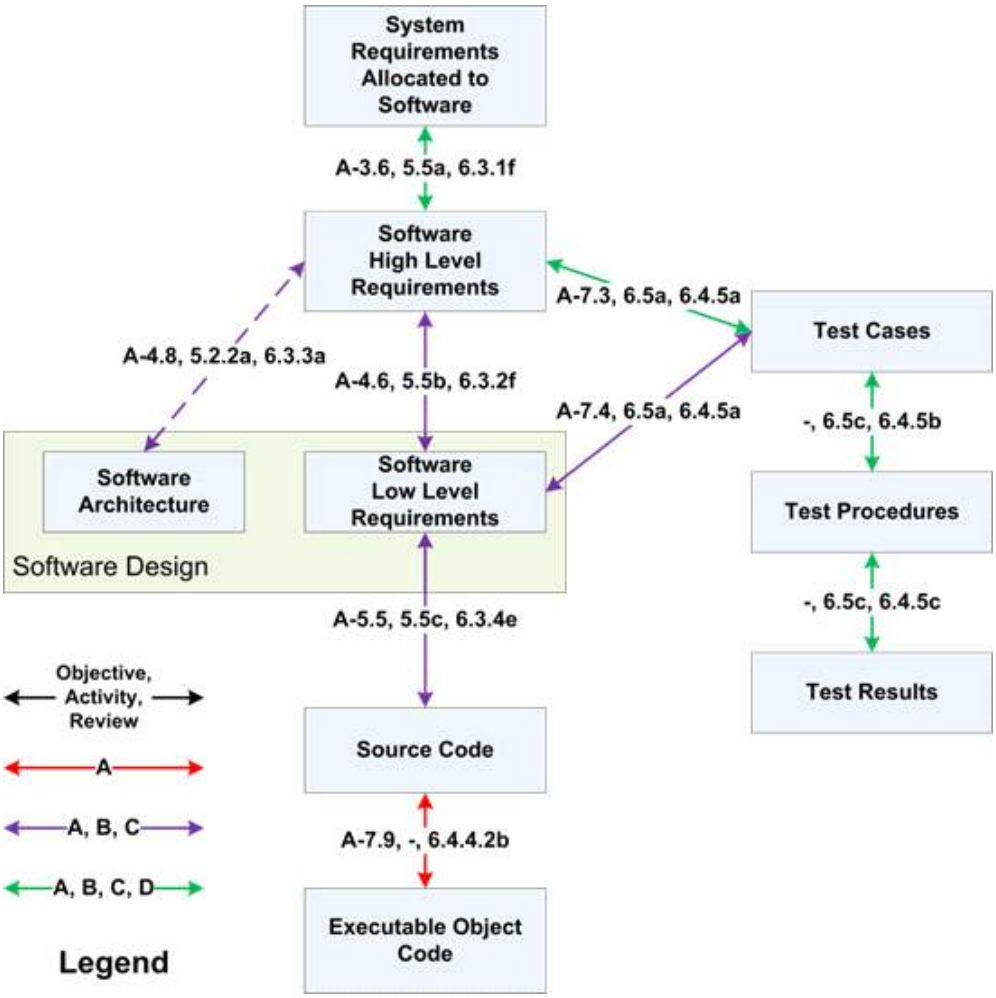
3. 항공 부문에서의 안전확보 체계 및 국제 표준

DO-178B/C 표준은 항공전자시스템에서 사용되는 안전 필수 소프트웨어의 가이드라인이다. 기술적인 가이드라인이지만, 항공전자 소프트웨어 시스템을 개발하기 위한 사실상의 표준으로 기능하고 있는 실정이다. 미국 연방항공청인 FAA (Federal Aviation Administration)가 인증을 위한 기술 표준 오더(Technical Standard Order, TSO)를 명시할 때, 소프트웨어가 항공 환경에서 신뢰할 수 있게 동작할 수 있는 지를 확인하기 위한 가이드로서 사용된다. 또한, DO-178C는 DO-178B에서 저 수준 요구사항(low-level requirements)에 대한 개념이 모호하여 기존에 제시되어 왔던 문제들이 완전히 해결되지 않을 수 있다는 점을 개선하기 위하여 새롭게 개정되었다.[18][19]

---

14) 유럽경제공동체 European Economic Community, 유럽경제위원회 Economic Commission for Europe
15) 동남아시아국가연합, Association of Southeast Asian Nations
16) SPRI (2016), 소프트웨어 안전성 확보 체계에 대한 연구.
17) 우경일 (2014), ISO 26262에 대한 국제 표준 및 기술 동향, 2014 자동차 SW 개발자 컨퍼런스 발표자료.
18) 위키백과 (2012), DO-178C, https://en.wikipedia.org/wiki/DO-178C
19) SPRI (2015), 소프트웨어 안전 산업동향 조사.

[그림 2-3] DO-178C 표준에서 안전 무결성을 위한 다이어그램



자료: 위키백과 (2012), DO-178C, https://en.wikipedia.org/wiki/DO-178C

붉은 색 : 레벨 A 추적. 보라색 : 레벨 A, B, C 추적. 녹색 : A, B, C, D 레벨 추적

항공 부문에서의 소프트웨어 안전은 자동 운항과 결부되어 있기 때문에 매우 상세한 표준으로 발전하였으며, 특히 항공이 발달한 미국의 정부 기관에서 여러 가지 표준을 제정하여 적용하고 있다. 또한 항공기는 그 용도별로 우주항공용, 국방용 및 민간상용으로 구분될 수 있으며, 이러한 용도에 따라 각각의 표준이 발전하였다.

항공용 소프트웨어의 인증을 위하여 다양한 소프트웨어 규격이 만들어졌으며, 이들은 크게 군/민간용으로 구분되어 미국 및 유럽 등의 주요국에 항공용 고신뢰성 소프트웨어를 위한 표준으로 적용되고 있다. 이러한 표준은 크게 평가 표준(Assessment Standards), 개발 표준(Development Standards) 및 보증 표준(Assurance Standards)로 나눌 수 있다. 평가 표준은 소프트웨어 개발기관의 소프트웨어 개발 능력과 품질적절성을 평가하기 위한 규격으로,

Capability Maturity Model (CMM), ISO 9000-3 등이 이에 포함된다. 개발 표준은 순차적이고 반복 가능한 소프트웨어 개발 프로세스에 개한 지침을 제공하기 위한 규격으로서, MIL-STD-498/2167/2167A/2168, DEF-STD 055/056등의 군용 규격과 IEC 12207 (FAA-STD-026)이 민간 용도의 규격으로서 이에 속한다. 개발규격은 개발프로세스 동안 생성하여야 할 문서와 자료들을 정의하고 있으며, 소프트웨어 유지보수에 유용하게 활용된다. 보증 표준은 소프트웨어 개발 프로젝트에 있어, 특정한 속성을 달성하기 위한 방법을 제공하는 규격으로, 어떻게 보다는 무엇을 수행하여야 할 것인가를 정의하고, DO-178B/C, DO-278 이 이 규격에 속한다.[20)]

특히, RTCA/DO-178B, “Software Considerations in Airbone Systems and Equipment Certification“은 항공기 탑재 소프트웨어에 대한 FAA인증 획득을 위해 준수해야 할 지침으로 1992년에 제정되었다. 이 문서는 RTCA(Radio Technical Commission for Aeronautics)와 EUROCAE(the European Organisation for Civil Aviation Equipment)의 합의하에서 국제적인 적용을 위하여 개발되었으며, 미국, 캐나다, 유럽의 항공업계가 주로 참여하여 작성되었다. 본 보고서에서는 FAA의 RTCA DO-178B/C에 대한 표준 인증에 대해 중점적으로 기술한다. RTCA 사에 의해 작성된 DO-178B (항공기 시스템과 장비 인증에 관한 소프트웨어 고려사항)는 항공기 시스템 및 장비의 소프트웨어 부분이 감항성(airworthiness) 인증 요구사항을 준수하는지 여부를 검증하는 소프트웨어 개발 표준이다. 이 표준은 RTCA와 EUROCAE에 의해 공동 개발되었으며, 이를 FAA가 항공기 소프트웨어 인증을 위한 용도로 승인하였고, 오늘날 항공기 소프트웨어를 위한 일반적인 국제 안전 표준으로 자리 잡았다.

FAA는 1993년 1월 11일에 AC 20-115B를 공시하였다. AC 20-115B는 전자 설비 또는 시스템을 사용하는 디지털 컴퓨터 기술의 TSO(Technical Standard Order), TC(Type Certification) 또는 STC(Supplemental Type Certification)를 위한 요청의 규제 준수를 증명하기 위하여 RTCA의 DO-178B를 사용할 수 있다. 이것은 FAR(Federal Aviation Regulations)의 파트 21, 23, 25, 27, 29, 33과 관련된다고 명시하였다. 그러나 DO-178B가 소프트웨어에 대한 FAA 승인을 확인받는 유일한 수단이 아님을 명시하였다. FAA Order 8110.49를 통하여 AIR (Aircraft Certification Service) 분야 사무소와 DER(Designated Engineering Representatives)을 대상으로 DO-178B 표준을 준수하는 소프트웨어 승인절차 가이드라인을 배포했다.

DO-178에서는 소프트웨어 치명도 수준을 A~E로 나누며, 요구사항을 기반으로 관련된 업무가 크게 강조되었다. 2012년에는 요구사항 정의, 프로세서 시작/종료 조건 등 DO-178B의 일부 취약점을 보완한 DO-178C, 그리고 최신 소프트웨어 개발 기법을 반영한 보충자료

20) 박무혁 (2007), 항공용 S/W 개발 및 인증 기술 동향, 항공우주산업기술 동향 5권 1호 pp.15-24.

DO-330(도구 검증), DO-332(객체지향), DO-331(모델링), 그리고 DO-333(정형기법)이 새로이 제정되었다.[21]

DO-178C는 항공기와 항공기 엔진, 보조 파워 장비, 프로펠러 등과 같은 항공용 시스템 및 장비에 활용되는 소프트웨어의 인증을 위한 문서이다. DO-178C는 총 4개의 보충 자료가 있으며, DO-248C문서는 DO-178C 와 DO-278A를 위한 추가적인 정보를 포함한다. DO-278A문서는 CNS/ATM[22] 시스템을 위한 소프트웨어 무결성 보증 관련사항을 포함한다. 또한, 비 항공용 소프트웨어의 보증을 위한 지침 및 안전신뢰도 수준에 해당하는 권고사항을 포함한다.

소프트웨어 개발 과정에서 계획된 모든 활동의 수행과 관련된 증거 제시에 의해, 모든 적용 가능한 요건이 만족되는 것으로 보여주는 것이 DO-178C의 핵심이다. DO-178C는 항공용 시스템과 장비에 활용되는 소프트웨어의 생산을 위해, 1) 소프트웨어 생명 주기에 대한 요건, 2) 요건을 만족시키기 위한 수단 제공, 3) 소프트웨어 생명 주기 데이터, 4) 소프트웨어 수준에 따르는 요건, 독립성, 소프트웨어 주기 데이터, 그리고 통제 카테고리의 변화 및 5) 기 개발 소프트웨어 등과 같은 추가적인 고려사항을 제공하고 있다. 이러한 내용을 포함하고 있는 DO-178C 문서의 구성과 문서사이의 추적은 [그림 2-3]과 같으며, 소프트웨어 개발에 관련된 시스템 측면과 소프트웨어 계획 및 개발 통합 프로세스, 그리고 소프트웨어 생명 주기데이터 및 추가 고려사항으로 나뉜다.

4. 철도 부문에서의 안전 확보 체계 및 국제 표준

철도 부문은 미국과 유럽 연합에서 표준으로 적용하고 있는 두 종류의 표준이 존재하고 있으며, 미국은 AREMA(American Railway Engineering and Maintenance of Way Association)에서 제정한 화물 및 저속 수송을 목적으로 하는 AREMA 2011 C&S Manual을 사실상 표준으로 적용하고 있고, 유럽연합은 승객 및 고속 수송을 목적으로 EN 50128을 적용하고 있다.

미국에서 적용하고 있는 표준인 AREMA에서 제정한 'The AREMA Communications and Signals Manual of Recommended Practices' (AREMA C&S Manual)는 전기/전자/소프트웨어 안전 표준(De-facto Standard)으로 미국 및 캐나다 철도 산업에서 인정받고 있다. 2011년에 개정된 AREMA 2011 C&S Manual의 소프트웨어 및 시스템 안전 관련 주요 항목을 살펴보

21) 김희성 항공용 소프트웨어 인증을 위한 DO-178C 적용 절차 개관, SBAS 정책 기술 동향, SBAS 사업단.
22) Communications, Navigation, Surveillance/Air Traffic Management, 항공통신/항공항행/항공감시 및 항공교통관리를 수행하는 항행안전시스템

면, Section 17 품질보장 부분에 안전 표준을 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.[23)24)]

유럽연합에서는 EN 50128는 철도 산업에 관련된 유럽의 안전 관련 소프트웨어 표준이며, 안전한 소프트웨어 개발을 위한 원리, 방법론, 방법 등을 규정한다. 현재 버전은 2012년 3월 발표되었다. 주요 원칙으로, 하향식 디자인 방법(Top-Down Design Method), 개발단계별 검증(Verification after each development step), 모듈성(Modularity), 검증 가능한 문서(Verifiable Document), 명확한 문서화(Clear documentation), 해당 기기에서의 소프트웨어 검증 테스트(Test the software on the target hardware: Validation)가 있다. 주요 구성요소는 소프트웨어 보증 등급(Software Assurance levels), 소프트웨어 개발 프로세스(Software Development Process), 크로스-프로세스 요구사항(Cross-Process Requirements), 기법 및 방법(Technique and Measures)이 있다. EN 50128 기반의 국제 표준으로 IEC 62279가 있으며, 서로의 내용은 동일하다. IEC 62279는 IEC에서, EC 50128은 CENELEC(European Committee for electro technical standard)에서 관장한다.

미국과 유럽에서 적용되고 있는 안전 표준은 다음과 같은 특징을 갖고 있다. 유럽 표준은 다른 안전 표준과 비슷하게 초기 설계부터 개발, 테스트, 생산까지 안전 시스템 라이프사이클 전반에 걸친 품질과 안전관리 강조하고 있다. 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)하고 있다. 또한, 미국 표준은 FRA(Federal Railroad Administration) 규정을 만족하기 위해 디자인 다양성과 자기 점검(Design Diversity and Self checking), 중복(Checked Redundancy), N-Version Programming[25)], Intrinsic Fail Safe Design[26)] 등의 개념을 도입하고 있고, 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 포함하고 있다.[27)]

---

23) 위키백과 (2015), EN_50128, https://de.wikipedia.org/wiki/EN_50128
24) AREMA, https://www.arema.org/publications/cs/index.aspx/
25) 소프트웨어 공학에서 동일한 기능을 가진 프로그램이 동일한 초기 사양에서 독립적으로 생성해서 소프트웨어의 중복을 구현하는 방법
26) 고장이 발생하여도 시스템 전체에 미치는 영향이 적고, 어느 기간 시스템의 기능을 계속하는 것이 가능한 상태로서 사고로까지 진행되지 않도록 하는 구현
27) 이익성 (2010), 리스크 분석에 의한 철도물류 운영기관의 안전경영시스템에 관한 연구, 신뢰성응용연구, 제 10권, 제 1호, pp. 73-91.

철도의 안전성 확보를 위한 체계로서, 미국의 경우 TTCI(교통기술센터, Transportation Technology Center, Inc.)에서 안전성 검사를 시행하는데, 테스트를 위해 48마일의 테스트 트랙을 설치하고 있다. 7개의 트랙은 테스트를 위한 다른 기능을 가지고 있으며, 특히 두 번째인 WRM(Wheel Rail Mechanism), 여섯 번째인 PTT(정밀 테스트, Precision Test Track)는 안전에 대한 테스트 구역이다. 또한, 미국은 철도차량 및 용품 안전 인증이 자동차의 경우와 같이 국가가 관여하지 않는 자율 인증의 형태이다. 그러나 연방 법령의 안전기준 준수 여부를 위한 사후 관리 및 감독 시 증빙자료를 요청할 수 있어 실질적으로는 이를 충족하기 위한 안전 인증이 실시되고 있다. 미 연방 철도국 FRA(Federal Railroad Administration)는 2005년 6월 49 CFR(Code of Federal Regulation) Part 236 Subpart H: 프로세스 기반의 시그널 및 철도 통제 시스템 개발 표준을 발표하였고, 2010년 1월 49 CFR Part 236 Subpart I: PTC(Positive Train Control System)를 발표하였다. 이 규정들은 철도 자체만이 아니라, 고용자들의 안전에도 관심을 갖고 있으며, 안전 시스템의 안전 개발 방법, 변경, 테스팅, 운영 방법 등을 포함하고 있다. 그러나 안전인증 획득을 위한 안전집행기관과 공급자 프로세스 등을 정해놓지는 않았다. 다시 말하면, FRA 규정을 만족하면 철도 사업자 들은 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) 수립에 활용이 가능한 검증 및 확인(V&V) 표준들이 열거되어 있다. 여기에는 AREMA를 포함한 미국 표준뿐만 아니라 유럽 표준에도 포함되어 있다.

제3절 소프트웨어 안전 전문가 자격제도의 연구 필요성

앞서 기술한 바와 같이, 최근 소프트웨어가 다양한 산업과의 융합화에 따라, 사람에게 직접적으로 제공되는 서비스에 결부되는 경우가 증가하고 있으며, 이에 따라 소프트웨어의 안전은 매우 중요한 소프트웨어 관련 역량으로 부각되고 있다. 또한 산업적으로도 소프트웨어 안전 분야는 부가가치가 높은 산업이며, 국가차원의 시장 창출의 새로운 기회 영역이 될 수 있는 부분이다. 이에 반하여 현재의 국내 소프트웨어 안전 진단 및 컨설팅 분야 시장은 다국적 기업에 의해 잠식된 상태로, 산업별 제품 특성의 지식을 갖춘 안전관련 설계 전문가의 육성의 필요성이 대두되고 있다. [28)]

국외의 경우 자동차, 의료, 원자력, 항공 등 다양한 산업에서 소프트웨어의 안전 보장을 위해 국제 표준 제정에 적극적으로 참여하고 있으며, 이러한 기술적 역량을 기반으로 소프트웨어 안전 진단 및 컨설팅 등 소프트웨어 안전 관련 산업과 이를 위한 교육 등 전문 인력 확보를 위한 노력 또한 활발히 진행되고 있다.

이에 비하여 국내의 경우 국제 안전 표준 준수 및 대응에 대한 관계 법령의 미비, 소프트웨어 안전에 대한 인식의 부재 등으로 국내 소프트웨어 안전 보장 수준은 낮은 상태이며, 이를 지원하기 위한 국가적 지원 체계와 인력 확보를 위한 방안의 마련이 시급한 상황이다.

이러한 국내 소프트웨어 안전 산업의 발전 및 인력 양성을 위해서는 법체계의 정비, 산업계의 적극적인 참여, 소프트웨어 안전 인력에 대한 보상체계 구축 등 다양한 방면의 노력이 필요하나, 소프트웨어 관련 전문 인력 배출을 위한 가장 중요한 방법 중의 하나로 소프트웨어 안전 전문가 자격제도의 국가공인자격에 대한 검토가 필요하다. 특히 국제 안전관련 표준을 이해하고, 이를 만족하는 소프트웨어 개발을 수행할 수 있는 능력을 갖는 소프트웨어 인력을 확보하기 위하여, 소프트웨어 안전 관련 기술 교육 프로그램을 고려한 소프트웨어 안전 전문가 자격 제도에 관한 연구가 요구된다.

28) 박태형, 외 (2015), SW안전 체계 확보와 중점 추진과제, SPRI Issue Report.

제3장 국내 및 해외 주요국의 소프트웨어 관련 전문가 자격제도

제1절 국가기술자격 설계 관련 선행 연구

1. 국가기술자격의 개요 및 분류

자격이란 근로자가 어떤 직무에서 요구되는 특정수준의 숙련도나 자질을 갖추었음을 공식적으로 인정하는 것이다. <자격기본법>에서는 자격을 "직무수행에 필요한 지식, 기술, 소양 등의 습득정도가 일정한 기준과 절차에 따라 평가 또는 인정되는 것"이라 정의하고 있다.

국내법령에서 사용되는 자격의 의미는 크게 8가지 유형으로[29] 나뉘어 사용되고 있었다. 이러한 8가지 유형의 자격의 의미는 자격기본법에서 제시된 '자격'과 사전적인 의미로서의 '자격'의 의미가 모두 포괄적으로 사용되고 있었다.

<표 3-1> 우리나라 법령에 제시된 '자격'의 의미

구분	자격의 의미 및 예시	빈도	비율
1	특정한 요건/조건/기준 예)응시자격, 임용자격, 회원의 자격.	2,585	38.7
2	포괄적 의미로서의 자격 예)국가기술자격, 자격기본법.	1,805	27.0
3	자격증 예)변호사의 자격이 있는 자, 건축사의 자격.	1,346	20.2
4	포괄적인 개인의 능력 예)학위자에 준하는 자격이 있다.	324	4.9
5	의미 강조 예)자격기준, 자격요건.	295	4.4
6	자격증의 효력 예)관세사 시험에 합격한 자는 관세사의 자격이 있다	186	2.8
7	자격취득에 따라 행사할 수 있는 특정한 권한 예)어업권 행사의 자격,입찰에 참가할 수 있는 자격	98	1.5
8	학력 예) ~한 자는 중학교 3학년의 자격을 인정한다	38	5.0
계	-	6,677	100

자료: 김현수 외 (2007). 자격의 활용성 강화를 위한 법제도 개선방안.

29) 김현수 외 (2007), 자격의 활용성 강화를 위한 법제도 개선방안, 한국직업능력개발원

법적인 의미 외에도 자격이라는 용어의 사용은 다양하게 이루어지고 있다.[30] 신분이나 지위, 능력이나 자질을 의미하는 포괄적인 의미의 자격이 있으며, 이는 우리말 '자격'과 qualification이 주로 사용된다. '자격증(certificate)', '수료증(이수증)', '면허증(license)', '인증(accreditation)', '졸업장(diploma)', '학위(degree)' 등은 능력이나 자질을 평가하고 인정하는 것을 의미한다. 이처럼 자격은 다양한 개념으로 정의되나, 대체로 세 가지 의미로 사용된다.

i) 어떤 신분이나 지위

ii) 특정 신분이나 지위 달성을 위해 필요한 능력이나 자질

iii) 이러한 능력이나 자질을 갖추고 있음을 공식적으로 인정하는 평가 및 인증 결과

<표 3-2> 자격의 개념별 활용과 예시

구분	활용	영문 용어	예시
i. 어떤 신분이나 지위	특정 신분	position, title	교수의 자격으로 참석하다, 국빈의 자격
	특정한 지위, 권한	right	어업권 행사의 자격
ii. 특정 신분이나 지위 달성을 위해 필요한 능력이나 자질	특정한 요건, 기준	requirement	응시자격, 임용자격, 자격기준, 자격요건
	포괄적 능력, 자질	capacity, competency	박사학위에 준하는 자격
iii. 이러한 능력이나 자질을 갖추고 있음을 공식적으로 인정하는 평가 및 인증 결과	증서, 증명서	Certificate	혼인, 출생, 사망 증명서
	자격증	Certificate	국가기술자격, 민간자격 등
	면허증	License	의사 면허, 운전면허
	인증서	Accreditation	품질인증서, 우수기업인증서
	수료증	Certificate	교육 수료증, 이수증
	학위	Degree	학사학위, 석사학위, 박사학위
	졸업장(증)	Diploma	고등학교 졸업장(증)
	상장, 표창장	award	우등상, 최고논문상
	기타	-	품질명장, 검정고시

자료 : 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석 1

이처럼 자격을 법령에서의 사용이나 개념별로 분류할 수도 있겠지만, 유형별로 분류할 수도 있다.[31] 자격의 유형별로 분류를 살펴보면 <표 3-3>과 같다.

30) 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 고용노동부

31) 임태수, 김동수 (2008), 소프트웨어 관련 국가기술자격제도 개선방안에 대한 연구, 한국전자거래학회지 제13권 제1호, 55-69

〈표 3-3〉 자격의 유형별 구분

구분	자격유형	자 격 내 용
기능별	업무독점형	- 해당 자격이 없으면 그 업무에 종사할 수 없는 자격 - 면허형 자격과 의무고용형 자격으로 나뉨
	능력인정형	- 해당 분야의 일정한 기능과 지식을 가지고 있음을 나타내며, 그 자격이 없다고 해당 업무에 종사할 수 없는 것은 아님
내용별	전문자격	- 특정 직종의 직무를 수행하는 데 필요한 지식과 기술의 습득정도를 나타내는 자격
	일반자격	- 여러 직종·업종에 걸쳐 직무수행의 효율성을 높일 수 있는 지식과 기술의 습득 정도를 증명해 주는 자격
시행 주체별	국가자격	- 국가가 신설하여 관리 및 운영하는 자격 - 국가가 직접 주관, 혹은 공공기관이나 민간에 위탁 시행
	민간자격	- 국가 외의 법인, 단체 또는 개인이 신설하여 운영 및 관리 - 공인민간자격과 순수민간자격으로 나눌 수 있음 - 사내자격이나 국제자격도 민간자격으로 분류됨

자료 : 임태수, 김동수 (2008), 소프트웨어 관련 국가기술자격제도 개선방안에 대한 연구

위의 표에서와 같이, 국가기술자격을 기능별로 구분하면 업무독점형과 능력인정형으로 나눌 수 있다. 먼저 업무독점형은 면허형 자격과 의무고용형 자격으로 나뉜다. 면허형 자격은 변호사나 공인회계사, 의사, 미용사, 조리사 등이 있으며 업무독점 및 자영업을 위한 조건의 자격을 말한다. 의무고용형 자격은 토목, 건설, 전기, 소방 등 건설업 분야에서 의무적으로 일정 인원 이상의 자격증 소지자를 고용해야하는 자격을 말한다. 능력인정형 자격은 업무독점형과 달리 업무종사에 제한이 없는 자격을 말한다.

〈표 3-4〉 우리나라 자격의 분류 및 현황

구분		종목수
국가자격	국가기술자격	526
	개별법령에 의한 국가자격	212
민간자격	공인민간자격	104
	민간자격	6,100 여개

자료 : 2016 국가기술자격 통계연보(Q-Net)[32], 국가자격종목별상세정보(Q-Net)[33], 민간자격현황(민간자격정보서비스)[34]

유형별 분류 외의 방법으로는 시행주체에 따라서 구분하는 방법이 있다. 시행주체에 따른 자격종목 현황을 살펴보면 〈표 3-4〉와 같다.

32) 고용노동부, 한국산업인력공단 (2016), 2016 국가기술자격통계연보
33) 큐넷 국가자격종목별상세정보, http://www.q-net.or.kr/crf005.do, (2016.12.18.)
34) 민간자격정보서비스 - 민간자격현황, https://www.pqi.or.kr/inf/qul/infQulSitRegView.do (2016.12.18)

2. 국가기술자격의 발전과정[35)]

국가기술자격의 발전과정은 총 일곱 가지의 시기로 구분할 수 있으며, 분산관리기, 통합관리체계 도입기, 자격확대 및 사후관리체계 강화기, 자격제도 다변화정책 전환기, 제1·2·3차 국가기술자격 기본계획 시기가 있다. <표 3-5>

1) 제1기 : 분산관리기 (1958년~)

1962년 국가경제개발사업 추진정책에 맞추어 숙련도가 높은 기술자 수요의 증가에 대비하여 정부 차원의 인력양성제도 구축과 직업능력개발 수단으로서 자격 도입이 요구되었다. 제1기는 개별 법령상 부처별로 자격제도가 분산되어 이루어지고, 직업훈련제도의 정비가 이루어졌다. 부처나 개별 법령상의 특수목적에 따른 자격이 마련되어 검정시행이 이루어지기 시작하였으며, 1967년 1월 직업훈련법이 제정되면서 국가차원의 직업훈련 기틀이 마련되었다.

하지만 부처나 개별 법령상의 특수목적에 따른 자격이 다양했기 때문에 자격기준 간의 불균형과 중복 및 유사자격이 난립하는 문제가 발생하였다.

2) 제2기 : 통합관리체계 도입기(1973년~)

정부의 경제발전 초점이 경공업 중심의 노동집약적인 산업에서 중화학공업의 기술집약적인 산업으로 전환되면서, 이러한 경제발전 전략에 알맞은 기술 인력을 안정적이고 체계적으로 공급하기 위해, 각 부처별로 산만하게 이루어지던 자격관리 체계의 일원화가 요구되었다. 제2기는 1973년 국가기술자격법이 제정되는 "자격제도의 통합관리체계 도입기"로서, 각 부처별로 산발적으로 이루어지던 관리체계를 일원화했다. 또한, 그 동안 허가받은 6개의 검정단체가 시행해 오던 자격검정을 노동청에서 담당하게 되었다.

35) 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 고용노동부

[자격내용 현장성 측면]

- 자격 내용을 과학기술처에서 일괄적으로 관리하면서 현장요구 수렴 체제의 일원화가 가능해짐.
- 기술자와 기능사의 자격의 향상, 자격제도의 공신력이 제고되는 효과를 부름.

[관리·운영 효율성 측면]

- 노동청 산하의 한국기술검정공단 일원체제로 자격검정업무를 담당하게 되면서 기술자격의 관리·운영 일원화가 가능하게 됨.
- 그 동안 부처와 자격별로 이루어져 혼란스럽던 자격검정 기준이 통일되는 체계를 갖추게 됨.

[노동시장 활용성 측면]

- 자격취득자에 대한 우대조치가 마련되면서 전문기술인력으로서의 사회적 지위향상 및 직업훈련제도의 개선 등의 긍정적인 결과를 유발함.
- 우수 기술 인력을 확보하는 중요한 정책수단으로서 자격제도가 기능하게 됨.

하지만 급속한 경제발전이 이루어지고, 산업화된 직업구조 정착이 진행되면서 현재의 자격종목이 3차 산업 중심으로 변화하는 분야를 포함하기 어렵고, 중복 및 불필요한 자격 종목이 증가하였다. 또한, 현행 검정체계로는 현장성과 효율성을 반영하기 어렵게 되었다.

<표 3-5> 국가기술자격제도의 발전 단계별 주요 내용

요소	제1기 ('58~'73)	제2기 ('73~'81)	제3기 ('82~'96)	제4기 ('97~'06)	제5기 ('07~'09)	제6기 ('10~'12)	재7기 ('13~'17)
	분산 관리기	통합관리체계 도입기	자격확대 및 사후관리체계 강화기	자격제도 다변화정책 전환기	제1차 국가기술자격 기본계획 시기	제2차 국가기술자격 기본계획 시기	제3차 국가기술자격 기본계획 시기
자격 내용 현장성	-	• 현장요구 수렴 체제의 일원화	• 보수교육실시 • 매 5년마다 등록 갱신 의무화 • 기능사 2급 응시요건 완화 • 자격종목과 연관성 부족한 현장근무 경력 확대인정 • 자격종목 신설,변경, 폐지, 통합 • 현장 실무경력 요구연수 축소 • 다기능기술자 등급 신설	• 8등급에서 5등급으로 등급 축소 • 현장실무경력 요구연수 축소 • 자격종목 변경, 신설, 폐지, 명칭 변경, 통합 등 • 보수교육 및 등록갱신규정 폐지(1997년)	• 자격검정의 현장성 강화 - 자격검정의 적정성 보장 - 자격인프라 확충 - 검정기관의 질 관리체계 구축 - 자격검정 서비스 질 향상	• 국가기술자격제도 운영의 산업현장성 강화 - 자격제도 운영에 산업계 참여 강화 - 시험과목 면제제도 정비 - 검정방법 개선을 통한 현장성 확보 • 국가기술자격제도 인프라 확충 - 직업(무)능력표준의 개발 및 활용 확대 - 자격제도 평가 및 피드백 시스템 구축 - 자격수요자의 편의성 제고를 위한 정보체계 구축 - 자격통계 개선	• 현장 맞춤형 우수 기술인재 배출 - 국가직무능력표준의 단계적 개발 - 국가직무능력표준의 활용 촉진 - 과정이수형 자격제도 도입 - 자격종목 신설 절차 개선 - 신성장 동력 분야 자격종목 신설 - 자격 효용성 평가 강화 - 자격등급 및 종목의 크기 재설계 - 자격출제 및 검정방법 내실화 - 자격 검정기관의 전문화·다양화 - 자격 취득자 배출의 체계적 관리
관리 운영 효율성	-	• 기술자격 관리 및 운영의 일원화 • 자격검정 기준 동일 • 유사 자격종목 통폐합	• 기술자격제도 심의위원회 설치 • 중복과목 면제 • 유사검정 금지 • 사무관리분야 검정 대한상공회의소 위탁	• 기술기능계 통합 • 국가이외의 자가검정을 행할 수 없는 기술자격 규정 신설 • 유사검정벌금 상향 조정	• 자격제도 운영 틀 개선 - 국가기술자격의 역할 재설정 - 유관제도와의 관계 정립 - 자격제도 운영주체의 다양화 및 체계화 - 자격정보 분석 및 평가체계 강화	• 산업현장에 부응하는 국가기술자격 틀 재설계 - 국가·민간,부처간 역할 정립 - 등급 및 분류 체계 개선 - 산업현장 수요를 반영한 종목의 신설·통합·폐지 - 응시요건 재정비	• 자격제도 운영 선진화 - 민간자격의 체계적 발전 지원 - 국가기술자격 운영체계 내실화
노동 시장 활용성	-	• 자격 취득자 우대조치 강고	• 자격취득자 우선 고용 • 영업허가,인가 및 권리설정, 기타 이익을 부여하는 경우 기술자격 취득자 우대 • 사업주의 기술자격취득자 우대 • 기술기능계 외 서비스계 추가	• 국제자격인정(APEC Engineer,일본과 IT 자격 상호인정)	• 자격취득자의 활용성 제고 - 자격취득자 우대 및 활용 지원 - 자격취득자 사후관리체계 구축 - 기술사의 전문성 및 실효성 제고 - 자격의 국제적 통용성 확대	• 자격취득자에 대한 활용 지원 강화 - 자격취득자에 대한 우대조치 강화 - 중소기업의 자격활용 지원 - 자격의 국제적 통용성 확대 - 자격활용에 대한 모니터링 강화	• 열린고용, 사회통합 및 평생능력개발 촉진 - 자격시험 응시기회 확대 - 현장 근무경력의 체계적 인정 - 중소기업 자격제도 운영 지원 - 취약계층 자격취득 지원 강화 - 평생경력개발경로 개발·보급 - 자격취득자 교육·훈련 지원 확대 - 자격취득자 보수교육 도입 - 자격취득자 해외진출 지원

자료 : 나승일 외, 국가기술자격 운영실태 및 현황분석 (2012)을 수정

3) 제3기 : 자격확대 및 사후관리체계 강화기(1982년~)

경제구조가 3차 산업 중심으로 서서히 변화되면서, 자격제도 관리와 운영 부분에서 국가의 영향력이 점차 약화됨으로써 민간에서의 역할이 필요하게 되었다. 제3기는 제2차 1981년 국가기술자격법 개정을 통해 “자격제도의 확대 및 사후관리체계 강화기”이다. 기술자격관리의 소관부처가 과학기술처에서 노동부로 이관되었으며, 국가기술자격검정을 전담했던 한국기술검정공단이 한국직업훈련관리공단으로 흡수통합 되었다. 또한, 국가기술자격제도가 전반적으로 확대되고, 검정/감독체계 등 사후관리가 강화되었다.

[자격내용 현장성 측면]

- 대한상공회의소, 시도교육위원회가 실시하였던 사무관리 분야 검정이「국가기술자격법」에 의한 기술자격으로 흡수 및 통합
- 1995년 ‘국가기술자격법 시행령’ 개정으로, 다기능기술자에 대한 19개 자격종목을 신설하였음.
- 보수교육 및 검정과목 면제제도 도입, 현장근무경력의 확대인정 등 규제 완화 등 추진

[관리·운영 효율성 측면]

- 기술자격제도심의위원회를 설치함.
- 사무관리 분야 검정을 대한상공회의소에 위탁함

[노동시장 활용성 측면]

- 자격취득자의 우선 고용, 사업주의 기술자격취득자 우대
- 기술기능계 외 서비스계 추가

국가기술자격제도에서 국가의 역할이 다소 축소되었고, 민간의 참여방법이 마련되었다고는 하지만, 여전히 국가주도로 이루어지고 있어 급변하는 산업기술변화에 대처하기에 어려움이 있었다.

4) 제4기 : 자격제도 다변화정책 전환기(1997년~)

경제구조가 3차 산업 중심으로 많이 선회되었으며, 산업기술의 변화 주기가 급격히 빨라지게 되었다. 이로써 정부주도의 자격제도 관리의 현장성이 저하되고, 민간의 참여가 활발히 요구되었다. 제4기는 1997년 자격기본법이 제정되는 "자격제도 다변화정책으로의 전환기"로, 민간기술자격의 국가공인제도가 도입되었으며, 자격등급은 8단계에서 5단계로 축소하였다. 이는 국가기반의 전문기술인력 양성체계에서 벗어나, 자격제도가 다변화되고, 보다 능력중심의 자격제도로 변화한 시기라고 할 수 있다.

[자격내용 현장성 측면]

- 8등급에서 5등급(기술사, 기능장, 기사, 산업기사, 기능사)으로 축소
- 현장 실무경력 요구연수 축소
- 자격종목 변경/신설/폐지/명칭 변경/통합 등
- 보수교육 및 등록갱신규정 폐지(1997년)

[관리·운영 효율성 측면]

- 국제자격인정(APEC Engineer[36],일본과 IT 자격 상호인정)

[노동시장 활용성 측면]

- 기술기능계 통합
- 국가이외의 자가 검정을 행할 수 없는 기술자격 규정 신설
- 유사검정 벌금 상향 조정

국가기술자격제도를 지속적으로 개선했음에도 불구하고, 여전히 산업현장성은 부족했으며,

36) 1995년, WTO(세계무역기구)는 '서비스 무역에 관한 일반협정'에서 '자격요건이나 기술사의 기준 및 면허조건이 서비스 무역에 불필요한 장애가 되지 않도록 한다'라는 규정를 두어 기술자격의 표준화·국제화를 추진. 한국건설기술인협회에서 APEC엔지니어 교육을 실시하며, 심사등록 업무와 관련 부대업무는 APEC엔지니어 심사등록위원회에서 맡음

직능수준 검정 기능은 약되었고, 자격종목 간의 중복성 문제가 제기되었다. 정책이 계획성 있게 시행되기 보다는 그때그때마다 대대적인 개편 위주로 진행되고 있어 자격제도 관리 및 운영의 중장기 계획성이 부족했다. 또한 자격보유자의 편의를 이유로 보수교육 및 등록 갱신규정을 폐지하였으나, 자격보유자의 직무능력을 관리 및 보증하는 데에는 좋지 않은 영향을 주었다.

