연구보고서 2015-001

소프트웨어 안전(Safety) 산업 동향 조사

Software Safety Industry Trends Study

2015.08

수행기관 : 트라이즈컨설팅

SPRi 소프트웨어정책연구소

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

제 출 문

소프트웨어정책연구소장 귀하

본 보고서를 『**소프트웨어 안전(Safety) 산업 동향 조사**』의 결과보고서로 제출합니다.

2015년 08월

수 탁 기 관 : 트라이즈컨설팅

총 괄 책 임 자 : 김석원(소프트웨어정책연구소 실장)
정영철(트라이즈컨설팅 대표이사)

과제관리책임자 : 박태형(소프트웨어정책연구소 선임연구원)

참 여 연 구 원 : 김태호(소프트웨어정책연구소 선임연구원)
박강민(소프트웨어정책연구소 연구원)
송현이(트라이즈컨설팅 이사)
박재형(트라이즈컨설팅 이사)

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

소프트웨어 안전(Safety) 산업 동향 조사

2. 연구 배경 및 목적

본 연구의 주요 목적은 소프트웨어 안전(Safety)에 대한 개념 정립에 도움을 주고, 현재 초기 단계인 소프트웨어 안전 산업 활성화를 위하여, 1. 주요산업도메인별 해외 주요국의 소프트웨어 안전 활동 사례와 2. 해외 TIC 선진업체 및 TIC 시장 동향을 조사하고, 3. 다양하고 객관적인 국내 소프트웨어 안전 산업 관련 기초 자료를 제공하는 것이다.

3. 연구의 구성 및 범위

본 연구는 첫 번째, 주요 산업도메인별(자동차, 철도, 우주항공, 원자력) 소프트웨어 안전 표준과 해외 선진국(미국, 유럽 또는 영국/독일, 일본)의 소프트웨어 안전 관련 활동을 조사하고, 두 번째, 해외 주요 TIC(Testing, Inspection and Certification) 기업인 SGS, Bureau Veritas, Intertek, DEKRA, DNV GL의 서비스 활동을 조사하고, 해외 TIC 시장 동향을 조사하였으며, 세 번째, 국내 소프트웨어 안전 산업 현황을 조사한 다음, 네 번째, 국내 및 해외 사례의 비교 분석(GAP 분석)과 SWOT분석(강점/약점/기회/위협 분석)을 통해 국내 소프트웨어 안전 제고를 위한 개선 전략으로 구성되어 있다.

4. 연구 내용 및 결과

해외 산업도메인별 소프트웨어 안전 선진국의 활동 현황 조사 결과, 조사한 산업도메인에서는 최소 한 개 이상의 소프트웨어 안전 표준이 존재하였다. 다만, 대부분의 소프트웨어가 실제로는 전자전기 시스템 內에서 동작되는 관계로, 법/제도 및 정부의 안전 활동 측면에서 보면 소프트웨어 안전 표준이 별도로 구별되어 법/제도 조항이나 안전 활동 요구 사항으로 제시되어 있지 않고(Explicitly), 안전한 부품/시스템/제품을 만들기 위해 준수해야 할 법/제도 조항 內 따라야 하는 여러 표준 중의 하나로 규정화되어 있고(Implicitly), 정부 기관 및 인증기관 등을 통해 인증 또는 승인 등의 방식으로 적용되고 있었다. 자동차 경우는 특이하게, 국제 표준(ISO 26262)은 존재하나, 법/제도적으로

명문화되거나 정부차원에서 관리되지는 않는다. 다만, 사고 발생 시 제조물 책임법 하에 사고를 유발한 부품/시스템이 최신 기법을 사용해서 개발했다는 것을 제조사가 증명해야 하는데, 현재 소프트웨어 관련 여러 기법 중 안전 관련 최신 기법으로 ISO 26262가 인정받고 있어, 업체들이 자발적으로 이를 준수해야 하는 방식으로 되어 있었다. 이 때문에, 모든 자동차 관련 제조사가 일괄적으로 ISO 26262를 준수하기 보다는, 매출이 높거나 업계를 선도하는 기업에서부터 자발적으로 준수하고, 차츰 다른 기업으로 적용 범위가 확대되는 중이었다.

TIC시장은 앞으로 2014년부터 2020년까지 CAGR (Compound Annual Growth Rate, 연평균성장률) 5.8% 수준의 꾸준한 성장을 통해 약 504억 달러 정도의 시장 규모로 성장할 것으로 추정된다. TIC 시장의 선진기업들은 고객 제품 및 자산가치에 대한 검사, 테스팅, 인증 서비스를 제공하고 있으며, 국제 표준과 관련된 가이드 연구 및 배포, 국제 표준 기관 활동 등을 수행하고 있었다. 두드러진 특징으로, 대다수 글로벌 선진 기업들은 최근 몇 년간 기업의 인수합병을 계속 추진하면서 서비스 포트폴리오 확장과 지역적/국제적인 네트워크 강화에 노력하고 있었다.

국내 TIC 시장에서 제공하는 주요 서비스로는 소프트웨어 기능안전(Functional Safety) 서비스와 소프트웨어 신뢰성(Reliability) 서비스로 구분할 수 있으며, 구체적으로, 기능안전 서비스는 시스템 소프트웨어 메카니즘 설계, 시스템 소프트웨어 구현, Safety 검증/인증 등이 있으며, 신뢰성 서비스는 정적 테스트, 동적 테스트 등이 있다. 국내 시장의 경우, 상기 서비스를 한 가지이상 복합적으로 제공하는 기업이 상당수 있었다.

국내 소프트웨어 안전 현황에서 조사/분석된 문제점들은 소프트웨어 안전 관련 문화/사회/산업적인 기반 부족에 관한 것들이 대부분이었으며 이러한 문제점들은 상호 인과관계로 연결되어 있었다. 문화적인 측면에서는 체계적인 절차와 방식에 따라 소프트웨어를 개발하는 문화가 부족하고, 사회적인 측면에서는 소프트웨어 안전에 대한 개념 및 인식이 낮아 중요성을 인정받지 못하며, 산업적인 측면에서는 소프트웨어 안전 활동에 대한 충분한 기간 및 대가를 인정받지 못하고 있다고 분석되었다. 이를 해결하기 위한 방안도 문화/사회/산업적인 기반 구축에 관한 것들로서, 소프트웨어 안전 개념 및 가이드 정립, 관련 법/제도 제정 등을 통한 문화/사회적인 기반 마련과 소프트웨어 안전 관련 분리 발주 제도, 공공 Sector 주도로 사업 발주 시 소프트웨어 안전 요건 포함, 소프트웨어 안전 적정 대가 및 기간 인정 등의 산업적 기반의 방안들이 조사되었다.