5) 제5기 : 제1차 국가기술자격 기본계획 시기(2007년~)

제1차 국가기술자격제도발전 기본계획은 산업현장성의 부족과 직능수준 검정 기능의 약화, 자격 종목 간의 중복성 문제를 해결하기 위해 추진되었다. 이 계획을 통하여 산업현장의 수요와 기술변화가 반영된 국가기술자격제도를 구축하고자 했다. 제5기는 2007년부터 2009년까지 추진된 "제1차 자격제도발전 기본계획기"이며, 『자격검정의 현장성 강화』, 『자격제도 운영 틀 개선』, 『자격 취득자의 활용성 제고』의 3대 정책영역의 12개 과제가 추진된 시기이다. 이 시기에는 대체로 민간기관에 대한 검정위탁 및 현장전문가 참여 확대, 산업현장에 부응하는 종목정비, 출제관리 시스템 개선, 자격통계 개선이라는 점에서 성과가 있었다.

[자격검정의 현장성 강화 측면]

- 자격검정의 적정성 보장
- 자격 인프라 확충
- 검정기관의 질 관리체계 구축
- 자격검정 서비스 질 향상

[자격제도 운영 틀 개선 측면]

- 국가기술자격의 역할 재설정
- 유관제도와의 관계 정립
- 자격제도 운영주체의 다양화 및 체계화
- 자격정보 분석 및 평가체계 강화

[자격취득자의 활용성 제고 측면]

- 자격취득자 우대 및 활용 지원
- 자격취득자 사후관리체계 구축
- 기술사의 전문성 및 실효성 제고
- 자격의 국제적 통용 확대

1차 기본계획의 다양한 성과에도 불구하고, 자격제도의 산업현장성을 반영하는 노력이 미흡하여 산업현장에서의 국가기술자격 활용도가 여전히 높지 않은 근본적인 한계가 있었다. 또한, 기본계획의 수립 주기가 짧아서, 장기적 안목의 정책추진이 어려웠으며, 구체적인 성과목표와 지표가 제시되지 않아 질적인 부분을 관리하는 데 소홀했다는 한계가 있었다.

6) 제6기: 제2차 국가기술자격 기본계획 시기(2010년~)

제2차 국가기술자격제도발전 기본계획은 1차 기본계획의 한계점이었던 산업현장성 제고노력의 미흡과 자격제도의 틀 등, 전반적인 제도 개편의 필요성에 의해 수립되었다. 제6기는 2010년부터 2012년까지 추진된 “제2차 자격제도발전 기본계획기”로서, 산업현장에 부응하는 국가기술자격의 틀을 재설계하고 국가기술자격제도 운영의 산업현장성 강화, 자격취득자 활용지원 강화, 국가기술자격제도 인프라 확충, 이 4개 영역에 15개 과제가 추진되었다.

- 산업현장에 부응하는 국가기술자격 틀 재설계를 전략으로 산업현장 수요가 반영된 종목의 신설/통합/폐지 및 응시요건 재정비, 국가·민간 부처사이의 역할 정립과 등급 및 분류 체계의 개선 등이 있음.
- 국가기술자격제도 운영의 산업현장성 강화 전략으로 시험과목 면제제도 정비와 산업계의 자격제도 운영 참여 강화, 검정방법 개선을 통한 현장성 확보 등이 있음.
- 자격취득자에 대한 활용지원 강화로는 자격취득자에 대한 우대조처 강화와 자격의 국제적 통용 확대, 중소기업의 자격활용 지원, 자격활용에 대한 모니터링 강화가 있음.
- 국가기술자격제도 인프라를 확충하기 위한 노력으로, 직업능력표준의 개발 및 활용 확대와 자격수요자의 편의성을 높이기 위한 정보체계 구축, 자격제도의 평가와 피드백 시스템 구축, 자격통계의 개선 등이 있음.

제2차 국가기술자격제도 발전 기본계획은 차질 없는 추진을 위해 각 과제별 유관 부처 및 기관의 시행계획을 종합하여 연차별로 시행계획을 수립하여 추진했다(고용노동부 외, 2011).

- 고용노동부에 의해 시행계획 수립지침이 각 기관에 통보됨으로써 추진부처, 기관, 협조기관이 시행계획을 수립하였으며, 각 부처·기관의 시행계획을 종합하여 당해년도 시행계획이 마련되면 관계부처와의 협의 후에 시행계획이 확정됨.

제2차 국가기술자격제도 발전 기본계획의 4대 정책영역·15대 중점 추진과제·32개 세부과제 수립에 따라서 고용노동부, 교육과학기술부 등 2개부처 7개 기관이 추진 중에 있다(고용노동부 외, 2011).

- 기본계획의 4대 정책영역인 『산업현장에 부응하는 자격제도 운영체계 구축과 운영』, 『 노동시장에서의 자격취득자 활용성 제고』, 『검정방법의 개선을 통한 자격제도 운영의 산업현장성 강화』, 『자격의 현장성 확보를 위한 자격제도 인프라 확충』에 따라서 교육과학기술부, 고용노동부, 한국산업인력공단 등 2개 부처 7개 기관에서 추진함.

제1차 국가기술자격발전제도 기본계획과 2차 기본계획의 성과 및 한계점을 살펴보면, 최초의 중장기 종합적 계획의 수립, 시행이라는 점에서는 의의가 있으나, 산업현장에서 요구되는 현장성 반영의 한계 및 자격취득자의 활용성 부족이라는 점 등의 한계점도 함께 가지고 있는 것으로 지적되었다.

7) 제7기: 제3차 국가기술자격 기본계획 시기[37](2013년~)

제3차 국가기술자격제도발전 기본계획은 1·2차 기본계획의 목적인 산업현장 수요 반영, 활용성 강화의 목적을 계승하며, 기존 기본계획의 한계점이었던 지속적인 질 관리 부분을 보완하고자 하였다. 특히, 신성장동력 산업의 대두, 기술의 융복합화, 기술주기의 단축 등 산업현장의 기술·숙련수요의 고도화에 대응하고, 저출산·고령화, 양극화 등 노동시장의 당면과제 해결에 기여할 수 있도록 자격제도 차원의 적극적 대응을 목표로 한다. 제7기는 2013년부터 2017년까지 시행된다. 그 주요 내용은 다음과 같다.

- 현장 맞춤형 우수 기술인재 배출 전략으로 <일-교육·훈련-자격>연계 강화와 산업현장에 맞는 자격종목·등급 운영, 현장성 높은 자격검정 시행 등이 있음.

37) 관계부처합동 (2012)

- <일-교육·훈련-자격>연계 강화는 국가직무능력표준의 단계적 개발, 국가직무능력표준의 활용 촉진, 『과정이수형 자격제도 도입』이 목표임.
- 산업현장에 맞는 자격종목·등급 운영은 자격종목 신설 절차 개선, 신성장동력 분야 자격종목 신설, 자격 효용성 평가 강화, 자격등급 및 종목의 크기 재설계가 목표임.
- 현장성 높은 자격검정 시행은 자격출제 및 검정방법 내실화, 자격 검정기관의 전문화·다양화, 자격 취득자 배출의 체계적 관리가 목표임.
- 열린 고용, 사회통합 및 평생능력개발 촉진을 전략으로 열린 고용 및 사회통합 촉진과 평생능력개발 지원 등이 있음.
- 열린 고용 및 사회통합 촉진은 자격시험 응시기회 확대, 현장 근무경력의 체계적 인정방안 마련, 중소기업 자격제도 운영 지원, 취약계층 자격취득 지원 강화가 목표임
- 평생능력개발 지원은 평생경력개발경로 개발·보급, 자격 취득자 교육·훈련 지원 확대, 자격 취득자 보수교육 도입, 자격 취득자 해외진출 지원이 목표임.

제3차 국가기술자격 기본계획은 신성장동력 산업, 기술의 융복합화, 기술주기의 단축 등 산업현장의 기술·숙련수요의 고도화에 대응하기 위하여 여러 가지의 자격종목을 신설할 계획을 수립하여 시행하고 있다.

특히, NCS (National Competency Standards, 국가직무능력표준)를 2015년까지 단계적으로 개발하여 산업현장에서의 직무수요를 분석하고, 해당 표준을 교육훈련과 자격제도에 유기적으로 접목시키고자 하였으며, 과정이수형 자격제도를 도입하여 직업교육 및 훈련, 자격의 산업 현장과의 유기적 연계를 추진하였다. 2013 ~ 2017년에는 검정형과 과정이수형 자격을 병행 운영하되, 우선적으로 기능사·산업기사 등급의 일부 분야에 우선 도입 후 성공모델 구축 및 단계적 확대할 계획으로 추진되고 있다.

자격취득자를 대상으로 보수교육을 도입함으로써, 자격취득자의 기술적 품질 유지를 도모할 계획이다. 특히, 국민의 생명과 건강, 안전에 직결되는 분야의 면허형 자격들을 대상으로 보수교육을 실시하여, 자격을 갱신 등록하는 방안을 검토 중이다.

8) 종합 및 시사점

(1) 제도적 체계화와 정부의 정책추진으로 자격내용의 현장성이 강화되어 왔지만, 여전히 산업시대의 틀과 내용 영역을 유지하고 있어 제한적이다. 1973년 국가기술자격법 제정으로

산업현장에서의 요구수렴 일원체제를 마련한 이후로 가속화되는 기술변화 속력에 대처하기 위해 민간부문의 역할을 증대하고, 현장성 강화를 위하여 현장경력의 확대 인정, 등급체계 개편(8등급→5등급, 1997년), 현장산업체의 참여 확대를 위해 노력하는 등의 정책이 추진되어 왔다는 점에서 현장성 강화를 위한 성과가 있었다. 하지만, 인력수준의 고도화와 산업기술은 빠른 변화양상에 비하면, 국가기술자격이 포괄하는 내용영역은 여전히 산업시대의 분류와 직무별로 이루어져 있어 제4차 산업혁명 시대에 맞는 자격제도로 개선되기 어려운 구조이다.

(2) 자격의 관리 및 운영 측면에서, 국가기술자격 체제가 마련되었다는 점에서 성과가 있다. 국가기술자격법과 자격기본법 등이 제정되면서 자격체계가 갖추어져 왔으며, 각종 위원회가 만들어지면서 자문이 이루어지고, 2007년부터는 제도발전 기본계획을 수립해 오면서 장기적인 안목으로 자격제도 관리 및 운영이 강화되었다는 점에서 성과가 있었다. 하지만, 국가기술자격과 타 자격, 학위 및 경력과의 연계 또는 호환을 강화하기 위한 시스템을 마련하지 못했다는 한계가 있었다.

(3) 자격의 활용성 측면에서 자격취득자에 대한 우대조치가 일부 마련되었으며, 모니터링을 하는 등 활용성 증진에 대한 성과가 있다. 1982년 자격취득자 우대조치가 강화되고, 국제자격인정(APEC Engineer, 일본과 IT 자격 상호인정 등)이 확대되었으며, 중소기업의 자격활용을 지원하는 등 자격취득자 활용을 위한 지원이 이루어져 왔다. 또한, 최근에는 자격활용에 대한 모니터링 시스템을 마련하였다. 하지만 정부의 노력에도 불구하고 면허형 자격과 같은 우대사항이 없는 국가기술자격 보유자의 사회적 우대는 대체로 감소되는 추세이기 때문에 자격의 활용성이 약화되는 한계가 있다. 또한, NQF(국가역량체계, National Qualifications Framework) 등이 구축되지 못하고 외국의 NQF와의 상호호환 체계가 마련되지 못하였기 때문에, 자격에 대한 국제적 통용이 여전히 미흡한 실정이다.

(4) 현재 시행되고 있는 제3차 국가기술자격제도발전 기본계획은, 빠르게 변화하는 산업현장의 특성을 고려하여, 신성상동력 산업과, 기술의 융복합화, 기술주기의 단축 등을 고려하여 여러 가지의 자격종목을 신설할 계획이다. 새로운 자격종목 뿐만 아니라 보수교육 제도를 도입함으로써 자격취득자의 기술적인 품질을 관리하고, 특히 국민의 생명과 건강 및 안전에 직결되는 분야의 자격들에 적용하여 보수교육 실시를 검토 중이다.

제3차 국가기술자격제도발전 기본계획에서 추진되었던 NCS(국가직무능력표준) 개발은 계획대로 2015년 12월까지 총 847개의 종목이 개발되었으나, 과정이수형 자격제도는 기존 계획과는 달리, 과정평가형 자격제도로 바뀌었다. 과정이수형 제도는 최종 자격검정에서 내부평가인 자체검정만 실시하지만, 과정평가형 제도는 자체검정 뿐만 아니라 외부평가를 실시하므로 자격증서의 남발을 예방하고 자격의 신뢰를 높였다. 현행 및 2017년 시행될 자격종목의 대상은 [그림 3-1]과 같다. 여기서 소프트웨어 부문에 해당하는 것은 웹디자인기능사, 정보처리산업기사가 있다.

[그림 3-1] 2017년 과정평가형 시행 적용 대상종목

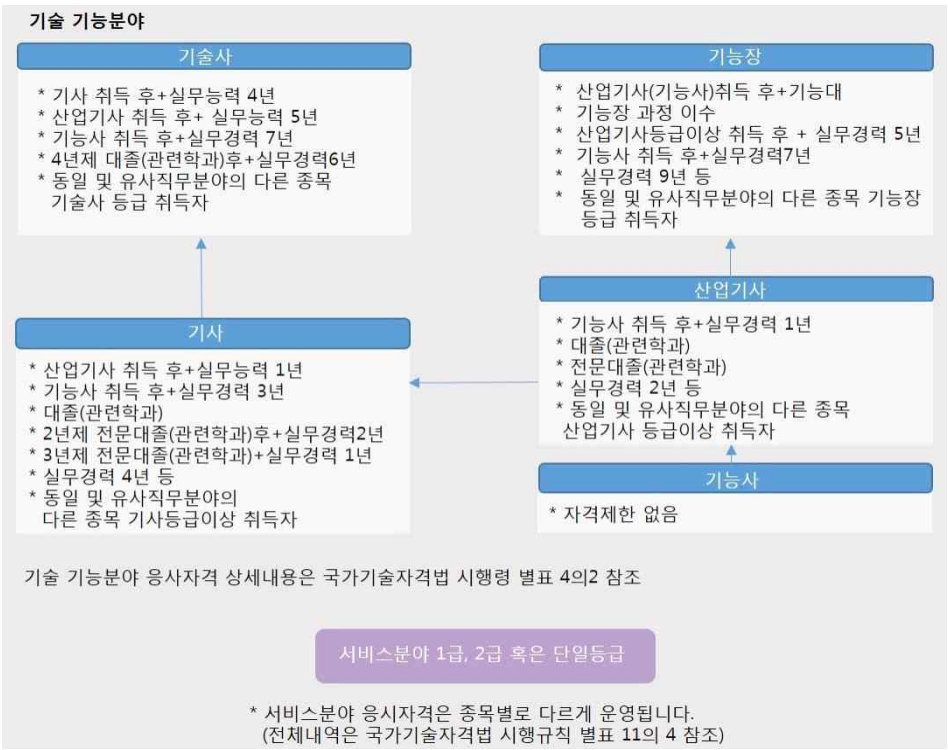
자료 : 국가기술자격제도 응시자격 조건체계 (Q-Net)[38]

38) 큐넷 2017년 과정평가형 시행 적용 대상종목, http://www.q-net.or.kr/crf006.do?id=crf00626

3. 응시자격 및 경력 연계와 우대정책

국가기술 자격 중에서는 응시에 필요한 조건을 요구하는 자격들이 있다. 자격을 취득하기 위하여 기본 자격이 필요한 것이다. 대표적으로 기술사 / 기사 / 산업기사 / 기능사 자격증이 있다. 응시자격 조건체계를 참고하면, 기술사 / 기사 / 산업기사 / 기능사 자격을 취득하기 위해서는 학력이나 하위의 자격증, 실무경력을 필요로 한다는 것을 알 수 있다. 실무경력을 필요로 한다는 점에서 현존하는 기술사 / 기사 / 산업기사 / 기능사의 응시자격 조건체계는 자격취득자의 기술숙련도 평가의 지표가 될 수 있으므로, 산업현장에서 우대받을 수 있는 기회가 된다.

[그림 3-2] 국가기술자격제도 응시자격



자료 : 국가기술자격제도 응시자격 조건체계 (Q-Net)[39]

정보통신 분야가 포함된 공사업 분야에서는 경력수첩이라는 체계가 있다. 경력수첩은 기술사 / 기사 / 산업기사 / 기능사 자격과 연계되어 경력사항을 증명하는 문서로, 취득자격증과 경력에 따라서 기술자 경력을 등급화하여 부여하는 제도이다. 정보통신 분야에서는 정보통신공사협회가 발급하는 정보통신기술자 경력수첩이 있으며 경력수첩에 따른 기술자격자 등급의 기준은 <표 3-6>과 같다.

39) 큐넷 국가기술자격제도 응시자격 조건체계, http://www.q-net.or.kr/crf006.do?id=crf00613, (2016.12.18)

정보통신기술자 경력수첩에서는 기술사 / 기사 / 산업기사 / 기능사 자격증이 실무경력과 연계되어 기술자, 즉 전문가로써 인정받을 수 있는 체계가 구비되어 있다. 이는 단순히 자격증에 그치는 것이 아니라 실무경력을 추가적으로 포함함으로써, 기업 차원에서 숙련도 높은 전문 인력으로 우대받을 수 있는 준거가 될 수 있다.

〈표 3-6〉 정보통신기술자 등급별 인정기준

등급구분		인정 기준	비고
기술계 정보통신 기술자	특급 기술자	기술사	자격취득 이전경력은 인정기간의 50%로 산정
	고급 기술자	기사(기능장을 포함한다. 이하 같다) 자격을 취득한 후 5년 이상 공사업무를 수행한 자	
		산업기사자격을 취득한 후 8년 이상 공사업무를 수행한자	
		기능사자격을 취득한 후 13년 이상 공사업무를 수행한 자	
	중급 기술자	기사자격을 취득한 후 2년 이상 공사업무를 수행한 자	
		산업기사자격을 취득한 후 5년 이상 공사업무를 수행한자	
		기능사자격을 취득한 후 10년 이상 공사업무를 수행한 자	
	초급 기술자	산업기사자격 이상의 자격을 취득한 자	
		기능사자격을 취득한 후 4년 이상 공사업무를 수행한 자	
기능계 정보통신기술자		기능사 자격을 취득한 자	

자료 : 한국정보통신공사협회 - 정보통신기술자 경력수첩[40)]

국가기술자격의 법률적 우대정책은 앞서 3장 1절의 1에서 언급하였던 자격의 유형과 관련이 깊다. 면허형 자격은 자격증 보유자에게 면허를 발급함으로써 자격증 보유자만이 자영업을 할 수 있거나 업무를 독점할 수 있게 한다. 또한, 의무고용형 자격의 경우 건설업 분야에서 의무적으로 관련 자격증 보유자를 고용하거나, 자격보유자만을 고용할 수 있게 한다. 마지막으로, 공무원 및 공사 채용시험 가산점을 부여하는 우대정책이 있다.

정보통신 및 소프트웨어 분야의 자격에서는 의무고용 형태와 가산점 부여 형태의 우대정책이 이루어지고 있으나, 실제 정보통신 및 소프트웨어 분야의 현업 종사자들에겐 큰 우대사항이 없다는 평이 대다수이며, 산업현장에서 이루어지는 개인의 기술수준 평가는 대개 경력에 의존하고 있다. 응시자 대부분이 채용시험 가산점을 위하여 응시하고 있는 상황이다.

40) 한국정보통신공사협회, https://www.kica.or.kr/web_app/CA/engine_engineer01.jsp, (2016.12.18)

4. 국가 기술자격 설계 관련 선행 연구

1973년 ‘국가기술자격법’의 제정으로 도입된 국가기술자격제도에 대한 연구는 국가기술자격제도 발전과 함께 꾸준히 진행되어 왔으며, 특히 2000년대 초반부터 주된 연구들이 수행되었다. 이들 연구들은 국가기술자격제도 전반에 대한 연구, 자격 등급 및 종목 정비, 출제 기준 및 문항 출제 개선, 관리 운영체계 및 국가기술 자격 효용성 평가 등에 관한 연구가 다양하게 진행되었다. 이들 중 최근의 주요 선행 연구의 내용은 다음과 같다.[41]

1) 국가기술자격제도 전반

<21세기를 향한 국가기술자격제도의 발전 방안 연구>[42]는 국가기술자격 취득자를 대상으로 설문조사 등을 기반으로 국가기술자격제도의 개편방향을 설정했다. 이러한 개편의 주요 방향으로는 기술 및 기능 분야의 합리화, 서비스분야의 합리화, 자격취득자의 우대, 자격취득과 원격교육과의 연계, 자격 정보체계 구축, 기초직업능력과의 연계, 민간자격으로 관리 및 운영 전환, 국제적 통용 확보, 통합국가자격체계 구축 등을 제시했다. <자격제도의 비전과 발전방안>[43]에서는 총체적, 종합적인 자격제도 검토를 통하여 자격제도의 개선 방향을 제안했다. <제2차 국가기술자격제도발전 기본계획 수립을 위한 기획연구>[44]에서는 기존에 수행된 제1차 국가기술자격제도발전 기본계획의 성과를 검토하고, 세계화, 고령화, IT산업기술의 변화, 고용구조의 변화 및 숙련 등의 영역으로 구분하여 제2차 국가기술자격제도발전 기본계획의 방향을 선정했다. 현재는 제3차 국가기술자격제도발전 기본계획 (‘13 - ’17)이 시행중에 있으며, 현장 맞춤형 우수 인재 배출 및 열린 고용, 사회통합 및 평생 능력 개발 촉진 등의 중점 추진과제로 설정하여, 일-교육·훈련-자격의 연계강화를 위한 과정 이수형 자격제도 도입, 자격 취득자 보수 교육 도입 등 평생능력개발 지원 등의 과제가 추진되고 있다.[45]

2) 국가기술자격제도의 등급 및 종목

<국가기술자격 종목 정비 및 제도 개선>[46]에서는 국가기술자격의 등급과 종목이 산업현장

41) 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 한국산업인력공단
42) 조정윤 외 (1998), 한국직업능력개발원
43) 강순희 (2003), 한국노동연구원
44) 주인중 외 (2008), 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 44쪽에서 재인용
45) 관계부처합동 (2012)
46) 조정윤 외 (2001), 한국직업능력개발원, 한국산업인력공단, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 45쪽에서 재인용

에서의 요구와 산업동향에 맞게 설계되었는지 진단하고, 이에 대한 개선방안을 제시하였다. 이를 위하여 산업동향과 인력수급 전망, 교육 및 훈련시장 현황, 자격검정 현황을 분석하여 직무분야를 구분하였으며 국가기술자격 종목의 통합/폐지/신설을 위한 기준을 제시했다.

3) 문제 출제 기준

<국가직무능력표준에 의한 자격 출제기준 시범개발>[47]에서는 국가직무능력표준을 기존 자격 검정방법에 사용할 수 있도록. 기존 과목 기반 자격구조 검정 시스템 내에서 출제기준에 국가직무능력표준의 내용을 반영할 수 있는 개발절차와 방법을 제시했다. <국가기술자격 출제기준 개선방안 연구>[48]에서는 출제기준의 활용실태와 외국사례를 분석하여 출제기준의 제정 및 개정, 문항출제 등의 개선방안을 제시했다.

4) 검정

검정 방법 관련 연구로는 <국가기술자격 검정방법 개선에 관한 연구>[49]에서는 국가기술자격 검정방법의 문제점과 세계 주요국의 검정방법을 분석하여 자격 등급별 검정방법의 개선방안을 제시하고. 전산화된 검정시스템 구축, 제도적 측면에서의 개선방안을 제시했다.

5) 자격제도 관리 및 운영

<국가기술자격제도 관리・운영체제의 국가 및 민간의 역할 분담>[50]에서는 국가기술자격의 관리와 운영현황을 분석하여, 현행 국가중심의 자격제도 운영의 한계점을 제시하며, 이러한 점을 극복하기 위하여 민간과의 역할 분담(안)을 제시했다. <국가자격시험 관리체계 개선을 위한 법제도 개선방안>[51]연구에서는 국가기술자격제도의 시험과 자격제도의 질 관리 규정을 분석하고 개선이 필요한 자격 법령과 질 관리 방안을 제시했다.

47) 김덕기, 박동열 (2006), 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 45쪽에서 재인용
48) 나승일 외 (2011), 한국산업인력공단, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 45쪽에서 재인용
49) 조정윤 외 (1999), 한국직업능력개발원
50) 조정윤 외 (2003), 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용
51) 김현수 외 (2007), 한국직업능력개발원

6) 효용 평가

국가기술체계의 효용에 대한 평가를 수행한 <국가기술자격의 효용성 평가체계 구축>[52]에서는 자격제도 전반에 대한 평가체계와 자격종목별 평가지표 및 방법을 제시했다. 다른 연구인 <자격제도 운영평가체제 구축 연구>[53]에서는 국가기술자격제도의 관리 및 운영 지침을 제시하며, 자체적인 평가 방법을 제시하였으며, <국가기술자격 효용성 평가>[54]에서는 106개의 국가기술자격 종목을 개인, 기업, 거시차원의 정량분석을 수행하였고, 정량분석이 어려운 부분은 정성분석을 통하여 효용성을 평가했다.

7) 결론 및 시사점

위와 같은 국가기술자격제도 관련 선행 연구를 통하여, 국가기술자격제도의 등급, 종목 등을 관련 기술의 발달과 사회의 변화에 따라 지속적으로 변화, 발전되어 왔음을 알 수 있었다. 최근에는 국가직무능력표준에 근거한 자격증 제도 구축을 위하여, 문제 출제 기준을 위한 연구 및 산업 현장의 요구에 부합하는 출제 기준 등을 설정하여 자격증의 실제적인 활용도를 높이는 방향 등에 대한 연구가 활발히 진행되고 있다. 검정 방법에 관한 연구에서는 주로 전산화된 검정 시스템 구축 등의 제도적 측면의 개선 방안이 제시되었다. 자격제도의 관리 운영 및 효용성 평가 등에 관련된 연구들에서는 주로 민간과의 역할 분담 관련 제도, 법령 정비 등에 대한 내용 및 운영 실태 및 성과에 대한 꾸준한 분석을 통한 평가 항목, 평가 지표의 설정 등이 필요함을 제시하였다. 최근에는 국가직무능력표준과 연계된 국가기술자격제도의 설계 관련 연구 등이 활발히 진행되고 있다.

52) 이동임 외 (2006), 한국직업능력개발원, 한국산업인력공단, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용
53) 이동임 외 (2008), 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용
54) 이동임 외 (2009), 한국직업능력개발원, 한국산업인력공단, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용

제2절 현행 국내 소프트웨어 관련 자격제도 분석

1. 현행 국내 소프트웨어 관련 자격제도 현황

현재 시행되고 있는 국내의 소프트웨어 관련 자격 제도는 공인중개사나 세무사 등 국가전문자격에 해당되지 않는 일반 국가기술자격이다. 또한, 기사/산업기사/기능사의 일부가 의무고용형이며 대부분이 능력인정형 자격이다. 시행주체에 따라서는 국가기술자격이 13개, 공인민간자격이 5개 정도이며, 그 세부 사항은 아래와 같다. 분류기준은 단순히 소프트웨어를 사용하는 자격증은 배제하였으며, 소프트웨어 개발 측면이 포함된 자격증을 선별하였다. 민간자격의 경우 민간자격의 총 개수가 수천 개에 이르기 때문에 일부 주요 자격만을 기술하였다.

<표 3-7> 현행 국내 소프트웨어 관련 자격제도

자격분류	자격명	신설년도
국가기술자격	정보처리기사	1974
	정보처리산업기사	1974
	정보처리기능사	1983
	전자계산기조직응용기사	1983
	정보관리기술사	1974
	임베디드기사	2011
	멀티미디어콘텐츠제작전문가	2002
	사무자동화산업기사	1993
	컴퓨터시스템응용기술사	1974
	정보보안기사	2013
	정보보안산업기사	2013
	게임그래픽전문가	2002
	게임프로그래밍전문가	2002
국가공인 민간자격	리눅스마스터	2008
	정보시스템감리사	2008
	컴퓨터운용사	2008
	SQL	2011
	데이터아키텍쳐	2008
민간자격	소프트웨어테스트전문가	2013
	컴퓨터프로그래머	2008
	모바일앱개발전문가(MAP)	2014
	소프트웨어설계기술인증시험	2009

해당 표 내에서 선별한 주요 자격증으로 정보처리기사와 임베디드기사, 정보보안기사, 정보시스템관리사 등에 대해서 분석하였다.

1) 1974년에 신설된 정보처리기사 자격증은 소프트웨어 개발 관련 자격증으로 정보기술 계열 국가기술자격 중에서는 가장 유명한 자격증이다. 데이터베이스 설계와 활용, 컴퓨터의 기본 구조, 운영체제의 이해 및 활용, 소프트웨어 개발을 위한 소프트웨어 공학, 데이터통신 및 네트워크에 대해 다루는 자격증으로, IT의 전반을 다룬다고 하여도 과언이 아닌 자격증이다. 정보처리기사는 필기검정과 실기검정을 함께 통과해야 자격을 취득할 수 있다.
정보처리기사 자격증은 긴 역사와 명성을 가졌지만 문제점도 적지 않다. 높지 않은 난이도로 인하여 매우 높은 합격률과 자격의 희소가치가 높지 않아, 산업현장에서의 해당 자격증 소지자에 대한 우대 등의 처우상의 혜택이 거의 없기 때문이다. 뿐만 아니라, 1회 취득으로 영구 유효한 자격증을 부여받기 때문에 자격보유자의 전문성 또한 보장할 수 없다. 정보처리기사 자격증은 “국내 소프트웨어 자격제도 현황 및 소프트웨어 안전과의 연관성” 부분에서 더욱 자세히 다룰 예정이다.

2) 2011년 신설된 임베디드기사 자격증은 임베디드 소프트웨어 및 하드웨어를 개발자를 위한 자격증이다. 검정 내용은 하드웨어의 가장 기본적인 요소인 논리회로와, 컴퓨터구조, 주변장치, 임베디드를 위한 펌웨어와 OS포팅, 디바이스 드라이버, 임베디드 OS, 리눅스 커널 프로그래밍, 시스템 및 네트워크 프로그래밍, 그리고 임베디드 프로그래밍과 개발도구 및 테스팅으로 구성되어 있다. 정보처리기사 자격증과 마찬가지로 1회 취득으로 영구 유효한 자격을 얻을 수 있다. 임베디드기사 자격증은 “국내 소프트웨어 자격제도 현황 및 소프트웨어 안전과의 연관성” 부분에서 더욱 자세히 다룰 예정이다.

3) 2013년 신설된 정보보안기사 자격증은 2008년 신설된 정보보호전문가 자격증을 전신으로 하는 국가기술자격이다. 정보보안시스템 및 솔루션을 개발하고 각종 보안 및 네트워크 장비를 관리하며 운영하는 직무를 수행하는, 보안전문가를 대상으로 하는 국가기술자격이다. 검정 내용으로는 운영체제 및 클라이언트, 서버 보안, 네트워크 보안과 인터넷응용, 전자상거래 등 어플리케이션 보안, 보안요소와 암호학, 보안법규 등을 다룬다. 다른 소프트웨어 관련 자격증과 비교했을 때, 난이도가 상당히 높으며 합격률도 낮은 수준을 보인다. 하지만 영구한 자격을 부여한다는 부분은 동일하다. 정보보안기사 또한 “정보보안 관련 자격제도 분석” 부분에서 더욱 자세히 다룰 예정이다.

4) 정보시스템감리사 자격증은 IT관련 감리사를 위한 자격증으로, 일반 국가기술자격과는 달리 필기전형과 실무(실기)전형, 면접전형으로 세 가시지의 전형을 거친다. 1차로 필기전형을 합격하면 면접전형 단계로, 면접전형을 합격하면 이론교육 단계로, 이론교육을 합격하면 실무교육을 거쳐 감리사 자격증을 얻을 수 있는 기존의 다른 자격들과 다른 평가 체계를 가지고 있다. 이처럼, 각 전형에 따른 교육을 수행하기 때문에 일반적인 검정형 자격과는 다르며, 정보화 관련법이나 가이드, 감리제도, 조직관리, 프로젝트 관리, 소프트웨어 공학, 데이터베이스, 시스템구조, 보안 등 정보 분야에서 감리사의 역할을 수행하기 위한 내용을 교육 및 검정하고 있다. 정보시스템감리사 자격증의 자세한 사항은 “국내 소프트웨어 자격제도 현황 및 소프트웨어 안전과의 연관성” 부분에서 다시 자세히 다루도록 한다.

2. 기존 소프트웨어 관련 자격의 문제점 요약[55)]

기존 소프트웨어 관련 자격에 대한 분석을 통하여 현행 소프트웨어 자격은 대부분이 능력인정형 자격이며, 일부 기사/산업기사/기능사 자격만이 의무고용형으로 운영되고 있음을 확인할 수 있었다. 또한 의무고용형에 해당하는 자격은 신설년도가 상당히 오래되어 현대의 방대해진 정보통신 분야에 맞지 않는 경향이 있으며, 보수교육이 이루어지지 않고 있다는 문제점도 있음을 알 수 있었다.

가장 많이 언급되는 소프트웨어 관련 국가기술자격의 문제로는 산업 현장에서 요구하는 실무능력 배양에 있어서 괴리감이 존재한다는 점이다. 위의 <표 3-7>을 참고하면 시행기간이 오래된 자격증일수록 자격명이 모호하고 포괄적인 경향이 있다. 전문적인 능력을 다루지 않기 때문에, 해당자격을 취득하더라도 산업현장에서 요구하는 직무수준을 보유하고 있다고 인정하기에 어려움이 있으며, 현장의 직무요구수준과 비교하면 초급에 가까운 수준을 테스트를 하고 있어 실무능력 배양과는 동떨어진 형태를 보이는 것을 알 수 있다. 게다가 소프트웨어와 관련되는 영역이 지속적으로 발전, 변화, 확장되고 있음을 감안할 때, IT 영역 전반에 대한 자격증은, 국가기술자격에서 부여하는 해당 분야의 실무 능력을 갖는 인재로서의 인증이라는 의미가 지속적으로 감소할 것으로 예상된다.

비교적 최근에 신설된 국가기술 자격의 임베디드기사나 민간자격의 SQL은 보다 전문적이고 해당 분야에 특화된 자격을 부여하고 있다. 이처럼 IT 분야에서도 각기 직무영역에 특화된 자격제도를 구비하는 것이 전문 인력 양성에 도움을 줄 것이며, 자격 자체의 효용을 높

55) 장진현 (2016), ICT 관점에서 바라본 국가기술자격제도 개선, 한국인터넷방송통신TV학회 논문지, Vol.16 No.2, 189-199p, 관련내용을 참고하여 결론 및 문제점을 도출함.

일 수 있는 방법이 될 것이다.

덧붙여 우대정책이나 사후관리가 미비하다는 점도 국내 소프트웨어 자격증의 한계 중 하나라고 꼽을 수 있다. 대부분의 국내 소프트웨어 자격증은 특별한 우대사항이 존재하지 않고, 자기 업무능력 개발을 위한 자격이기 때문에, 회사의 입사 시 가산점을 부여하는 등의 이유가 아니라면 응시자 수가 감소하는 경향을 보이기도 한다. 이에 따라 단순한 능력인정형 자격이 아닌, 업무와 연계되거나, 어떤 직무나 과제를 수행할 때 해당 자격증을 보유한 인력의 참여가 요구되는 등의 강제성이 있는 자격증 제도를 구축하여야 국가기술자격의 획득을 준비하며, 해당 자격이 요구하는 실제적인 역량을 보유한 인력으로 발전할 수 있는 기재로 작용할 수 있도록 하는 것이 필요할 것으로 판단된다.

제3절 국내 소프트웨어 자격제도 현황 및 소프트웨어 안전과의 연관성

본 절에서는 국내에서 시행 중인 소프트웨어 자격제도를 조사하고, 소프트웨어 안전과의 연관성 및 특징에 대하여 분석하였다. 국내에서 시행 중인 소프트웨어 자격제도 중 소프트웨어 안전과 연관이 자격제도는 소프트웨어 공학, 품질평가 및 시험(Testing)에 관한 것으로, 해당 요소를 다루고 있는 국가공인 및 비(非)공인 소프트웨어 자격증을 위주로 조사하였다.

1. 국가기술자격

소프트웨어 안전에 관련된 국가기술자격은 임베디드기사와 정보처리기사가 있으며, 두 자격증 모두 기사 자격증으로 기사자격의 응시자격[56]은 다음과 같다.

(1) 산업기사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 1년 이상 실무에 종사한 사람

(2) 기능사 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 3년 이상 실무에 종사한 사람

(3) 응시하려는 종목이 속하는 동일 및 유사 직무분야의 다른 종목의 기사 등급 이상의 자격을 취득한 사람

(4) 관련학과의 대학졸업자등 또는 그 졸업예정자

(5) 3년제 전문대학 관련학과 졸업자등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 1년 이상 실무에 종사한 사람

(6) 2년제 전문대학 관련학과 졸업자등으로서 졸업 후 응시하려는 종목이 속하는 동일 유사 직무분야에서 2년 이상 실무에 종사한 사람

(7) 동일 및 유사 직무분야의 기사 수준 기술훈련과정 이수자 또는 그 이수예정자

(8) 동일 및 유사 직무분야의 산업기사 수준 기술훈련과정 이수자로서 이수 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 2년 이상 실무에 종사한 사람

(9) 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 4년 이상 실무에 종사한 사람

(10) 외국에서 동일한 종목에 해당하는 자격을 취득한 사람

56) 큐넷 국가기술자격제도 응시자격별 안내, http://www.q-net.or.kr/crf006.do?id=crf00603, (2016.12.18.)