국내 소프트웨어 안전 산업(안전, 품질, 신뢰성 포함)은 최근 5년간 CAGR 약 15%로 타 산업대비 높은 성장세를 기록하였으며, 시장 규모는 최소 약 2,600억 이상으로 추산

되었다.

벤치마킹 및 국내현황 조사 결과를 토대로 GAP 및 SWOT 분석을 실시하였고, 이를 통해 4대 개선 전략을 도출하여 아래와 같이 정리하였다.

1. 소프트웨어 안전 산업의 제도적 기반 구축

- 소프트웨어 안전 관련 최소한의 표준 준수 규정 제정
- 관리, 감독을 위한 기관 또는 단체 지정(단, 독립성, 무결성을 위한 관리, 감독, 인증기관 분리 필요)
- 다 부처 참여의 소프트웨어 안전 협의체 필요
- TIC 산업(소프트웨어 안전포함)을 표준 산업 군으로 분류
- 개발 초기 단계에서부터 안전 요건 정의 및 안전 활동 요건 의무화

2. 소프트웨어 안전 표준 및 가이드 제정

- 정부/연구단체/산업도메인 선도업체 주도의 소프트웨어 안전 표준 및 가이드 제작(표준 번역 및 해석, 상세 수행 가이드, 및 측정 가능한 수준의 명확한 소프트웨어 안전 개념 정립)
- 국제 표준 활동에 국내 안전 및 품질 단체 참여

3. 소프트웨어 안전 인적 기반 구축

- 초기 교육 과정부터 체계적인 소프트웨어 개발 교육 제공
- 개발자를 위한 업종/업무 사례 중심 교육 필요
- 기업에 대한 소프트웨어 안전 교육/연구 지원
- 소프트웨어 안전 분야를 정규 교육화하고 전문 양성기관 신설
- 인증 및 자격증 제도 도입(자격증/인증 제도는 소프트웨어 안전 인식 및 신뢰성 제고를 위한 최소한의 규정으로 필요하며 민간 주도 권고)

4. 소프트웨어 안전 業 환경 개선

- 적정 사업대가 책정(소프트웨어 안전 및 신뢰성에 소요되는 적정 MM 및 테스트 기간 포함)
- 차별화된 소프트웨어 안전 인력 단가 체계 적용
- 공공기관 과제 발주 시, 소프트웨어 안전 요건 포함

- 국내 기업의 중국, 동남아 등지의 해외시장 진출 지원
- 사업 참여 업체와 인력의 최소한의 자격 요건(CMMI, TMMI, SP, SPICE 등) 구비 필요

SUMMARY

Last 20 years, as rapid development of the IT technology and industry has transformed simple devices into IT devices, the importance of software which control or operate IT devices has increased. The growing number of IT devices used in everyday lives makes greater influence to everyone's life. In particular, because the impact of failure of safety critical IT devices becomes far greater to even risk lives of the people, the concept and the methods of the software safety is being developed and researched. The software safety is being discussed very actively and recognized as one the important industries in overseas, especially in developed countries, but in Korea it is in the early stages, it has been recognized as one of the leading industries.

The purpose of this survey is to assist to formulate the concept of software safety and to establish laws and policies by providing basic understanding of software safety industry and market.

Two Main studies were conducted: Benchmarking and Trends Survey on Software Safety Industry in Korea. The Benchmarking was mainly focus on major safety related industrial domains like Automobile, Railway, Aeronautics, and Nuclear to give insights on how other advanced countries like US, Germany, UK, etc. are handling software safety in terms of policies, government authorities, regulations, and etc. TIC(Testing, Inspection and Certification) Industry was also studied by providing trends of world market and major global TIC companies. The trends survey of software safety industry in Korea was performed by surveying and analyzing on policies, industry environment, problems, and suggestions on Governing Sector(Academic and public institutions), TIC Sector(Testing, Inspection and Certification Companies), and End-User Sector(Companies who use TIC services) Based on the results, 4 strategic directions were derived to promote software safety in Korea by GAP and SWOT analysis.

4 strategic directions derived from GAP and SWOT analysis for Software Safety were as follows:

1. Establish Institutional Foundation
2. Set up Standards and Guidelines
3. Build Human Resources Foundation

4. Improve Business Environment

CONTENTS

제1장 서 론

제1절 개요

1. 배경 및 필요성

최근 국내외에서 발생한 크고 작은 안전사고를 계기로 안전 관련 정책 추진체계, 점검체계, 사고예방 및 대응체계 등에 대한 관심이 증가하고 있으며, 특히, 소프트웨어 중심사회가 정착되고 고도화될수록 소프트웨어의 복잡성과 소프트웨어에 대한 의존성이 확대되고 있다. 이러한 복잡성과 의존성이 증가됨에도 불구하고, 국내 소프트웨어 안전에 대한 개념은 현재 미 정립 상태이며, 소프트웨어 안전 정책 및 안전 방안(소프트웨어 사고발생시 사고 회피 방안) 또한 걸음마 상태이다. 이로 인하여, 소프트웨어 사고 발생 가능성 및 사고발생시 대규모 피해를 초래할 가능성이 증가하고 있다. 이에, 안전에 대한 국민의 요구에 부응하고, 소프트웨어 문제로 발생하는 사고를 예방·대응함으로써 소프트웨어 중심사회의 안전성 확보와 소프트웨어 분야에 대한 국민의 안전신뢰성 제고를 위한 기초 자료를 제공하기 위하여 본 연구를 수행하게 되었다.

2. 목적

본 연구의 주요 목적은 소프트웨어 안전(Safety)에 대한 개념 정립에 도움을 주고, 현재 초기 단계인 소프트웨어 안전을 위한 정책 방안을 수립하기 위한 다양하고 객관적인 소프트웨어 안전 관련 기초 데이터를 제공하는 것이다. 구체적으로 서술하자면, 첫 번째, 주요 산업도메인별 소프트웨어 안전 표준과 해외 선진국 소프트웨어 안전 관련 활동을 분석하고, 두 번째, 선진 TIC(Testing, Inspection and Certification) 기업과 해외 TIC 시장을 분석하였으며, 세 번째, 국내 소프트웨어 안전 산업 현황을 분석하고, 네 번째, 국내 및 해외 사례의 비교 분석(GAP 분석)과 국내 기업의 강점/약점/기회/위협에 대한 분석(SWOT 분석)을 통해 국내 소프트웨어 안전 제고를 위한 개선 전략을 도출하기 위함이다.

제2절 연구방법 및 범위

1. 국내 소프트웨어 안전 현황 연구 방법

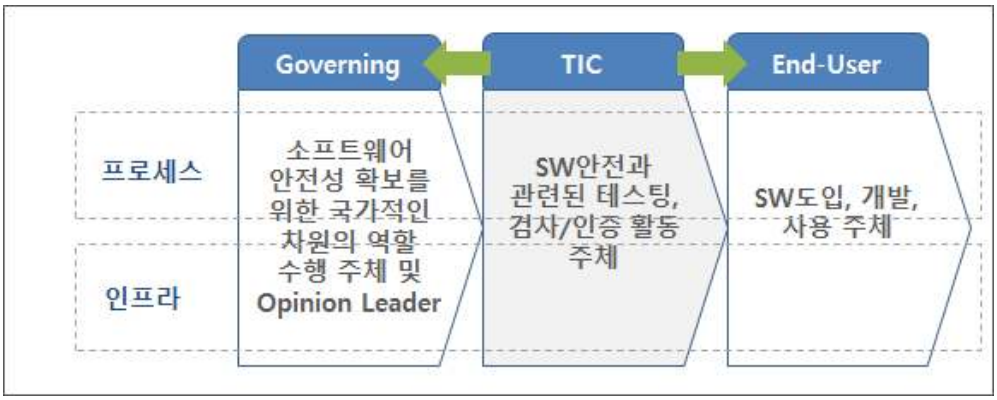
1) 범위 및 대상

앞에서 언급되었듯이, 현재 국내 소프트웨어 안전에 대한 인식 및 개념 등이 미 정립되어 있는 상황이므로 조사 범위 및 대상이 명확하지 않은 상황이다. 따라서 본 현황조사에서는 향후 소프트웨어 안전 인식 및 개념 정립에 도움이 될 수 있도록, 국내 소프트웨어 안전 조사 범위 및 대상을 포괄적으로 정의하여 조사하였다. 소프트웨어 안전 서비스를 공급하는 기업뿐만 아니라 해당 서비스를 사용하는 기업을 함께 조사하고, 한편으로 본 산업을 선도하는 학계/공공기관까지 조사함으로써, 1. 소프트웨어 안전 산업 현황 조사 결과가 특정 조사 대상에 의하여 편향되지 않고, 2. 각 조사 대상의 현황을 상세히 파악하면서, 3. 거시적인 측면에서의 현황, 문제점 및 향후 개선 방안을 도출할 수 있도록 하였다. [그림 1-1]에서 보듯이, 소프트웨어 안전 분야 사업을 수행하고 있는 기업(TIC Sector)을 주요 조사대상으로 하고, 소프트웨어 안전 관련 학계 및 공공기관(Governing Sector)과 실제 소프트웨어를 도입, 개발, 사용하는 기업(End-User Sector)을 조사대상으로 선정하였다. 해외의 경우 소프트웨어 안전은 별도로 구별되어 있지 않고, TIC(Testing, Inspection and Certification) 산업에 포함되어 있으며, 글로벌 시장 조사 기관의 시장 조사 또한 TIC Sector로 구분되어 있었다. 또한, 소프트웨어 안전의 개념이 Safety와 Reliability 측면에서 정의 되고 언급되는 경우가 많은 관계로, 본 연구도 소프트웨어 안전 산업을 TIC 산업으로 정의하여 조사를 수행하였다. 소프트웨어 도입, 개발, 사용기업의 경우, 2014년 2월 안전행정부에서 발간된 ‘ 2014년 국가기반체계 보호지침’ 에서 제시된 주요 국가기반시설 관리 대상을 근간으로 하였고, 추가로 민간 부문의 주요 산업에서 소프트웨어 안전이 중요한 산업을 추출하여 각 산업별 상세 조사 대상을 선정하였다. (정보보호 차원에서 선정된 조사 대상 기업 목록은 제공하지 않는다. <표 1-1> 참조).

<표 1-1> 소프트웨어 도입, 개발, 사용 기업(End-User) 관련 주요 산업

구분	주요 산업 도메인	상세 산업
주요 국가기반 시설	에너지	전기
		석유
		가스
	정보통신	
	교통수송	철도
		항공
		항만
		도로
		지하철
	금융	
	보건의료	의료서비스
		혈액
	원자력	
	환경	
	식용수	
민간 부문 주요 산업	식품안전	
	석유화학	
	방위산업(무기체계)	
	1차금속제조	
	기계장치제조	엔진
		터빈
	전기 장비, 기구 및 구성요소	조선
		자동차
		항공우주제품
		철도차량
		전기장비
	민간 금융	은행
		증권
		카드

[그림 1-1] 국내 소프트웨어 안전 현황 조사 범위



2) 조사 항목

앞에서 정의된 조사 대상에 대하여, 소프트웨어 안전 프로세스 및 인프라는 공통적으로 조사하였고([그림 1-1] 참조), 각 조사 대상별 특성을 고려하여, 추가적인 조사 항목을 포함하여 조사를 실시하였다. 학계 및 공공기관(Governing Sector)의 경우, 소프트웨어 안전에 대한 개념, 정책 방향 등의 항목을 조사하였으며, 소프트웨어 안전 분야 사업 기업(TIC Sector)의 경우, 기업의 일반 및 재무 현황과 정책에 대한 요구사항, 소프트웨어 도입/개발/사용 기업(End-User Sector)에서는 정책요구 사항 등을 추가하여 조사하였다. (<표 1-2> 참조).

<표 1-2> 조사 대상별 조사 항목

조사 대상	주요 조사 항목
학계 및 공공기관 (Governing Sector)	• 소프트웨어 안전 개념 • 소프트웨어 산업 현황 및 문제점 • 소프트웨어 안전 산업 현황 및 문제점 • 해결방안: 법/제도/인증, 표준/절차/가이드, 조직/기관, 교육, 業 환경개선, 프로세스
소프트웨어 안전 분야 사업 기업 (TIC Sector)	• 기업일반현황 • 프로세스 측면: 예방, 탐지, 대응, 사후 활동 • 인프라 측면: 표준/매뉴얼, 인력/조직, 시스템 • 지원 요청 사항
소프트웨어 도입, 개발, 사용 기업 (End-User Sector)	• 프로세스 측면 활동: 예방, 탐지, 대응, 사후 활동 • 인프라 측면: 표준/매뉴얼, 인력/조직, 시스템 • 지원 요청 사항

3) 조사 방법 및 경과

상기 도출된 조사대상 및 조사 항목에 따라 특화된 상세 설문지를 작성하였고, 학계 및 주요기관에서는 총 5곳, 소프트웨어 안전 분야 사업 기업 총 18곳, 소프트웨어 도입, 개발, 사용 기업 총 5곳 기업을 대상으로 방문 인터뷰 또는 설문 조사를 실시하였다. (<표 1-3> 참조). 소프트웨어 안전 분야 사업 기업 및 소프트웨어 도입/개발/사용 기업은 기업 정보가 누출되는 우려를 제기하여 본 연구에서는 기업의 실명 및 1차 Raw Data를 제공하지 않고, 2차 또는 3차로 가공된 결과를 제공한다.