※ 비고

(1) “졸업자등”이란 「초·중등교육법」 및 「고등교육법」에 따른 학교를 졸업한 사람 및 이와 같은 수준 이상의 학력이 있다고 인정되는 사람을 말한다. 다만, 대학(산업대학 등 수업연한이 4년 이상인 학교를 포함한다. 이하 “대학등”이라 한다) 및 대학원을 수료한 사람으로서 관련 학위를 취득하지 못한 사람은 “대학졸업자등”으로 보고, 대학등의 전 과정의 2분의 1 이상을 마친 사람은 “2년제 전문대학졸업자등”으로 본다.

(2) “졸업예정자”란 국가기술자격 검정의 필기시험일(필기시험이 없거나 면제되는 경우에는 실기시험의 수험원서 접수마감일을 말한다. 이하 같다) 현재 「초·중등교육법」 및 「고등교육법」에 따라 정해진 학년 중 최종 학년에 재학중인 사람을 말한다. 다만, 「학점인정 등에 관한 법률」 제7조에 따라 106학점 이상을 인정받은 사람(「학점인정 등에 관한 법률」에 따라 인정받은 학점 중 「고등교육법」 제2조제1호부터 제6호까지의 규정에 따른 대학 재학 중 취득한 학점을 전환하여 인정받은 학점 외의 학점이 18학점 이상 포함되어야 한다)은 대학졸업예정자로 보고, 81학점 이상을 인정받은 사람은 3년제 대학졸업예정자로 보며, 41학점 이상을 인정받은 사람은 2년제 대학졸업예정자로 본다.

(3) 「고등교육법」 제50조의2에 따른 전공심화과정의 학사학위를 취득한 사람은 대학졸업자로 보고, 그 졸업예정자는 대학졸업예정자로 본다.

(4) “이수자”란 기사 수준 기술훈련과정 또는 산업기사 수준 기술훈련과정을 마친 사람을 말한다.

(5) 이수예정자”란 국가기술자격 검정의 필기시험일 또는 최초 시험일 현재 기사 수준 기술훈련과정 또는 산업기사 수준 기술훈련과정에서 각 과정의 2분의 1을 초과하여 교육훈련을 받고 있는 사람을 말한다.

1) 정보처리기사[57)]

정보처리기사 자격증은 국내 IT 자격증 중 가장 오래되고 권위 있는 자격증이다. 대부분의 전산직 인력이 취득하는 자격증으로, 근래에는 각종 국가공무원 시험에서 가산점 혜택이 있기 때문에 비전공자들 또한 취득하는 추세이다.

정보처리기사 자격증은 소프트웨어 관련 내용의 기본이 되는 부분을 다룬다는 점에서 소프트웨어 안전과 일정 정도 연관을 가지고 있으며, 소프트웨어 공학 과목은 소프트웨어 안전에 필요한 기본 지식으로써 소프트웨어 안전 자격제도의 시행 시 응시자격으로 활용가능하다. 또한, 국내에서 실시중인 자격증 중에서 가장 대표적인 소프트웨어 관련 자격증이라는 점에 의의가 있다.

<표 3-8> 정보처리기사 자격증의 기본 정보

항목	내용
자격명	정보처리기사 (Engineer Information Processing)
관련부처	미래창조과학부
시행기관	한국산업인력공단
필기검정방법	객관식, 100문항, 2시간 30분
필기합격기준	100점을 만점으로 하여 과목당 40점 이상, 전과목 평균 60점 이상
실기검정방법	필답형, 3시간
실기합격기준	100점을 만점으로 하여 60점 이상
실시기관 홈페이지	http://www.q-net.or.kr

개요 : 컴퓨터를 효과적으로 활용하기 위해서 하드웨어뿐만 아니라 정교한 소프트웨어가 필요 하다. 이에 따라 우수한 프로그램을 개발하여 업무의 효율성을 높이고, 궁극적으로 국가 발전에 이바지하기 위해서 컴퓨터에 관한 전문적인 지식과 기술을 갖춘 사람을 양성 할 목적으로 제정됨.

변천과정 :

<표 3-9> 정보처리기사의 변천

’74.10.16. 대통령령 제7283호	’98.05.09. 대통령령 제15794호	현재
정보처리기사1급	정보처리기사	정보처리기사

57) 큐넷 정보처리기사, http://www.q-net.or.kr/crf005.do, (2016.12.18.)

수행직무 :

정보시스템의 생명주기 전반에 걸친 프로젝트 업무를 수행하는 직무로서 계획수립, 분석, 설계, 구현, 시험, 운영, 유지보수 등의 업무 수행

진로 및 전망 :

기업체 전산실, 소프트웨어 개발업체, SI (system integration)업체 (정보통신, 시스템 구축 회사 등), 정부기관, 언론기관, 교육 및 연구기관, 금융기관, 보험업, 병원 등 컴퓨터 시스템을 개발 및 운용하거나, 데이터 통신을 이용하여 정보처리를 시행하는 업체에서 활동하고 있다. 품질검사 전문기관 기술 인력과 감리 자격을 취득하여 감리 전문회사의 감리 담당자로 진출할 수 있다. 3년 이상의 실무경력이 있는 자는 측량분야 수치지도제작업의 정보처리 담당자로 진출가능하고, 정보통신부의 별정우체국 사무장, 사무주임, 사무보조 등 사무원으로 진출할 수 있다.

과목 및 과목의 세부사항 :

정보처리기사 자격증은 필기고사와 실기고사로 나누어져 있고, 필기과목은 총 다섯 가지로 ‘데이터베이스’, ‘전자계산기 구조’, ‘운영체제’, ‘소프트웨어 공학’, ‘데이터 통신’이 있다.

<표 3-10> 정보처리기사 과목 목록

주요항목	과목	세부항목
필기과목	데이터베이스	데이터베이스의 이해, 일반
	전자계산기 구조	연산 및 제어장치, 기억 및 입출력장치 컴퓨터 구조의 응용
	운영체제	운영체제의 이해, 일반, 활용
	소프트웨어 공학	S/W 공학의 이해 객체지향 기법 , S/W 공학 동향
	데이터통신	데이터 전송 및 제어방식 네트워크 및 프로토콜
실기과목	정보처리 실무	정보처리 실무응용, 정보기술 응용이해

데이터베이스 과목에서는 데이터베이스의 기초, 자료구조, SQL언어, 데이터모델링, 데이터베이스설계 등 데이터베이스 분야의 전반을 다루고 있다.

<표 3-11> 정보처리기사 필기과목 1 : 데이터베이스

주요항목	세부항목	세세항목
데이터베이스의 이해	1. 데이터베이스의 개념	1. 정보처리시스템과 데이터베이스의 개념 2. DBMS(DataBase Management System)의 기능 3. 데이터베이스 시스템의 구성
	2. 자료구조의 기본	1. 기본자료형 2. 선형 및 비선형 구조 3. 정렬, 탐색기법 4. 인덱스구조 5. 파일조직기법
데이터베이스 일반	1. 관계 데이터베이스 모델과 언어	1. 관계데이터모델 2. 관계데이터언어(관계대수, 관계해석) 3. SQL언어(Data Definition Language, Data Manipulation Language, Data Control Language, Embedded SQL) 4. 시스템카탈로그와 뷰
	2. 데이터모델링 및 설계	1. 데이터모델 개념 2. 개체-관계(E-R)모델 3. 논리적 데이터모델(관계형, 계층형, 네트워크형) 4. 물리적 데이터베이스 설계 5. 관계 데이터베이스의 정규화
	3. 데이터베이스 고급기능	1. 트랜잭션 개념 2. 데이터베이스제어(보안, 무결성, 병행제어, 회복기법) 개념 3. 분산 데이터베이스
	4. 전산영어	1. 자료구조 관련 용어 2. 데이터베이스 관련 용어

전자계산기 구조 과목에서는 컴퓨터의 기본적인 구조에 대해서 다룬다. 이를 위하여 논리회로부터 프로세서 및 제어, 메모리, 입출력, 마지막으로 병렬컴퓨팅까지 다루고 있다.

<표 3-12> 정보처리기사 필기과목 2 : 전자계산기 구조

주요항목	세부항목	세세항목
연산 및 제어장치	1. 논리회로	1. 조합논리회로, 2. 순서논리회로
	2. 프로세서	1. 명령어(Instruction) 2. 레지스터와 ALU(Arithmetic Logic Unit) 구조
	3. 명령실행과 제어	1. 마이크로 오퍼레이션, 2. 제어데이터 3. 제어규칙
기억 및 입출력장치	1. 기억장치	1. 메모리 계통, 2. 주 및 보조기억장치의 특성 3. Cache, associative 기억장치 4. Virtual 기억장치 등
	2. 입력 및 출력	1. 입·출력에 필요한 기능 2. DMA 및 채널, 3. 인터럽트 체제와 동작원리
컴퓨터 구조의 응용	1. 병렬컴퓨터 구조	1. 병렬컴퓨터 구조의 기본

운영체제 과목에서는 운영체제의 기초에 해당하는 개요부터 프로세스 관리, 메모리 관리, 정보 관리, 분산운영체제, 운영체제의 활용을 다룬다.

<표 3-13> 정보처리기사 필기과목 3 : 운영체제

주요항목	세부항목	세세항목
운영체제의 이해	1. 운영체제의 개요	1. 운영체제의 개념 및 종류 2. 시스템 소프트웨어의 종류
운영체제 일반	1. 프로세스 관리	1. 프로세스의 개념, 2. Concurrent 프로세스 3. 교착상태, 4. 스케줄링
	2. 기억장치 관리	1. 주기억장치 관리기법, 2. 가상기억장치 3. 보조기억장치, 4. 기억장치 계층
	3. 정보관리	1. 파일시스템, 2. 자원보호, 3. 보안
	4. 분산운영 체제의 기본	1. 개념 및 특징, 2. 분산운영체제 3. 병렬처리시스템
운영체제의 활용	1. 운영체제의 실제	1. UNIX의 기본 2. PC-운영체제의 기본

소프트웨어 공학 과목에서는 소프트웨어 공학의 개념을 시작으로 프로젝트의 계획이나 일정, 품질보증 위험관리 등을 포함하는 프로젝트 관리와 개발방법론, 객체지향 분석, 설계, 개발, 그리고 최근 소프트웨어 공학의 동향에 대해서 다룬다.

<표 3-14> 정보처리기사 필기과목 4 : 소프트웨어 공학

주요항목	세부항목	세세항목
SW 공학의 이해	1. SW 공학의 개념	1. S/W 공학의 개념, 발전, 2. S/W의 특성 3. S/W 수명주기 개념, 모형
	2. SW 프로젝트 관리	1. 개념, 2. 프로젝트 계획 및 예측 3. 프로젝트 일정, 4. S/W 품질보증, 5. 위험관리
	3. 전통적 SW 개발 방법론	1. 분석, 2. 설계, 3. 구현, 4. 시험, 5. 유지 보수
객체지향 기법	1. 객체지향 SW 공학	1. 개념 및 원칙, 2. 객체지향 분석, 설계, 테스트
SW 공학 동향	1. SW 공학의 발전적 주제	1. S/W 재사용, 재공학 2. Client/Server S/W 공학 3. Computer Aided S/W 공학(CASE) 4. 기타 S/W 공학 발전 동향

데이터통신 과목에서는 기초적인 데이터전송에 관한 내용을 기반으로, 통신 및 네트워크에 대한 내용을 다룬다. 데이터전송 이론과 전송제어, 네트워크, 통신프로토콜 통신제어 등도 함께 평가한다.

<표 3-15> 정보처리기사 필기과목 5 : 데이터통신

주요항목	세부항목	세세항목
데이터 전송 및 제어방식	1. 데이터 전송 이론	1. 전송속도, 2. 아날로그, 디지털 데이터 전송방식 3. 신호변환방식
	2. 전송제어 방식	1. 전송제어 절차, 2. 베이직, 동기, 비동기 제어 3. 에러제어 방식
네트워크 및 프로토콜	1. 네트워크	1. 전용회선, 공중회선 방식, 2. VAN(Value-Added Network), 3. LAN(Local Area Network) 4. 인터네트워킹, 5. ON-Line 과 OFF-Line 접속
	2. 통신 프로토콜	1. OSI 7계층, 2. X. 25, 3. TCP/IP
	3. 통신제어 프로그램	1. 라우팅동기, 2. 회선제어/ 회선망제어 3. OS 통신제어
	4. 회선망 제어	1. Statistical MUX(Multiplexer), TDX(Time Division eXchange), FDM,(Frequency Division Multiplexing) Concentration

실기과목은 정보처리 실무 과목에서는 필기에서 보았던 과목내용의 전반을 다룬다. 업무 프로세스와, 데이터베이스 설계, 구축, 관리, 어플리케이션의 설계 및 개발과 전산 분야의 최근 동향에 대하여 다룬다.

<표 3-16> 정보처리기사 실기과목 : 정보처리 실무

주요항목	세부항목	세세항목
정보처리 실무응용	1. 업무 프로세스 재설계 수행	1. 업무 프로세스를 재설계 등에 대한 실무 개념을 파악할 수 있다. 2. 업무 프로세스를 파악하고 분석할 수 있다. 3. 업무 프로세스의 개선점을 파악할 수 있다. 4. 새로운 업무 프로세스를 설계할 수 있다.
	2. DB 설계, 구축 및 관리	1. 데이터 아키텍처에 대하여 이해할 수 있다. 2. 모델링 작업을 할 수 있다. 3. 데이터 변환을 설계할 수 있다. 4. 스키마를 구성할 수 있다. 5. 무결성을 확인할 수 있다. 6. 정규화 작업을 할 수 있다. 7. 관계 데이터 연산을 할 수 있다. 8. DB 운영 관리를 할 수 있다.
정보처리 실무응용	3. 어플리케이션 설계 및 개발	1. 어플리케이션을 설계할 수 있다. 2. 어플리케이션을 개발할 수 있다. 3. 알고리즘 실무 작업을 처리할 수 있다.
정보기술 응용이해	1. 신기술 동향	1. 최신 기술 용어의 개념을 파악할 수 있다. 2. 신기술의 동향을 파악할 수 있다.
	2. 전산 영어 실무	1. 일반 개념에 관한 내용을 파악할 수 있다. 2. 기타 일반 실무에 관한 내용을 파악할 수 있다.

정보처리 기사 자격의 특징 및 문제점:

정보처리기사 자격증은 국내에서 가장 오래 된 정보기술 관련 자격증으로 유서 깊은 역사를 자랑하며, 전산분야 및 소프트웨어 개발에 관련된 가장 대표적인 자격증으로 여겨지고 있다. 그러나 한편으로는 가장 오래된 자격증이라는 면에서 또한 많은 문제점이 지적되고 있다.

첫 번째로 출제기준의 개정 주기 및 범위에 관련된 문제를 지적할 수 있다. 출제기준이 3년 주기로 바뀌기 때문에 신속히 변화하는 정보기술의 변화를 어느 정도 반영할 수 있다.

실기평가에 “신기술 동향” 항목이 존재하여 해당 문제를 어느 정도 보완할 수 있도록 하고 있으나, 이 부분의 배점이 상대적으로 낮기 때문에 그 영향이 크지 않다는 점은 개선이 필요한 부분이라 하겠다. 또한, 정보기술 분야가 갈수록 심화 및 분화되는 경향을 보이고 있기 때문에, 전산 및 소프트웨어 개발에 대한 전반적인 내용을 다루는 정보처리기사 자격증의 산업현장에서의 실제적인 직무능력을 반영하는 것이 점차 어려운 것으로 판단된다.

두 번째로 실기시험의 문제형식이 부적합한 부분이 존재한다는 점이다. 2016년 2회 시험까지는 40개의 보기 가운데 정답을 마킹하는 40선다 객관식 문제였다. 이는 연간 10만 명이상이 응시하는 정보처리기사 자격증에 있어서, 채점의 편의성을 가져왔다. 하지만, 수험자가 문제의 답 항으로부터 답안을 찾게 되는 등, 실기시험에 어울리지 않는 문제형식을 가지고 있는 단점이 있었다. 이를 보완하고자 2016년 3회 시험부터는 유형이 변경되어 주관식 문제를 출제하도록 바뀌었으며, 2017년부터는 국가직무능력기반(NCS)를 반영하여 출제방식이 변화될 것으로 예정되어 있다.

세 번째로 너무 많은 사람이 정보처리기사 자격증을 보유하고 있으며, 지금도 응시하고 있다는 것이다. 본디 전문가 양성 및 검정을 위하여 만들어진 정보처리기사 자격증이지만, 응시자격의 기준이 비교적 낮기 때문에 연간 10만 명 이상의 상당히 많은 인원이 응시하고 있다. 다른 기사자격증의 경우, 4년제 대학에서 관련학과를 졸업해야 응시자격이 주어지지만, 정보처리기사는 전공에 제한 없이 4년제 대학만 졸업한 사람이라면 모두 응시할 수 있기 때문에 이공계열 비전공자의 응시자가 상당히 많으며, 비전공자들에겐 이공계열 자격증을 취득하기 위한 관문으로 여겨지고 있다. 특히 가산점 축소 및 폐지가 있기 전 까지는 공무원시험 열풍과 함께, 많은 사람들이 단지 공무원시험 가산점을 받기 위하여 응시하곤 했으며, 그로 인하여 자격증의 난이도뿐만 아니라 희소성이 매우 하락하여 실제 산업현장에서는 유명무실한 자격증으로 대우받고 있다. 2015년 정보처리기사 자격증의 합격률은 필기검정 51.3%, 실기검정 56.2%로 매우 높은 합격률을 보이고 있다.

마지막으로, 기출문제 암기만으로 통과가 가능한 필기시험과 사후관리의 미비가 여전한 문제점으로 지적되고 있다.

2) 임베디드기사[58)]

임베디드시스템은 자동차, 의료, 항공, 철도, 모바일, 통신장비, IoT디바이스 등 다양한 산업에서 필수적으로 쓰이고 있는 추세이며, 이러한 임베디드시스템 전문가를 위한 자격증이 바로 임베디드기사 자격증이다. 임베디드시스템의 특성상 특수한 하드웨어 플랫폼을 사용하기 때문에 범용 플랫폼과는 달리 까다로운 품질검증과 테스팅을 필요로 한다. 특히 임베디드시스템은 자동차, 의료, 항공, 철도 등 인간의 안전에 직결되는 부문에서 많이 사용되기 때문에 안전에 대한 요구가 상당히 높은 분야라고 할 수 있겠다.

임베디드기사 자격증은 소프트웨어 안전과 관련된 요구사항 분석 및 설계, 테스트, 품질관리에 대한 내용을 검정 내용에 포함하고 있으며, 특히 컴퓨터 구조의 메모리나 I/O 인터페이스에 대한 부분은 소프트웨어 안전을 보장하는데 중요한 요소로, 소프트웨어 안전 보장의 기본 지식이라 할 수 있다.

<표 3-17> 임베디드기사 자격증의 기본 정보

항목	내용
자격명	임베디드기사 (Engineer Embedded)
관련부처	산업통상자원부
시행기관	한국산업인력공단
필기검정방법	객관식, 80문항, 2시간
필기합격기준	100점을 만점으로 하여 과목당 40점 이상, 전과목 평균 60점 이상
실기검정방법	필답형, 2시간 30분
실기합격기준	100점을 만점으로 하여 60점 이상
실시기관 홈페이지	http://www.q-net.or.kr

개요 :

임베디드 시스템의 하드웨어를 분석하여 하드웨어에 대한 초기화 및 테스트 수행, 운영체제(OS) 부팅을 위한 부트로더를 포함하는 펌웨어와 임베디드 시스템의 OS 관련한 플랫폼 소프트웨어 및 응용 소프트웨어를 설계, 구현하는 능력 평가

변천과정 : 신설 <2011.11.23. 고용노동부령 제35호>

58) 큐넷 임베디드기사, http://www.q-net.or.kr/crf005.do, (2016.12.18.)

수행직무 :

임베디드 시스템 하드웨어에 대한 이해, 임베디드 소프트웨어 플랫폼, 임베디드 시스템 응용 소프트웨어에 대한 기초 지식과 설계 및 응용 능력을 바탕으로 임베디드 시스템에 펌웨어, 운영체제를 이식하고, 응용 프로그램을 설계, 구현 및 테스트를 수행하는 업무 또는 이와 관련된 지도적 업무를 수행하는 직무

진로 및 전망 :

임베디드시스템 하드웨어, 임베디드 소프트웨어 플랫폼, 임베디드 시스템 응용 소프트웨어 분야

과목 및 과목의 세부사항 :

임베디드기사 자격증은 필기고사와 실기고사로 나누어져 있고, 필기과목은 총 네 가지로 '임베디드 하드웨어', '임베디드 펌웨어', '임베디드 플랫폼', '임베디드 소프트웨어'가 있다.

<표 3-18> 임베디드기사 과목 목록

주요항목	과목	세부항목
필기과목	임베디드 하드웨어	논리회로, 컴퓨터 구조와 마이크로프로세서 주변장치
	임베디드 펌웨어	펌웨어, OS(운영체제) 포팅 디바이스 드라이버 개발
	임베디드 플랫폼	OS 리눅스 커널프로그래밍, 시스템 프로그래밍 네트워크 프로그래밍
	임베디드 SW	임베디드 프로그래밍 개발도구 및 테스팅 소프트웨어공학
실기과목	임베디드 실무	임베디드 하드웨어 임베디드 펌웨어 임베디드 플랫폼 임베디드 소프트웨어 장애 대응

필기 과목인 임베디드 하드웨어 과목은, 가장 기본적인 하드웨어 지식인 논리회로부터 시작하여, 하드웨어 기술 언어 (HDL), CPU와 메모리, I/O 등의 컴퓨터구조와 주변장치에 대한 내용을 다루고 있다.

<표 3-19> 임베디드기사 필기과목 1 : 임베디드 하드웨어

주요항목	세부항목	세세항목
논리회로	1. 논리회로 기초	1. 디지털 시스템의 정의 2. 불 대수, 3. 논리식 간소화, 4. 수의 표현
	2. 조합논리회로	1. 각종 논리게이트 2. 각종 조합논리회로(디코더, 인코더, 멀티플렉서, 가산기 패리티, 에러수정코드 등) 3. 조합논리회로 분석, 설계
	3. 순서논리회로	1. 래치와 플립플롭 2. 각종 순서논리회로(레지스터, 카운터, 시프터 등) 3. 순서논리회로 분석, 설계
	4. 메모리	1. 각종 메모리(RAM, ROM, EPROM, EEPROM, AND/NOR 플래시)
	5. HDL(HW Description Language)	1. 프로그래머블 로직, FPGA(Field-Programmable Gate Array) 2. Verilog, VHDL(VHSIC Hardware Description Language) 3. Verilog를 이용한 논리회로설계
컴퓨터 구조와 마이크로프로세서	1. CPU(중앙처리장치) 구조	1. CPU/마이크로프로세서의 구조 2. 버스 시스템, 3. 명령어(instruction) 집합 구조 4. 어드레싱 모드, 5. 마이크로 아키텍처 (파이프라인, 퍼스칼라, 분기예측 등), 6. ARM CPU
	2. 메모리 시스템	1. 메모리 계층구조, 2. 캐시메모리 3. MMU(Memory Management Unit)와 가상메모리 시스템, 페이징
	3. I/O 인터페이스	1. 입·출력장치의 매핑, 2. 폴링, 인터럽트 3. DMA(Direct Memory Access), 4. 입·출력 버퍼링
	4. 임베디드 시스템	1. 임베디드 시스템 구조, 개발
주변장치	1. 입·출력 포트	1. GPIO(General Purpose Input/Output)의 설정과 이용 2. 입·출력 레지스터 (Command/Status) 3. 입·출력 포트 멀티플렉싱, 4. 데이터시트의 개념
	2. 주요주변장치	1. 시리얼 포트, 2. 타이머 3. Analog/Digital, Digital/Analog 변환 4. 각종 센서(초음파, 적외선, 온도) 5. 모션 센서(가속, 자이로, 지자기) 6. 입·출력 버스 : I2C(Inter-Integrated Circuit), SPI(Serial Peripheral Interface) 7. 통신장치(Ethernet, Wifi 등), 8. USB 9. 전원제어 인터페이스, 10. 칩 실렉트 로직

임베디드 펌웨어 과목에서는 가장 기본적인 부분인 펌웨어와 부트로더를 시작으로 하여 개발환경 구축, 리눅스 OS포팅, 디바이스 드라이버 개발까지의 내용을 포함하고 있다.

<표 3-20> 임베디드기사 필기과목 2 : 임베디드 펌웨어

주요항목	세부항목	세세항목
펌웨어	1. 펌웨어	1. JTAG 하드웨어 2. 스타트업 코드 3. 메모리 초기화
	2 부트로더	1. 부트로더의 종류와 기능 2. OS 부트과정 3. 플래시 메모리관리 4. 초기 RAM Disk 이미지 5. 네트워크 파일 시스템 이용 6. 부트로더 작성 및 타깃시스템 이식
	3. 전원관리	1. 전원관리 하드웨어 2. OS 전원관리 3. 부트로더의 전원관리
OS 포팅	1. 개발환경구축	1. 리눅스 시스템과 개발 툴에 대한 개요 2. 교차개발 환경의 이해 및 도구 설치 3. 원격 커널 디버깅
	2. 리눅스 내부구조 개요 및 포팅	1. 커널의 소스 트리 구조 2. 커널 빌드 과정 개요 3. 커널 구성(configuration) 방법
	3. 리눅스 부팅	1. 리눅스 부팅 과정 2. init 스크립트 3. busybox와 셸 4. 커널 모듈 관리 5. 공유 라이브러리 관리
디바이스 드라이버 개발	1. 디바이스 드라이버 개념	1. 디바이스 드라이버의 개념 2. 디바이스 드라이버의 종류 3. 리눅스 커널 모듈
	2. 디바이스 드라이버	1. 표준 문자드라이버 API(Application Programming Interface) 2. 시스템 콜에 의한 드라이버 접근 3. 커널 모듈 원격 디버깅
	3. 디바이스 드라이버와 커널 서비스	1. 커널의 주요자료 구조 2. 디바이스 드라이버에서의 버퍼관리 3. 커널 메모리 할당과 해제 4. 상호배제 지원함수 5. 동기/비동기 드라이버 개념 6. 스케줄러를 이용한 대기 7. 커널 타이머 8. 세마포 9. 인터럽트 서비스 10. DMA(Direct Memory Access) 개념

임베디드 플랫폼 과목에서는 운영체제, 리눅스 프로그래밍, 시스템 프로그래밍, 네트워크 프로그래밍 등 개발에 필요한 부분을 다룬다. 메모리 관리 및 I/O 부분은 소프트웨어 안전 보장을 위한 기본 지식이다.

<표 3-21> 임베디드기사 필기과목 3 : 임베디드 플랫폼

주요항목	세부항목	세세항목
OS (운영체제)	1. OS의 기본개념	1. 가상머신, 2. 자원관리자, 3. OS의 분류(실시간 OS, 분산 OS 등)
	2. 프로세스관리	1. 스레드와 프로세스, 2. 프로세스 상태, 3. 스케줄링 기초
	3. CPU 스케줄링	1. 단일프로세서, 멀티프로세서 스케줄링 기법 2. 실시간 스케줄링 기법
	4. 병행성 제어	1. 상호배제, 2. 세마포, 모니터, 3. 교착상태, 4. 교착상태 대처방법
	5. 메모리관리방법	1. 캐시메모리, 2. 가상메모리, 3. 페이징과 세그먼테이션
	6. 장치관리방법	1. 디스크 관리, 2. 파일시스템
리눅스 커널프로그래밍	1. 리눅스 개요	1. 리눅스 설치 및 관리, 2. 커널 구조
	2. 커널 서비스	1. 시스템 콜, 2. 시그널과 인터럽트 3. /proc, /sys 파일 시스템, kobject
	3. 메모리 관리	**1. 주소 공간 및 구조, 2. 가상 메모리, 메모리 매핑** **3. 페이징, 스위칭, 캐싱, 4. 프로세스 관리 및 스케줄링**
	4. 디바이스 관리	1. 디바이스 드라이버 구조. 2. 디바이스 파일 시스템(devfs) 3. 하드웨어 I/O
	5. 파일시스템	1. 가상 파일시스템 (Virtual File System) 2. LVM(Logical Volume Manager)과 RAID 3. JFS(Journaled File System)
	6. 네트워크	1. 멀티플렉싱과 디멀티플렉싱, 2. 리눅스 TCP/IP 스택
시스템 프로그래밍	1. 프로세스 및 파일 처리	1. fork, exec 계열, 2. 저수준과 고수준 파일 핸들링
	2. 메모리	1. 메모리 할당 및 해제, 정렬 및 검색, 2. 메모리 Lock
	3. IPC	1. 메모리맵(mmap), 2. 공유메모리, 3. 세마포. 4. 메시지큐 * IPC : Interprocess Communication
	4. I/O 인터페이스 및 멀티플렉싱	**1. PIPE와 FIFO(First-In, First-Out), 2. 소켓, 3. select, pselect** **4. Non-blocking I/O, 5. poll, epoll**
	5. 스레드 프로그래밍	1. 프로세스의 모듈화, 2. pthread API : 스레드의 생성, 종료 3. Mutex와 조건 변수, 4. Barrier, 여러 가지 locks 5. 스레드의 응용
	6. 시그널처리	1. 유닉스/리눅스 표준 시그널, 2. 시그널 전송과 시그널 핸들링 3. SIGCHLD 시그널과 자식 프로세스
네트워크 프로그래밍	1. 리눅스 OS 개요	1. 리눅스 OS 구조와 시스템 콜, 2. 라이브러리와 시스템 콜
	2. 컴퓨터 네트워크	1. 컴퓨터 네트워크 기본, 2. OSI계층 프로토콜 3. TCP, UDP, IP, 4. 클라이언트/서버 프로그램
	3. 스레드의 개요	1. 스레드 개념, 2. 스레드 생성 및 제어, 3. 스레드간 동기화
	4. 소켓 프로그래밍	1. 소켓의 정의, 2. TCP 소켓, UDP 소켓, 4. 소켓 프로그래밍 응용
	5. 시그널 기본	1. 시그널의 정의, 2. 시그널 핸들러, 3. 시그널전송 에러처리

임베디드 소프트웨어 과목에서는 데이터구조와 C언어, 객체지향 프로그래밍 등의 프로그래밍에 대한 부분과 테스팅 및 개발도구, 소프트웨어공학에 대한 부분을 다룬다. 테스팅 및 개발도구, 소프트웨어공학 과목은 소프트웨어 안전 보장을 위한 기본 지식이다.

<표 3-22> 임베디드기사 필기과목 4 : 임베디드 소프트웨어

주요항목	세부항목	세세항목
임베디드 프로그래밍	1. 데이터 구조	1. 알고리즘의 표현과 분석 2. 배열, 3. 연결 리스트 4. 스택과 큐, 5. 트리, 6. 그래프
	2. C프로그래밍	**1. 데이터 타입과 연산자** **2. 제어흐름, 3. 함수와 프로그램구조** **4. 포인터와 배열, 5. 구조, 6. 입력과 출력**
	3. 객체지향 프로그래밍	**1. 객체지향원리** **2. C++ 개요, 3. C++ 객체지향기능** **4. Java 개요, 5. Java 객체지향기능**
	4. 멀티미디어 정보처리	1. 멀티미디어 정보표현, 2. 멀티미디어 압축 3. 영상 및 신호 처리, 4. 멀티미디어 통신 5. 편집도구 및 저작도구
개발도구 및 테스팅	**1. 개발도구**	**1. 컴파일러, 2. 링커(로더), 3. 디버거**
	2. 테스팅	**1. 테스트계획수립, 2. 테스트설계** **3. 테스트기법, 4. 테스트 자동화 도구**
소프트웨어공학	**1. 개발프로세스**	**1. 기본원리** **2. 프로세스 모델** **3. 요구사항 분석** **4. 시스템 아키텍처** **5. 설계기법** **6. 소프트웨어 테스팅** **7. UML(Unified Modeling Language) 다이어그램**
	2. 프로젝트관리	**1. 프로젝트관리 개요, 2. 품질관리**

실기과목인 임베디드 실무에서는 필기과목에서의 내용을 기초로 하여 필답형으로 수험을 진행한다. 필기과목 중 하나였던 소프트웨어 공학 과목은, 임베디드 소프트웨어 항목의 일부가 되어, 임베디드 소프트웨어 항목에서의 분석 및 설계 부분이 되었다. 추가적으로는 장애대응에 관한 내용이 포함된다.

<표 3-23> 임베디드기사 실기과목 : 임베디드 실무

주요항목	세부항목	세세항목
임베디드 하드웨어	1. 하드웨어 및 회로 분석하기	1. 조합논리회로 및 순서논리회로를 분석, 설계할 수 있다. 2. ROM, EPROM, SRAM, DRAM, 플래시 등 메모리 회로 분석, 설계
	2. 임베디드시스템 성능 및 구조 분석하기	1. 임베디드 프로세서를 위한 기계어 프로그램을 분석, 개발할 수 있다. 2. 임베디드 시스템의 성능에 영향을 미치는 요소를 분석하고 최적화 3. 가상 메모리 시스템을 이해할 수 있다. 4. 임베디드시스템을 구성하는 하드웨어 모듈들 사이의 인터페이스를 이해
	3. 임베디드시스템 주변장치 분석하기	1. 데이터시트를 분석하여 주변 장치의 상태를 읽고 입·출력을 제어하는 프로그램을 작성할 수 있다. 2. 인터럽트 방식의 입·출력, DMA를 이용한 데이터 전송 프로그램 작성 3. 단순 입·출력, 스캐닝 입·출력, 시리얼 포트, 타이머 등을 이용하기 위한 프로그램을 작성할 수 있다. 4. 각종 센서를 이용하기 위한 프로그램을 작성할 수 있다.
임베디드 펌웨어	1. 펌웨어 설계, 구현 및 테스팅하기	1. 컴파일 결과 만들어지는 ELF 포맷과 binutil 도구의 사용법 이해 2. 스타트업 코드를 이해하고 수정할 수 있다. 3. 칩 실렉트 로직을 이해하여 프로그램하며, 메모리 초기화를 할 수 있다. 4. OS의 부트과정을 이해할 수 있다. 5. OS의 부팅에 필요한 초기 RAM Disk를 이해하고 구성할 수 있다. 6. 플래시 메모리 제어 및 관리 프로그램을 작성할 수 있다. 7. OS의 전원관리 기법, 하드웨어의 전원관리 방법, 부트로더의 역할을 이해하고 프로그램 할 수 있다.
	2. 임베디드의 이해 및 포팅하기	1. 커널의 포팅 과정을 이해할 수 있다. 2. 부트로더의 동작을 이해하고 설명할 수 있다 3. 교차개발 환경에 필요한 도구를 이용할 수 있다.
	3. 디바이스 드라이버 작성하기	1. 데이터시트를 이해하고 레지스터의 표현과 메모리 맵을 제시할 수 있다. 2. 디바이스 드라이버의 표준 API를 정의할 수 있다. 3. OS와의 연동을 위한 저수준의 OS API를 활용할 수 있다. 4. 디바이스 초기화 및 데이터 송·수신 프로그램을 작성할 수 있다. 5. Make파일을 이해하고 작성할 수 있다. 6. 인터럽트 처리를 할 수 있다. 7. 구현에 필요한 프로그래밍 언어들(C, C++, Java)을 이해할 수 있다.
임베디드 플랫폼	1. 임베디드 OS의 이해하기	1. 커널의 구조를 이해하고 디렉터리의 역할을 설명할 수 있다. 2. 커널의 주요 기능에 관하여 이해할 수 있다.
	2. 임베디드 커널 프로그래밍하기	1. 프로세스 관리, 메모리 관리, 디바이스 관리, 파일시스템 관리를 위한 시스템 콜을 이해하고 활용할 수 있다.

		2. 스레드 동기화를 위한 세마포, MUTEX 등을 이해하고 적용할 수 있다. 3. 소켓을 이용한 네트워크 프로그래밍을 할 수 있다. 4. IDE(Integrated Development Environment), 교차개발 환경에 필요한 도구를 이용할 수 있다.
임베디드 SW	**1. 임베디드 프로그램 분석 및 설계하기**	**1. 주어진 요구사항을 분석하여 UML 등 소프트웨어 공학적인 다이어그램으로 작성할 수 있다.** **2. 설계 관련 산출물을 읽고 이해할 수 있다.** **3. 개발 환경에 맞는 기술 문서 및 매뉴얼 작성을 할 수 있다.**
	2. 임베디드 프로그램 작성하기	**1. 구현에 필요한 프로그래밍 언어들(C, C++, Java)을 이해할 수 있다.** **2. 주어진 설계결과를 이용하여 목표 프로그래밍언어로 표현할 수 있다.** **3. 개발환경에 적합한 형태로 코딩을 수행할 수 있다.**
	3. 개발도구 및 테스팅기법 활용하기	**1. 컴파일러, IDE 등 개발에 필요한 도구를 이용할 수 있다.** **2. 디버깅 도구를 이용하여 디버깅을 수행할 수 있다.** **3. 사용하는 언어 및 개발 환경에 따라 단위 테스트를 위한 방법을 선정하고, 각 단위간의 상호 작용을 고려한 테스트를 수행할 수 있다.** **4. 단위 테스트를 위한 테스트 케이스를 작성할 수 있다.**
장애 대응	1. 장애 접수 처리하기	1. 임베디드SW 장애대응을 위하여 접수된 장애 내용 유형에 따라 분류 2. 임베디드SW 장애대응을 위하여 분류된 장애에 대해 장애등급 지정 3. 임베디드SW 장애대응을 위하여 처리절차에 따라 관련자에게 이관
	2. 장애 대응 방안 수립하기	1. 임베디드SW 장애 대응 방안 수립을 위하여 식별된 장애의 영향력, 발생가능성, 발생시점을 분석하여 우선순위를 정할 수 있다. 2. 임베디드SW 장애 대응 방안 수립을 위하여 장애의 원인 분석 3. 임베디드SW 장애 대응 방안 수립을 위하여 장애 복구에 소요되는 시간 및 자원을 정의 할 수 있다. 4. 임베디드SW 장애 대응 방안 수립을 위하여 장애를 복구하기 위한 세부 계획을 수립할 수 있다.
	3. 장애 복구하기	1. 임베디드SW 장애복구를 위하여 장애 복구에 필요한 자원 확보 2. 임베디드SW 장애복구를 위하여 장애 원인을 제거할 수 있다. 3. 임베디드SW 장애복구를 위하여 장애 복구에 대한 작업내역 기록 4. 임베디드SW 장애복구 시 예외사항이 발생되었을 경우 비상조치 실시 5. 임베디드SW 장애복구 후 장애 처리 결과를 고객에게 전달
	4. 장애 이력 관리하기	1. 임베디드SW 장애 이력관리를 위하여 장애 조치 완료 보고서를 작성할 수 있다. 2. 임베디드SW 개선을 위하여 장애 처리 결과에 대한 이력 관리 3. 임베디드SW 개선을 위하여 장애 이력을 분석하여 개선사항 도출
	5. 고객 만족도 조사하기	1. 임베디드SW 장애복구 완료 후 장애 처리결과에 대한 고객 만족도를 조사를 할 수 있다. 2. 임베디드SW 장애복구 완료 후 고객 만족도 조사결과를 분석할 수 있다. 3. 임베디드SW 장애복구에 대한 고객만족도 분석 결과를 활용하여 장애 대응 체계를 개선할 수 있다.

임베디드 기사 특징 및 문제점:

임베디드 기사 자격증은 2011년 신설된 자격증으로, 기존의 정보처리기사 자격증으로는 부족했던 하드웨어 부분의 역량과 임베디드 분야의 특수성을 반영하기 위하여 만들어졌다. 정보기술 분야의 폭발적인 성장으로 인해 급속히 변화하는 산업현장에 맞도록 전문화된 자격증이라 할 수 있겠다. 특히, 컴퓨터와 사물과의 융합이 가속화되면서 임베디드시스템 전문가의 수요는 나날이 늘어나고 있다는 점에서 이를 반영하는 자격제도라고 할 수 있을 것이다.

해당 자격증의 합격률은 2015년 기준으로 실기검정 37.9%, 필기검정 18.9%이다.

이 자격증의 문제점으로는 먼저 출제기준의 개정 주기에 관련된 문제를 지적할 수 있다. 정보처리기사 자격증과 비교해 보면, 보다 구체적이고 전문적인 분야를 다루고 있다는 점에서 전문가의 역량을 평가하는 데에는 적합하다고 할 수 있다. 하지만 제도적 측면에서, 3년을 주기로 출제기준을 개정하기 때문에 신속히 변화하는 정보기술 분야에 적합하지 않을 수 있다. 정보처리기사 자격증은 이러한 점을 보완하기 위해서 기술동향에 관련된 영역을 추가로 출제하고 있다. 이처럼 신속히 변화하는 정보기술 분야의 특성을 반영하기 위하여 정보처리기사 자격증의 기술동향 부분을 차용하는 것을 고려해볼 만하다. 또한, 임베디드 시스템의 특성을 고려할 때 기존의 필답형 실기검정체계를 탈피하고 실전능력을 테스트할 수 있는 검정 방법에 대한 검토도 필요할 것으로 판단된다.

2. 국가공인민간자격

1) 정보시스템감리사[59]

정보시스템감리사는 정보시스템의 구축과 운영에 관한 부분을 종합적으로 점검 및 평가하고, 개선이 필요한 사항을 감리하여 의뢰인에게 상담과 권고를 하는 인력을 목표로 하는 자격증이다. 소프트웨어 안전은 소프트웨어의 개발이나 테스팅 뿐만 아니라, 컨설팅, 감리/감사, 관리 등도 매우 중요한 부분임을 감안할 때, 소프트웨어 안전 관련 자격을 설계에 주요하게 연관되는 자격이라 할 수 있다. 또한 정보시스템감리사 자격이 이미 보수교육제도를 실시하고 있으며, 세 가지 단계의 전형을 거치는 다방면의 검정방식을 가지고 있다는 특징이 있으며, 이러한 특징은 소프트웨어 안전 전문가 자격의 설계에 고려하여 반영하였다. 세 가시지의 전형은 필기전형과 실무(실기)전형, 면접전형이다. 1차로 필기전형을 합격하면 면접전형 단계로, 면접전형을 합격하면 이론교육 단계로, 이론교육을 합격하면 실무교육을 거쳐 감리사 자격증을 얻을 수 있다. 합격률은 5% 정도로 다른 자격증에 비해 낮은 편이다.[60]

<표 3-24> 정보시스템감리사 자격증의 기본 정보

항목	내용
자격명	정보시스템감리사 (Infomation Systems Auditor)
관련부처	없음(민간)
자격발급기관	한국정보화진흥원
필기검정방법	객관식, 120문항, 2시간
실시기관 홈페이지	http://auditor.nia.or.kr/

개요 : 최근 급증하고 있는 감리수요의 충족과 민간부문의 감리 활성화를 위하여 한국정보화진흥원에서는 2001년부터 국가공인 정보시스템감리사 자격검정을 매년 1회 실시하고 으며, 정보처리 분야에서 고급기술자 이상의 자격을 갖춘 자를 대상으로 자격검정(필기전형, 면접전형, 이론교육 및 실무교육)을 실시한 후 정보시스템 감리사 자격증을 교부하고 있다.

응시자격요건 :

(1) 기술사

59) 한국정보화진흥원, http://auditor.nia.or.kr, (2016.12.18.)
60) 2015년 기준, http://www.ddaily.co.kr/news/article.html?no=133924

(2) 기사 자격 취득 후 정보처리분야의 실무경력 7년 이상인 자

(3) 산업기사 자격 취득 후 정보처리분야의 실무경력 10년 이상인 자

(4) 박사학위 취득 자(정보처리분야 학위소지자)

(5) 석사학위 취득 후 정보처리분야의 실무경력 6년 이상인 자

(6) 학사학위 취득 후 정보처리분야의 실무경력 9년 이상인 자

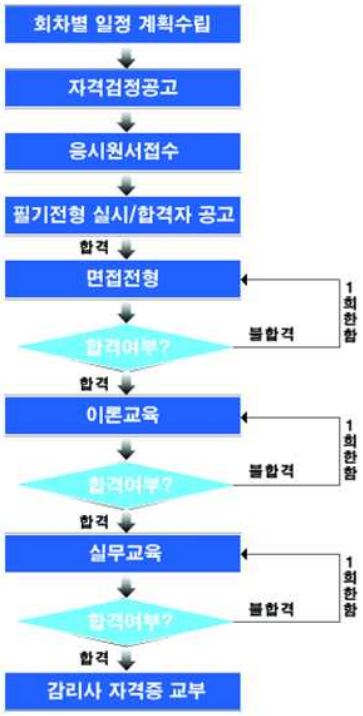
(7) 전문대학 졸업 후 정보처리분야의 실무경력 12년 이상인 자

(8) 고등학교 졸업 후 정보처리분야의 실무경력 15년 이상인 자

<표 3-25> 정보시스템감리사 자격검정절차

주요항목	과목	세부항목
필기전형	시험 과목	감리 및 사업관리
		소프트웨어 공학
		데이터베이스
		시스템구조
		보안
	합격자 선정	전형 과목별 100점 만점에 과목별 40점 이상인자 중 고득점자 순으로 합격자 선정(40점미만 과락)
면접전형	대상자	해당 회 차의 필기전형 합격자 이전 회 차의 면접전형 탈락자로 1회의 면접전형 기회 부여자
	합격자 선정	면접전형 평가에 따라 합격자 선정
이론교육	대상자	해당 회차 면접전형 합격자 이전 이론교육 탈락자로 차회 1회에 한하여 재교육 기회 부여자
	방법 및 과목	이론 강의 및 감리사례 실습을 병행하여 실시 이론 강의 : 정보시스템 감리를 위해 필수적인 감리관련 전문지식을 중점적으로 교육
	합격자 선정	이론교육 시험, 출석률을 토대로 결정
실무교육	대상자	해당 회 차의 이론교육 합격자 이전 회 차의 실무교육 탈락자로 1회의 재교육 기회 부여자
	교육 방법	개인의 희망분야 및 전문분야를 고려하여 감리가능 분야를 선정 감리실무교육 기간 중 개인별로 실무 결과보고서 작성 및 제출
	합격자 선정	실무결과 보고서 및 인터뷰 등을 근거로 평가하여 합격자 선정

[그림 3-3] 정보시스템감리사 자격검정절차



과목 및 과목의 세부사항 :

정보시스템 감리사의 자격검정절차를 보면 기존의 기사/산업기사 자격증과는 달리 필기전형과 실무(실기)전형, 면접전형으로 세 가지의 전형을 거친다. 이와 더불어 각 전형에 따른 교육을 수행하기 때문에 일반적인 검정형 자격과는 다르다고 할 수 있겠다. 과목으로는 '감리 및 사업관리', '소프트웨어 공학', '데이터베이스', '시스템구조' 그리고 '보안' 까지 5개의 과목으로 구성되어 있다. 기출문제는 필기전형의 문제만 공개하고 있기 때문에 면접전형이나 실무전형에서의 문제를 알 수는 없겠지만 필기전형에 해당하는 내용을 기준으로 출제가 될 것으로 예상된다.

정보시스템감리사 자격의 특징:

정보시스템감리사 자격증의 특징으로는 자격검정에서 면접전형과 이론전형, 실무전형으로 이루어진 세 단계의 전형을 거친다는 점이다. 기존 국가기술자격제도에서의 문제점으로 거론되는 기출문제를 통한 단순암기식 자격취득이 면접과 교육을 통하여 비교적 예방될 수 있는 형식으로 판단된다. 또한 위에 언급했던 두 개의 기사자격증과는 달리 자격의 유효기간이 있다. 5년의 유효기한을 부여하며 보수교육을 이수하여야만 자격을 갱신하는 방식으로 기존 자격증에서 공통적으로 문제점으로 지적되던 부분을 어느 정도 해소하였다.

〈표 3-26〉 정보시스템 감리사 필기과목

주요 항목	세부항목	세세항목
감리 및 사업 관리	1. 정보화 관련 법/제도 및 국내외 지침, 가이드	○ 국가정보화기본법, 전자정부법, 소프트웨어산업진흥법 등 각종 법령 ○ 계약예규, 중앙행정기관 전자정부사업 사전협의 지침 등 각종 예규 ○ 정보시스템 구축운영 지침, 공공기관의 데이터베이스 품질관리 지침, 행정정보 데이터베이스 표준화 지침, 전자정부서비스 호환성 준수 지침, 소프트웨어사업 하도급계약의 적정성 판단기준 등 각종 고시 ○ 행정기관을 위한 정보화사업 단계별관리·점검가이드, CBD(Component-Based Development) SW개발 표준 산출물관리 가이드, 소프트웨어 사업대가 산정가이드 등 각종 가이드 ○ IT 거버넌스, CoBIT(Control Objectives for Information and Related Technologies) 등 국외 관련 지침
	2. 감리 관련 법제도 및 관련 기술	○ 전자정부법 및 동법 시행령, 정보시스템감리기준 등 감리 법제도 ○ 정보시스템감리 발주관리가이드 및 감리수행가이드, 정보시스템감리 점검가이드(구 감리지침 V1.0, '09.5. 28), 정보시스템 감리원 윤리 가이드(NIA, 2015) 등 가이드, ○ 감리 방법론, 감리기법 및 도구
	3. 조직 관리론	○ 조직구조, 조직이론, 조직설계, ○ 인적 자원관리, 의사소통관리
	4. 프로젝트관리	○ KS A 21500(ISO 21500) 등 프로젝트관리 관련 표준 ○ 범위/일정/품질/위험/형상/비용/통합 관리 등
소프트웨어 공학	1. 개발방법론	○ 구조적, 정보공학, 객체지향 ○ CBD, Agile, AOP(Aspect-Oriented Programming) 등 ○ 프로세스 모델: 폭포수, 프로타이핑, 점진적, 진화적, 나선형, V 모델 등
	2. 요구사항분석	○ 요구사항도출, 분석, 명세, 추적
	3. 설계	○ 객체지향 개념, 설계원리, 설계패턴, UML모델링 ○ 아키텍처 스타일(계층구조, 클라이언트서버, 트랜잭션처리, MVC(Model-View-Controller), 이벤트중심 등) ○ 사용자 인터페이스 설계
	4. 구현	○ 프로그래밍언어이론, ○ 프로그래밍언어 및 환경(코딩원리, 코딩오류, 코딩스타일, UML과 코딩 등) ○ 웹접근성, 웹호환성 점검
	5. 시험	○ 단위, 모듈, 연계, 통합, 시스템, 성능, 인수 등 ○ 테스팅 방법 및 도구 ○ ISO 29119, ISO 33063 SW테스트 관련 표준
	6. 유지관리 및 운영	○ 유지관리 개념 및 방법, ○ 형상관리 ○ ITSM(IT Service Management) ○ ITIL(Information Technology Infrastructure Library) : SLA(Service-Level Agreement), SLM(Service-Level Management) 등 ○ 재사용, 재공학, 역공학. 아웃소싱

	7. SW 품질	○ SW Product 품질, ○ 품질보증 ○ SW Process 품질 (CMM : Capability Maturity Model, SPICE : Software Process Improvement and Capability dEtermination, SP : Software Process 인증 등) ○ ISO 9126, 품질체계, 품질 속성 ○ ISO 25000 SQuaRE(System and SW Quality Requirements and Evaluation) 프레임워크 SW 품질관련 표준
	8. 비용산정	○ 비용산정 모델
	9. SW 아키텍처	○ 웹기반기술구조, J2EE, 닷넷 등 개발 플랫폼 ○ 분산컴포넌트 기술, XML 등 ○ 전자정부표준프레임워크 ○ SOA(Service Oriented Architecture) ○ 웹서비스 : SOAP(Simple Object Access Protocol), REST(Representational State Transfer)
데이터베이스	1. DB 개념 및 설계	○ 데이터베이스시스템 개념 및 이론 ○ 데이터 모델의 개념, 관계형/객체지향 DB ○ 데이터베이스 설계, 정규화 ○ 데이터 아키텍처, 데이터베이스 구축 방법론v.4.0(NIA, 2014) ○ 공공데이터베이스 품질관리 지침, 데이터베이스 표준화 지침
	2. DB 언어	○ 관계대수, ○ SQL, 내장 SQL, 절차형 SQL, ODBC/JDBC 등
	3. DBMS 기술	○ DB 성능(인덱스, 튜닝), 트랜잭션, 동시성 제어 ○ 데이터 백업 및 복구, 데이터 마이그레이션 ○ 저장장치, 메모리 DB, ○ 데이터베이스 보안
	4. DB 응용	○ 웹기반정보시스템 ○ 정보검색, 검색엔진 ○ 멀티미디어, GIS(Geographic Information System) 등 ○ 분산 DBMS, 모바일DBMS, Open API, 공공데이터
	5. 빅데이터	○ 빅데이터 관련기술(저장, 처리, 분석, 시각화) ○ NoSQL ○ 데이터마이닝, DW(Data Warehouse)
시스템 구조	1. 공통 기술	○ IT 및 정보화 관련 표준, 국내외 표준화 동향
	2. 아키텍처 설계 및 구축	○ 하드웨어 아키텍처(이중화, 가상화, 고가용성, 원격 백업기술 등) ○ 네트워크 아키텍처(가상화, 이중화, 망분리, L4/L3 스위치 등) ○ 정보기술 아키텍처(EA), ○ 시스템 시험, 시험운영, 시범운영, 전개
	3. 시스템 성능/용량 산정	○ 시스템 성능: 부하 분산, 최적화, 용량산정 등
	4. 컴퓨터시스템	○ 분산시스템, 실시간 시스템, 내장형시스템, 시스템 모델링 및 성능분석 ○ 시스템소프트웨어(운영체제)

	5. 통신시스템	○ 무선통신, 유선통신, 컴퓨터 통신/멀티미디어통신, 이동통신/위성통신, 광통신, 데이터 통신/부가통신, 영상통신/화상통신, 광대역 통신
	6. 네트워크	○ N/W 구조 및 설계(이중화, 스위칭 이론, IPV6 등) ○ N/W 관리 ○ N/W 장비(라우터, 스위치, 허브 등) ○ N/W 기술(홈네트워크, WPAN, BcN, IPTV, Wibro, HSDPA 등)
	7. 경영정보시스템	○ 경영정보(SCM(Supply Chain Management), CRM(Customer Relationship Management), BPM(Business Process Management), ERP(Enterprise Resources Planning), 전자상거래 등)
	8. 기타 신기술	○ 컴퓨팅 기술(Green IT, 클라우드/그리드 컴퓨팅 등) ○ 모바일 컴퓨팅 ○ 빅데이터플랫폼, 사물인터넷(IoT)
보안	1. 암호 및 보안 프로토콜	○ 암호알고리즘, 해쉬함수, 전자서명, 인증, 키 관리, PKI 등 ○ SSL(Secure Socket Layer), Kerberos, IPSec, PGP(Pretty Good Privacy), S-MIME 등
	2. 네트워크 및 시스템	○ F/W, DMZ(DeMilitarized Zone), IDS(Intrucsion Detection System), IPS(Instrusion Prevention System), VPN(Virtual Private Network), NAC(Network Admission Control) 등 ○ 접근제어(인증, 권한, SSO 등), PC/서버 보안, 무선랜, 망분리 보안
	3. 응용 및 신기술	○ DB, WEB보안/OWASP(Open Web Application Security Project), EAM(Extranet Access Management), DRM(Digital Rights Management), 모바일 앱 및 단말보안 등 ○ 디지털 포렌식, 클라우드 보안, IoT 보안, 최신해킹, 전자거래보안 등 보안 이슈
	4. 개발 및 운영	○ 요소별(서버, DB, 응용, 네트워크, 단말기) 보안관리 ○ 소프트웨어 개발보안, 보안취약점 진단, 외주용역 보안, 개발환경 보안 등
	5. 정보보호 관리 및 법규	○ ISMS(Information Security Management System) 국제표준(ISO/IEC 27000 시리즈) ○ KISA ISMS 관리과정 및 대책(거버넌스, 위험관리, 조직, 인적보안, 업무연속성 관리 등) ○ 정보보호 법규(정보통신망법, 정보통신기반보호법, 정보통신산업진흥법 등) ○ 정보보호 평가제도(ISMS인증, 보안관리 등급제, 정보보호 준비도 평가 등)
	6. 개인정보보호	○ 개인정보보호 법규, 표준, 지침 등 ○ 개인정보보호 제도(개인정보영향평가, PIMS 등) ○ 기술적, 관리적 보호조치(내부관리계획, 암호화, 접근통제 등)

3. 비(非)공인자격

1) 소프트웨어 테스트 전문가 자격증[61]

소프트웨어 테스트 전문가 자격증은 개발업무 중에서도 테스팅에 관련된 능력을 중점적으로 평가하는 자격증이다. 안전에 관련된 소프트웨어일수록 면밀하고 강도 높은 테스트가 요구된다는 점에서 소프트웨어 안전 분야와 밀접한 관련이 있다고 할 수 있는 자격 제도이다.

<표 3-27> 소프트웨어 테스트 전문가 자격증의 기본 정보

항목	내용
자격명	소프트웨어 테스트 전문가 자격증
영문명	CSTS: Certified Software Test Specialist
관련부처	없음(민간)
자격발급기관	한국정보통신기술협회 (TTA)
검정방법(일반과정)	객관식, 50문항, 80분
검정방법(고급과정)	총 2시간 객관식+주관식(40문항), 복합형(2문항)
실시기관 홈페이지	https://edu.tta.or.kr/

개요 : 검증된 소프트웨어 테스트 전문 인력을 양성하고, 국내 소프트웨어 품질향상을 위한 기반을 마련하고자 소프트웨어 테스트 전문가 자격시험을 실시한다.

소프트웨어 테스트 전문가 자격의 특징 및 문제점:

소프트웨어 테스트 전문가 자격증은 이전에 소개했던 자격증들과는 달리 비공인 자격증이다. 한국정보통신기술협회(TTA)에서 주관하는 자체적인 교육을 실시하고 있으며, 교육을 이수하지 않아도 시험에 응시할 수 있다. 앞서 언급한 두 가지의 기사자격증과는 달리, 소프트웨어 테스트 전문가 자격증 고급과정에서는 실기시험에서 필답형 문제와 더불어 작업형의 문제도 출제된다. 이는 채점 편의성을 위하여 실기시험답지 않게 진행되고 있는 소프트웨어 관련 국가기술자격과 대비되는 부분으로, 실무능력을 직접 검정한다는 점에서 긍정적이라 할 수 있겠다.

단점으로는, 먼저 국가공인을 받지 못했다는 점이 있다. 이에 따라 정부차원의 우대혜택이

61) TTA 아카데미, https://edu.tta.or.kr, (2016.12.18.)

나 경력우대 등을 얻을 수 없는 것이다. 또한, 해외에서 운영하는 국제적인 소프트웨어 테스트 전문가 대비 인지도가 높지 않다는 점과 특별한 사후관리 정책이 없다는 것이 아쉬운 부분이라 하겠다.

과목 및 과목의 세부사항 :

i. 일반과정 - CSTS Foundation Level

검정기준 : 소프트웨어 테스트 계획, 설계, 수행, 관리 등에 대한 기본지식을 갖추고 있어 소프트웨어 테스트 실무 업무를 수행할 수 있는 수준

<표 3-28> 소프트웨어 테스트 전문가 자격증 일반과정 세부사항

검정방법	총문항수	제한시간	합격기준
객관식	50문항	80분	75점 이상 (100점 만점)

검정범위	세부항목
테스트 개요	테스트의 개념 및 필요성, 원칙 SW 개발 모델과 테스트 테스트 환경
블랙박스 테스트 (동적테스트)	블랙박스 테스트 이해 블랙박스 테스트 케이스 설계기법
화이트박스 테스트 (동적테스트)	화이트박스 테스트 이해 화이트박스 테스트 케이스 설계기법
정적 테스트	정적 테스트 이해 정적 테스트 종류 및 기법 활용
테스트 계획 및 관리 (분석/설계/완료)	테스트 계획, 분석, 설계, 관리,완료
테스트 자동화	테스트 자동화 필요성, 도구
테스트 환경구축	테스트 환경 구축 개요 동적/정적 분석 도구

ii. 고급과정 - CSTS Advanced Level

검정기준 : 일반자격에서 요구되는 기본지식에 더하여 소프트웨어 개발 단계별 테스트를 계획, 설계, 실행할 수 있고, 성능테스트, 표준적합성 테스트 등 전문적인 테스트를 계획, 설계, 수행 및 평가할 수 있는 수준

응시자격 : 소프트웨어 개발 및 테스트 관련 분야 5년 이상의 경력자 또는 CSTS 일반 자격취득자 중 해당 분야 3년 이상의 경력자

※ 경력인정 학위 조건

① 소프트웨어 관련 분야 석사학위 보유 시 경력 1년 인정

② 소프트웨어 관련 분야 박사학위 보유 시 경력 3년 인정

〈표 3-29〉 소프트웨어 테스트 전문가 자격증 고급과정 세부사항

검정방법	총문항수	배점	제한시간	합격기준
객관식, 주관식	40문항	80점	120분	75점 이상 (100점 만점)
실기(복합형)	2문항	20점		

검정범위	세부항목
테스트 개요	테스트의 이해, 종류, 테스트 환경
SW 개발 단계별 테스트	SW 테스트 국제 표준 SW 구조적 분석 및 설계 테스트 계획 및 실행
블랙박스 테스트	블랙박스 테스트 이해 블랙박스 테스트 케이스 설계기법
화이트박스 테스트	화이트박스 테스트 이해 화이트박스 테스트 케이스 설계기법
정적 테스트	정적 테스트 이해 정적 테스트 종류 및 기법 활용
성능 테스트	성능 테스트 개요, 전략, 실행
표준적합성 테스트	표준적합성 테스트 개요, 실행
테스트 계획 및 관리	테스트 계획, 환경 분석, 문서, 관리

제4절 정보보안 관련 자격제도 분석

본 절에서 다루는 정보보안 관련 자격제도는 정보보안 관련 국가기술자격인, 정보보안기사와 정보보안산업기사 중 상위 자격증인 정보보안기사를 근간으로 분석을 수행하였다.

1. 정보보안 관련 정책 현황[62)]

2014년 한국수력원자력의 원전설계도 유출사건으로 인하여 정부는 범정부차원의 사이버안보 역량 강화, 핵심기술 개발 및 인력양성, 국제공조 확대, 업무수행체계 정비, 컨트롤타워 강화 등의 핵심과제를 담은 <2005년 국가 사이버안보 강화방안>을 마련하였다. 그 내용으로는 국가 정책적으로 사이버안보에 대한 투자와, 전문화된 인적자원 양성 등의 내용이 담겨 있다.

<표 3-30> 2015년 국가 사이버안보 강화방안

목표	실천방안
범정부 차원의 사이버안보 역량 강화	1. 중앙행정기관, 지방자치단체와 주요기반시설 관리기관의 보안능력 확충을 위한 사이버보안 전담조직의 신설·확대의 추진 2. 각급기관의 정보보호예산을 별도 항목으로 분리하고 취약점 분석·평가 지원, 사이버징후 탐지·대응 3. 기구 운영, 업무망과 인터넷 분리 등 관련 예산의 확대 4. 민·관·군 합동 사이버위기 대응 실전훈련을 강화 5. 사이버위협 정보 종합 수집·분석·공유 시스템의 보강
사이버안보 핵심기술 개발 및 정예요원 육성을 적극 추진	1. 사이버 능력이 우수한 특기자 전형의 사이버특화 고교·대학의 확대 2. 軍에서 전문 인력을 효과적으로 활용할 수 있도록 하기 위한 '한국식 탈피오트(Talpoit)[63)]' 체계의 구축 3. 軍전역 후 사회 각 분야에서 활용되도록 사이버인력 생태계 조성 4. 전문기관의 사이버안보 핵심기술 개발 투자 확대 5. 벤처기업 펀딩 및 정부지원사업 확대
사이버 대응작전 조직·인력 확충 및 산업 증진	1. 국가 사이버 대응작전 수행 조직·인력의 확충 2. 관련 연구개발 예산의 확대 3. 주요 정보통신망에 대한 해킹 방지기술 등 보안기술 및 부품 개발 등 관련 산업 육성
국제공조확대	1. 사이버공격에 대해 국제 사회와 공조 대응하기 위해 주요국과 사이버안보 관련 정책 및 정보공유 확대

62) 박영철 외 (2015), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원
63) 탈피오트는 우수한 인재가 군복무 기간 동안 과학기술 분야에서 연구할 수 있도록 한 이스라엘의 군복무제도

	2. 국제기구와의 긴밀한 협력을 통하여 사이버공격에 대한 억지력 강화 및 국제규범 마련 노력에 적극 동참
사이버안보 관련 법령 정비 추진	국가 사이버안보 정책 의사결정의 일원화 등을 위해 사이버안보 관련 법령을 보완하여 업무수행체계 기반을 지속 정비

자료 : 국무조정실 보도자료, “‘국가 사이버안보 태세 역량’ 대폭 강화한다.”, 박영철 외 (2015), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원, 17쪽에서 재인용

실제로 2015년 이후 뿐만 아니라, 그 이전 시기에도 정보 보안 관련 전문인력 양성에 대한 요구 및 이에 대한 정책적 대응이 꾸준히 진행되어 왔다. 사이버보안관 양성(2009 국가사이버위기 종합대책), 정보보호학과 증설(2011년 국가 사이버안보 마스터플랜), 최정예 정보보호 전문가 양성사업(2013년 국가 사이버안보 종합대책) 등이 이러한 대응의 사례들이다.

2. 정보보안 관련 법체계[64)]

사이버보안에 관련된 국내법은 일반법은 없고 각 분야별 개별법이 존재하는 상황이다. 사이버보안에 관련된 국내법으로는 〈정보통신기반보호법〉, 〈국가정보화기본법〉, 〈전자정부법〉, 〈국가사이버안전관리규정〉, 〈전자금융거래법〉, 〈군사기밀보호법〉, 〈보안업무규정〉, 〈국가사이버안전관리규정〉, 〈정보통신기반보호법〉, 〈개인정보보호법〉이 있다.

그 중에서도 자격제도에 관련한 부분은 〈전자정부법〉의 제2절 제53조 1항에서 찾아볼 수 있으며 그 내용은 아래와 같다.

〈표 3-31〉 정보보안 관련 법안 - 전자정부법

제2절 (정보자원의 효율적 관리기반 조성) 제53조 (정보화인력 개발계획의 수립 등) 1항
중앙사무관장기관의 장은 공무원의 정보화 역량 향상 및 정보자원의 효율적인 관리 등을 도모하기 위하여 정보화인력 개발계획 및 전문인력의 양성, **자격제도** 등에 관한 시책을 수립·추진할 수 있다.

64) 박영철 외 (2015), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원

마찬가지로 자격제도에 관련한 법 내용이 <정보통신망법>에도 수록되어 있다.

<표 3-32> 정보보안 관련 법안 - 정보통신망법

제1장 (총칙) **제11조 (정보통신망 응용서비스의 개발 촉진 등)** **2항**
정부는 민간부문에 의한 정보통신망 응용서비스의 개발을 촉진하기 위하여 재정 및 기술 등 필요한 지원을 할 수 있으며, 정보통신망 응용서비스의 개발에 필요한 **기술인력을 양성**하기 위하여 다음 각 호의 시책을 마련하여야 한다. 1. 각급 학교나 그 밖의 교육기관에서 시행하는 인터넷 교육에 대한 지원 2. 국민에 대한 인터넷 교육의 확대 3. 정보통신망 기술인력 양성사업에 대한 지원 4. 정보통신망 전문기술인력 양성기관의 설립·지원 5. 정보통신망 이용 교육프로그램의 개발 및 보급 지원 6. **정보통신망 관련 기술자격제도의 정착** 및 전문기술인력 수급 지원 7. 그 밖에 정보통신망 관련 기술 인력의 양성에 필요한 사항

현재 시행되고 있는 정보보안기사 및 산업기사 자격증의 국가기술자격화는 위의 내용처럼 정부의 정책적 중요성 표명과, 이에 따른 법적, 제도적 장치의 제정 등을 통하여 발전하여 왔다고 할 수 있다. 본 보고서에서 다루고 있는 소프트웨어 안전 관련 자격증도, 자격증 제도 신설로 이루고자 하는 소프트웨어 안전 관련 핵심 역량을 갖는 인력의 배출이라는 목표를 달성하기 위해서는 일반의 소프트웨어 안전에 대한 인식 제고와 함께 정부의 법체계 및 자격자 우대 정책 등의 정책적 노력이 뒷받침이 필수적이라 하겠다.

3. 정보보안기사 현황[65)]

<표 3-33> 정보보안기사 자격증의 기본 정보

항목	내용
자격명	정보보안기사 (Engineer information security)
관련부처	미래창조과학부
자격발급기관	한국인터넷진흥원
필기검정방법	객관식, 100문항, 2시간 30분
필기합격기준	100점을 만점으로 하여 과목당 40점 이상, 전과목 평균 60점 이상
실기검정방법	필답형, 3시간
실기합격기준	100점을 만점으로 하여 60점 이상
실시기관 홈페이지	http://kisq.or.kr

개요 : IT 및 정보통신 기술에 대한 이론 및 실무지식을 바탕으로 정보보안시스템 및 솔루션 개발, 주요 운영체제 및 네트워크 장비, 정보보안 장비에 대한 운영 및 관리, 조직의 정보보안정책의 수립과 대책수립 및 관리, 정보보호 관련 법규 적용 등의 직무 수행

과목 및 과목의 세부사항 :

정보보안기사기사 자격증은 필기고사와 실기고사로 나누어져 있고, 필기과목은 총 다섯 가지로 ‘시스템 보안’, ‘네트워크 보안’, ‘어플리케이션 보안’, ‘정보보안 일반’, ‘정보보안 관리 및 법규’가 있다.

65) 큐넷 정보보안기사, http://www.q-net.or.kr/crf005.do, (2016.12.18.)

<표 3-34> 정보보안기사 과목 목록

주요항목		세부항목
필기과목	시스템 보안	운영체제 클라이언트 보안 서버보안
	네트워크 보안	네트워크 일반 네트워크 활용 네트워크 기반 공격 이해 네트워크 장비 활용 보안기술 네트워크 보안 동향
	어플리케이션 보안	인터넷 응용 보안 전자상거래 보안 기타 어플리케이션 보안
	정보보안 일반	보안요소 기술, 암호학
	정보보안 관리 및 법규	정보보호 관리 정보보호 관련 법규 정보보호 관련 법규
실기과목	정보보안 실무	시스템 및 네트워크 보안특성 파악 취약점 점검 및 보완 관제 및 대응 정보보호계획 수립 위험분석

시스템 보안 과목에서는 유닉스, 윈도우, 리눅스 등의 주요 운영체제부터 클라이언트에 관련된 대표적인 위협인 트로이목마, 키로그 등 클라이언크 보안과 서버보안을 다루고 있다.

<표 3-35> 정보보안기사 필기과목 1 : 시스템 보안

주요항목	세부항목	세세항목
운영체제	1. 운영체제 개요	1. 운영체제의 주요기능, 구조 3. 운영체제의 기술발전 흐름
	2. 운영체제의 주요 구성기술	1. 프로세스 관리, 2. 기억장치 관리 3. 파일 시스템 관리, 4. 분산 시스템
	3. 운영체제 사례별 특징과 주요 기능	1. 유닉스, 2. 윈도우, 3. 리눅스 4. 보안운영체제 특징
클라이언트 보안	1. 윈도우 보안	1. 설치 및 관리, 2. 공유자료 관리 3. 바이러스와 백신 4. 레지스트리 활용
	2. 인터넷 활용 보안	1. 웹브라우저 보안 2. 메일 클라이언트 보안
	3. 공개 해킹도구에 대한 이해와 대응	1. 트로이목마 SW 2. 크래킹 SW, 3. 키로그 SW
	4. 도구활용 보안관리	1. 클라이언트 보안도구 활용 2. 클라이언트 방화벽 운영
서버보안	1. 인증과 접근통제	1. 계정과 패스워드 보호 2. 파일 시스템 보호 3. 시스템 파일 설정과 관리 4. 시스템 접근통제 기술
	2. 보안관리	1. 운영체제 설치 2. 시스템 최적화 3. 시스템 로그 설정과 관리 4. 서버 해킹 원리 이해 5. 서버관리자의 업무
	3. 서버보안용 SW 설치 및 운영	1. 시스템 취약점 점검도구 2. 시스템 침입 탐지 시스템 3. 무결성 점검도구 4. 접근통제 및 로깅도구 5. 스캔 탐지도구 6. 로깅 및 로그분석도구

네트워크 보안 과목에서는 네트워크의 가장 기초적인 부분인 OSI-7레이어와 TCP/IP, 유닉스/윈도우 네트워크 서비스 등을 다룬다. 그 외에도 라우팅, 유무선 네트워크 장비, 네트워크 기반 프로그램 등이 포함되며, DOS, DDOS, 스니핑 등 공격에 대해서도 다루고 있다.

<표 3-36> 정보보안기사 필기과목 2 : 네트워크 보안

주요항목	세부항목	세세항목
네트워크 일반	1. OSI 7 Layer	1. 각 레이어의 기능 및 역할 2. 레이어별 네트워크 장비
	2. TCP/IP 일반	1. IPv4, IPv6 Addressing 2. 서브네팅 설계 및 활용 3. CIDR, LSM, 4. 데이터 캡슐화 5. 포트주소 의미와 할당 원칙 6. IP, ARP, IGMP, ICMP, UDP, TCP등 각 프로토콜의 원리 및 이해 7. Broadcast 및 Multicast 이해
	3. Unix/Windows 네트워크 서비스	1. DNS(Domain Name System), DHCP(Dynamic Host Configuration Protocol), SNMP(Simple Network Management Protocol), Telnet, FTP(File Transfer Protocol), SMTP(Simple Mail Transfer Protocol) 등 각종 서비스의 원리 및 이해 2. Workgroup 과 Domain 3. 터미널서비스 등 각종 원격관리 서비스 4. 인터넷공유 및 NAT(Network Address Translation) 원리, 활용
네트워크 활용	1. IP Routing	1. IP Routing 종류 및 프로토콜
	2. 네트워크 장비 이해	1. 랜카드, 허브, 스위치 및 브리지 기능 2. VLAN(Virtual LAN) 구성 및 관리 3. 라우터 설정 4. 네트워크 장비를 이용한 네트워크 구성
	3. 무선통신	1. 이동/무선통신 보안
	4. 네트워크기반 프로그램 활용	1. Ping, Traceroute 등 네트워크기반 프로그램의 활용 2. Netstat, Tcpdump 등 활용 3. 네트워크 패킷분석 및 이해 4. 네트워크 문제의 원인분석과 장애처리

네트워크 기반 공격 이해	1. 서비스 거부(Dos) 공격	1. 각종 DoS 공격원리와 대처 방법 2. SYN flooding, smurfing 등 각종 flooding 공격의 원리, 대처
	2. 분산 서비스 거부 공격	1. DDoS 공격 원리 및 대처 방법
	3. 네트워크 스캐닝	1. Remote finger printing 2. IP 스캔, 포트스캔
	4. IP spoofing, Session hijacking	1. IP spoofing 과 Session hijacking의 원리 및 실제
	5. 스니핑 및 암호화 프로토콜	1. 스니핑 공격 원리와 대처 방법
	6. 원격접속 및 공격	1. 각종 공격의 인지 및 이해 2. Trojan, Exploit 등 식별, 대처
네트워크 장비 활용 보안기술	1. 침입탐지시스템(IDS)의 이해	1. 원리, 종류, 작동방식, 특징, 단점 2. False Positive / Negative 이해
	2. 침입 차단시스템(Firewall)의 이해	1. 원리, 종류, 작동방식, 특징, 단점
	3. 가상사설망(VPN)의 이해	1. 원리, 작동방식, 특징, 구성, 단점
	4. 라우터보안 설정	1. 라우터 자체 보안설정
	5. 각 장비의 로그 및 패킷 분석을 통한 공격방식의 이해 및 대처	1. 호스트, IDS, 방화벽, 라우터 등 각종 네트워크 장비 로그 및 패킷 분석
네트워크 보안 동향	1. 최근 네트워크 침해사고 이해	1. 분산반사 서비스 거부 공격 2. 봇넷을 이용한 공격
	2. 최근 네트워크 보안 솔루션	1. 역추적시스템 2. 침입방지시스템 3. ESM(Enterprise Security Management) 4. NAC

어플리케이션 보안 과목에서는 인터넷과 전자상거래, 기타 어플리케이션의 보안을 다룬다. 잘 알려진 FTP, 메일, 웹, 운, 데이터베이스 등의 보안뿐만 아니라 전자상거래의 SSL과 같은 프로토콜을 평가한다.