<표 1-3> 상세 조사 대상 및 수행 결과

구분	조사 대상	수행 결과
학계 및 공공기관 (Governing Sector)	• 고려대, 숭실대, 상명대: 3개 대학 • 공공기관(한국정보통신기술협회, 한국산업기술시험원): 2개 기관 • 총 5개	• **총 5개 모두 방문 인터뷰 수행**
소프트웨어 안전 분야 사업 기업 (TIC Sector)	• TIC 기업: 26개 기업 • 소프트웨어 안전 전문 기업: 4개 기업	• TIC 기업: 7곳 설문, 7곳 방문 인터뷰 수행 • 소프트웨어 안전 전문 기업: 4곳 방문 인터뷰 수행 • **총 18개 설문 및 방문 인터뷰 수행** • **총 12개 기업 매출, 영업 이익, 성장률 등 재무 조사 수행**
소프트웨어 도입, 개발, 사용 기업 (End-User Sector)	• 주요 산업 도메인별 주요 대상 기업 (<표 2-1> 참조).	• 방위산업 1개 기업 • 전기/기구 제조 1개 기업 • 정보통신 2개 기업 • 금융 1개 기업 • **총 5개 모두 방문 인터뷰 수행**

2. 해외 선진사례 조사 방법

1) 범위 및 대상

해외 선진사례 조사는 1. 주요 산업도메인별 소프트웨어 안전 활동 조사와, 2. 해외 TIC 선진사 및 글로벌 TIC 시장 현황에 대한 문헌 조사를 수행하였다.

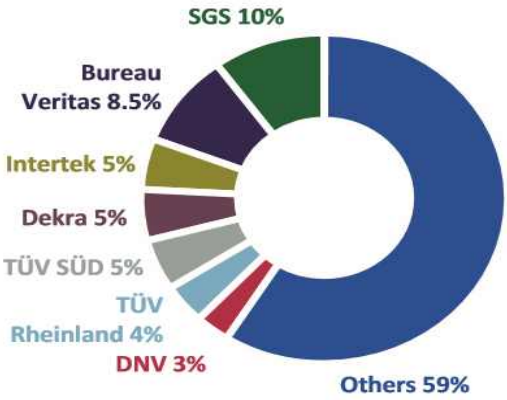
주요 산업 도메인별 소프트웨어 안전 활동 조사의 경우, 개인의 안전과 직접적인 관련이 많거나 사고발생시 국가적인 재난 사태가 발생하거나 매우 높은 수준의 시스템 및 소프트웨어 신뢰도가 요구되는 자동차, 철도, 우주항공, 원자력의 4개 산업도메인을 선정하였고, 해당 도메인별 선진국의 소프트웨어 안전 정책 및 적용 사례를 조사하였는데, 산업도메인별 표준 적용방식이 크게 상이하여, 주로 미국, 유럽 또는 유럽의 선진국인 영국/독일과 필요할 경우 일본 사례를 조사하는 방식으로 도메인별로 조사가 필요한 국가를 유연하게 선정하여 수행하였다.

<표 1-4> 산업도메인별 조사 범위 및 대상

산업도메인	미국	유럽 (영국 / 독일)	일본
자동차	1. 도메인별 표준 및 주요 구성 요소 2. 주요 국가 별 표준 도입 현황 (법/규정, 기관 등) 3. 기타 주요사항		
철도			
우주항공			
원자력			

해외 TIC 선진사의 경우, 글로벌 선진 TIC(Testing, Inspection and Certification) 시장의 Key Players 중, 2014년도 매출 상위 5개 기업을 선정하여 TIC 시장 현황을 조사하였다. 매출 상위 5개 기업을 대상으로 하는 이유는, 상위 5개 기업이 TIC 시장 매출의 40%이상을 점유하고 있기 때문에 주요 Players들의 활동을 통하여 전체 TIC 시장을 가늠할 수 있기 때문이다. 2012년의 자료를 참조해 보면 ([그림 1-2]), 주요 Key Player들의 TIC 시장 매출 비중은 40% 이상을 차지하고 있으며, 나머지 기업에서 59% 정도를 차지하고 있었다. 이들 중, SGS와 Bureau Veritas가 압도적인 리더로 전체 시장의 18.5%를 점유하고 있으며, 2011년부터 Intertek이 3위로 부상하여 순위를 유지하고 있다. 그 밖의 기업들은 DEKRA, TUV, DNV를 제외하고 나머지 기업이 60% 정도의 시장을 차지하고 있는 것으로 보고되었다.

[그림 1-2] 2012년 TIC 시장 점유율



자료: Mergers and Alliance. Global Testing, Inspection and Certification M&A update. 2012 [22)]

이를 토대로 5개 기업 선정을 위한 주요 기업 별 2014년도 매출을 조사하였다. 주요 Key Players 샘플링 대상으로는 Marketsandmarkets에서 제시하고 있는 TIC 시장의 Company Profile 대상 11개 기업과 그 외 4개 기업을 추가하여 각 기업의 매출을 조사하였으며, 전체 대상 기업은 아래와 같이 구분된다.