<표 3-37> 정보보안기사 필기과목 3 : 어플리케이션 보안

주요항목	세부항목	세세항목
인터넷 응용 보안	1. FTP 보안	1. FTP 개념, 서비스 운영 2. FTP 공격 유형, 보안대책
	2. MAIL 보안	1. MAIL 개념, 서비스 운영 2. MAIL 서비스 공격유형, 3. SPAM 대책 4. 악성 MAIL 및 웜 대책 5. MAIL 보안 기술
	3. Web 보안	1. WEB 개념, 서비스 운영 2. WEB 로그 보안, 3. WEB 서비스공격 유형, 4. WEB 보안 개발, 방화벽
	4. DNS 보안	1. DNS 개념 2. DNS 서비스 운영 3. DNS 보안 취약성 4. DNSSEC 기술
	5. DB 보안	1. DB 데이터 보안 2. DB 관리자 권한 보안 3. DBMS 운영 보안 4. DB 보안 개발
전자상거래 보안	1. 전자상거래 보안	1. 지불게이트웨이 2. SET(Secure Electronic Transaction) 프로토콜 3. SSL(Secure Socket Layer) 프로토콜 4. OTP(One Time Password)
	2. 전자상거래 프로토콜	1. 전자지불 방식별 특징 2. 전자지불/화폐 프로토콜 3. 전자입찰 프로토콜 4. 전자투표 프로토콜
	3. 무선 플랫폼에서의 전자상거래 보안	1. 무선플랫폼에서의 전자상거래 보안
	4. 전자상거래 응용보안	1. e-biz를 위한 ebXML 보안
기타 어플리케이션 보안	1. 응용프로그램 보안개발방법	1. 취약점 및 버그방지 개발 방법
	2. 보안기술	1. SSO(Single Sign-On) 2. HSM(Hardware Security Module) 3. DRM

정보보안 일반 과목에서는 보안요소 기술과 암호학에 대해서 다룬다. 디바이스나 사용자 인증기술, 접근통제, 키 분배 프로토콜, 전자서명 인증서 등과 암호알고리즘과 해쉬함수 등 보안에 관련한 보다 심층적인 부분을 평가한다.

<표 3-38> 정보보안기사 필기과목 4 : 정보보안 일반

주요항목	세부항목	세세항목
보안요소 기술	1. 인증기술	1. 사용자 인증기술 2. 메시지출처, 디바이스 인증기술 3. Kerberos 프로토콜
	2. 접근통제정책	1. 접근통제정책 구성요소 2. 임의적, 강제적, 역할기반 접근통제정책 3. 역할기반 접근통제정책 4. 접근통제행렬과 AC(Access Control)
	3. 키 분배 프로토콜	1. KDC(Key Distribution Center) 기반 키 분배 2. Needham-Schroeder 프로토콜 3. Diffie-Hellman 프로토콜 4. RSA 이용 키 분배 방법
	4. 전자서명과 공개키 기반구조(PKI)	1. 전자인증서 구조, 2. 전자서명 보안 서비스 3. PKI 구성방식(계층, 네트워크) 4. CRL(Certificate Revocation List) 구조 및 기능 5. OCSP(Online Certificate Status Protocol) 동작절차 6. 전자서명 관련법규
암호학	1. 암호 알고리즘	1. 암호 관련용어, 2. 암호 공격방식 3. 대칭키, 공개키 암호시스템 특징 4. 대칭키, 공개키 암호시스템 활용 5. 스트림 암호 , 6. 블록 암호 7. 블록 암호공격 8. 인수분해 기반 공개키 암호방식 9. 이산로그 기반 공개키 암호방식
	2. 해쉬함수와 응용	1. 해쉬함수 일반 2. 전용 해쉬함수별 특징 3. 메시지 인증 코드(MAC) 4. 전자서명, 5. 은닉서명, 6. 이중서명

정보보안 관리 및 법규 과목에서는 정보보호와 위험관리 등의 개념이나 절차, 역할, 책임 등을 다루며 정보통신망법이나 전자서명법, 공인인증기관, 공인인증서 등 정보보안 관련 법규를 다루고 있다.

<표 3-39> 정보보안기사 필기과목 5 : 정보보안 관리 및 법규

주요항목	세부항목	세세항목
정보보호 관리	1. 정보보호관리 개념	1. 정보보호의 목적 및 특성 2. 정보보호와 비즈니스 3. 정보보호관리의 개념
	2. 정보보호 정책 및 조직	1. 정보보호 정책의 의미 및 유형 2. 정보보호 정책수립 절차 3. 조직 체계와 역할/책임
	3. 위험관리	1. 위험관리 전략 및 계획수립, 2. 위험분석 3. 정보보호 대책 선정 및 계획서 작성
	4. 대책구현 및 운영	1. 정보보호 대책 구현, 2. 정보보호 교육 및 훈련, 3. 컴퓨터/네트워크 보안운영
	5. 업무연속성 관리	1. 업무지속성 관리체계, 2. 업무연속성 계획 수립, 3. 업무연속성 유지관리
	6. 관련 표준/지침	1. 국제/국가 표준, 2. 인증체계
정보보호 관련 법규	1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 ※ 개인정보보호 기타 정보보호 관련조항에 한정	1. 용어의 정의 2. 정보통신망이용촉진 및 정보보호 등 시책 3. 개인정보 보호, 4. 정보통신망의 안정성 확보, 5. 정보통신망 침해행위
	2. 정보통신기반 보호법	1. 용어의 정의 2. 주요정보통신기반시설 보호체계 3. 주요정보통신기반시설의 지정과 취약점 분석 4. 주요정보통신기반시설의 보호 및 침해 사고의 대응
	3. 정보통신산업 진흥법	1. 지식정보보안컨설팅 전문업체
	4. 전자서명법	1. 용어의 정의, 2. 전자서명의 효력 3. 공인인증기관, 4. 공인인증서
	5. 개인정보보호법	1. 용어의 정의, 2. 개인정보 보호위원회 3. 개인정보의 수집, 이용, 제공 등 단계별 보호기준, 4. 고유 식별정보의 처리제한 5. 영상정보처리기기의 설치 제한 6. 개인정보 영향평가제도 7. 개인정보 유출사실의 통지·신고제도

		8. 정보주체의 권리 보장 9. 개인정보 분쟁조정위원회

실기과목에서는 앞서 필기시험 내용을 기반으로 시스템과 네트워크의 보안특성 및 취약점을 파악하고 점검 및 분석을 하는 내용을 다룬다.

<표 3-40> 정보보안기사 실기과목 : 정보보안실무

주요항목	세부항목	세세항목
시스템 및 네트워크 보안 특성 파악	1. 운영체제별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다. 2. IT환경을 구성하고 있는 개인용 PC 또는 서버에 설치된 운영체제 및 버전정보를 파악할 수 있다. 3. 운영체제 및 버전별로 제공되는 보안서비스, 보안정책 설정, 보안 취약점들을 파악할 수 있다. 4. 내부 사용자와 네트워크 사용자에게 공유되는 객체들의 정보를 수집하고 보안목표에 따라 보안정책이 적절히 설정되었는지 점검할 수 있다. 5. 운영체제별로 동작하는 악성코드의 종류 및 특징을 파악할 수 있다. 6. 운영체제별로 동작하는 악성코드의 종류 및 특징을 파악할 수 있다. 7. 운영체제에서 생성되는 로그 파일 관리가 적절히 설정되어 있는지 점검 할 수 있다. 8. 보안 운영체제가 제공하는 보안서비스 ACL(Access Control List) 강제적 접근 통제정책 설정방법을 파악할 수 있다.
	2. 프로토콜 특징 및 취약점 파악하기	1. OSI 7계층 및 TCP/IP 프로토콜 구성, 각 계층별 기능, 동작구조를 이해할 수 있다. 2. TCP/IP 각 계층에서 처리하는 PDU(Protocol Data Unit) 구조 및 PDU 헤더별 필드 기능을 이해할 수 있다. 3. ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol) 프로토콜 동작절차와 취약점을 이해할 수 있다. 4. IP, ICMP(Internet Control Message Protocol), IGMP(Internet Group Management Protocol) 및 각 Routing 프로토콜 동작절차 및 취약점을 이해할 수 있다. 5. TCP, UDP, SSL, IPSec 프로토콜의 동작절차와 취약점을 이해할 수 있다. 6. 서비스 거부 공격 및 DDos, DRDoS 공격 절차를 이해할 수 있다. 7. 무선 프로토콜 동작 구조 및 보안 취약점을 이해할 수 있다.
	3. 서비스별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. FTP 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다. 3. MAIL 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다. 4. 웹 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다. 5. DNS 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다.

		6. DB 보안 서비스, 환경 설정 및 보안 취약점을 이해할 수 있다. 7. 전자서명, 공개키 기반 구조 구성 및 보안 특성을 이해할 수 있다.
	4. 보안장비 및 네트워크 장비 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집 2. NIC, 허브, 스위치, 브리지 장비의 동작 절차를 이해할 수 있다. 3. VLAN 보안 서비스 및 설정 방법을 이해할 수 있다. 4. 라우터 설정 절차 및 트래픽 통제 기능을 이해할 수 있다. 5. F/W, IDS, IPS 보안 장비의 보안 서비스 및 설정 방법을 이해할 수 있다. 6. NAT 종류 및 동작 절차를 이해할 수 있다. 7. VPN 구현 방법 및 동작 절차를 이해할 수 있다.
	5. 관리대상 시스템 및 네트워크 구조 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집 2. 조직의 보안대상 관리시스템과 네트워크 장비를 파악할 수 있다. 3. 네트워크 구성도를 분석하여 사용 중인 IP 주소, 서브넷 정보를 파악 4. SNMP를 이용한 원격관리기능 또는 스캐닝 도구를 이용하여 관리대상 시스템이 제공하는 서비스를 파악 할 수 있다.
취약점 점검 및 보완	1. 운영체제 및 버전별 취약점 점검, 보완하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다. 2. 운영체제별 보안관리 매뉴얼이나 해당 운영체제 제조사 사이트를 게시된 보안 관리방법과 보안 취약점 정보를 수집할 수 있다. 3. 불필요한 계정이 존재하는지, 악성코드가 설치되어 있는지 점검・보완 4. 공유 폴더에 적절한 접근통제가 보안목표에 적합한지 점검하며, 폴더가 불필요하게 공유되어 있지 않는지 점검・보완할 수 있다. 5. 운영체제별 보호 대상 객체(파일, 디렉터리) 권한 설정이 보안목표에 따라 설정되어 있는지 점검・보완 할 수 있다. 6. 운영체제별 이벤트 로그정보 생성과 관리가 보안목표에 따라 설정되어 있는지 점검・보완할 수 있다. 7. 운영체제 종류 및 버전 정보가 불필요하게 노출되어 있지 않은지 점검・보완할 수 있다. 8. 원격접속 및 원격관리 기능이 보안목표에 따라 설정되어 있는지 점검・보완 할 수 있다.
	2. 서비스 버전별 취약점 점검, 보완하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다. 2. 조직에서 제공하지 않는 서비스가 동작하고 있는지 점검한 후 제거할 수 있다. 3. 파일서버, FTP 서버에 권한이 없는 사용자가 접근할 수 있게 설정되어 있는지, 각 사용자별로 접근할 수 있는 파일/ 디렉터리가 적절히 설정되어 있는지 점검 할 수 있다. 4. 메일 서버 설정에서 스팸 메일 릴레이가 허용되어 있는지, 메일 송수신 프로토콜(SMTP, POP, IMAP) 보안 설정이 적절한지 점검할 수 있다. 5. 웹 서버 설정에서 다양한 공격 유형들(XSS, SQL Injection, 관리자 접근권한설정 등)과 관리자 접근권한 공격으로부터 적절히 보호되고 있는지 점검할 수 있다. 6. DNS 서버 설정에서 불필요한 명령어 수행이 허가되어 있지 않은지, DNS 보안조치(DNSSEC 등)가 적절히 설정되어 있는지 점검할 수 있다.

		7. DB 서버 설정에서 중요 정보가 암호화되어 저장되고 있는지, DB 객체(테이블, 칼럼, 뷰 등)별 접근통제가 적절히 설정되어 있는지 점검
	3. 보안장비 및 네트워크 장비 취약점 점검 보완하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집 2. 스위치, 라우터 장비의 관리자 계정 보안이 적절히 설정되어 있는지 점검할 수 있다. 3. F/W 장비 및 라우터의 보안 설정(IP별 통제, Port별 통제, 사용자 ID별 통제 등)이 보안목표에 따라 적절히 설정되어 있는지 점검 4. IDS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검 5. IPS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검 6. NAT 설정이 보안목표에 따라 적절히 설정되어 있는지 점검 7. 무선접속 장비가 보안목표에 따라 암호화 및 접근통제가 적절히 설정되어 있는지 확인할 수 있다.
	4. 취약점 점검 및 보완사항 이력관리하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집 2. 운영체제별 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완사항을 기록할 수 있다. 3. 조직에서 사용중인 주요 서비스에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 4. 유·무선 네트워크 장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안 취약점 및 보완 사항을 기록 할 수 있다. 5. 보안장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안 취약점 및 보완 사항을 기록할 수 있다.
관제 및 대응	1. 운영체제별 로그정보 점검하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집 2. 스위치, 라우터 장비의 관리자 계정 보안이 적절히 설정되어 있는지 점검할 수 있다. 3. F/W 장비 및 라우터의 보안 설정(IP별 통제, Port별 통제, 사용자 ID별 통제 등)이 보안목표에 따라 적절히 설정되어 있는지 점검 4. IDS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검 5. IPS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검 6. NAT 설정이 보안목표에 따라 적절히 설정되어 있는지 점검 7. 무선접속 장비가 보안목표에 따라 암호화 및 접근통제가 적절히 설정되어 있는지 확인할 수 있다.
	2. 서비스별 로그정보 점검하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다. 2. 주요 서비스(FTP, MAIL, WWW, DNS, 보완 DB 등) 및 버전별로 생성되는 로그정보 저장위치를 파악하고 로그 내용을 분석할 수 있다. 3. 주요 서비스별로 제공되는 로그정보 관리도구를 이용하여 로그정보의 생성수준, 로그정보 구성요소, 로그정보 저장위치 및 저장 공간 등을 설정할 수 있다. 4. 조직의 보안목표에 따라 주요 서비스별 로그정보가 적절히 생성되며 관리되고 있는지 점검할 수 있다.
	3. 보안장비 및 네트워크	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집 2. 유·무선 네트워크 장비(스위치, 라우터, 무선접속 AP 등)별로 생성

	장비 로그정보 점검하기	되는 로그정보 저장위치를 파악하고 로그내용을 분석할 수 있다. 3. 주요 보안장비(F/W, IDS, IPS) 별로 생성되는 로그정보 저장위치를 파악하고 로그 내용을 분석할 수 있다. 4. 유·무선 네트워크 장비별로 제공되는 로그정보 관리 도구를 이용하여 로그정보의 생성수준, 로그정보 구성요소, 로그정보 저장위치 및 저장공간 등을 설정할 수 있다. 5. 주요 보안장비별로 제공되는 로그정보 관리 도구를 이용하여 로그정보의 생성수준, 로그정보 구성요소, 로그정보 저장위치 및 저장공간 등을 설정할 수 있다. 6. 조직의 보안목표에 따라 네트워크 장비/ 보안장비별 로그정보가 적절히 생성되며 관리되고 있는지 점검할 수 있다
	4. 로그정보 통합 및 연관성 점검하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별 보안로그 정보를 통합할 수 있다. 3. 시간대별로 통합 보안로그를 정렬하여 내·외부 공격 시도 및 침투 여부를 점검할 수 있다. 4. IP 주소를 기준으로 통합 보안로그를 검색하여 내·외부 공격 시도 및 침투 여부를 점검 할 수 있다. 5. 통합 보안로그를 점검하여 관리자 계정의 불법 접근 및 변경 여부를 점검할 수 있다.
	5. 데이터 백업, 증거 수집 및 침입자 추적하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 통합 보안로그 분석과정에서 침입 시도 또는 침입이 발견된 경우 침입 대상 시스템 및 장비의 주요 정보 및 보안 설정 정보를 백업할 수 있다. 3. 침입대상 시스템을 대상으로 삭제 또는 변경된 파일에 대한 복구 작업을 수행할 수 있다. 4. 침입자로 의심되는 사용자 및 발신지 IP를 이용하여 통합 보안로그에서 침입자의 침입경로를 추적할 수 있다.
정보보호 계획 수립	1. IT현황 및 자산 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 보호대상 정보자산에 대한 비밀성, 무결성, 가용성 측면의 중요도를 평가할 수 있다. 3. 보호대상 정보 자산의 기능과 저장 위치, 그리고 각 정보 자산에 접근할 수 있는 사용자 또는 역할에 대한 정보를 수집, 분석할 수 있다.
	2. 조직의 요구사항 파악하기	1. 조직이 수행하는 핵심 비즈니스 내용 및 목적을 수집, 정리할 수 있다. 2. 컨설팅 대상 조직의 요구사항과 조직을 구성하는 물리적 환경 및 IT 환경, 기업정보 및 개인정보보호 조직에 대한 정보를 수집할 수 있다. 3. 조직에서 제공하는 주요 서비스 및 네트워크 구조 정보를 수집

	3. 관련법령 검토하기	1. 조직의 비즈니스 내용 및 보안목표 문서를 수집할 수 있다. 2. 조직의 비즈니스 내용과 관련된 법률 및 규정 정보를 수집할 수 있다. 3. 조직의 비즈니스 수행 중 발생될 수 있는 정보보호 의무사항 위반 시 적용되는 법률 및 규정 정보를 수집할 수 있다. 4. 정보보호 관련 법률 및 규정을 준수하기 위해 필요한 조직의 물리적, 관리적 보안대책을 수립할 수 있다.
위험분석	1. 내·외부 위협 분석하기	1. 조직의 비즈니스 목표 및 세부 비즈니스 관련 문서를 수집할 수 있다. 2. 조직의 IT환경 설계도 및 네트워크 구성도를 수집할 수 있다. 3. 조직 내의 주체(사용자), 객체(자원), 접근 연산에 대한 정보를 분석할 수 있다. 4. 조직 내·외부 사용자로부터의 위협 요인을 분석할 수 있다. 5. IT환경을 구성하는 서버, PC, 상용 패키지, 자사 개발 패키지로부터의 위협 요인을 분석할 수 있다. 6. 조직의 네트워크를 구성하는 네트워크 장비, 보안장비로부터의 위협 요인을 분석할 수 있다.
	2. 자산별 취약점 분석하기	1. 조직의 비즈니스목표, IT환경 설계도, 네트워크 구성도 및 내·외부 보안 위협에 대한 정보를 수집할 수 있다. 2. 조직의 H/W 자산(PC, 서버, 네트워크 및 보안장비), S/W자산(운영체제, 상용 및 자가개발 패키지), 정보자산(기업정보 및 고객정보)을 조사하고 식별할 수 있다. 3. 조직의 비즈니스 목표를 기준으로 보호대상 자산별 중요도를 결정할 수 있다. 4. IT환경을 구성하는 서버, 개인용 PC에 설치된 운영체제별로 취약점을 분석할 수 있다. 5. IT환경을 구성하는 상용 패키지 및 자사 개발 패키지에 대한 취약점을 분석할 수 있다.
	3. 취약점 점검보고서 작성하기	1. 조직의 비즈니스 목표, IT 환경 설계도, 네트워크 구성도 및 내·외부 보안 위협 및 취약점 분석 결과 정보를 수집할 수 있다. 2. 조직의 H/W 자산(PC, 서버, 네트워크 및 보안장비)에 대한 중요도, 내·외부 위협 및 취약점 분석 내용을 정리할 수 있다. 3. 조직의 S/W 자산(운영체제, 상용 및 자가 개발 패키지)에 대한 중요도, 내·외부 위협 및 취약점 분석내용을 정리할 수 있다. 4. 조직의 정보 자산(기업정보 및 고객정보)에 대한 중요도, 내·외부 위협 및 취약점 분석 내용을 정리할 수 있다.

4. 정보보안기사 자격증의 특징

정보보안기사 자격증의 경우는 기존의 IT와 관련된 국가기술자격과는 달리 합격률이 매우 낮은 경향을 보인다. 2015년을 기준으로 합격률을 분석해 보면, 필기시험에서 35.78%가 합격하였고, 실기시험에서 12.67%가 합격하였다.[66]

[그림 3-4] 정보보안기사 합격률

자료 : Q-Net, 2015년 정보보안기사 합격률

IT분야의 대표적인 국가기술자격인 정보처리기사는 필기시험 합격률이 51.39%, 실기시험 합격률이 2015년 56.24%에 이르므로, 정보처리기사와 비교하면 합격률 면에서 상당한 차이를 보이고 있다. 이러한 차이의 이유로는 먼저 평가하는 지식의 범위가 넓은 것을 들 수 있다. 정보보안기사는 시스템에 대한 지식으로부터 네트워크, 암호학, 정보보호 관련 법규나 보안 동향까지 검정에서 요구하는 지식의 범위가 넓기 때문에 학습하기도 쉽지 않을뿐더러 출제할 수 있는 범주가 상당히 광범위하다. 간혹 실무적인 문제가 출제되기 때문에 난이도의 편차가 매우 큰 모습을 보이기도 한다. 또한 낮은 합격률의 가장 핵심적인 요소로는 시험문제의 유출이 없다는 부분이다. 대부분의 국가기술자격 시험은 문제은행식 출제방법을 가지므로, 분야에 대한 이해가 없더라도 기출문제만을 암기하여 수험을 보고 자격을 취득할 수 있다. 물론 정보보안기사도 문제은행식으로 출제되지만 필기 실기 모두 문제가 유출되지 않는다는 점에서 상당한 차이를 보인다.

66) 큐넷 정보보안기사, http://www.q-net.or.kr/crf005.do, (2016.12.18.)

제5절 해외 주요국의 소프트웨어 안전 전문가 자격제도

본 절에서는 해외의 소프트웨어 안전 전문가 자격에 대한 사례를 제시하며, 자격 및 인증을 획득 과정, 교육 내용에 대하여 다룬다. 분석한 사례의 해외의 안전 전문가 자격 및 인증 과정들은 교육을 수료 받은 이후 별도의 검정과정을 통하여 개인에 대한 인증을 주는 것과, 정해진 수순에 따라서 교육을 수료하는 경우 인증을 받을 수 있는 과정평가 형태의 인증방법이 함께 존재함을 확인할 수 있었다. 또한 사례에서 다루고 있는 표준은 IEC61508과 같이 포괄적인 범주에서의 소프트웨어 안전부터, ISO26262등과 같이 특정 산업 분야에 맞는 소프트웨어 안전에 대한 내용까지 다양한 표준을 기준으로 존재함을 확인할 수 있었다. 그러나 대다수가 기업에 의한 유료 교육과 함께 자격 획득이 연결되어 있으며, 커리큘럼 등의 정보의 공개를 대다수가 하지 않고 있어, 확인 가능한 정보를 기반으로 조사 및 분석을 수행하였다.

1. TUV SUD의 기능 안전 전문가 인증[67]

<표 3-41> TUV SUD의 기능 안전 전문가 인증의 레벨 구분

수준	자격	평가내용	필수 요건
1	ISO 26262 기능 안전 엔지니어	ISO 26262 표준에 대한 기본 지식을 기반으로 후보자들을 평가	없음
2	ISO 26262 기능 안전 프로페셔널	ISO 26262 표준에 대한 기본 지식 및 실제 응용을 기반으로 후보자들을 평가	- **6년 이상의 관련 산업 경력** (관련 전공 및 학위에 따라 다름) - 두 개 이상의 기능 안전 프로젝트에 참여한 경험
3	ISO 26262 기능 안전 전문가	ISO 26262 표준에 대한 기본 지식 및 실제 응용을 기반으로 후보자들을 평가	- **10년 이상의 관련 산업 경험** (관련 전공 및 학위에 따라 다름) - 기능 안전 관련 보유 지식을 잘 나타내는 두 개 이상의 프로젝트 수행 사례 제출

자료 : TUV SUD (2016.12.18.)

67) TUV SUD, http://www.tuv-sud.com/industry/automotive-transportation/automotive-solutions/quality-and-safety-services/automotive-functional-safety/iso-26262-functional-safety-certified-programme#tab_1427105746588994541307 (2016.12.18.)

TUV SUD는 개인을 대상으로 한 표준화된 시험 및 인증 서비스(Functional safety certification programme, FSCP)를 제공하고 있으며, 해당 서비스는 ISO 26262(자동차)에 대한 전반적인 기능 안전을 다루고 있다. 자격의 수준을 Level 1 ~ level 3까지 단계로 나누고 있으며, 해당 전문가 레벨에 따른 평가 내용 및 자격 요건은 위와 같다.

해당 전문가 수준은 모두 ISO 26262의 기능 안전에 관련된 내용을 다루고 있으나, 수준이 높아짐에 따라서 실제 산업의 경력과 프로젝트 진행의 경험을 중요시 하는 것을 확인할 수 있었다.

2. TUV Rheinland[68)]

TUV 라인란드는 국제표준 ISO 26262(자동차) 의 요구조건을 충족할 수 있도록 다양한 사례와 예제 위주로 기능 안전 교육을 제공하며, 총 3일간의 교육을 이수하는 것을 통하여 시험에 응시하는 것이 가능하다. 해당 시험을 통과한 경우에는 TUV 라인란드에서 발급하는 TUV Functional Safety Engineer (Automotive) 자격증 취득 요건 중 한 가지를 충족하게 된다.

<표 3-42> TUV Rheinland : ISO 26262의 요구사항에 맞는 개발

항목	주요 내용
요구사항 분석	- 일반적인 방법론 및 요구사항 - 안전 관계 시스템과 컴포넌트의 측면에서 고려해야 할 수명 사이클 - 기능 안전 관리에 관한 요구사항 - 기능 안전성 평가/판단 요구사항
ASIL	- 선택된 ASIL에 따른 요구사항 정의, ASIL의 의미
결함 모델	- 결함 및 결함 모델의 고려사항 - 결함 대책의 정의
설계 및 개발	- 설계, 개발, 생산 단계에서의 고려사항 - 안전 목표 위반 확률 계산 - 설계 및 개발에 대한 제약 및 조건 - 하드웨어 구성 요소의 인증 - 상황에 맞는 안전 요소 (Safety elements out of context, SEooC) - 검증 된 인수의 사용

자료 : TUV Rheinland (2016.12.18.)

68) TUV Rheinland, http://www.tuv.com/ko/korea/hot_topics_kr/functional_safety.jsp (2016.12.18.)

해당 교육 및 자격의 대상은 시스템 개발자, 프로젝트 책임자, 품질 관리자, 테스트 담당자 등에 해당되며, TUV 라인란드에서는 구체적인 교육 일정 혹은 내용 대신 ISO 26262의 요구사항에 맞춘 개발에 필요한 내용을 공개해두고 있다. 『TUV SUD의 기능 안전 전문가 인증』보다는 구조화되지 않았으나, 자동차 안전 표준 관련 유사 자격증이라 할 수 있다.

3. Engineering safety consultants (ESC)[69]

ESC에서는 IEC 61508 및 IEC 61511과 관련된 다양한 교육을 수행하며, 교육 수료에 관한 인증서를 부여한다. 국제 표준에 맞춘 안전 기능 교육이 1일 ~ 3일까지 다양한 코스가 존재한다. 예시로 IEC 61508 과정의 교육 목표는 기능 안전 관리, 안전 수명주기 개념, IEC 61508 준수 프레임 워크, 위험 감소 매개 변수 및 허용 가능한 위험의 개념, 허용 가능한 위험을 성취하기 위한 안전 조치, SIL 결정 방법 등의 내용을 다룬다. 전체적인 코스는 [그림 3-4]와 같다.

[그림 3-5] Engineering safety consultants 코스

IEC 61508 Software Safety Training Course Outline

Programme for 1 day Software Safety Training Course

Session	Time	Title	Coverage
1	8:30 – 9:30	IEC 61508 Part 3 Overview	• How does Part 3 fit in the overall IEC 61508 and E/E/PE system lifecycle • Overview of the IEC 61508 Part 3 scope, structure and content • Differences between software and hardware • Compliance framework for software

2	9:30 – 10:30	IEC 61508 Part 3 Software requirements (generic requirements)	• Software development lifecycle and safety lifecycle
			• Requirements applicable throughout software development lifecycle
			  • Software configuration management
			  • Software forward and backward traceability
			  • Software verification and validation (V&V)
			  • Software modification
			  • Software tool qualification

REFRESHMENTS			
3	10:45 – 12:30	IEC 61508 Part 3 Software requirements (specific requirements)	• Requirements applicable to specific software development lifecycle stages • Differences between system and application software

69) Engineering safety consultants, http://www.esc.uk.net/training/iec-61508-software-safety-training-course-outline (2016.12.18.)

4	13:30 – 14:30	Software safety in the context of other related standards	• Similarities and differences between IEC 61508 and other standards, including • IEC 61511 • EN 50128 • Def Stan 00-55 • DO-178, ARP4754, CAP 670
5	14:30 – 15:30	IEC 61508 Part 3 potential new developments	• IEC 61508 maintenance committee activities • Key software safety topics being discussed and debated • Software lifecycle • Proven in use • Tool qualification • Data safety
REFRESHMENTS			
6	15:45 – 16:15	Workshop	• Questions on lectures given (multi-choice) • Discussion
7	16:15 – 17:00	Open Forum	• Discussion/questions on any issues covered on the course
17:00 COURSE FINISH			

자료 : Engineering safety consultants (2016.12.18.)

ESC의 소프트웨어 안전 훈련 과정은 IEC 61508을 기준으로 이루어지기 때문에, 기타 산업별로 존재하는 표준에 맞춘 교육에 비하여 소프트웨어를 중심으로 다루고 있는 것을 확인할 수 있다. 세션 4의 과정에서는 타 표준과의 유사도 및 차이점에 대한 훈련을 진행하는 것을 통하여 다양한 산업 분야에 대한 고려를 할 수 있도록 하고 있다.

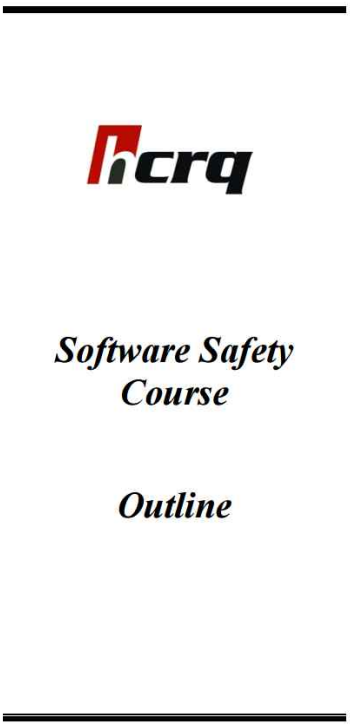
4. HCRQ 소프트웨어 안전 훈련 및 인증[70)]

HCRQ에서는 국방에서부터 철도(EN 50128, IEEE 1483 등), 항공(DO-178, NASA 등), 일반 분야(IEEE 1228, IEC 61508, MISRA 등)와 같이 전반적인 분야에서 소프트웨어 안전에 관한 내용을 총 4일 간 훈련하며, 훈련내용에 맞는 인증서를 발급해 준다. 전체 교육 훈련 코스는 [그림 3-6]에 제시한 바와 같다.

다양한 산업별 분야에 대해서 훈련을 진행하되, 소프트웨어 안전에 특화된 훈련과정으로 이루어진 것을 확인할 수 있으며, C 코딩의 가이드라인으로서 활용되는 MISRA C에 대한 교육을 일반 분야에 대해서 훈련하고 있는 것을 확인할 수 있다.

70) HCRQ, http://www.hcrq.com/software-safety-course.html (2016.12.18.)

[그림 3-6] HCRQ Software Safety 코스



Software Safety Course

Outline

- Introduction
  - Software Safety
    - Overview, Benefits
  - Myths
- Software-Caused Accidents
  - Examples
  - Lessons Learned – First Hand
  - Safety Loopholes
  - Ergonomic Factors
  - Their Nature
    - Why Haven't We Seen More?
  - Their Cause
    - Source of Errors in Systems
    - Complexity Issues
      - Simplicity, Determinism
    - Personnel
      - Independence
    - Why V & V Fails
  - Minimizing Them in Already Commissioned Systems
- Software Safety Incentives
  - Accidents - Devastating Effects
  - Software Liability
  - Software Engineering Malpractice?
- Safety And Reliability Concepts
  - Definitions
- Dependability Concepts
- Generic Integrity Levels
  - System, Software
- Safety Integrity
  - Systematic & Random Failure Integrity Levels
- Robustness
- System/Software
  - Designing In Safety
  - Validating Safety
    - Can We Always Validate Safety?
    - How Can We Validate Safety:
      - When Our System Contains COTS Elements?
      - When Little or No Documentation Exists?
      - When We Are Given Only the Software?
- Expected Probability of Failure of Systems
- Risk Concepts
  - Risk Engineering
  - Socioeconomic Factors
  - Definitions
    - Severities & Probabilities
      - Defined By Standards
  - System Risk Assessment
    - Risk Assessment Matrix/RACs
    - Risk Classes
    - Safety Integrity Level (SIL) Determination
      - System, Software
      - Reducing Software Integrity Levels
  - Software Criticality Assessment
    - Software Control Categories (SCCs)
    - Software Criticality Indexes (SwCIs)
      - Same As Software Integrity Levels?
    - Software Safety Criticality Matrix (SSCM)
  - Software Development Assurance Levels (SDALs)
    - With Respect to RTCA DO-178
      - Same As Software Integrity Levels?
      - Same As Software Criticality Indexes?
  - SoftWare Assurance Levels (SWALs)
    - Determination
- Basic Approaches to Safe Design
- Software Safety Stds., Guidelines & Regulations
  - Defense
    - Joint Services Software Safety Engineering Handbook
    - MIL-STD-882E(System Safety)
      - Relevance to Software Safety
    - AMCOM 385-17
    - AOP-52
    - STANAG 4404
  - Aerospace
    - NASA Software Safety Standard
    - NASA Guidebook
    - FAA System Safety Handbook
    - SAE ARP4754A/4761
      - Relevance to Software Safety
    - RTCA DO-178
      - Relevance to Software Safety
    - ESARR 3, ESARR 4, ESARR 6
    - ED-153
  - Rail
    - EN 50128
    - IEEE 1483
  - General
    - IEEE 1228 (Software Safety Plans)
    - IEC 61508
    - ISO/IEC 15026
      - System & Software Integrity Levels
    - UL 1998 (Safety-Related Software)
    - MISRA Guidelines
- Formal Methods
  - Introduction
  - Study of Industrial Experience
    - Program Function Table Analysis
  - Relevance
  - Formalism
- Fault Tolerant Techniques
  - N Version Programming, Recovery Blocks
  - Other Techniques
    - Data Redundancy
- Safe Design Techniques
  - Security Kernels, Safety Kernels, Firewalls
  - Barriers
    - Lockins, Lockouts - Baton Passing
    - Interlocks - Types, Precautions
  - Checks
    - Hardware, Assertions
    - Audit, Supervisory
  - Fail Safe, Fail Soft
    - Fail Operational, Passive, Active
    - Recovery Techniques
- Safety Assurance Concepts
  - Software Assertions
  - Many Others
- Software Requirements Checklist
- Software Design Checklist
- Programming Languages
  - Importance?
  - Language Subsets
  - Reality?
- System Safety Programs (SSP)
  - Objectives
  - General Requirements
  - Tailoring
  - Flow-Down of Safety Requirements
  - Safety Integration
  - Safety Requirements Traceability
    - Tools
  - Design/Implementation/Testing Influence
  - Chronology
  - Safety Program Results
- System Safety Program Plans (SSPP)
  - Dangers Lurking
  - Guidelines
- Software Safety Program Plans (SwSPP)
  - Guidelines
- Software Safety Working Group (SwSWG)
- Hazard Mitigation Precedence
- Hazard Tracking
- Preliminary Hazard Analysis (PHA)
  - Objectives
  - System Boundary
  - Analyst Credentials
  - Format
    - Life-Cycle, Post-Design
  - Guidelines - Keys To Success
  - In-Class Assignment
- Functional Hazard Analysis (FHA)
- Determining/Lowering Software Criticality
- Degree Of Rigor In Software Development
- Subsystem Hazard Analysis (SSHA)
- System Hazard Analysis (SHA)
- Software Safety Analysis Process
  - Software Requirements Analysis
    - Types of Analysis
  - Software Design Analysis
    - Types of Analysis
  - Software Code Analysis
    - Types of Analysis
  - Software Change Analysis
- Tools
  - Static Code Analyzers
  - Many Others
- Software FMEA
  - Types
  - Examples
  - Guidelines
- Software FMECA?
- Fault Tree Analysis (FTA)
  - History
  - Qualitative/Quantitative
    - Human Failure Rate Derivation
  - Versus FMEA/FMECA
  - Advantages/Disadvantages
  - Fault Tree Symbols and Terminology
    - Definitions, Special Symbols
  - Examples
  - Software FTA
    - Software Failure Rate Derivation
  - Immediate, Necessary and Sufficient Concept
  - Basic Rules
  - System Operational Modes
  - Guidelines - Keys to Success
    - Increased Accuracy, Consistency, Economy
    - Best Kept Secrets?
  - Maintainability
  - Fault Tree Notes
  - Step Size Precautions
  - Similar Subtrees
    - Limiting Fault Tree Size, Sharing Subtrees
  - Improving Consistency
  - Fault Tree Reviews
  - Design/Implementation Influence
  - Cut Sets, Minimal Cut Sets
  - Minimal Cut Set Analysis
    - What This Really Means
  - Common Mode Analysis
  - Importance Analyses
  - Acceptance/Rejection Criteria
    - 20 Attributes
  - Limiting Fault Tree Production
    - Class Exercise
  - Fault Tree Analysis Programs
- Other Analysis Techniques
  - Software Sneak Analysis (SSA)?
  - Petri Nets
  - Other Techniques
- Software Safety Cases
- Dealing with COTS Elements
  - RTOS's
    - VxWorks, Integrity, LynxOS
    - OSE, QNX, Linux
  - Windows?
  - And more
- Safety Verification
  - Testing
- Now, Let Us Step Back
  - What Is Really Do-able?
  - Avoiding The Monetary Sink Hole

HCRQ, Inc.
P.O. Box 264
Williamsburg, VA 23187
Tel: (757) 564-7703
Fax: (757) 564-7704

web: http://www.hcrq.com/Training.html
e-mail: training@hcrq.com

자료 : HCRQ (2016.12.18.)

5. DNV-GL ISO 26262 engineer qualification course[71)]

DNV-GL에서는 ISO 26262(자동차)에 부응하는 기능안전 교육과 인증 서비스를 제공하고 있다. 교육 수강생은 훈련과정을 모두 이수한 경우 수료증을 발급받을 수 있으며, 이후 시험에 응시할 수 있는 자격이 주어진다. 해당 시험에서 합격기준(70점)을 달성하는 경우에는 인증서를 받는 것이 가능하다.

ISO 26262에 대한 훈련 일정은 하단의 표에서 보이고 있다. 소프트웨어 안전 훈련은 4일차에 진행하는 것으로 나와 있으며, 5일차에는 ASIL에 대해서 다루는 것을 확인할 수 있다.

[그림 3-7] DNV-GL ISO 26262 engineer qualification course

구 분	내 용
Day 1	10:00~11:30 Functional Safety 개념, ISO 26262의 국제적 동향 및 용어정의 11:30~12:30 ISO 26262 Part 2 기능안전성 경영 part 1 (management of functional safety) 12:30~13:30 중식 13:30~16:00 ISO 26262 Part 2 기능안전성 경영 part 2 (management of functional safety) 16:00~18:00 ISO 26262 Part 8 지원 프로세스(Supporting process) I
Day 2	09:00~12:00 ISO 26262 Part 3 개념단계(Concept phase) 12:00~13:00 중식 13:00~17:30 ISO 26262 Part 4 제품개발: 시스템단계(Product Development : System level)
Day 3	09:00~12:00 ISO 26262 Part 5 제품개발: 하드웨어(Product Development : Hardware level) 12:00~13:00 중식 13:00~16:30 ISO 26262 Part 5 제품개발: 하드웨어(Product Development : Hardware level) 16:30~17:30 ISO 26262 Part 8 지원프로세스(Supporting process) II
Day 4	09:00~12:00 ISO 26262 Part 6 제품개발: 소프트웨어(Product Development : Software level) 12:00~13:00 중식 13:00~16:30 ISO 26262 Part 6 제품개발: 소프트웨어(Product Development : Software level) 16:30~17:30 ISO 26262 Part 8 지원 프로세스(Supporting process) III
Day 5	09:00~10:30 ISO 26262 Part 7 생산 및 운전(Production and operation) 10:30~12:00 ISO 26262 Part 9 ASIL 및 안전지향 분석(ASIL & Safety oriented analysis) 12:00~13:00 중식 13:00~13:30 Epilogue 13:30~16:30 Testing and Examination

자료 : DNV · GL (2016.12.18.)

71) DNV·GL, https://www.dnvgl.co.kr/services/page-3324 (2016.12.18.)

6. SGS ISO 26262 자동차 기능안전훈련[72)]

SGS에서는 ISO 26262 자동차 기능안전 훈련 및 인증 서비스를 제공하며, 훈련 단계를 모듈화 하여, 각 단계를 모두 거친 후에 시험에 응시하는 자격을 부여한다. 대략적인 교육 훈련 및 인증의 흐름은 아래와 같다.

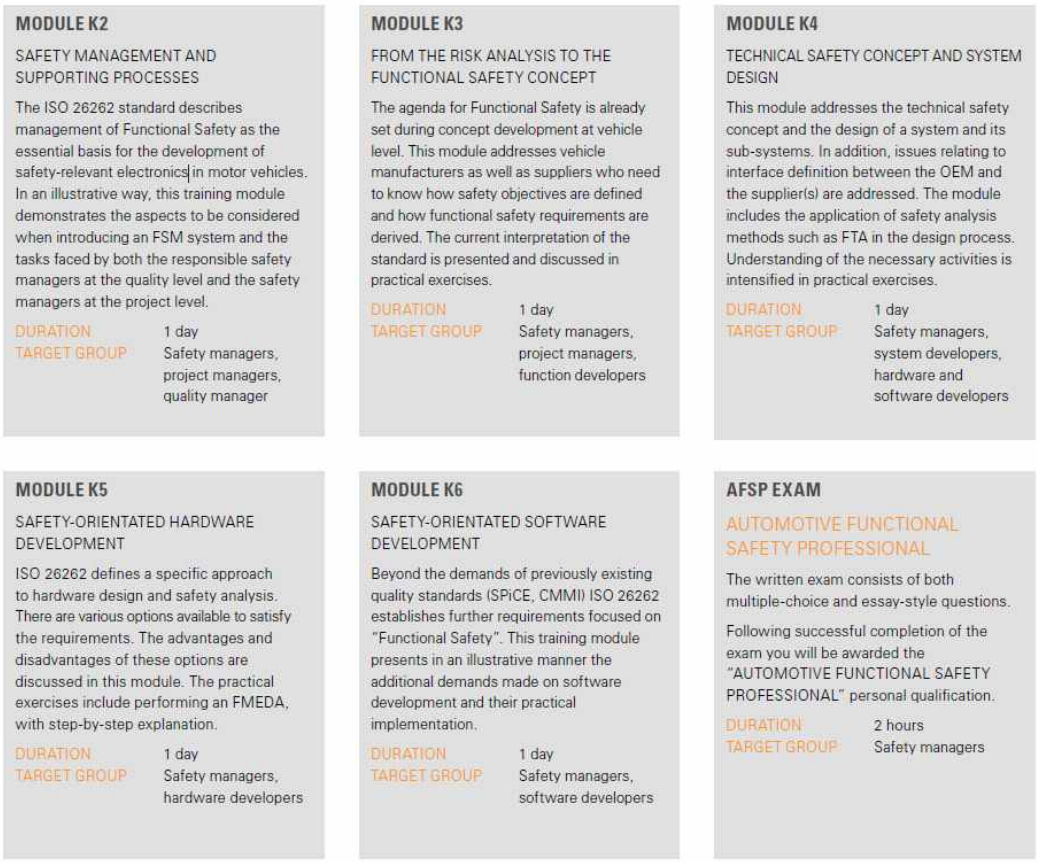
교육 과정에서 MODULE 4, MODULE 6이 소프트웨어 안전과 직접적으로 연관이 있다고 볼 수 있으며, 총 5일간의 교육 과정으로 구성되어 있다. 해당 교육은 모듈 별로 따로 신청하여 수료하는 것이 가능하며, 12개월 내에 모든 모듈을 이수해야만 시험의 자격을 얻을 수 있다. 특이점으로는, 시험을 통과하여 인증서를 받은 이후 3년간만 해당 인증서가 유효하다는 점이 있다. 추후 업데이트 워크샵에 참석 및 간단한 시험을 통하여 해당 기간을 갱신하는 것이 가능하다.

[그림 3-8] ISO 26262 자동차 기능안전훈련

자료 : SGS (2016.12.18.)

72) SGS, http://www.sgsgroup.kr/ko-KR/Training-Services/Industry-Based-Training/Automotive/Automotive-Functional-Safety-Training/ISO-26262-Automotive-Functional-Safety-Training.aspx (2016.12.18.)

[그림 3-9] ISO 26262 자동차 기능안전훈련 모듈의 상세 내역



자료 : SGS (2016.12.18.)

각 교육의 모듈 별 설명 및 소요 기간은 위의 그림과 같다. SGS의 ISO 26262는 지속적으로 해당 인증서를 유지하기 위하여 갱신이 필요하다는 점에서 여타 교육 및 인증 서비스를 제공하는 업체와 차별점이 있는 것을 확인할 수 있었다.

7. EUROCONTROL[73)]

EUROCONTROL은 항공에 관련된 표준에 대한 다양한 교육 및 인증을 서비스하고 있다. ED-12C, DO-178C, IEC 61508, EDD-109A, ED-153의 표준에 대한 교육을 시행하고 있으며, 각 교육과정을 수료하면 인증서를 발급해 준다. 소프트웨어 안전의 내용을 포함하는 교육 및 인증 과정은 Introduction to Safety Assessment, ATM software safety assessment가 있으며, 각 교육 별 다루는 내용은 다음과 같다.

73) EUROCONTROL , https://trainingzone.eurocontrol.int/ilp/pages/landingpage.jsf?faces-redirect=true (2016.12.18.)

[그림 3-10] EUROCONTROL Introduction to safety assessment

DAY/TIME	09:00			13:00	14:00	17:00
Monday		**10:00**	00 Course Introduction	01 Introduction to Safety Management	02 Key Concepts for Safety Assessment	03 Road Traffic Exercise
Tuesday	Debrief 1st day	04 Safety Assessment Overview & Illustration		05 Safety Regulatory Framework	06 Safety Argument & Safety Case Principles	15 Safety Assessment of ATM/ANS Change Exercise (Example 2), Part 1
Wednesday	Debrief 2nd day	07 Scoping, hazard identification & safety criteria determination Exercise (Example 1)		08 Risk Assessment	09 Risk Assessment Exercise (Example 1)	10 Risk Mitigation
Thursday	Debrief 3rd day	11 Risk Mitigation Exercise (Example 1)		12 Verification & Monitoring	13 Safety Assessment of Implementation Exercise (Example 1)	14 Safety Assessment of Transfer into Operations Exercise (Example 1)
Friday	Debrief 4th day	15 Safety Assessment of ATM/ANS Change Exercise (Example 2), Part 2		16 Summary & Practicalities / 17 Test & Debrief	**13:00**	

자료 : EUROCONTROL (2016.12.18.)

해당 과정에서는 안전성 평가 중에 수행해야 할 주요 단계, 안전성 평가 프로세스와 품질 및 안전 관리 시스템 간의 관계 등을 다루고 있다.

ATM software safety assessment

[그림 3-11] EUROCONTROL ATM software safety assessment

DAY/TIME	09:00	10:00	12:00	13:00		17:00
Day 1		Session 00 Welcome	Session 01 Software & Safety	Session 02 Example Accidents	Session 03 Software Impact on Safety - Exercise	Session 04 Software & Safety Lifecycles
Day 2	Session 05 System & Software Requirements	Session 06 Assurance Levels	Session 07 Requirements - Exercise	Session 08 Software Safety Assurance	Session 09 EC 482 – SAM – SWAL	
Day 3	Session 10 Software Standards and Software Standards Exercises			Session 11 SW Supply Models & Contracting for assurance		Session 12 Practicalities of a Project
Day 4	Session 12 Practicalities of a project Continued			Session 13 Major Case Study		
Day 5	Session 14 Major Case Study Continued		Session 15 Course Debrief			

자료 : EUROCONTROL (2016.12.18.)

ATM 소프트웨어에 대한 안전성을 위하여 소프트웨어 요구사항 식별, SWAL(software assurance level)할당 및 준수, 소프트웨어 생명 주기 등에 대한 교육과정을 포함하고 있다. 또한 해당 과정은 소프트웨어 공학에 대한 개념 및 방법론에 대한 지식이 충분한 청중을 대상으로 하는 훈련 및 인증서비스이다. 훈련 과정은 다음과 같다.

EUROCONTROL 협회는, 초급 과정에 해당하는 인증과 고급과정에 해당하는 인증을 나누어서 코스를 다루고 있다는 것이 특징이며, 고급과정에 해당하는 교육에서는 특정 산업 분야에 특화된 코스로 구성되어 있음을 확인할 수 있었다.

8. AAMI 자격 인증 연구소[74)]

AAMI 자격 인증 연구소에서는 의료 기술 전문가에 대한 자격 증명을 부여한다. 다른 기업과 마찬가지로 교육 훈련 과정을 서비스하고 있으나, 해당 사항이 자격시험 응시에 필수적인 요소는 아니다. 지원하고 있는 자격증으로는 생체 의학 장비 인증 프로그램 기술자(CBET : Certification programs for Biomedical Equipment Technicians), 방사선 장비 전문의(CRES : Certification programs for radiology equipment specialists), 실험 장비 전문가(CLES : Certification programs for laboratory equipment specialists) 3가지의 소프트웨어 안전 내용을 포함하는 자격을 인증해준다. AAMI는 각 자격제도의 주요 항목과 문항 개수 등의 정보를 공개하고 있으며, 내용은 다음과 같다.

74) Advancing safety in healthcare technology, http://www.aami.org/professionaldevelopment/content.aspx?itemnumber=1134&navItemNumber=577 (2016.12.18.)

[그림 3-12] AAMI는 각 자격제도의 주요 항목

Certified Biomedical Equipment Technician Content Outline

Anatomy & Physiology – Approximately 12%

A. Systems
   1. Respiratory
   2. Gastrointestinal
   3. Nervous
   4. Circulatory
   5. Musculoskeletal
   6. Endocrine
B. Organs
   1. Heart
   2. Lungs
   3. Liver
   4. Kidneys
   5. Brain
   6. Gallbladder
   7. Pancreas
   8. Other
C. Blood
   1. Components
   2. Metabolism
D. Terminology

Public (employee, patient, visitor) Safety in the Healthcare Facility – Approximately 15%

A. Electrical
   1. Microshock/Electrical Safety Testing
   2. Other
B. Chemical
   1. Material Safety Data Sheet
   2. Other
C. Radiation Hazards
   1. Light Spectrum
   2. Types of Rays
D. Biological
   1. Standard Precautions
   2. Other
E. Fire
   1. Class
   2. Fire Extinguishers
F. Codes and Standards
   1. Credentialing and Certification
      a. Joint Commission Comprehensive Accreditation Manual
      b. AABB
      c.. American College of Radiology
   2. NFPA 99
      a. Gas and Vacuum Systems
      b. Electrical Systems
   3. FDA
      a. SMDA
      b. Other
   4. OSHA
   5. Other (NEC, ANSI, FCC, etc.)

Fundamentals of Electricity & Electronics – Approximately 13%

A. Transducers
B. Calculations and Conversions
   1. Hex/Decimal/Binary
   2. Other
C. Circuits and Components
   1. Active Devices
      a. Solid-State Devices
         1. Analog
         2. Digital
      b. Other (CRTs, X-Ray tubes, photomultipliers, etc.)
   2. Power Supplies
   3. Passive Devices
D. Power Distribution and Storage Systems
   1. Transformers
   2. Distribution
   3. Batteries
   4. UPS/Line Conditioning
E. Terminology

Healthcare Technology and Function – Approximately 25%

A. Monitoring Systems (ECG, EEG, Blood Pressure, Pulse Oximetry, Fetal Monitor)
B. Portable Equipment (Infusion Devices, Syringe Pumps, PCA Pumps, Hypo/Hyperthermia)
C. Life Support Equipment (Defibrillators, Anesthesia Machines, Critical Care Ventilators, Balloon Pumps)
D. Therapeutic Equipment (Infant Warmers, Ultrasound Therapy)
E. Laboratory Equipment (Centrifuges, Water Baths, Analyzers)
F. Diagnostic Imaging (Ultrasound, Radiographic/Fluoroscopy)
G. Operating Room (Electro Surgical Generators, Video Carts, Lasers, Tourniquets, Sterilizers, Warmers)
H. Test Equipment (Electrical Safety, Defibrillator, Electro Surgical, Physiologic Simulators, Oscilloscopes, Meters)
I. Diagnostic Equipment
J. Terminology

Healthcare Technology Problem Solving – Approximately 25%

A. Electronic Component Level, Block Level
B. Monitoring Systems (ECG, EEG, Blood Pressure, Pulse Oximetry, Fetal Monitor)
C. Portable Equipment (Infusion Devices, Syringe Pumps, PCA Pumps, Hypo Hyperthermia)
D. Life Support Equipment (Defibrillators, Hemodialysis, Anesthesia Machines, Critical Care Ventilators, Balloon Pumps)
E. Therapeutic Equipment (Infant Warmer, Ultrasound Therapy)
F. Laboratory Equipment (Centrifuges, Water Baths Analyzers)
G. Diagnostic Imaging (Ultrasound, Radiographic/Fluoroscopy)
H. Operating Room (Electro Surgical Generators, Video Carts, Lasers, Tourniquets, Sterilizers, Warmers)
I. Diagnostic Equipment
J. Situational (User Error, User Training, Applications)

Healthcare Information Technology – Approximately 10%

A. Regulatory and Safety
   1. Medical Device Data Systems (MDDS)
   2. IEC 80001 – Application of Risk Management for IT Networks
   3. Health Insurance Portability and Accountability Act (HIPAA)
   4. Digital Millennium Copyright Act (DMCA)
B. Foundations
   1. Hardware
      a. Topology
      b. PCs/Laptops/Servers
      c. Wiring/Structured Cabling/Connectors
      d. Switches/Hubs/Routers
      e. Wireless Communications
      f. Other
   2. Software/Middleware/Applications
      a. EMR/EHR
      b. Healthcare Information Systems (PACs, LIS, RIS)
      c. Network Protocols (IP, CCP, UDP)
      d. Operating Systems
C. Function and Operation
   1. Hardware
      a. PCs, Switches, Patch Panels
      b. Networks, Topology
      c. Peripherals
      d. Other
   2. Integration
      a. Bedside Medical Device Integration (BMDI)
      b. Medical Device Integration (MDI) (Labs, Printers, etc.)
      c. Mobile Devices (Handhelds, Smart Phones, Tablets, etc.)
   3. Test Equipment
      a. Cable Test Devices (Copper, Fiber)
      b. Network Test Devices
   4. Security
D. Problem Solving
   1. Computer Networks
   2. Integration
   3. PCs, Switches, Hubs
E. Terminology

The CBET exam is a three-hour closed book exam consisting of 165 multiple choice questions.

Candidates will have access to a simple calculator during the exam. Cell phones, iPads or other electronic devices that have internet capabilities are not allowed into the testing room.

Score required to pass: The minimum score required to pass the CBET examinations is 116/165.

자료 : EUROCONTROL (2016.12.18.)

CBET의 시험 내용 중에서는 IT관련 부분이 포함되어 있으며, IEC 80001 표준에 기반을 두어 안전성 등의 문제를 다루고 있는 것을 확인할 수 있다. CRES, CLES의 경우도 장비를 다루기 위한 자격이기 때문에 장비의 종류에 따른 항목의 차이가 있을 뿐 모두 IEC 80001의 안전 표준을 기반으로 하는 IT관련 항목을 시험에서 포함하고 있다. 자격을 취득한 후, 해당 자격의 유지를 위해서는 3년 동안 최소 15개의 활동 점수를 축적하고 수수료와 함께 지속적인 실무 저널의 제출이 이루어져야 한다. 활동 점수는 교육회의, 학회 참여 등을 통하여 획득할 수 있다.

9. USC Viterbi SFT course[75)]

항공 안전 및 보안 대학원에서 교육 및 인증을 해 주고 있으며, 교육을 이수하는 것을 통하여 항공 안전 및 보안과 시스템 안전, 두 종류의 인증서를 받는 것이 가능하다. 이 중, 소프트웨어 안전에 부합하는 부분은 시스템 안전에서 이루어지며 7년 이내에 3가지의 필수 코스와 두 가지의 선택 코스를 이수하는 것을 통하여 인증서를 수여하는 것이 가능하다. 해당 필수 코스 및 선택 코스는 다음과 같다.

<표 3-43> USC Viterbi SFT course의 필수 및 선택코스

필수 요구 코스
▪ 시스템 안전 (System safety, SSC) ▪ 소프트웨어 안전 (Software safety, SFT) ▪ 시스템 안전을 위한 인간 오류 분석 (Human error analysis for system safety, HEASS)
선택 코스
▪ 시스템 안전을 위한 손상 평가 (Damage assessment for system safety, DASS) ▪ 고급 시스템 안전 분석 (Advanced system safety analysis, ADVSS) ▪ 위험: 효과 및 제어 전략 (Hazards: effects and control strategies, HAZ) ▪ 시스템 안전 분석을 위한 수학 (Mathematics for system safety analysis, MATH)

자료 : USCViterbi (2016.12.18.)

75) USCViterbi, http://viterbi.usc.edu/aviation/courses/sft.htm (2016.12.18.)

필수 코스 중, 소프트웨어 안전의 주요 교육 코스의 기본 내용은 다음과 같다.

<표 3-44> USCViterbi SFT course의 주요 교육 코스 기본 내용

소프트웨어 안전 교육 (SFT)	
▪ 소프트웨어 개요	▪ 정의 및 컨셉
▪ 설계 요구사항	▪ 소프트웨어 규정
▪ 시스템 안전	▪ 시스템 안전 팀 조직
▪ 위험 처리/관리	▪ 에이전시에 의한 위험
▪ 신뢰성 문제	▪ 확률
▪ 위험 고려사항/분석	▪ 위험 평가 및 위험 수준
▪ 프로그램 문서	▪ 소프트웨어 신뢰성/위험
▪ 소프트웨어 공학/요구사항	▪ 소프트웨어 안전수명주기 목표
▪ 보안 공학	▪ VHDL 합성
▪ 오류 분류 및 종류	▪ 소프트웨어 안전 요구사항 추적성
▪ Petri-Net 모델링	▪ 소프트웨어 안전 체크리스트
▪ 결함 트리 분석 (Fault tree analysis)	▪ 주요 위험 분석
▪ 소프트웨어 언어 분석	▪ 수학 모델
▪ 소프트웨어 안전 테스팅	▪ 소프트웨어 안전 신뢰성/유지

자료 : USCViterbi (2016.12.18.)

해당과정은 학교에서 진행하는 개인 인증 교육 훈련이며, 위험 관리, 소프트웨어 안전 라이프 사이클, 소프트웨어 안전 테스트 등을 다루고 있다. 특이점으로는 보안에 관한 부분이 포함된 점과 VHDL synthesis에 관한 내용이 포함된 점이 있다.

10. Risknowlogy Functional safety assessor[76)]

Risknowlogy 사에서 인증해 주는 기능안전평가자 자격증은 국제안전표준에 해당하는 IEC61508, EN50128, EN 50129, EN50126 등에 공통으로 적용되는 안전 평가자 자격증이다. 해당 자격증에서는 시스템 안전과 소프트웨어 안전 두 가지 측면에서 전문가 수준의 역량을 요구하며, 감사 및 독립적인 안전 평가에 관한 보고서 등을 작성할 수 있어야 한다. 기본적으로 자격을 얻기 위하여, IEC61508에 관련된 공식 교육 내용 및 실무 수행에 관한 내용을 제출해야하며 기능안전평가의 전문가와 인터뷰를 통하여 검증한다. 해당 자격은 전문가 등급과 마스터 등급으로 나뉜다. 전문가의 경우 기능안전관리 프로젝트 시간이 1500시간

76) https://risknowlogy.com/rkb/functional-safety/functional-safety-assessment/

이상(일 8시간 경우, 187.5일), 마스터는 3000시간(일 8시간 경우, 375일)의 수행 경력을 요구한다. (년 근무일은 250일 정도)

Risknowlogy 사의 기능안전평가자 자격의 경우 실제 전문가와의 인터뷰 및 공인 교육에 대한 확인서 등으로 비교적 단순하게 자격을 부여하는 절차로 진행되는 점이 특징이며, 실제 직무 수행 사실에 근거하여 점수를 부여하여 기본 자격에 대한 여건을 검사하는 점에서 해당 업무를 수행하기 위한 경력을 중시하는 점을 확인할 수 있다.

11. Project management professional (PMP)[77]

프로젝트 관리 전문가는 1969년 설립된 비영리기관, PMI(Project management institute)에서 자격을 관리하는 국제자격증이며, 국내에서도 제휴를 통하여 교육 및 자격시험을 연계해 주는 기관이 다수 존재한다. 해당 자격증은 소프트웨어 안전과 직접적인 연관이 있지는 않으나, 안전관리자 자격제도 검토에 참고하고자 검토하였다.

프로젝트 팀 및 리더의 프로젝트 관리 역량 강화를 목적으로 설계된 자격증이며, 지원 조건은 프로젝트 실무 경력을 각각 학사학위 이상은 36개월 4500시간, 학사학위미만은 60개월 7500시간 이상으로 정해 두었으며, 프로젝트 관리 관련 교육을 35시간 이상 이수한 실적이 존재해야 자격시험에 응시할 수 있다.

시험은 총 200문항이 출제되며, 전 문항이 객관식으로 출제된다. 문제 당 1점의 점수가 배정되며, 25문항은 추가 번외 (dummy) 문제로서, 해당 문항에 대해서는 배점이 없어 총 만점은 175점이며, 합격 기준은 106점으로, 도메인별 문제 출제 비중은 아래의 표와 같다.

<표 3-45> PMP 자격증의 시험 출제 범위

도메인	출제 비중
■ 프로젝트 착수 (Project initiating)	11%
■ **프로젝트 계획 (Project planning)**	23%
■ **프로젝트 수행 (Project execution)**	27%
■ **프로젝트 관찰 및 통제 (Project monitoring and controlling)**	21%
■ 프로젝트 마감 (Project closing)	9%
■ 전문가적 사회적 책임 (Professional and social responsibility)	9%

77) https://www.pmi.org/certifications/types/project-management-pmp

시험 출제 비중에서는 프로젝트의 계획, 실행, 모니터링 및 통제에 가장 큰 비중이 있으므로 해당 파트를 가장 중요시하는 것으로 보이며, 해당 자격증은 시험 자격 요건에서 상당히 오랜 시간의 실무 경력을 필요로 하는 점이 특징이라 할 수 있다.

12. 해외 안전자격제도 조사 결과 분석

해외 안전자격제도는 주로 표준에 따른 생산제품의 인증 등을 담당하는 기업 혹은 협회로부터 자격 혹은 인증을 수여하는 방식으로 되어 있는 것을 확인할 수 있었으며, 대학도 일부에서 인증 교육을 진행하는 것을 확인할 수 있었다. 또한 대다수의 경우, 인증서를 수여하기 위하여 정해진 교육을 수료하면 되는 형태로 되어 있는 것을 확인할 수 있었다.

인증 및 자격의 획득을 위한 요구사항들에는 대부분 특정 산업의 표준들에 대한 항목으로 이루어져 있기에, 공통된 인증 및 자격에 대한 부분이 많지 않으며, 각 산업 별로 소프트웨어 안전 자격 및 인증이 따로 있는 것을 확인할 수 있다. 그러나 IEC 61508의 경우에는 대부분의 소프트웨어 안전의 기반이 되기 때문에 다양한 산업에서도 인증을 위한 요구사항에 포함되어 있는 것을 확인할 수 있었다. 또한, 프로젝트 관리 및 기능 안전 평가 등과 같이 높은 전문성과 경험을 필요로 하는 자격들은 검증 과정에서 프로젝트의 경험을 반영하기 위한 다양한 자격 요건이 정해져 있는 모습을 확인할 수 있었다.

국내 소프트웨어 관련 자격증들은 국가 공인 자격증이 중시되고 있는 상황이며 이는 자격제도의 유지 및 객관성 측면에서 장점이 있는 반면, 시시각각 변화하는 기술에 대응하기 힘들다는 문제점도 있는 실정이다. 소프트웨어 안전 관련 자격제도 역시 이와 같은 이유로, 신자격제도 등에서도 별도의 소프트웨어 안전을 위한 자격이 존재하지 않는 것을 확인할 수 있었다. 그러므로 소프트웨어 안전 관련 자격제도는 IEC 61508과 같이 넓은 범위에서 적용 가능한 국제 표준의 경우에는 보안자격증 등과 같이 국가 공인으로 유지하는 것이 적합하나, 실질적으로 변화되는 산업에 맞추어가야 하는 점들을 고려할 때 해외의 사례와 같이 국가공인 민간자격 형태로 자격을 설계하여 진행하는 것이 바람직할 것으로 판단된다.

제6절 현행 국내 소프트웨어 관련 자격제도의 문제점

1) 시험내용의 적절성

정보통신 분야의 국가기술자격제도 기사 종목은 크게 다음과 같은 4가지가 문제점을 가지고 있는 것으로 판단된다.[78)]

첫 번째는 시험의 변별력이 낮다는 것이다. 문제은행식으로 3~5배수의 문제를 기준으로 출제하기 때문에 과년도 문제만 공부하고도 충분히 합격할 수 있어, 시험의 변별력이 상당히 낮다. 해당과목의 이해나 실무경험이 없더라도 과년도 문제를 반복하여 풀어보는 등 단순암기식 학습을 통해서 자격증을 취득할 수 있다는 점에서, 지원자의 역량을 정확하게 평가할 수 없다는 문제점을 가지고 있다.

두 번째는 빠르게 변화하는 IT 기술의 발전을 반영하지 못하는 기존 문제로 평가를 수행함에 의해서 발생하는 문제를 가지고 있다. 이에 따라 최근의 정보통신 기술의 현황을 반영하지 못하고 과거에 다루어지던 문제들이 출제되면서 현재 IT 산업에서 요구하는 기술 역량을 반영하지 못하는 문제를 가지고 있다.

세 번째는 오류가 있는 문제가 출제되는 경우가 발생한다는 점이다. 출제기준과 문항 수에 맞추어 억지로 문제를 출제하다 보니 복수의 정답을 가지는 문제가 출제되거나, 문제 자체가 성립하지 않는 문제가 출제되는 경우가 발생하며, 이는 자격 검정 체계의 신뢰성 하락이라는 측면의 문제가 발생하는 요인이 된다.

마지막으로 네 번째로는 검정과목의 적절성에 있다. 현재 시행되고 있는 ICT 국가기술자격은 대부분의 검정이 유사한 검정과목으로 구성되어 각 자격증 간 특색이 부족하다. 자격 자체가 모호하고 포괄적인 성격을 가지고 있기 때문에, 오늘날 분화된 IT업계의 구조를 충분히 반영하지 못하는 문제를 안고 있다. 이는 자격증을 취득하더라도 산업현장에서의 전문가 수준의 직무수준을 충족할 수 없다는 것을 의미하며, 결국 IT 산업군에 따른 고급 전문 인력을 양성하는 데에는 부적합하다고 볼 수 있다.

2) 우대정책의 미비

현존하는 소프트웨어 관련 국가기술자격은 업무독점형 자격이 있긴 하지만, 의무고용형에

78) 장진현 (2016), ICT 관점에서 바라본 국가기술자격제도 개선, 한국인터넷방송통신TV학회 논문지, Vol.16 No.2, 189-199p

속하고 그 마저도 희소가치가 크지 않기 때문에 능력인정형 자격에 가까운 실정이다. 이는 소프트웨어 관련 국가기술자격의 가치가 관련업계의 전문가를 판별하기에 적절하지 않다는 것을 의미한다. 특히 정보처리기사, 정보처리산업기사 등의 자격증들은 IT의 전공기술적인 소양이나 능력을 검증하기 보다는 취업 시 가산점을 목적으로 취득하는 경우가 많고, 또한 문제은행식 출제로 인하여 합격률이 매우 높은 것이 문제가 되고 있다. 이는 국가로부터 전문가임을 인증하는 “자격증”으로써의 가치를 상당부분 상실했다고 보아도 될 수준에 이르고 있는 것이다. 이러한 실태는 해당 자격에 대한 우대정책을 시행하는 데에도 큰 걸림돌이 되고 있는 상황이다.

정리하면, 보다 나은 우대정책을 펼치기 위해서는 먼저 자격제도의 변화가 선행되어야 한다는 것이다. 현존하는 능력인정형 위주의 소프트웨어 자격 보다는 업무독점형에 가까운 자격이 필요하며, 기존의 문제은행식 출제에서 탈피한 보다 변별력 있고 높은 난이도를 갖는 검정시스템을 통하여 전문가임을 검증할 수 있는 시스템이 함께 구축되어야, 이를 기반으로 실질적인 우대정책 수립 및 시행이 타당한 근거를 가질 수 있을 것으로 판단된다.

3) 사후관리의 부재

현존하는 대부분의 국가기술자격은 그 기한이 영구적이기 때문에 1회 취득으로도 평생 동안 보유할 수 있다는 특징을 가지고 있다. 이는 자격의 품질을 해치는 원인이기도 하며, 국가로부터 전문가임을 인증 받은 인력임에도 불구하고 개개인별로 지식 및 기술수준의 편차 발생하므로 자격취득자의 능력을 보증하는 데 걸림돌이 된다. 이러한 점을 극복하기 위해서는 유효기간 도입 및 자격 갱신제도 등을 통하여, 해당 자격 소지자의 일정 수준 이상의 능력 보장을 꾸준히 지속하며, 해당 기술자격보유자 인원을 적정한 수준으로 유지할 수 있도록 하는 부수적인 효과도 기대할 수 있다. 또한 유효기간 도입은 자격취득자 개인에게도 지속적인 자기개발을 도모하게 만들고, 특히 기술발전이 매우 빠른 IT분야에서 자격 관련 신기술에 대응할 수 있는 전문지식을 지속적으로 습득하도록 하는 기재로 작동할 수 있을 것이다.

4) 전문화된 자격증의 부재

정보기술 분야의 폭발적인 성장 및 발전은 소프트웨어 산업을 여러 분야로 분화시켰고, 다양한 분야의 전문가를 요구하고 있다. 이러한 양상을 반영하여, 임베디드기사나 정보보안기사와 같이 특정 영역을 다루는 자격증이 만들어지고 있고, NCS를 개발하는 등 노력을 펼

치고 있다. 하지만, 급변하는 정세에 대응하기엔 정부차원의 대처만으로는 부족하며, 산업현장의 요구사항과 학계 등 연구기관과의 협동이 보다 긴밀해져야 한다. 특히, 소프트웨어 중심사회로 변모한 현대 사회에서 소프트웨어 안전 관련 전문가는 반드시 필요한 인재로써 지속적으로 양성해야 하며, 그러한 소프트웨어 안전 전문가를 인증하기 위한 자격 제도는 국민안전을 위하여 반드시 필요할 것으로 보인다.

5) 실무능력 평가의 취약점

현존하는 소프트웨어 관련 국가기술자격은 비록 실기평가를 수행하고 있긴 하지만 실무능력을 직접 평가하기 보다는 서술형에 가까운 필답형으로 이루어지고 있다. 소프트웨어 개발 분야가 이론적인 부분보다는 실무와 경력이 우선시되는 분야임에도 불구하고, 실기평가가 '서술형식을 가진 필기평가' 에 그친다는 것은 결코 좋은 현상이 아니며 개선되어야 할 부분이다. 물론, 실기평가 방식이 지금까지 유지되어온 것은 비용적인 측면이나 채점의 용이성 등 여러 가지 이점이 있었기 때문이지만, 자격증의 가치를 높이기 위해서는 지금보다는 실무능력을 보다 효과적으로 평가할 수 있도록 바꾸어야 할 것이다.

제4장 소프트웨어 안전 관련 국제 인증에 부합하는 전문가 자격제도 모델

제1절 소프트웨어 안전 전문가 자격제도의 설계 방향

1. 소프트웨어 안전 관련 국제 표준과의 연계

앞선 3장에서 기술한 바와 같이, 전기/전자/프로그램 가능한 전자 시스템에 대한 기능안전을 명시한 국제 표준은 IEC 61508을 중심으로, 각 산업 분야별 특성에 따라 ISO 26262(자동차 부문), DO-178B/C(항공 부문), EN-50129(철도 부문), IEC 60601(의료 부문) 등으로 세분화되어 제정되었다.

IEC 61508은 기능 안전의 대표적인 표준으로서, 안전수명주기를 통하여 시스템 개념단계에서 구현, 양산, 관리, 폐기에 이르기까지의 전사적인 과정을 명시하고 있으며, 안전 무결성을 만족하는 안전 제어시스템은 개발부터 운영 환경 및 다양한 상황에서 잠재된 위험원을 도출하고, 해당 위험원을 허용할 수 있는 수준까지 감소시키고자 하는 데 목적을 두고 있다.

이러한 안전 무결성의 도출 및 평가의 기준으로 IEC 61058의 Safety Integrity Level(SIL) 을 기준으로 표 1과 같이, 각 산업 분야별로 안전 무결성을 만족시키기 위한 요구 수준을 결정하고 잠재적 위험원을 제거하기 위한 방안을 소프트웨어 및 시스템 레벨에서 요구하고 있다. 각 SIL을 사용하는 표준은 IEC 61508과 관련된 IEC 61511 (장치 산업, Safety instrumented systems for the process industry sector), IEC 61513(원자력), IEC 62061 (기계), EN 50128(철도), EN 50402 (Gas-detection systems), ISO 26262(자동차) 등이 있다.

<표 4-1> 자동차, 항공, 철도 부문에서의 SIL 등급과 각 도메인간의 SIL 관계

도메인	각 도메인에서의 SIL 레벨				
일반 (IEC 61508)	-	SIL-1	SIL-2	SIL-3	SIL-4
항공 (DO-178B/C)	DAL-E	DAL-D	DAL-C	DAL-B	DAL-A
철도 (EN 50126)	-	SIL-1	SIL-2	SIL-3	SIL-4
자동차 (ISO 26262)	QM	ASIL-A	ASIL-B/C	ASIL-D	

SIL 등급은 표 1에서 보인바와 같이, 4가지 등급으로 구분되고 높은 등급을 가질수록 엄격한 안전무결성을 요구한다. 또한, 요구된 SIL 에 대한 적합성 여부를 검증하기 위해 두 가지 측도를 명시하고 있다. 먼저, 구조적 측도는 시스템 결함의 허용 수준인 Hardware Fault Tolerance(HFT)와 진단 비율인 Safe Failure Fraction(SSF)에 대한 측정 및 평가를 수행함으로써, 시스템의 구조적 강건성을 평가한다. 또한, 시스템의 고장 확률을 평가하기 위해서, Probability of dangerous Failure on Demand(PFD) 와 Frequency of dangerous Failure per Hour(PFH)로 구분되고 각각 다른 평가기준을 갖게 된다.