- Marketsandmarkets에서 제시한 11개 Key Players:

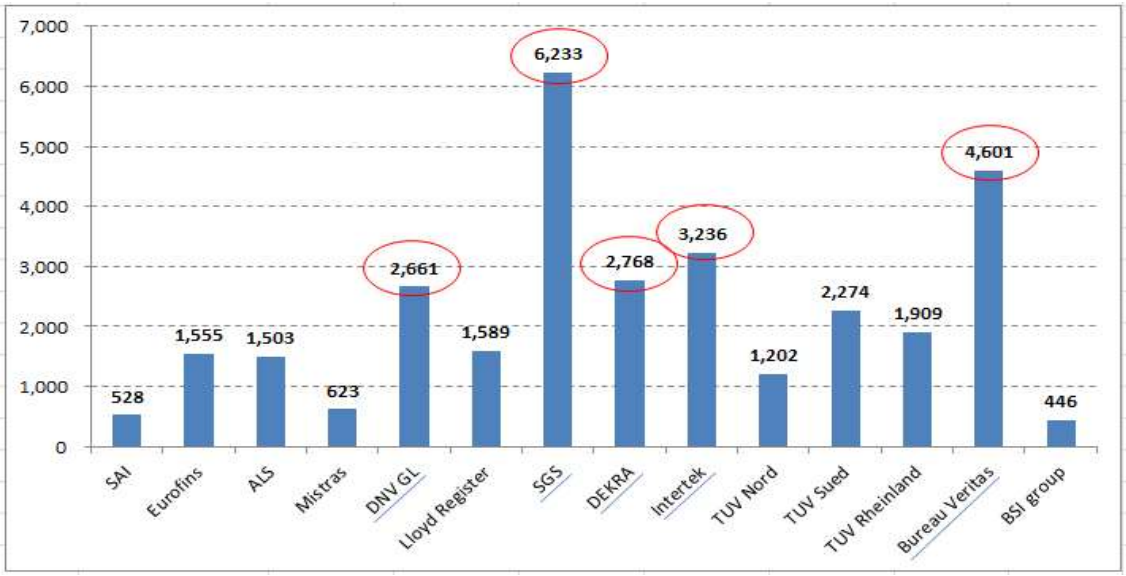
ALS Global (Australia), BSI Group (U.K.), Bureau Veritas SA (France), DEKRA Certification GmbH (Germany), Intertek Group PLC (U.K.), SAI Global (Australia), SGS Group (Switzerland), TÜV NORD Group (Germany), TÜV Rheinland Group(Germany), TÜV SUD Group (Germany), and UL LLC (U.S.)

- 그 외 TIC 주요 기업

Eurofins (Luxembourg), Mistras (U.S.), Lloyd Register(UK), DNV GL(Norway)

각 기업의 매출 규모는 2014년 Annual Report에서 추출하였으며, 각 기업의 화폐단위는 US달러로 통일하였다. 단, UL LLC의 경우, 2014년 Annual Report에 매출규모를 공표하지 않았기 때문에 UL은 매출현황에서 제외되었다. 2014년 매출 현황에서 보면, SGS가 62억 달러로 TIC 시장 1위를 차지하고, Bureau Veritas, Intertek 등이 그 뒤를 잇고 있었다. 조사된 매출 현황을 바탕으로 선정된 기업은 SGS, Bureau Veritas, Intertek, DEKRA, DNV GL의 5개 기업이며, 이들을 대상으로 사업 현황을 조사하였다.

[그림 1-3] 2014년도 주요 TIC 기업의 매출 현황 (단위, $ millions)



2) 조사 항목

주요 산업도메인별 소프트웨어 안전 활동 조사의 경우 산업 도메인별 선진국의 소프트웨어 안전 표준 적용 사례를 조사하였는데, 해당 도메인별 표준(Standard)이거나 표준(De-Facto Standard)로 인정되는 소프트웨어 안전 표준들을 대상으로 주요 선진국에서 해당 표준들의 적용방식과 법/규정 및 이를 수행하는 관련 기관에 대하여 조사하였다. 또한, 도메인별 한 개 이상의 표준이 존재하는 경우, 이해를 돕기 위한 배경 조사와 이들 사이의 관계도 포함하여 조사하였다.

해외 TIC 선진사의 경우, 회사 일반 현황, 매출 규모, 소프트웨어 안전 관련 주요 제공 서비스 등을 조사하였고, 글로벌 TIC 시장의 경우 시장의 특징, M&A 활동, TIC 시장의 향후 전망 등을 조사 분석하였다.

3) 조사 방법 및 경과

대부분의 조사는 인터넷 등을 활용한 문헌조사를 토대로 이루어졌으며, 도메인별 표준의 경우, 표준제정위원회인 IEC(International Electrotechnical Commission), ISO(International Organization for Standardization), CENELEC(European Committee for Electrotechnical Standardization) 등에서 제정한 표준 관련 공식 문서와 해당 국가들의 주요 법/규정 및 유럽연합 법(Regulation)/지침(Directive)/결정(Decision) 등을 조사하였

다. 또한, 기타 주요 연구기관에서 발표한 자료 등을 수집/분석하였다.

해외 TIC 선진사의 경우, 회사 일반 현황 및 소프트웨어 안전 관련 제공 서비스 등은 조사되었으나 소프트웨어 안전 부분에 대한 상세 매출은 별도로 구분되어 있지 않아 소프트웨어 안전에 특화된 매출은 조사가 어려웠다.

제2장 소프트웨어 안전(Safety) 개요

제1절 소프트웨어 안전의 이해

1. IEC 61508의 소프트웨어 안전 정의

IEC 61508은 산업에 적용되는 규칙으로 IEC(국제전기기술위원회, International Electrotechnical Commission)에서 작성한 국제표준으로서, 표준의 전체 명칭은 “ Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES) 즉, 전기/전자/프로그램 가능한 전자 안전 관련 시스템의 기능 안전 (Functional Safety)” 이다. IEC 61508은 모든 종류의 산업에 적용 가능한 기본적인 기능안전 표준을 목적으로 작성되었다. IEC 61508에서는 기능 안전을 다음과 같이 정의한다.

"E/E/PE 안전 관련 시스템의 정확한 기능, 다른 기술 안전 관련 시스템과 외부적인 위험 감소 설비에 의존하는 제어 대상 장비(EUC, Equipment Under Control)와 제어 대상 장비(EUC)를 제어하는 시스템 관련된 부분적 또는 전반적인 안전"

2. IEC 61508에서 소프트웨어 안전의 위험 레벨 정의

제어 대상 장비(EUC) 위험은 각각 확정된 위험 이벤트에 대하여 평가, 예측하는 위해도와 위험 평가 수행이 필요하며, 위해도 분석의 하나로 6가지 발생가능성과 4가지의 결과 항목을 기초로 프레임워크를 제시한다.