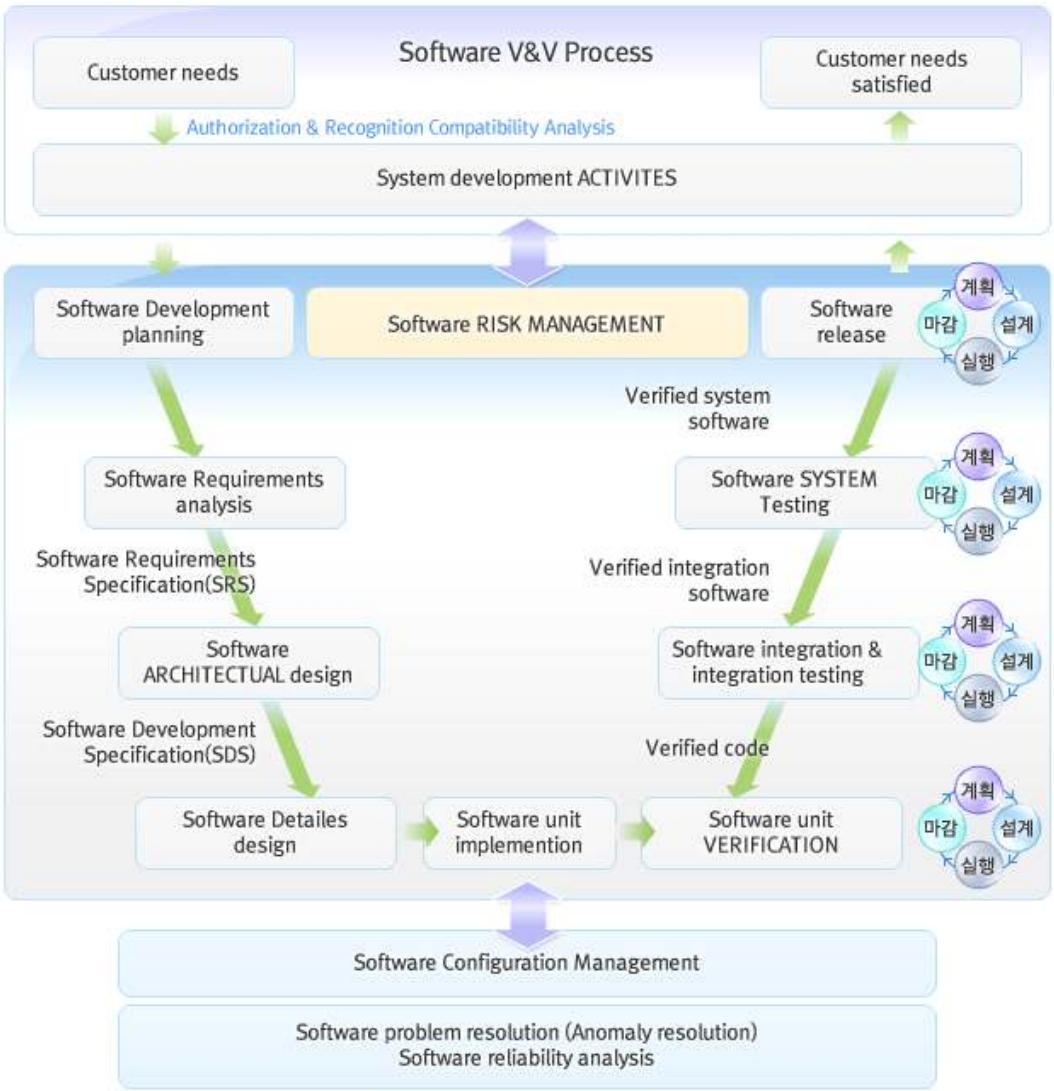
한편, 소프트웨어 개발 수준에서는 임베디드 시스템의 코드 안전성, 호환성, 신뢰성 확보를 위해, Motor Industry Software Reliability Association (MISRA) 에서 개발된 코딩 가이드라인을 표준으로서 따르고 있다. C++ 언어에 대한 가이드라인으로는 MISRA C++가 존재한다. MISRA-C는 자동차 산업으로부터 작성된 모델이지만, 자동차 산업 이외의 산업에 다양하게 쓰이고 있다. MISRA-C는 우주/항공, 의료장비, 국방, 철도 등 다양한 산업에서 실례로서 광범위하게 적용되는 가이드라인이라고 할 수 있다. MISRA-C:2004는 총 141개의 규칙이 있으며, 121개의 필수 규칙과 20개의 권고 규칙으로 구성되어 있다. MISRA-C 만족을 위한 코드 분석 도구는 Synopsys Coverity, Suresoft Technologies의 Code Inspector, MDS technologies의 Code Inspection 등이 존재한다.

위와 같이, 전기/전자/프로그램 가능한 전자 시스템의 안전 무결성을 만족시키기 위해 높은 기술 수준과 함께 다양한 표준은 무결성 사항을 요구하고 있고, 이는 소프트웨어의 안전성 산업 부문에 새롭게 진입하는 데 높은 기술적 장벽으로서 작용하고 있다. 또한, 해외 국제 안전 표준 컨설팅 기업의 사례를 살펴보면, 소프트웨어 안전 표준 및 가이드에 기반으로 하여 계획, 설계, 개발, 구현, 운영, 폐기까지의 전 과정에 대해 검사/테스팅/인증 업무에 대하여 서비스를 제공하며, 고가의 비용을 청구하고 있다. 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 컨설팅 업체의 고부가가치 서비스로의 전환 등이 이루어지고, 이를 통해 수준 높은 전문 인력이 유입 또는 육성되는 선순환 구조를 마련하는 것이 매우 중요한 과제라고 할 수 있을 것이다.

또한, 대학 및 대학원 등 고등 교육 체계를 통해 신규인력을 양성하여 시장에 해당 인력들을 공급함과 동시에, 산업체 재직자를 위한 소프트웨어 안전 전문 교육프로그램을 개설하여 전문역량을 강화시키는 것도 중요하다. 이와 연계하여 소프트웨어 안전 분야에 국가자격제도를 도입하고, 이를 기반으로 신뢰성 있는 전문가로의 위상 강화 등을 수행하는 것도 필요한 것으로 판단된다.

이에 대해 본 보고서에서 제시하는 안전 관련 국제 표준에 부합하는 자격제도 설계를 위한 연계 방안은, 국제 안전 표준에서 명시된 종합적인 프로세스에 대한 이해, 소프트웨어의 안전성을 만족시키기 위한 개발 실무, 그리고 전기/전자 시스템의 안전 무결성을 만족시키기 위한 하드웨어 기반 설계 등을 검정 과목에 포함하여, 해당 검정을 통과하여 자격을 취득한 해당 인력이 안전 관련 국제 표준을 만족하는 소프트웨어를 개발할 수 있는 능력을 보유할 수 있도록 하는 것이 필요하다.

[그림 4-1] 소프트웨어 V&V (Verification & Validation)



출처: KTL 한국산업기술시험원

각 산업별 국제 안전 표준은 소프트웨어 안전성 확보를 위해, 공통적으로 [그림 4-1]과 같이 시스템 개념단계에서 구현, 양산, 관리, 폐기에 이르기까지의 전사적인 과정을 명시하고 있다. 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 등 다양한 산업에 적용되고 있다. 소프트웨어 V&V는 소프트웨어 개발계획, 요구사항 분석, 아키텍처 설계, 기본/상세 설계, 구현, 테스팅, 설치 및 점검, 유지보수, 결함 관리 등 종합적인 개발 프로세스에서 시행되어야 한다.

다음은 국제 안전표준에 부합하는 인력의 자격 검증을 위한 조건이다.

첫 번째로 국제 안전표준에 부합하는 인력의 자격검증을 위해서는 각 국제 안전 표준에서 공통적으로 권고하고 명시하고 있는 [그림 4-1]과 같은 소프트웨어 V&V에 따른 프로세스에 대한 깊은 이해와 적용 방법에 대한 이론적 검증이 필요할 것이다. 이와 더불어, 개발된 소프트웨어와 탑재될 시스템이 도출된 요구사항에 부응하는 안전기능을 만족하는 지에 대한 테스트에 관련된 프로세스를 인지하고 있는 가에 대한 평가를 수행하는 것이 필요할 것이다.

두 번째로 소프트웨어 안전성을 만족시키기 위한 실제 소프트웨어 개발에서의 자격 검증과 평가를 수행하도록 하는 것이 요구된다. 이를 위해 대표적으로 소프트웨어의 설계에 앞서 위험원을 분석할 수 있는 능력과, 소프트웨어 개발에 있어 안전성 및 호환성 등 다양한 소프트웨어 안전 무결성 보장 기술을 기반으로 하는 국제 표준에 부합하는 소프트웨어 개발 실무 능력을 평가하도록 한다. 이에 대한 예시로 소프트웨어의 안전성을 높이기 위한 대표적인 임베디드 소프트웨어 프로그래밍 가이드인 MISRA를 꼽을 수 있다. MISRA는 임베디드 소프트웨어의 안전성을 높이기 위해 C/C++/Java 언어 프로그래밍 가이드라인을 배포하였으며, 자동차의 소프트웨어 개발을 목적으로 출간되었으나, 현재 자동차 분야뿐만 아니라 항공, 철도 등 소프트웨어의 안전성을 필요로 하는 다양한 산업군들에서 활용되고 있다. 따라서 MISRA를 준수하여 개발할 수 있는 능력을 자격 검정에서 평가하도록 하여 실제 소프트웨어 산업에서 중요하게 여기는 개발 실무 능력을 평가할 수 있고, 기존의 자격검정 제도가 갖는 필기 위주 평가의 한계점 또한 극복함으로써, 실제 소프트웨어 안전 관련 산업계에서 요구하는 역량을 가지고 있는지의 여부를 평가할 수 있는 적절한 척도로서 활용될 수 있을 것이다.

마지막으로 소프트웨어 개발뿐만 아니라 안전 무결성을 만족시키기 위한 하드웨어 설계 방법 및 능력을 평가하는 것 또한 고려할 수 있다. IEC 61508을 비롯한 각 국제 안전 표준은 소프트웨어만이 아닌 하드웨어 레벨까지 포함하는 전체적인 전기/전자 시스템에 대한 안전 무결성을 추구하고 있다. 소프트웨어 안전은 하드웨어 안전과 통합적 검토되어야 하며,

이를 위해서는 하드웨어에 대한 기본적인 지식이 있어야 한다. 하드웨어 능력평가의 대표적인 예시로는, 하드웨어의 결함 감내(Fault tolerant)가 가능한 시스템을 설계할 수 있는가에 대한 평가를 수행하는 것을 들 수 있다. 결함 감내는 시스템을 구성하는 부품의 일부에서 결함 또는 고장이 발생하여도 정상적 또는 부분적으로 기능을 수행할 수 있는 능력으로, 자동차, 철도, 플랜트, 의료, 금융, 항공 등과 같은 안전 중요(safety-critical) 임베디드 시스템에서 활용된다. 결과적으로, 국제 표준에서 명시하고 있는 SIL 등급의 분해(SIL Decomposition) 등을 수행하기 위해 소프트웨어뿐만 아니라 하드웨어 레벨에서의 안전 레이어(Safety Layer)를 설계하는 등의 기술적 방법의 숙지 여부를 평가함으로써, 국제 안전 관련 표준에 부합하는 역량을 보유한 소프트웨어 안전 전문가 자격제도를 설계하도록 한다.

2. 소프트웨어 안전 전문가 교육 및 산업현장의 역량 수요 반영 방안

소프트웨어 안전 분야는 다른 소프트웨어 관련 분야와 달리, 안전이 매우 중요한 자동차, 철도, 의료, 항공 등 다양한 산업군에 적용되고 있으며, 최근에는 IoT (Internet of Things) 기술 발전에 따라 그 적용 분야가 확대되고 있다. 이에 따라 기존의 소프트웨어 분야에 비하여 단순한 소프트웨어 개발 지식뿐만 아니라, 산업별 제품 특성에 대한 지식의 필요성이 매우 크다, 또한 자동차 산업의 사례를 보면, 자율 주행 자동차 등 신기술이 도입됨에 따라, 소프트웨어에 의하여 구동되고 제어되는 기능이 크게 증가하고 있으며, 이에 따라 신제품 개발에 따른 새로운 소프트웨어 안전에 대한 요구가 생성되는 특징을 가지고 있다.

이러한 점을 고려하면, 소프트웨어 안전 전문가 자격제도의 성공을 위해서는 다양한 산업계와의 지속적인 교류를 통하여 해당 분야에서의 소프트웨어 안전 관련 요구 역량의 도출 및 보완이 매우 중요하다. 또한 이러한 신기술의 발전에 따른 빠른 변화를 고려하여, 검정 평가 내용의 꾸준한 개선 및 자격 보유자에 대한 재교육 및 재인증 등의 제도를 도입하여, 소프트웨어 안전 개발자가 산업 현장에서 요구하는 소프트웨어 안전 관련 신기술을 꾸준히 습득하고 유지할 수 있도록 해야 한다.

소프트웨어 안전성 관련 국제 표준은 IEC 61508을 중심으로 존재하고 있으며, 각 산업분야 별로 세분화되어 제정되고 있으며 새로운 산업 분야에 대한 안전 관련 국제 표준들이 신설되고 있다. 하지만, 국내에서는 항공, 원자력 등 특정 산업을 제외하고는 아직까지 국내 실정에 부합하는 공통적 기준이 마련되지 않았거나, 적용에 어려움을 느끼고 있다. 산업별로 특정 도메인에서는 소프트웨어 안전 필수 시스템 발주기관과 개발 기업들도 소프트웨어

안전에 대한 표준에 대한 지식은 물론 소프트웨어 안전 인식도 부족한 실정이다. 다음은 2016년 SPRi에서 수행한 소프트웨어 안전 관련 전문가 심층인터뷰 분석 내용이다.

[그림 4-2] 산업별 소프트웨어 안전 인식 및 역량 분석 및 교육 방향

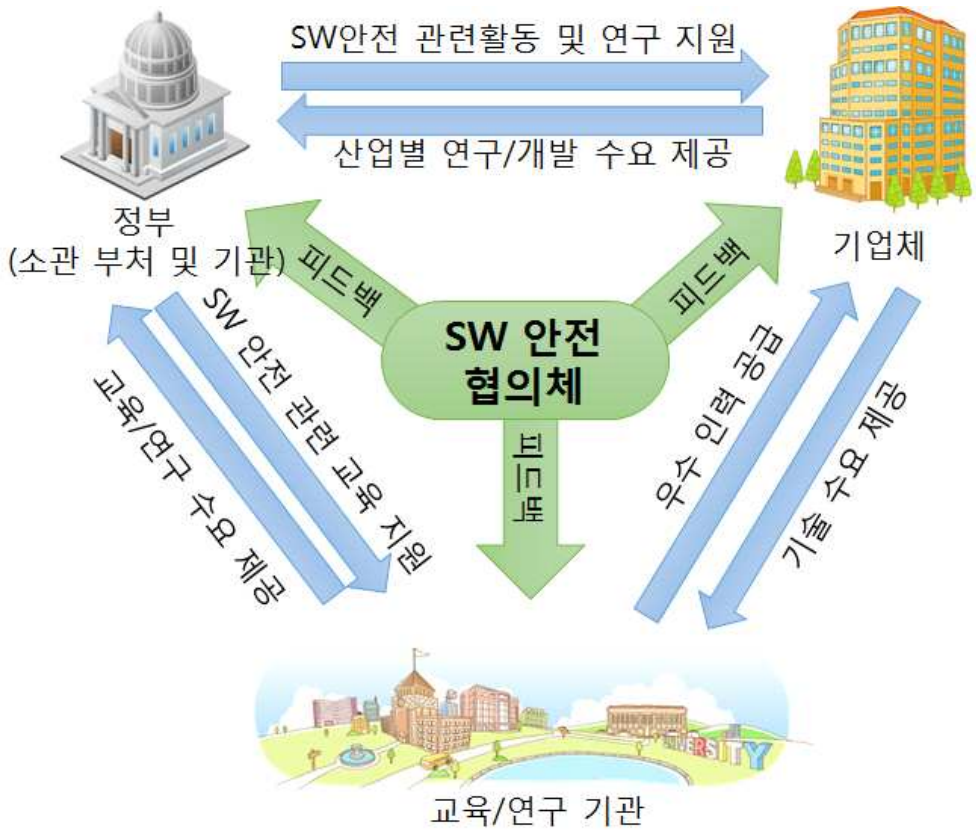
자료 : SPRi 소프트웨어 안전 재직자를 위한 교육, 전문가 심층 인터뷰

전문가 심층인터뷰 결과, 자동차, 항공, 원자력 등 기존 안전이 중요 시 되는 산업에서는 기능안전 관련 국제 표준이 존재하고, 수출이나 국내 안전을 위해 국제 표준 적용이 비교적 체계적으로 적용되고 있다. 그러나 IoT, 로봇 등 신기술 분야는 안전 의식이 부족하고, 기본적인 소프트웨어 안전에 대한 지식이 습득되어 있지 않다.

기존 산업은 물론 신기술을 이용한 새로운 산업에서 소프트웨어 안전을 보장하기 위해서는 산업체, 교육계, 정부출연 연구기관, 소프트웨어 안전 관련 정책 수립기관 등을 포함하는 소프트웨어 안전 자격 관련 협의체를 구성하여, 산업 수요에 맞는 교육 및 검정 과목 설정 및 보완을 진행하는 것이 요구된다. 나아가 소관 부처 및 전문 기관에서는 국내 실정에 부합하는 안전 표준의 제정과 더불어 각 산업별로 존재하는 국제 표준에 부합하는 소프트웨어 안전 기준을 마련하고, 산업별 안전 관리 규정에 소프트웨어 안전 기준을 현실적으로 반영할 필요가 있다. 또한, 소프트웨어 안전 관련 국제 표준에 대응하기 위해, 관련 국제회의 및 기구 등에 적극적으로 참여할 수 있도록 정부차원에서의 지원체계를 강화할 필요가 있으며, 이를 통해 안전 관련 소프트웨어 산업의 선진국과의 기술격차를 좁히기 위한 노력 또한 요구된다.

이러한 다양한 활동을 위하여, 소프트웨어 안전 관련 산업계, 학계, 정부출연 연구기관 및 소프트웨어 안전 관련 정책 수립기관을 아우르는 협의체를 구성하여, 소프트웨어 안전 관련 기술 동향의 공유, 소프트웨어 안전 전문가 자격에서 평가할 소프트웨어 안전 전문가의 필수 역량, 안전 관련 국제 표준화 동향의 공유 등의 수행이 요구된다.

[그림 4-3] 소프트웨어 안전 협의체 구성도



SW 안전 협의체를 통하여, 소프트웨어 안전 전문가 자격제도의 효과적인 실시 및 유지를 위한 각종 법, 제도적 장치를 도출하고, 자격의 실효성을 높이기 위한 방법으로 정부 발주 사업의 자격증 소지자 우대 정책, 자격증 소지자에 대한 유지 보수 교육 정책, 국제 안전 표준 동향 정보 발간 및 요구되는 소프트웨어 안전 관련 가이드라인의 도출 및 제정 등의 업무를 진행하는 것이 필요할 것으로 판단된다. 국내의 국제 표준화 활동 지원 사업이나 국가 표준기술력 향상 사업 등 국제 표준화 기반 강화를 위한 지원 사업의 확대 방안 등도 함께 협의함으로써 실제 산업의 수요와 요구에 맞는 인력 수급 계획과 표준 제정을 진행하며, 이러한 결과를 소프트웨어 안전 전문가 자격 제도에 반영한다.

SW 안전 협의체의 구성 및 활동과 더불어, 소프트웨어 개발 기업, 안전 컨설팅 기업, 전담기관 담당자, 발주 담당자 등의 소프트웨어 안전 관련 인식 제고를 위하여, 정기적으로 소프트웨어 안전 관련 컨퍼런스나 세미나 등을 개최하여 산업계, 학계, 정부 등의 적극적인 참여를 유도하고, 이들의 요구사항을 자격제도 등에 반영 할 필요가 있다. 이외에 금융, 교육, 국방, 정보통신 분야에서 이미 구축되어 있는 정보공유분석센터(ISAC, INFORMATION SHARING AND ANALYSIS CENTER)과 같이 인허가를 관장하는 전담기관 간의 정보공유 체계를 강화하고, 공통 기술, 사고 사례, 문제 해결 사례 등을 적극 공유한다. 또한, 실제 산업의 수요를 분석하고 반영하기 위해 각 산업별 선도 기업들의 기술 개발 및 인사 담당자의 설문 등을 통해, 산업에서 요구하는 기술과 역량 등과 같은 피드백 정보를 수집하여, 이에 대응하는 자격제도의 보완을 지속적으로 수행하도록 한다.

제2절 소프트웨어 안전 관련 국제 인증에 부합하는 전문가 자격제도 모델

본 절에서는 3장에서 수행한 기존 소프트웨어 관련 자격제도에 대한 분석과 4장 1절에서 제시한 소프트웨어 안전 관련 국제 인증에 부합하는 전문가 자격제도와의 연계를 위한 방안을 고려하여, 본 연구의 목표인 소프트웨어 안전 전문가 자격제도 모델의 세부 사항을 제시한다. 이를 위해, 먼저 본 보고서에서 제시하는 소프트웨어 안전 전문가 자격제도 모델의 개요를 기술하고, 제시하는 자격제도 모델에서 요구되는 핵심 역량을 기술함으로써 소프트웨어 안전 전문가로서 요구되는 직무능력을 제시한다. 마지막으로, 본 보고서에서 제시하는 소프트웨어 안전 전문가 자격제도에서 수행하는 평가 방식, 과목, 자격, 검정 방법 등의 세부 모델에 대한 내용을 제시한다.

1. 소프트웨어 안전 전문가 자격제도 모델의 개요

본 연구에서 제안하는 소프트웨어 안전 전문가 자격 모델은 소프트웨어 안전 분야의 전문가를 배출하는 목적을 가지고 설계되었다. 전문가 수준에 맞는 자격 제도의 설계를 위하여 전산 및 소프트웨어 개발 관련 직종에 필요한 기초적인 소양에 해당하는 부분은 과감히 배제하였으며, 국가기술자격제도에서의 기사 등급 이상의 자격을 지향하도록 설계하였다.

소프트웨어 안전의 핵심 역량 추출을 위하여 NCS(국가직무능력표준)와 해외의 국제 안전 표준 인증기관 등에서 시행하는 소프트웨어 안전 관련 자격증을 참고하였으며, 이를 통하여 도출한 소프트웨어 안전 전문가가 보유해야 할 핵심역량으로 소프트웨어 관련 국제 표준에 따른 소프트웨어 설계 및 개발, 소프트웨어의 안전 무결성 수준(SIL), 기능안전평가 및 테스트, 코딩 표준 외에도 일반적인 소프트웨어의 프로젝트 관리, 품질보증 등을 정의하였다.

도출한 핵심 역량에 따라 소프트웨어 안전 전문가를 분류하였으며, 각 핵심역량을 기준으로 요구되는 검정과목을 도출하였다. 본 보고서에서 제안하는 자격제도는 기존 국가기술자격에서의 검정형이 아닌 과정평가형의 형태를 지님으로써, <제3차 국가기술자격 기본계획>에서의 과정이수형 자격제도 도입 정책에 대응하고, 교육과정을 통하여 상대적으로 접근하기 어려운 국제안전표준의 접근성 문제를 해소하도록 하였다.

또한, 자격의 질적 관리를 위하여 기출문제 유출 방지를 시행하고, 보다 실무적인 형태의 실기검정을 위하여 기존의 필답형이 아닌, 코딩 및 소프트웨어 테스팅 등의 실무적인 지식에 대한 검정을 포함하여 시행하도록 설계하였다. 이와 더불어 자격의 재검정 제도를 도입

함으로써, 매 3년마다 재검정을 통하여 자격을 갱신하여 자격취득자의 역량을 유지할 수 있는 방안을 마련하였다.

그 외에도 대학 등 교육기관과의 연계를 통하여 소프트웨어 안전에 관한 관심과 중요성에 대한 인식의 제고를 추진하며, 교육기관에서 소프트웨어 안전 관련 과목을 이수한 경우, 과정이수 및 검정에서 일부 과목의 이수 면제 등의 혜택을 부여함으로써 자격제도와 교육기관과의 연계성을 도모하도록 설계하였다.

2. 소프트웨어 안전 전문가 자격에서 요구되는 핵심 역량

소프트웨어 안전 전문가의 핵심역량을 도출하기 위하여 현존하는 NCS(국가직무능력표준)의 분류체계를 참고하여 소프트웨어 안전 분야에 관련된 직무를 정리하였다. 이는 소프트웨어 안전 전문가에게 필요한 개발능력과 품질보증 및 평가, 테스팅 등을 포함한다.

<표 4-2> 소프트웨어 안전 관련 NCS 국가직무능력표준 항목

소분류	세분류
정보기술개발	응용SW엔지니어링
정보기술운영	IT시스템관리
정보기술관리	IT프로젝트관리
	IT품질보증
	IT테스트

자료 : NCS 국가직무능력표준 홈페이지, NCS분류, 편집[79)]

그러나 NCS 분류체계만을 가지고는 소프트웨어 안전에 관련된 핵심 역량을 도출해내는데 한계가 있다. 이는 NCS는 국내에 현존하는 주요 직종을 위주로 편성되어 있는 관계로, 국내에서 해당 산업이 비교적 부진한 상황인 소프트웨어 안전 관련 분야의 전문적인 분류에 관한 내용은 없는 상태이다. 특히 국제 안전 표준에 해당하는 부분은 소프트웨어 안전 전문가에게 핵심적인 역량이지만, 현재의 NCS 분류체계로는 국제 안전 표준에 관련된 부분을 반영하지 못하고 있는 실정이다.

79) 자료 : NCS 국가직무능력표준 홈페이지. NCS분류
https://www.ncs.go.kr/ncs/page.do?sk=P1A1_PG01_002 편집

이러한 점을 감안하여 소프트웨어 안전 관련 표준에 부합하는 소프트웨어 안전 전문가의 핵심역량 도출을 위하여 IEC 61508, ISO 26262 등의 표준 내용 및 본 보고서에서 분석한 해외 자격제도 인증 및 교육과정을 참고하여, NCS 분류체계에서 제시되지 않은 핵심역량을 자체적으로 정의하여 추가하였다. 해당 핵심역량은 소프트웨어 안전 분석 및 설계, 안전 무결성 수준(SIL), 기능안전 평가 및 인증 등이며, 각 핵심 역량을 정리한 표는 <표 4-3>과 같다.

<표 4-3> 국제 표준에 부합하는 소프트웨어 안전 전문가 핵심역량

핵심 역량	역량의 세부 내용
소프트웨어 안전 분석 및 설계	소프트웨어 안전관련 국제 표준의 이해
	위험 요인 판단 및 분석
	소프트웨어 안전 요구사항 분석
	소프트웨어 안전 국제 표준에 따른 개발 방법론
	소프트웨어 안전 설계
소프트웨어의 안전무결성수준(SIL)	안전무결성수준 결정
	안전무결성 요구에 따른 시스템의 구조 결정
소프트웨어 안전 검증	소프트웨어 안전 테스트 수행
	평가대상별로 목적 및 적용 요구사항에 대한 객관적인 평가기술을 활용하여 기능안전 검증절차를 수행하는 능력

소프트웨어 안전 분석 및 설계 파트에서는 위험 요인을 판단 및 분석, 소프트웨어 안전 요구사항 분석, 안전수명주기의 개념 및 개발 방법론, 소프트웨어 안전 설계의 기법 및 절차들을 다룬다. 소프트웨어 안전 무결성 수준(SIL)은 개발하고자 하는 소프트웨어의 안전에 대한 기준이 되는 것으로, 이를 결정하는 과정과 목표 안전 무결성 수준(SIL)을 달성하기 위한 시스템의 구조를 결정하는 역량을 포함한다. 마지막으로 소프트웨어 안전 검증에서는 소프트웨어 안전 테스트 수행 및 안전 무결성 수준(SIL)의 달성을 확인하기 위한 평가기술 및 검증 절차들을 수행할 수 있는 역량을 포함한다.

상기 핵심역량과, NCS 국가직무능력표준의 소프트웨어 안전 관련 항목들을 포함하는 안전 전문가 핵심역량을 <표 4-4>에 제시하였다. 이는 <표 4-3>에 제시한 안전 관련 국제 표준에

서 요구하는 핵심 역량과, <표 4-2>에 제시한 NCS 국가직무능력표준의 해당 직무 항목에서 요구되는 세부 핵심 역량을 포함하여 정의하였다.

<표 4-4> 소프트웨어 안전 전문가의 핵심 역량

핵심 역량	역량의 세부 내용
안전 관련 국제 표준	소프트웨어 안전 이론
	소프트웨어 안전 관련 국제 표준 및 규제
소프트웨어 안전 분석 및 설계	위험 요인 판단 및 분석
	소프트웨어 안전 요구사항 분석
	소프트웨어 안전 설계
소프트웨어 개발	소프트웨어 개발 기법
소프트웨어 안전 테스트	소프트웨어 안전 테스트 수행
소프트웨어 안전 평가	기능안전 검증 및 평가
소프트웨어 안전 관리	프로젝트 관리
	소프트웨어 형상관리
	소프트웨어 안전 품질 관리

3. 소프트웨어 안전 전문가 자격제도의 세부 모델

도출된 핵심역량에 따라서 평가 형식은, 이론적인 부분을 관장하는 필기과목과 실무에 대한 지식 및 절차에 대한 평가를 위한 실기과목으로 진행하는 것이 적합한 것으로 판단한다. 본 항목에서는 자격제도의 세부 모델을 위하여 각 시험 형식 및 과목에 따른 세부항목 및 세세항목에 대한 내용은 아래와 같이 정리하였다.

1) 소프트웨어 안전 전문가 자격제도 분류

소프트웨어 안전 전문가 자격제도의 세부 모델의 정의에 앞서, 소프트웨어 안전 전문가의 역할에 따른 자격제도의 분류를 아래 그림과 같이 제시하였다. 각기 요구되는 핵심 역량에 따라서 소프트웨어 안전 전문가는 개발자, 설계자, 테스터, 안전 관리자의 총 4가지의 자격제도로 구성하도록 설계하였으며, 세부적으로 각 전문가가 수행하는 업무 및 역량은 <표 4-5>와 같다.

<표 4-5> 소프트웨어 안전 전문가 분류 및 필요 역량

분류	필요 역량	역할
공통	안전 관련 국제 표준	소프트웨어 안전 기본 소양
소프트웨어 안전 전문 개발자	소프트웨어 개발	소프트웨어 안전을 위한 코딩 표준을 준수하여 소스코드를 작성하며, 개발된 소프트웨어를 대상에 적용시키는 역할 수행한다.
소프트웨어 안전 전문 설계자	소프트웨어 개발	아키텍처에 따른 소프트웨어 설계를 소프트웨어 안전 관련 표준에 입각하여 수행한다. 소프트웨어 설계 시에는 소프트웨어의 요구사항을 명확히 인지하고, 적합한 설계 방법을 선택해야 한다.
	소프트웨어 설계	
소프트웨어 안전 전문 테스터	소프트웨어 안전 테스트	소프트웨어의 안전성을 테스트할 수 있는 계획을 수립하며, 테스트를 수행한다. 테스트 상에서 예상 결과에서 벗어난 것을 파악하며, 이를 개발자, 설계자 등에게 통보한다.
소프트웨어 안전 관리자	소프트웨어 개발	프로젝트에 대한 품질관리 시스템을 적용 및 소프트웨어 국제 안전 표준의 절차에 따라 소프트웨어가 개발되고 있는 것을 보증해야한다.
	소프트웨어 안전 설계	
	소프트웨어 안전 테스트	
	소프트웨어 안전 관리	

위에서 제시한 4개 종류의 전문가를 위한 자격제도는 공통적으로 소프트웨어 안전 관련 국제표준에 대한 기반 지식을 요구한다. 이는 개발자부터 안전 관리자까지 공통적으로 요구되는 역량으로 소프트웨어 안전의 개념 및 기초 이론 등을 포함한다. 소프트웨어 안전 전문 개발자는 설계자에 의해서 설계된 소프트웨어를 코딩 표준을 활용하여 개발하며, 안전 전문 설계자는 소프트웨어의 요구사항을 인지하고 소프트웨어가 활용되는 시스템의 구조에 따라서 적합한 방식으로 소프트웨어를 설계할 수 있는 역량을 보유해야 한다. 소프트웨어 안전 전문 테스터는 주어진 안전 요구 사항에 부합하는 테스트 계획을 세워야 하며, 개발된 소프트웨어의 안전성을 테스트하여 개선 사항에 대한 피드백을 주어야 한다. 마지막으로 전반적인 소프트웨어 안전을 관리하며, 평가할 수 있는 소프트웨어 안전 관리자는 개발자, 설계자, 테스터 전문가들의 기본적인 역량을 모두 보유하며, 품질관리 및 안전 관련 국제표준에 따른 프로젝트 관리에 대한 역량을 필요로 한다. 소프트웨어 안전 관리자는 상기 4개 종류의

자격 중, 요구되는 경험 및 역량 등이 가장 높은 자격으로 설계하였다.

소프트웨어 안전 관련 국제표준에서는 이 외에도 전체 프로젝트가 표준에 부합하게 진행되는지를 감사하는 평가자, 해당 도메인별로 도메인에 맞는 위험을 분석하는 위험 분석 전문가 또한 고려되어 있다. 평가자의 경우에는 도메인 관련 지식이 다른 전문가에 비해 많이 요구되며, 최고 수준의 자격증으로 설계하기에 앞서, 국내 산업계에 현실을 고려한 수행역할 및 요구사항 등에 대한 분석과 가장 중요시되는 평가자로서의 경험을 평가할 수 있는 기준 등에 대한 면밀한 검토가 추가적으로 필요할 것으로 판단된다. 위험 분석 전문가도 해당 도메인의 전문가들과 협의가 필요하며, 도메인과 밀접하게 연관된 자격증으로서 역량 평가 및 전문가 양성 방안 등에 대한 추가 연구가 필요하리라 본다. 본 연구에서는 관련 자격을 제시하지 않았으며, 추후 후속 연구를 통하여 해당 역할에 대한 자격증 제도의 추가를 고려해야 할 것으로 사료된다.

2) 응시자격

소프트웨어 안전 전문가 자격증은 해당 분야의 전문가에 해당하는 수준을 목표로 구성하였다. 따라서 응시자격은 기본적으로 국가기술자격법 시행령에서 요구하는 기사의 응시자격을 달성해야하며, 기사의 응시자격 내용은 본문 3장의 3절의 1에 설명되어 있다. 더욱 상위 수준의 자격에 해당하는 소프트웨어 설계자, 소프트웨어 안전 관리자의 자격에 대해서는 추가적으로 요구되는 응시자격이 있으며 이는 하단의 표와 같다.

<표 4-6> 소프트웨어 안전 자격증의 응시자격

등급	응시자격
개발자 등급	유사 직무분야에 종사했거나 및 관련학과를 졸업한 사람으로, 국가기술자격 중 기사자격의 응시자격을 차용한다.
테스터 등급	
설계자 등급	개발자 등급을 취득하여 보유하고 관련 직무분야에서 4년 이상 종사한 사람.1
안전관리자 등급	설계자 등급 및 테스터 등급을 함께 취득하여 보유한 후 관련 직무분야에서 3년 이상 종사한 사람.

3) 시험과목

앞서 기술한 시험의 형식, 과목, 주요 항목의 정의는 <표 4-7>에 제시한 바와 같다.

<표 4-7> 소프트웨어 안전 전문가 자격제도의 과목 목록

시험 형식	과목	주요항목
필기과목	안전 관련 국제표준	소프트웨어 안전 국제 표준 개요 및 법규
		소프트웨어 안전 개념 및 이론
		안전무결성 수준 (SIL)
	소프트웨어 개발	소프트웨어 구현
		코딩 표준
		소프트웨어 개발 플랫폼
	소프트웨어 설계	위험 요인 판단 및 분석
		소프트웨어 안전 요구사항 분석
		소프트웨어 안전 설계
	소프트웨어 안전 테스트	테스트 계획 및 관리
		테스트 방법론
		블랙박스 및 화이트박스 테스트
		표준적합성 테스트
	소프트웨어 안전 관리	소프트웨어 프로젝트 관리
		소프트웨어 형상관리
		소프트웨어 안전 품질 관리
실기과목	소프트웨어 개발	소프트웨어 코드 안전 검증
	소프트웨어 설계	안전무결성 결정
		위험감소
		소프트웨어 안전 설계
	소프트웨어 안전 테스트	기능 안전 검증
		단위테스트 및 통합테스트
		블랙박스 및 화이트박스 테스트
	소프트웨어 안전 관리	소프트웨어 프로젝트 관리
		소프트웨어 형상관리
		소프트웨어 품질관리

소프트웨어 안전 국제 표준 및 법규에서는 국제 표준에 부합하는 소프트웨어의 개념을 주요 항목 및 세부항목으로 나누었으며, 소프트웨어 안전 국제 표준 개요 및 법규, 소프트웨어 안전 개념 및 이론, 안전 무결성 수준의 주요항목으로 나뉜다. 안전 관련 국제표준 항목은 모든 자격에서 공통적으로 요구하는 역량으로서, 기본적인 국제 표준 및 소프트웨어 안전의 개념 및 이해도를 평가한다.

<표 4-8> 공통 필기과목 : 국제 안전 표준 이론과 법규

과목	주요항목	세부항목
안전 관련 국제표준	1. 소프트웨어 안전 국제 표준 개요 및 법규	1. 소프트웨어 국제 안전 표준 개요 2. 소프트웨어 안전 국제 표준 법규
	2. 소프트웨어 안전 개념 및 이론	1. 소프트웨어 안전의 정의 2. 소프트웨어 기능안전 및 품질 3. 안전수명주기
	3. 안전 무결성 수준 (SIL)	1. 안전 무결성 개념 2. 안전 무결성 수준에 따른 안전도

소프트웨어 개발 항목에서는 소프트웨어 구현, 코딩 표준, 소프트웨어 개발 플랫폼에 대한 지식을 주요 항목을 평가한다. 해당 필기과목에서는 소프트웨어 설계자에 의하여 설계된 소프트웨어를 실제 코딩 표준 및 정해진 플랫폼의 제약사항에 맞게 구현하기 위한 이론들에 대하여 평가한다.