1) Risk Class Matrix

<표 2-1> Risk Class Matrix

	Consequence			
Likelihood	**Catastrophic**	**Critical**	**Marginal**	**Negligible**
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

(1) Class 정의

- Class I: 어떤 상황에서도 받아들일 수 있는 위험 영역
- Class II: 위험 감소가 실행불가능하거나 그 소요비용이 개선과 상당히 비례하지 않는 경우에만 용인될 수 있는, 바람직하지 못한 위험 영역
- Class III: 위험감소비용이 개선비용을 넘어서는 경우에 용인할 수 있는 위험 영역
- Class IV: 모니터링이 필요하기는 하나, 그대로 용인할 수 있는 위험 영역

(2) 발생가능성 (Likelihood) 항목 정의

- Frequent: 시스템 운영동안 매우 자주 발생, 즉, 년 10^{-3}보다 큼.
- Probable: 시스템 운영동안 여러 번 발생, 즉, 년 10^{-3}에서 10^{-4}까지.
- Occasional: 시스템 운영동안 한 번 발생, 즉, 년 10^{-4}에서 10^{-5}까지.
- Remote: 시스템 운영동안 발생할 것 같지 않음, 즉, 년 10^{-5}에서 10^{-6}까지.
- Improbable: 매우 발생할 것 같지 않음, 즉, 년 10^{-6}에서 10^{-7}까지.
- Incredible: 발생할 것이라고 믿을 수 없음, 즉, 년 10^{-7}보다 작음.

(3) 결과 (Consequence) 항목 정의

- Catastrophic: 다수의 인명 손실
- Critical: 한명의 인명 손실

- Marginal: 한 명 이상의 중상
- Negligible: 최악의 피해 수준이 경상 정도

2) SIL (Safety Integrity Level)

SIL은 시스템 개발에 관하여 달성해야 하는 목표를 제공한다. SIL은 안전기능(Safety Function)으로 제공되는 위험 감소에 대한 상대적인 수준으로써 정의하거나 또는 위험 감소에 대한 목표 수준을 명시하는 것이다. 그러나 SIL은 모든 기능 안전 표준에 일관적이지는 않다. 위험 평가에 의하여 목표 SIL을 산출하고, 이것은 최종 시스템에 대한 요구사항이 된다. 이러한 요구사항은 개발 프로세스를 설정하는 방법 (적절한 품질관리, 프로세스 관리, 확인과 검증 기술, 고장분석 등)을 알려주며, IEC 61508의 파트2, 3에서는 SIL을 달성하는데 필요한 수행 활동 가이드를 제시하고 있다.

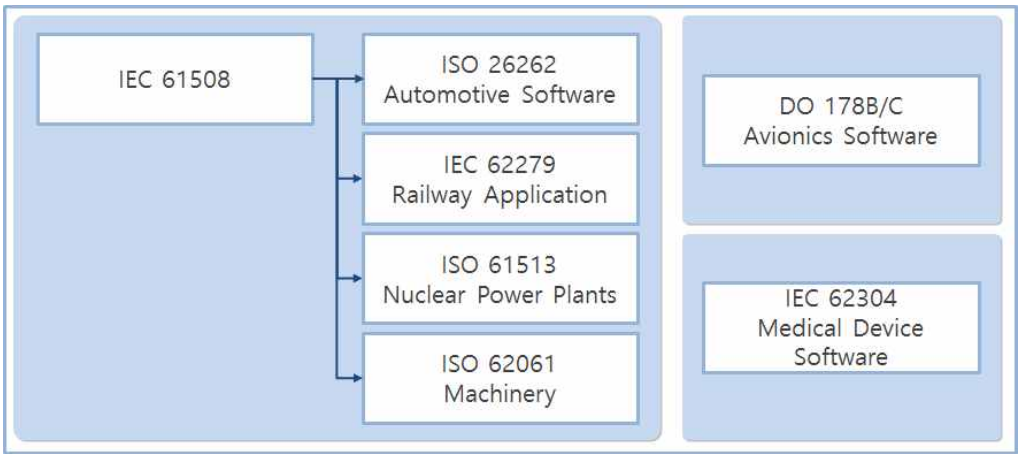
신뢰성이나 위험 감소의 측도로써 SIL을 사용하는 표준은 아래와 같다.

- IEC EN 61508 (Functional safety of electrical/electronic/programmable electronic safety related systems)
- IEC 61511 (Safety instrumented systems for the process industry sector)
- IEC 61513 (nuclear industry)
- IEC 62061 (safety of machinery)
- EN 50128 (railway applications – software for railway control and protection)
- EN 50129 (railway applications – safety related electronic systems for signalling)
- EN 50402 (fixed gas-detection systems)
- ISO 26262 (automotive industry)

제2절 산업별 소프트웨어 안전 표준

IEC 61508 정립 이후, IEC 61508을 근간으로 소프트웨어 안전이 필요한 각 산업 군별로 산업 특성을 고려한 소프트웨어 안전 표준을 제정하거나, 자체적으로 안전 표준을 제정하게 되었는데, 철도, 원자력, 기계, 자동차 산업의 경우 IEC 61508을 기초한 표준을 작성하였고, 항공의 경우 DO-178을 만들어 항공전기산업의 기준으로 활용하고 있으며 의료 분야의 경우 IEC 62304를 작성하여 유럽과 미국 표준으로 사용하고 있다.

[그림 2-1] 소프트웨어 안전관련 국제표준 관계도



1. IEC 61508에서 파생된 특정 산업 표준

1) Automobile Software - ISO 26262

ISO 26262는 자동차 전기/전자 시스템 안전(Functional Safety)을 위하여 IEC 61508을 근간으로 제정한 표준으로서 주요 자동차 제조업체에 채택되고 있다. ISO 26262 전에는 안전 관련 자동차 시스템을 위한 소프트웨어의 개발은 주로 자동차 산업 소프트웨어 신뢰성 협회(MISRA)의 가이드라인이 적용되었다. MISRA C는 MISRA에서 개발한 자동차 산업용 임베디드 시스템 소프트웨어의 코드 안정성, 호환성, 신뢰성 향상을 위한 C 프로그래밍 언어 개발 가이드라인이다.

2) Railway Application - IEC 62279 / EN 50128

IEC 62279는 철도 어플리케이션에 대한 IEC 61508의 해석을 제공한다. 이것은 커뮤니케이션, 시그널링 및 처리시스템에 대한 철도 제어와 보호를 위한 소프트웨어 개발을 포함하고 있다.

3) Nuclear Power Plants - ISO 61513

ISO 61513은 원자력발전소의 안전에 중요한 시스템의 장치와 제어에 대한 요구사항 및 권고사항을 제공하는데, 종래의 하드와이어드 (Hardwired) 장비, 컴퓨터기반 장비

또는 두 장비의 조합을 포함하는 시스템에 대한 일반적인 요구사항을 제시한다.

4) Machinery - ISO 62061

ISO 62061은 IEC 61508 표준의 기계 특화된 시스템 구축에 관한 표준이다. 이것은 모든 종류의 기계 안전 관련 전기 제어 시스템의 시스템 레벨 디자인과 복잡하지 않는 서브시스템 또는 장치 디자인에 적용할 수 있는 요구사항을 제공한다.

2. 항공 산업 표준 - DO-178B/C

DO-178B 표준은 항공전자시스템에서 사용되는 안전 필수 소프트웨어의 안전성을 취급하는 가이드이다. 기술적인 가이드이기는 하나, 항공전자 소프트웨어 시스템을 개발하기 위한 사실상의 표준이다. FAA(Federal Aviation Administration)가 인증을 위한 기술 표준 오더 (Technical Standard Order, TSO)를 명시할 때, 소프트웨어가 항공 환경에서 신뢰할 수 있게 수행할 수 있는지를 확인하기 위한 가이드로서 DO-178B를 사용한다.

제3장 해외 선진사례 조사 분석

제1절 주요 산업도메인별 소프트웨어 안전 활동 조사

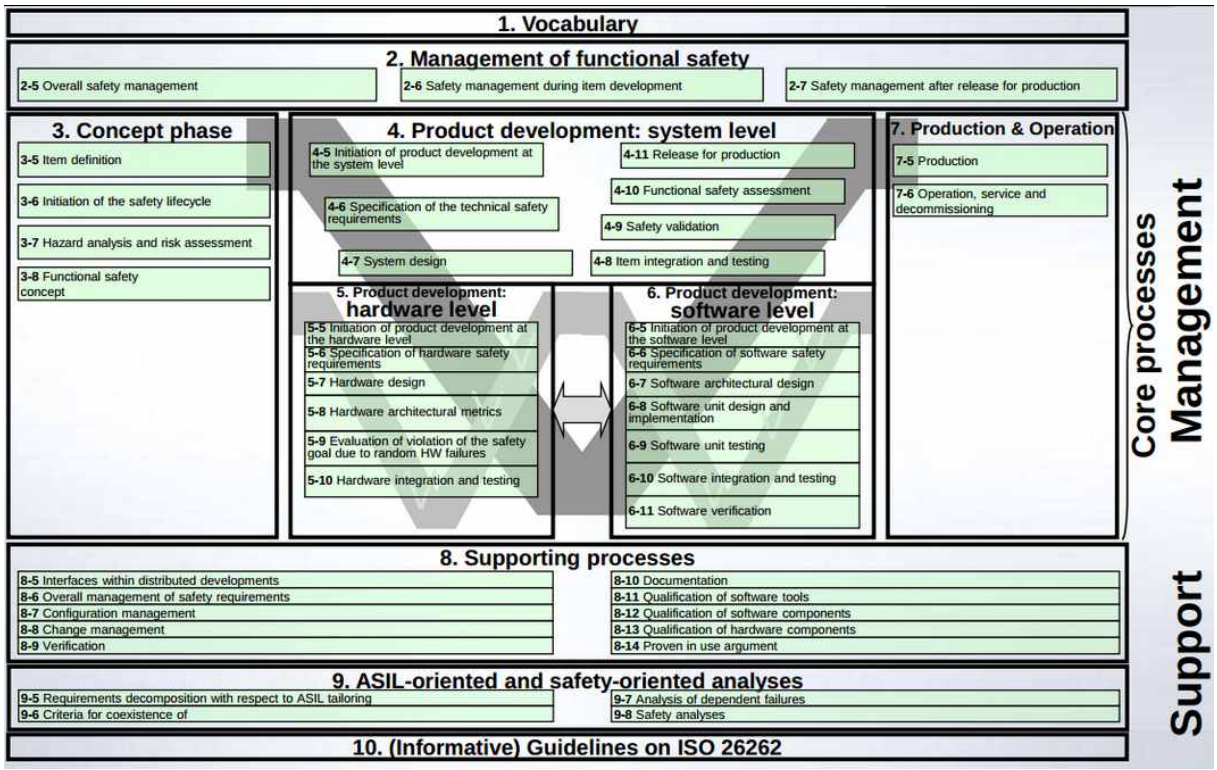
1. 자동차 부문

메타 표준인 IEC 61508에서 파생된 자동차 소프트웨어 안전 표준인 ISO 26262의 적용에 대하여 미국, 유럽 전역과 일본은 다른 형태로 적용되고 있기 때문에 각 나라별로 표준 적용 방식을 구분하여 기술하였다. 미국과 유럽은 제조물 책임법이라는 간접조항에 따라 안전 표준 준수를 유도한다는 공통점과 자동차 판매 승인 방식에서의 차이점에 대하여 조사하였고, 일본은 ISO 26262를 적용하는 과정에서 정부와 민간이 문제점을 극복하는 노력에 대한 사례를 조사하여 본 보고서에 기술하였다.

1) 소프트웨어 안전 관련 주요 표준

ISO 26262는 3500kg 이하의 차량에 적용되는 기능 안정성(Functional Safety) 표준이며 (소프트웨어 부분은 Part 6), 메타 기능 안전 표준인 IEC 61508에서 자동차 부문 전기, 전자 시스템의 오류로 인한 사고방지를 위해 구체화하여 작성되었다. ISO 26262는 위험 기반의 안전 표준으로서, 위험을 초래하는 운영 상황의 위험을 정량화하고 시스템적 또는 하드웨어적인 문제를 감지/제어하거나 이들의 영향을 최소화하기 위한 안전 조치에 대하여 정의한 것이며, 충분 또는 수용가능한 수준의 안전을 달성하기 위하여 ASIL(Automotive Safety Integrity Levels)을 측정하고 위해도 분석(Hazard Analysis) 및 리스크 평가(Risk Assessment)를 수행한다. ISO 26262는 차량 개발 프로세스 기획 단계부터 전기/전자 시스템의 오작동에 의해 발생할 수 있는 위험 인자를 식별하고 관리하여 차량 안정성을 확보하는데 그 목적을 두고 있다. 시스템 개발 시 요구되는 안전 관련 활동으로는, 아이템 정의(Item Definition), 위해도 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. ISO 26262 전체 구조는 총 10개 Part로 구성되어 있으며, 시스템 개발(Part 4), 하드웨어 개발(Part 5), 소프트웨어 개발(Part 6), 자동차 ASIL 기반의 위험 평가(Part 9)가 제시되어 있다. [1)]

[그림 3-1] ISO 26262 Structure



자료: Dr. Qi Van Eikema Hommes. ASSESSMENT OF THE ISO 26262 STANDARD, " ROAD VEHICLES - FUNCTIONAL SAFETY." 2012 [2)]