<표 4-9> 소프트웨어 안전 전문 개발자 필기과목

과목	주요항목	세부항목
소프트웨어 개발	1. 소프트웨어 구현	1. 소프트웨어 구현 언어 2. 지원 도구
	2. 코딩 표준	1. 코딩 표준의 이해 2. 소프트웨어의 검증 및 분석
	3. 소프트웨어 개발 플랫폼	1. 하드웨어 및 소프트웨어 플랫폼 2. 시스템 별 제약사항

소프트웨어 설계 항목에서는 위험 분석을 통하여 위험 요소를 정의하기 위한 이론적인 기법과 소프트웨어 안전 설계를 위한 설계 및 검증 절차, 소프트웨어 안전성 관리, 소프트웨어 안전을 위한 코딩의 표준에 대한 항목으로 주요 항목 및 세부항목을 나누었다.

<표 4-10> 소프트웨어 안전 전문 설계자 필기 과목

과목	주요항목	세부항목
소프트웨어 설계	1. 위험 요인 판단 및 분석	1. 위험의 개념 2. 위험 요소 정의 3. 위험 요소 분석 기법
	2. 소프트웨어 안전 요구사항 분석	1. 소프트웨어 도메인의 특성 분석 2. 소프트웨어 안전 요구사항 결정
	3. 소프트웨어 안전 설계	1. 소프트웨어 구조 설계 2. 소프트웨어 안전 메커니즘 설계

소프트웨어 테스팅 항목에서는 테스트를 계획하고 관리하는 절차와 관련된 표준에 대한 내용을 다루고 있으며, 테스트 기법에 대한 이론을 다루고 있다.

<표 4-11> 소프트웨어 안전 전문 테스터 필기 과목

과목	주요항목	세부항목
소프트웨어 안전 테스트	1. 테스트 계획 및 관리	1. 테스트 계획 2. 테스트 설계 3. 테스트 관리 4. 테스트 자동화 도구 5. 소프트웨어 테스트 국제 표준
	2. 테스트 방법론	1. 정적 테스트 2. 동적 테스트
	3. 블랙박스 및 화이트박스 테스트	1. 블랙박스 테스트 이해 2. 화이트박스 테스트 이해 3. 블랙박스 테스트 케이스 설계
	4. 표준적합성 테스트	1. 표준적합성 테스트 개요 2. 표준적합성 테스트 수행

소프트웨어 안전 관리 분야는 안전 관리자의 자격으로서, 소프트웨어 안전 관련 국제 표준에 부합하는 프로젝트 수행절차를 관리하며, 형상관리 및 소프트웨어 품질 관리에 대한 지식을 평가한다. 해당 과정은 전반적으로 소프트웨어 안전 관련 국제 표준에 맞게 개발이 되고 있는지를 판단하고, 관리할 수 있는 역량을 평가하는 과정이므로, 앞선 모든 자격에 대한 기본적인 지식을 함께 요구한다.

<표 4-12> 소프트웨어 안전 관리자 필기 과목

과목	주요항목	세부항목
소프트웨어 안전 관리	1. 소프트웨어 프로젝트 관리	1. 프로젝트 계획 및 예측 2. 국제 표준에 따른 프로젝트 수행 절차
	2. 소프트웨어 형상관리	1. 형상관리의 이해 2. 형상관리 도구 3. 형상관리
	3. 소프트웨어 안전 품질 관리	1. 안전 관리자 및 품질 관리의 이해 2. 기능 안전 관리 3. 안전 품질 최적화 4. 안전 감사

실기과목에서는 소프트웨어 안전 관련 국제 표준에 부합하는 소프트웨어 설계, 소프트웨어 개발 및 소프트웨어 안전 테스트와 같이 직접적인 실무에 대한 지식이 필요한 항목으로 구성하였으며, 국제 표준 이론 과목은 실기과목으로 평가하지 않는다.

<표 4-13> 소프트웨어 안전 전문 개발자 실기 과목

과목	주요항목	세부항목
소프트웨어 개발	1. 소프트웨어 코드 안전 검증	1. 코딩 표준 준수 코딩 2. 코드 레벨 안전 검증기법

<표 4-14> 소프트웨어 안전 전문 설계자 실기 과목

과목	주요항목	세부항목
소프트웨어 안전 설계	1. 안전무결성 결정	1. 소프트웨어 요구사항 2. 안전무결성 수준 결정
	2. 위험감소	1. 위험감소 방안 2. 시스템 구조 설계
	3. 소프트웨어 안전 설계	1. 소프트웨어 구조 설계 2. 소프트웨어 안전 메커니즘 디자인

<표 4-15> 소프트웨어 안전 전문 테스터 실기 과목

과목	주요항목	세부항목
소프트웨어 안전 테스트	1. 기능 안전 검증	1. 평가기술 2. 기능안전 검증
	2. 단위테스트 및 통합테스트	1. 소프트웨어 버그 파악 및 품질보증을 위한 테스팅
	3. 블랙박스 및 화이트박스 테스트	1. 취약점 및 버그 파악을 위한 테스팅

<표 4-16> 소프트웨어 안전 관리자 실기 과목

과목	주요항목	세부항목
소프트웨어 안전 관리	1. 소프트웨어 프로젝트 관리	1. 국제 표준에 따른 프로젝트 수행
	2. 소프트웨어 품질관리	1. 안전 및 품질 결정 및 관리 2. 안전 감사

4) 평가 형식

소프트웨어 안전 전문가 자격증은 안전한 소프트웨어 설계 및 국제표준을 준수하는 소프트웨어 개발을 위하여 국제 안전표준의 가장 기본이 되는 표준인 IEC 61508과 상기 서술한 핵심 역량에 기반을 두어, SIL (Safety Integrity Level), 그리고 안전에 관련한 국내외 지침 등을 평가한다. 본 자격증의 경우 IEC 61508과 같은 국제 안전 관련 표준의 내용을 포함하고 있으나, 해당 표준의 자료는 유료로 구해야 하는 내용이며, 개인이 구매하기에는 상당한 비용 부담이 필요하다는 문제점이 있다. 그러므로 검정평가형의 방식보다는 과정평가형 방식을 도입하는 것을 통하여 안전에 관련한 교육을 특정 인증된 기관 등에서 이수한 후 시험에 응시하는 것으로 자격증을 발급하는 방식이 적합하다. 이와 더불어 일본 등에서 수행하고 있는 바와 같이 국제 안전 표준 정보에 대한 해설서 및 가이드라인 등을 정부연구기관 및 산업별 유관 기관에서 제작 보급하여, 자격 취득 희망자가 경제적인 부담 없이 해당 내용에 대한 학습을 진행할 수 있는 지원이 필요할 것으로 생각된다.

교육과정은 상기의 핵심역량과 시험 과목의 주요항목 및 세부항목으로 구성되어야 한다. 각 소프트웨어 안전 관련 자격의 교육과정을 이수 후 및 응시자격을 충족시킨 경우 시험에 자격 별 응시가 가능하며, 문제유형은 기존의 국가기술자격시험과 같이, 필기 및 실기시험으로 나뉜다. 필기시험의 경우 이론 위주의 객관식 문제로 개인의 역량을 평가하며, 실기시험은 작업형과 서술형의 복합형으로 진행하여 평가한다. 각 역할 별 자격증 검정 기준의 문항수에 따른 시험 시간 및 합격기준은 기존의 정보처리기사 자격증 및 임베디드기사 자격증을 참고하여 다음 표와 같이 작성하였다.

<표 4-17> 소프트웨어 안전 전문 개발자 자격증의 검정기준

평가 형식	과목	문제수	배점	시험 시간	문제 유형	합격기준
필기 검정	소프트웨어 안전 관련 국제 표준	20	100	150 분	객관식	각 과목 : 40점 이상 4과목 평균 : 60점 이상
	소프트웨어 구현	20	100			
	코딩 표준	20	100			
	소프트웨어 개발 플랫폼	20	100			
실기 검정	소프트웨어 코드 안전 검증	-	100	180 분	복합형	60점 이상

<표 4-18> 소프트웨어 안전 전문 설계자 자격증의 검정기준

평가 형식	과목	문제수	배점	시험 시간	문제 유형	합격기준
필기 검정	위험요인 판단 및 분석	20	100	150 분	객관식	각 과목 : 40점 이상 3과목 평균 : 60점 이상
	소프트웨어 안전 요구사항 분석	20	100			
	소프트웨어 안전 설계	20	100			
실기 검정	안전무결성 결정	-	100	180 분	복합형	60점 이상
	위험 감소	-	100			
	소프트웨어 안전 설계	-	100			

<표 4-19> 소프트웨어 안전 전문 테스터 자격증의 검정기준

평가 형식	과목	문제수	배점	시험 시간	문제 유형	합격기준
필기 검정	소프트웨어 안전 관련 국제 표준	20	100	150 분	객관식	각 과목 : 40점 이상 3과목 평균 : 60점 이상
	테스트 계획 및 관리	20	100			
	테스트 방법론	20	100			
	블랙박스, 화이트박스 테스트	20	100			
	표준적합성 테스트	20	100			
실기 검정	기능 안전 검증	-	100	180 분	복합형	60점 이상
	단위테스트 및 통합테스트	-	100			
	블랙박스, 화이트박스 테스트	-	100			

<표 4-20> 소프트웨어 안전 관리자 자격증의 검정기준

평가 형식	과목	문제 수	배점	시험 시간	문제 유형	합격기준
필기 검정	소프트웨어 프로젝트 관리	20	100	150분	객관식	각 과목 : 40점 이상 3과목 평균 : 60점 이상
	소프트웨어 형상관리	20	50			
	소프트웨어 안전 품질 관리	20	150			
실기 검정	소프트웨어 프로젝트 관리	-	100	180분	복합형	60점 이상
	소프트웨어 형상관리	-	50			
	소프트웨어 안전 및 품질 관리	-	150			

소프트웨어 안전 전문가 자격 과목에서, 공통적으로 포함되는 과목인 『소프트웨어 안전 관련 국제표준』은 제안하는 모든 전문가 자격제도의 기본이 되는 지식이므로, 전문가 자격제도 중에서 가장 하위 단계의 자격제도인 소프트웨어 개발자 및 소프트웨어 테스터의 경우에만 필기과목에 포함되어 있다. 여기서 평가하는 국제표준은 도메인 공통으로 포함되는 소프트웨어 안전에 대한 부분으로, 소프트웨어 안전 관련 국제표준 전체의 내용을 포괄하는 것은 아니다.

덧붙여, 기존 국가기술자격의 단점으로 거론되었던 암기식 학습을 방지하기 위한 방법으로 본 자격의 필기검정에서는 정보보안기사의 정책을 차용하여, 기출문제 등을 유출시키지 않음으로써 문제의 변별력을 높이고, 자격 취득자가 보다 높은 기술적 이해도를 갖출 수 있도록 한다. 또한, 소프트웨어 안전에 관련된 최근의 경향과 실무적인 부분을 다루는 문제를 일정 비중 이상 출제함으로써 최근 산업현장에서의 동향을 파악토록 유도한다. 실기검정에서는 단순 필답형이 아닌, 실제 코딩를 수행하고 소프트웨어 테스팅을 수행하는 수준의 실기검정을 시행함으로써 변별력을 높이고 산업 현장에서 요구하는 실무 능력의 보유 여부를 평가하도록 한다.

5) 재검정 제도

기존 국가기술자격에서의 단점으로 거론되었던 부분인, 1회 취득으로 영구적인 자격을 취득하는 문제를 해결하기 위하여, 3년 주기의 재검정 제도를 실시하도록 설계하였다. 현재 시행되는 국가기술자격은 일회의 자격 검정 통과로 영구적인 자격을 취득하기 때문에, 자격 취득자가 스스로 지속적인 자기개발을 하지 않으면, 같은 자격을 가진 인력임에도 불구하고 기술적으로 심각한 격차를 유발하는 문제가 있다. 해외 사례로 SGS의 〈ISO 26262 자동차 기능안전훈련〉 의 자격은 매 3년마다 재검정을 통하여 자격을 갱신하는 형태로 운영되고 있다.

6) 업무독점형 형태의 자격

현존하는 소프트웨어 관련 국가기술자격은 능력인정형 자격이 대다수로, 상대적으로 특별한 우대정책을 실시하기에 어려움이 있다. 현재 시행하는 소프트웨어 관련 국가기술자격의 특성상, 국민의 생명과 건강, 안전에 직결되는 의사나 전기기사, 소방설비기사 등의 자격과는 다른 성향을 띄기 때문으로 판단된다. 하지만 소프트웨어 안전의 경우, 국민의 생명과 건강, 안전에 직결되는 분야라고 할 수 있으며, 소프트웨어 안전 전문가는 공공기관이나 국

가 인프라 등 국민안전에 직결된 분야에서 고정적인 수요가 있을 것으로 판단됨으로 특정 부분에 있어서는 업무독점형 자격으로 인정하는 방안을 고려하는 것이 필요할 것이다.

4. 소프트웨어 안전 전문가 자격제도의 정착을 위한 교육 모델

소프트웨어 안전 전문가 자격제도의 정착을 위해서는, 소프트웨어 안전에 대한 인식의 제고가 우선적으로 필요하다. 이는 해당 기술에 대한 사회적 요구 및 수요 등의 기반이 마련되어야, 이를 위한 소프트웨어 안전 자격제도가 효율적으로 정착할 수 있기 때문이다. 하지만 우리 사회는 아직까지 소프트웨어 안전에 대한 인식 및 중요성에 대한 공감대 형성이 부족한 상황이며, 심지어 소프트웨어 안전의 개념조차도 명확히 정립되어 있지 않은 상태이다.

1) 학교 등 교육기관과 자격제도와의 직접적 연계

이러한 실태를 개선하기 위하여, 학교 등의 교육기관과의 연계 및 역할분담을 고려하였다. 대부분의 대학의 컴퓨터공학과 등의 소프트웨어 관련학과에서는 소프트웨어 안전 관련 과목을 개설하지 않고 있어, 소프트웨어 안전에 관한 교육 및 인식의 제고는 미비한 실정이다. 물론, 소프트웨어 공학 과목을 소프트웨어 안전의 일부로 볼 수 있겠으나, 소프트웨어 안전에 대한 내용을 거의 다루지 않거나, 교육 내용 또한 소프트웨어 안전과 관련된 내용을 위주로 진행하지 않기 때문이다. 이처럼 소프트웨어 안전 과목의 신설 등을 추진함과 더불어, 해당 과목을 이수한 사람에게 검정의 일부 면제 혜택이나 과정평가에서 해당 이수과정 면제 등의 혜택을 부여함으로써 대학교육과의 연계를 유도하는 것이 필요할 것으로 판단된다. 이러한 방안은 기존 국가기술자격에서 활용하던, 학력 취득 시 응시자격을 부여하는 우대정책에 비하면 보다 연계성이 높은 방법이라 할 수 있으며, 이를 통하여 소프트웨어 안전에 대한 사회적 인식의 향상 및 대학의 소프트웨어 안전 관련 과목 신설을 유도할 수 있는 요인이 될 것이다.

또한 대학에서 개설하는 과목과의 연계를 높이기 위하여 소프트웨어 안전 자격에서 쓰이는 국제 안전 표준 및 안전을 위한 소프트웨어 코딩에 대한 가이드라인이나 시험 출제 기준, 기출문제 등을 교수자에게 배포함으로써, 교육과정 구성에 활용하도록 도울 수도 있을 것이며, 직접적으로 표준 교재나 교안을 작성하여 배포하는 방법을 통해서, 새로운 과목 신설의 부담을 경감하여 줌으로써, 보다 많은 소프트웨어 안전 관련 과목의 개설을 유인할 수 잇을 것으로 기대된다.

이러한 정책은 비단 대학뿐이 아니라 IT 관련 특성화 고교, 전문학원에서도 충분히 적용할 수 있으며 관련업계 재직자 대상으로 소프트웨어 안전 코스를 개설하거나 기존의 코스를 연계한다면 산업현장에서의 활용 또한 기대할 수 있다.

2) 소프트웨어 안전 의식 제고

위에서 제시한 내용처럼 과목이수를 통한 면제혜택 등의 직접적인 우대 이외에도, 사회적으로 소프트웨어 안전 전문가 자격제도의 필요성을 인식하도록 돕고, 접근성을 향상시켜 관련 분야로의 진입장벽을 낮추는 형태의 연계방법의 시행도 고려할 수 있다.

이미 언급한 바와 같이 대부분의 국제 안전 표준 및 코딩 가이드라인은 영문으로 구성되고, 표준문서를 구입해야 하는 등 일반인에 대한 접근성이 좋지 않은 문제점이 있다. 이처럼 낮은 접근성을 극복하기 위하여 일본 등에서 시행하고 있는 방식과 유사하게, 안전 관련 국제 표준의 해설서 및 코딩 가이드라인을 작성하여 제공함으로써 소프트웨어 안전 관련 표준 및 코딩 가이드라인에 대한 학습을 간접적으로 도울 수 있을 것이며, 이는 자격제도의 접근성 향상에도 도움이 되어 소프트웨어 안전 전문가 자격의 응시인원을 증대하는 효과를 기대할 수 있다.

그 외에도 소프트웨어 안전 업계 동향, 발전방향, 중요성 및 유관 산업의 현황 등에 대한 홍보 등을 활발히 수행하여 소프트웨어 안전 관련 전반에 대한 사회 전반의 인식을 고취시킴으로써, 소프트웨어 안전 전문가 자격제도의 정착을 돕는 방안들을 병행 추진하는 것이 좋을 것으로 판단된다.

5. 소프트웨어 안전 전문가 자격제도의 효과적인 유지 방안

자격의 가치와 취득자의 기술적인 품질을 유지하기 위한 방법은 대표적으로 우대정책과 자격 유효기간 도입, 자격의 희소성 확보 등의 방법이 있으며, 이에 대한 구체적인 내용을 아래에 제시한다.[80]

1) 우대정책

먼저 우대정책은 자격 취득자의 입장에서 자격을 보유함으로써 얻는 이점을 말한다. 기존의 IT 및 소프트웨어 관련 국가기술자격은 능력인정형 자격이 대부분으로, 취업 시 가산점을 얻기 위하여 취득하는 일이 많다. 실제 산업현장에서도 자격취득자에게 직접적인 우대가 있기 보다는, 회사 입장에서 관련자격 취득자를 보유하는 편이 대기업 및 협력사나 국가 프로젝트 수주에 유리하기 때문에 선호하는 수준인 것으로 판단된다. 이러한 우대정책의 한계는 국가기술자격의 선호 및 가치를 높이지 못하는 원인이 된다.

이러한 이유로, 소프트웨어 안전 관련 자격증 등 소프트웨어 관련 전문가를 위한 국가기술자격은 업무독점형 자격의 성격을 일정부분 가지도록 설계하는 것이 필요할 것으로 판단된다. 소프트웨어 중심 사회에서의 소프트웨어 안전 인력은 국가기관이나 공공기관, 국가인프라 관리부서 등, 국민안전이 보장되어야 하는 곳에는 반드시 필요한 인력이다. 이를 감안하여 소프트웨어 안전 부문자격 소지자의 경우에 건설 분야, 기계 분야, 산업 분야의 건설안전기사, 기계안전기술사, 산업안전기사 등 안전관련 국가 자격 등과 같이, 소프트웨어 안전기사 자격 역시 국가 기반 시설 소프트웨어 안전 점검 등에 자격자 활용을 의무화 하는 등의 방안으로 소프트웨어 안전 관련 국가 자격의 수요 창출 방안[81]을 고려하는 것이 필요하다. 또한 각종 소프트웨어 안전표준 인증기관이나 안전표준 준수를 필요로 하는 산업에 자격취득자를 의무적으로 고용하도록 법제를 정비함으로써 자격의 취득가치를 높일 수 있을 것이다.

---

80) 장진현 (2016), ICT 관점에서 바라본 국가기술자격제도 개선, 한국인터넷방송통신TV학회 논문지, Vol.16 No.2, 189-199p, 관련내용을 기반으로 방안을 도출함.

81) 박태형 외, SW 안전체계 확보와 중점 추진 과제, SPRi Issue Report (2015)

2) 사후관리

현재 시행되는 대부분의 국가기술자격은 1회 취득으로 영구적인 자격을 취득하는 형태이다. 이러한 체계는 매우 빠른 속도로 발전하는 현대의 IT 기술에는 적합하지 않은 방식으로, 자격취득자가 스스로 지속적인 자기개발을 하지 않는 이상, 자격 취득 시기에 따라 자격 보유자 간의 관련 역량의 심각한 격차를 유발하게 된다는 단점이 있다. 이러한 자격취득자 개개인의 역량차이는 결국 자격의 가치를 신뢰할 수 없게 되는 문제를 야기하게 된다는 점을 고려하여, 3년 정도의 자격의 유효 기한을 설정하는 것이 필요하며, 보수 교육 및 재인증을 통하여 자격을 갱신하는 체계의 구축이 필요하다.

3) 자격의 희소성 확보

현존하는 IT 관련 국가기술자격은 자격보유인원에 제한을 두고 있지 않다. 정보처리기사만 하더라도 2015년 한해 자격취득자가 2만2천여명이 될 정도로 상당히 많은 인원이 자격을 취득하고 있으며, 50% 이상의 합격률을 보이고 있다. 이러한 지표는 해당 자격을 취득하는 것이 어렵지 않으며, 그로 인하여 희소가치가 높지 않음을 의미한다. 이처럼 정보처리기사 자격이 높은 합격률을 보이는 이유로는 문제은행식 출제로 인한 난이도 조정 실패 및 기출 문제에 집중한 자격시험 준비로 지원자의 보유 역량에 기반을 두지 않은 자격증 취득의 문제를 야기한다. 이러한 점을 고려하여 본 연구에서 제안하는 소프트웨어 안전 전문가 자격은 앞 절에서 제시한 소프트웨어 안전 협의체 등을 통하여, 국제 표준의 변화 및 필요 기술의 변화를 반영하여 시험 과목의 변경 및 추가 평가 문항 확보 등을 수행하여, 산업 현장에서 요구되는 기술변화에 능동적으로 대응함과 동시에, 기출 문제에 대한 학습만으로 자격을 취득하기 어렵게 하는 효과를 갖도록 하여, 최신 기술을 반영한 자격 평가가 이루어지도록 한다. 적절한 난이도의 설정과 함께 앞에서 언급한 자격의 유효 기간의 설정 및 절대평가 방식이 아닌 상대평가 형식의 검정방식의 도입도 고려해볼 수 있을 것이다. 이러한 자격의 희소성 확보 및 우수한 사후 관리 제도에 따라 자격 보유자의 역량에 대한 신뢰가 확보되면, 자격자에 대한 보다 강력한 우대 정책의 시행이 가능하게 되고, 이러한 우대 정책의 시행이 다시 해당 자격에 대한 선호를 유발하는 선순환 구조를 구축함으로써, 소프트웨어 안전 전문가 자격제도의 안정적인 유지를 보장할 수 있을 것으로 판단된다.

제5장 결론 및 시사점

소프트웨어는 다양한 산업과 융합되어 가고 있으며, 최근 AI 및 IoT등과 같은 새로운 기술의 등장과 함께 급격한 발전을 이루며 그 복잡도 또한 크게 증가하고 있는 추세이다. 이러한 소프트웨어 기술은 사람들의 삶과 밀접하게 연계된 기기들에 적용되어 가는 추세가 지속되면서, 소프트웨어는 사람의 생활과 안전에 매우 밀접한 관계를 갖는 수준까지 이르게 되었다. 특히, 이러한 소프트웨어가 집적된 IT 기기 중 사람의 안전에 직접 연관된 기기의 경우, 이들의 오작동 등의 문제는 사람의 인명에까지 영향을 끼칠 수 있는 상황이 되므로, 소프트웨어의 안전에 대한 요구가 크게 증가하고 있다. 이러한 소프트웨어 안전 관련 기술 및 중요성에 인식의 초기 진입 단계인 한국의 실정과 달리, 이미 해외 주요 선진국에서는 표준 제정, 지원 체계 등 다양한 정책적, 기술적 분야에서 활발하게 진행되고 있으며, 주요한 고부가가치 산업 중 하나로 인식되어 육성되고 있는 실정이다.

한국의 경우, 소프트웨어 안전성에 관련된 제도적, 사회적, 산업적 기반이 매우 빈약하고 표준 제정 및 지원 체계 등 안전성 관련 활동 또한 매우 미미한 실정이다. 이에 대한 근본적인 이유 중 하나는 소프트웨어 안전에 대한 명확한 개념이 정립되지 못하였을 뿐만 아니라 이를 제도적으로 지원하고 활성화하기 위한 기반 체계가 미흡한 것 등을 꼽을 수 있을 것이다. 이러한 원인으로 소프트웨어 안전에 대한 사회적 인지도 또한 낮은 수준이고, 이러한 낮은 인지도에 병행하여 수준 높은 전문 인력 유입의 부재, 안전 무결성을 충족하는 소프트웨어 개발 기술의 미비와 같은 다양한 문제들이 존재한다. 이러한 여러 요인들로 인하여 국내의 소프트웨어 안전에 관련된 전반적인 사회적, 기술적 수준이 주요 선진국에 비해 크게 낮은 수준이고, 국내의 기업들이 관련 기술 및 서비스를 해외의 안전성 관련 컨설팅 업체 등에 의존하면서 국내 기술의 유출 및 관련 산업의 발전이 어려운 현실이다.

이러한 현실을 고려할 때, 국내 소프트웨어 안전 관련 인식 제고와 관련 산업의 활성화를 위해 국내 소프트웨어 안전 관련 제도적 기반을 구축하는 일이 시급하다고 판단되며, 무엇보다도 소프트웨어 안전 기술에 대한 역량과 지식을 갖춘 고급 인력에 대한 확보와 그를 위한 제도적인 장치의 정비가 우선적으로 요구된다고 판단된다. 이러한 면에서 국내에 아직까지 소프트웨어 안전 관련 검정 및 자격 제도가 존재하지 않는다는 점도 크게 우려할 상황이라 하겠다. 따라서 소프트웨어 안전을 경제적 논리로서의 접근이 아닌, 국민의 기본권 보장 차원에서 인식하고 이에 대한 지원이 필요하며, 이러한 인식을 강화하기 위해 소프트웨어 안전 적용을 강제할 법제도의 개선과 그에 따른 부수적인 정책방안들이 필요하다. 이

러한 방안 중의 한 가지로서 소프트웨어 안전 전문가 자격제도 신설을 통하여 소프트웨어 안전 분야에 대한 인식과 기술력을 진일보시킬 수 있을 것으로 판단된다. 이러한 소프트웨어 안전 전문가 자격제도의 도입을 기반으로 소프트웨어 안전 산업이 성숙, 발전하게 되면 소프트웨어 안전 방법론, 기법, 기술, 검증 등의 다양한 기술 수출로 이어질 수 있어, 관련 산업의 발전을 통한 경제성 또한 함께 성취가 가능할 것으로 기대된다.

그러나 국내에서 수행되고 있는 소프트웨어 관련 자격제도는 소프트웨어 공학, 특히 테스팅 및 보안과 같은 과목을 자격 역량으로서 평가하고 있으나, 소프트웨어의 안전을 위한 표준, 가이드라인, 기술적 요구사항 등에 부합하지 않으며, 일부의 평가를 수행함으로써 지엽적인 소프트웨어 안전에 대한 기초적 지식의 평가 수준에 이르고 있다. 이러한 점을 고려하여 본 연구에서는 국내 소프트웨어 안전에 대한 전문가 수준의 인력 확보를 통한 산업 기반 강화의 선순환 체계를 구축하기 위해, 국제 안전 관련 표준에 부합하는 소프트웨어 안전 전문가 자격제도를 설계하였다. 이러한 자격 제도의 설계를 위하여 각 산업별 안전 관련 국제 표준에 대한 요구사항과 필요 역량을 분석하였으며, 이를 기반으로 소프트웨어 안전 전문 개발자, 설계자, 테스터 및 소프트웨어 안전 관리자의 4종류의 자격을 가지는 자격제도를 제안하였으며, 국제 안전 표준에 부합하는 소프트웨어 안전 전문가 자격제도의 상세 수행 모델을 설계하였다. 이와 더불어, 제시한 자격 모델을 활성화하고 체계적인 유지를 위한, 교육 및 기술적 체계를 제안하였으며, 마지막으로 산업계/학계/정부부처 간의 유기적인 지원/보완 체계를 구축하기 위하여 소프트웨어 안전 관련 협의체를 구성함으로써, 지속적인 피드백을 통한 자격 제도의 효과적인 유지 및 개선 방안을 제시하였다.

본 연구는 국제 표준에 부합하는 소프트웨어 안전 전문가 자격 모델과 이에 대한 연계 방안 등 다양한 측면에서 소프트웨어 안전 전문가 확보와 활성화를 위한 다각적인 방안을 함께 제시하였다. 그러나 최근 소프트웨어의 도입이 매우 광범위한 범위에서 융합되고 있으며, 국제 표준 또한 다양한 산업별로 제정되어 있다. 따라서 차후, 소프트웨어 안전 산업 기반이 마련되고 성숙됨에 따라, 소프트웨어 전문가에 대한 수요 및 공급 예측, 각 산업별로 존재하는 국제 표준에 대한 자격제도에 대한 심도 있는 조사, 분석이 꾸준히 필요할 것으로 판단되며, 역량 평가 및 유지보수에 대한 교육 모델 또한 더욱 구체성을 갖는 수준으로 연구되어야할 것으로 판단된다. 이와 더불어 본 연구에서 제시한 소프트웨어 안전 전문가 국가자격제도 시행을 위한 세부 설계 등에 관한 후속 연구가 필요할 것으로 판단된다.

참 고 문 헌

국내 문헌

DNV·GL, https://www.dnvgl.co.kr/services/page-3324 (2016.12.18.)

NCS 국가직무능력표준 홈페이지. NCS분류 https://www.ncs.go.kr/ncs/page.do?sk=P1A1_PG01_002 편집

SGS, http://www.sgsgroup.kr/ko-KR/Training-Services/Industry-Based-Training/Automotive/Automotive-Functional-Safety-Training/ISO-26262-Automotive-Functional-Safety-Training.aspx (2016.12.18.)

TTA 아카데미, https://edu.tta.or.kr, (2016.12.18.)

강순희 (2003), 자격제도의 비전과 발전방안, 한국노동연구원

고용노동부, 한국산업인력공단 (2016), 2016 국가기술자격통계연보

관계부처합동 (2012), 제3차 국가기술자격제도 발전기본계획

국무조정실 보도자료, "'국가 사이버안보 태세 역량'대폭 강화한다.", 박영철 외 (2015), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원, 17쪽에서 재인용

김덕기, 박동열 (2006), 국가직무능력표준에 의한 자격 출제기준 시범개발, 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 44쪽에서 재인용

김석원 외 (2015), 소프트웨어 안전(Safety) 산업 동향 조사, 소프트웨어정책연구소

김성수, 김용수 (2014), 기능 안전을 위한 IEC 61508의 안전수명주기에 관한 연구, 신뢰성 응용 연구, 제 14권, 제 1호, pp. 81-91.

김정환, 김범수, 양재모, 장창봉, 김민섭, 정상용, 고재욱 (2011), SIL (Safety Integrity Level) 선택에 의한 리스크 감소에 관한 연구, 한국가스학회지, 제 15권, 제 5호, pp. 57-62.

김현수 외 (2007), 국가자격시험 관리체계 개선을 위한 법제도 개선방안, 한국직업능력개발원

김현수 외 (2007), 자격의 활용성 강화를 위한 법제도 개선방안, 한국직업능력개발원

김희성, 항공용 소프트웨어 인증을 위한 DO-178C 적용 절차 개관, SBAS 정책 기술 동향, SBAS 사업단.

나승일 외 (2011), 국가기술자격 출제기준 개선방안 연구, 한국산업인력공단

나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 고용노동부

도요타 자동차 급발진 사고 사례, http://www.etnews.com/20140320000188

문창진 (2014) 생명과 직결되는 자동차 임베디드 SW 테스트 기법과 사고방지를 위한 국제 표준 (ISO 26262) 적용 사례, 윈드리버 코리아.

민간자격정보서비스 - 민간자격현황, https://www.pqi.or.kr/inf/qul/infQulSitRegView.do (2016.12.18)

박무혁 (2007), 항공용 S/W 개발 및 인증 기술 동향, 항공우주산업기술 동향 5권 1호 pp.15-24.

박영철 외 (2015), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원

박태형 외 (2015), SW안전 체계 확보와 중점 추진과제, SPRI Issue Report, 소프트웨어정책연구소

박태형 외 (2016), 소프트웨어 안전성 확보 체계에 대한 연구, 소프트웨어정책연구소

우경일 (2014), ISO 26262에 대한 국제 표준 및 기술 동향, 2014 자동차 SW 개발자 컨퍼런스 발표자료.

위키백과 (2012), DO-178C, https://en.wikipedia.org/wiki/DO-178C

위키백과 (2015), AUTOSAR, https://ko.wikipedia.org/wiki/AUTOSAR.

위키백과 (2015), EN_50128, https://de.wikipedia.org/wiki/EN_50128

이근상 (2015), IoT 산업의 키, 소프트웨어 안전, JBTP 이슈앤테크, vol 49.

이동임 외 (2006), 국가기술자격의 효용성 평가체계 구축, 한국직업능력개발원, 한국산업인력공단, , 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용
이동임 외 (2008), 자격제도 운영평가체제 구축 연구, 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용
이동임 외 (2009), 국가기술자격 효용성 평가, 한국직업능력개발원, 한국산업인력공단, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용
이익성 (2010), 리스크 분석에 의한 철도물류 운영기관의 안전경영시스템에 관한 연구, 신뢰성응용연구, 제 10권, 제 1호, pp. 73-91.
임태수, 김동수 (2008), 소프트웨어 관련 국가기술자격제도 개선방안에 대한 연구, 한국전자거래학회지 제13권 제1호, 55-69
장승연 (2015), 안전소프트웨어를 위한 소프트웨어 테스팅 관점에서의 차량기능안전 표준(ISO 26262), 적용방안 논의, 정보과학회지, 33(7).
장진현 (2016), ICT 관점에서 바라본 국가기술자격제도 개선, 한국인터넷방송통신TV학회 논문지, Vol.16 No.2, 189-199p
정은기, 권혁무, 이민구, 김동준, 홍성훈 (2013), 자동차 기능안전 ISO26262와 대응방안, Korean Soc Qual Manage, 41.
조병선, 조상섭 (2014), 소프트웨어의 산업의 특징 및 구조변화에 대한 분석, 전자통신동향분석 제 29권 제 2호, 한국전자통신연구원(ETRI)
조정윤 외 (1998), 21세기를 향한 국가기술자격제도의 발전 방안 연구, 한국직업능력개발원
조정윤 외 (1999), 국가기술자격 검정방법 개선에 관한 연구, 한국직업능력개발원
조정윤 외 (2001), 국가기술자격종목 정비 및 제도 개선, 한국직업능력개발원, 한국산업인력공단, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 45쪽에서 재인용
조정윤 외 (2003), 국가기술자격제도 관리·운영체제의 국가 및 민간의 역할 분담, 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 47쪽에서 재인용
주인중 외 (2008), 제2차 국가기술자격제도발전기본계획 수립을 위한 기획연구, 한국직업능력개발원, 나승일 외 (2012), 국가기술자격 운영실태 및 현황분석, 44쪽에서 재인용
중소기업청 (2012), 중소기업통합기술로드맵
채승엽, ISO 26262 해외 가이드라인 쉽게 이해하기, http://www.autoelectronics.co.kr/article/articleView.asp?idx=1416
큐넷 2017년 과정평가형 시행 적용 대상종목, http://www.q-net.or.kr/crf006.do?id=crf00626, (2016.12.18.)
큐넷 국가기술자격제도 응시자격 조건체계, http://www.q-net.or.kr/crf006.do?id=crf00613, (2016.12.18.)
큐넷 국가기술자격제도 응시자격별 안내, http://www.q-net.or.kr/crf006.do?id=crf00603, (2016.12.18.)
큐넷 임베디드기사, http://www.q-net.or.kr/crf005.do, (2016.12.18.)
큐넷 정보보안기사, http://www.q-net.or.kr/crf005.do, (2016.12.18.)
큐넷 정보처리기사, http://www.q-net.or.kr/crf005.do, (2016.12.18.)
한국정보통신공사협회, https://www.kica.or.kr/web_app/CA/engine_engineer01.jsp, (2016.12.18.)
한국정보화진흥원, http://auditor.nia.or.kr/ (2016.12.18.)

국외 문헌

Advancing safety in healthcare technology, http://www.aami.org/professionaldevelopment/content.aspx?itemnumber=1134&navItemNumber=577 (2016.12.18.)

AREMA, https://www.arema.org/publications/cs/index.aspx/, (2016.12.18.)

Engineering safety consultants, http://www.esc.uk.net/training/iec-61508-software-safety-training-course-outline (2016.12.18.)

EUROCONTROL , https://trainingzone.eurocontrol.int/ilp/pages/landingpage.jsf?faces-redirect=true (2016.12.18.)

HCRQ, http://www.hcrq.com/software-safety-course.html (2016.12.18.)

ISO, https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en (2016.12.18.)

TUV Rheinland, http://www.tuv.com/ko/korea/hot_topics_kr/functional_safety.jsp (2016.12.18.)

TUV SUD, http://www.tuv-sud.com/industry/automotive-transportation/automotive-solutions/quality-and-safety-services/automotive-functional-safety/iso-26262-functional-safety-certified-programme#tab_142710574658899454 1307 (2016.12.18.)

USCViterbi, http://viterbi.usc.edu/aviation/courses/sft.htm (2016.12.18.)

연구보고서 2016-021

SW 안전 전문가 자격제도 연구

2017년 05월 인쇄
2017년 04월 발행

발행처 정보통신산업진흥원 부설 소프트웨어정책연구소
경기도 성남시 분당구 대왕판교로712번길22 A동 4층
Homepage: www.spri.kr

ISBN : 978-89-6108-382-9

주 의

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

ISBN : 978-89-6108-382-9