MISRA C는 MISRA(Motor Industry Software Reliability Association)에서 개발한 자동차 산업에 사용되는 임베이드 시스템 소프트웨어의 코드 안정성, 호환성, 신뢰성 향상을 위한 C 프로그래밍 언어에 대한 개발 가이드라인이다.(C++의 경우 MISRA C++가 있다) MISRA C는 자동차 산업을 위해 개발되었지만, 우주/항공, 의료장비, 국방, 철도 등의 다양한 산업의 Best Practices로 진화되어 활용되고 있다. MISRA C:2012의 경우 총 143개 규칙과 16개의 지침으로 구성되어 있다. ISO 26262와 MISRA C의 차이점은, MISRA C가 코딩 표준인데 반하여 ISO 26262는 차량용 시스템의 계통적 고장(Systematic Failure)과 우발 고장(Random Failure)에 대해 회피 또는 제어를 하기 위한 방법과 조치를 정의한 것이다. [3)]

2) 주요 국가별 안전 표준 준수 활동

(1) 미국

자동차 산업의 소프트웨어 안전에 대한 표준 준수 요구는 명확히 소프트웨어 안전 부분이 법률적으로 명시되어 있지 않는 반면, 자동차, 자동차 시스템, 자동차 부품 차원에서 안전 표준을 제시하고 이를 지키도록 명시하고 있다. 안전 표준 준수는 명확한 법률에 근거한 강제적인 준수보다는 포괄적인 법률 적용에 따른 자동차 제조사들의 자발적인 준수가 핵심이다. 미국에서 제조사의 자발적 준수를 유도하는 제도적인 장치와 정부의 활동은 크게 2가지로 볼 수 있는데, 1. 미국 내에서 판매되는 자동차 안전 준수 관련 법/제도 부분에 따른 교통국(Department of Transportation) 산하 NHTSA(National Highway Traffic Safety Administration)에서 수행하는 자국 내 판매 자동차의 안전 표준 준수 여부 확인 활동이 있고, 2. 제조물 책임법(Products Liability Law)에 근거하여, 제조사가 안전사고 발생 시 예상되는 소송에 대비하여 안전 표준에 따른 자동차의 설계 및 제조를 유도하는 간접적인 장치가 있다.

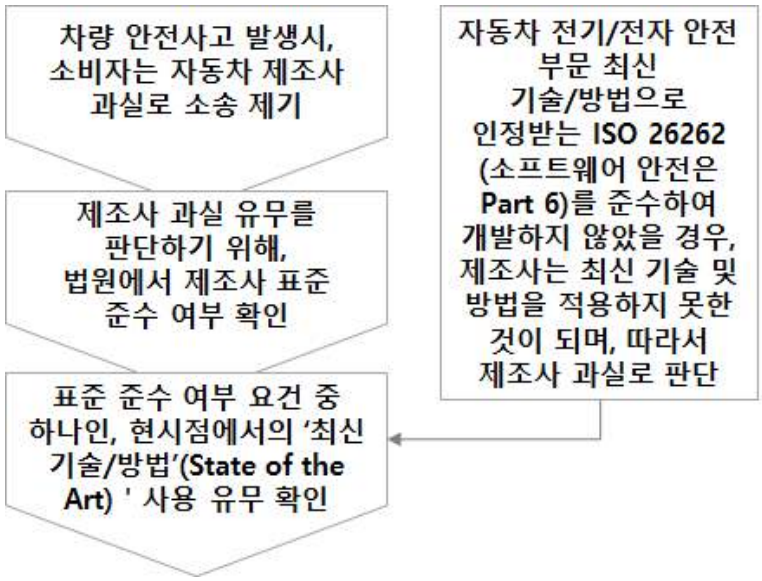
NHTSA는 자동차 제조사에 FMVSS(Federal Motor Vehicle Safety Standards)를 준수하게 하고, 도난 방지, 연료 효율 등에 대한 규정 제정 및 시험 평가를 수행하는 미교통국 산하 기관이다. FMVSS는 미국 법 Title 49 Code of Federal Regulation Part 571에 성문화되어 있으며, NHTSA에 의해 제정되고 집행된다. FMVSS는 자동차, 자동차 안전 관련 부품 및 시스템에 대한 설계, 제작, 성능 및 내구성 요구사항에 대한 규정이며, 충돌 방지, 충돌 안전도, 충돌 후 생존 가능성의 3가지 부분으로 되어 있다.

NHTSA는 안전에 대한 표준을 제정하고, 자동차 사고에 대한 방대한 양의 DB를 축적하고 자동차 및 자동차 부품이 안전 관련 법조항을 만족하도록 규제하고 있으나, 자동차나 자동차 부품에 대한 표준 준수 인증 및 준수 관련 정보 수집을 자동차 제조사로부터 직접 하지 않는다. 자동차 제조사는 미국 자동차의 모든 안전관련 규정을 준수했다는 자체 인증을 실시하고 자체적으로 테스팅 및 리콜에 대한 책임을 지고 있다. 대신, NHTSA는 새로운 자동차 모델이 시장에 출시되고 난 후, 해당 모델을 구입하여 자체 테스팅 설비에서 테스팅을 진행하여, 표준 준수 여부를 확인하는데(ODI: Office of Defect Investigation), 만일 표준을 만족하지 못할 경우 자동차 제조사에 리콜을 권고하거나 리콜을 강제화할 수 있으며, 심할 경우 벌금을 부과하기도 한다.

제조물 책임법은 자동차 제조사로 하여금 차량 및 차량 부품에 대한 안전 표준을 따르게 하는 포괄적이고 간접적인 조항이다. 차량 안전사고 발생시, 소비자는 자동차 제조사에 대하여 원칙적으로 제조사의 과실, 명시 및 묵시담보의 위반, 무과실 책임의 3가지 요건에 근거하여 소송을 제기할 수 있다. 이 경우, 자동차 안전에 대한 문제는 주로 과실의 측면에서 다루어질 수 있다. 제조사 과실이라 함은 제조사가 동일 또는

유사한 상황에서 최선의 노력을 하지 않았다는 의미를 내포하며 법원에서는 과실을 판단하기 위하여 여러 가지 요소를 검토하는데, 특히 연방 규정에서 규정된 표준의 준수 여부가 그 중 한 가지 요소이다. 즉, 연방 규정에서 규정된 표준을 준수하지 않았을 경우, 이는 곧 설계를 적정하게 하지 못한 것이며(설계 결함), 제조사의 과실로 판단된다. 설계 결함에 대한 최신 기술(State of the Art)이라는 용어는 해당 시점에 자동차의 설계 결함이 있었는지를 판단하는 주요 기준 중의 하나로서 법정에서 자주 사용되고 있다. 즉, 해당 시점에 최신 기술 및 방법을 사용하지 않았을 경우, 제조사가 자동차 제조 시 상당한 노력을 하지 않았다는 증거가 되며, 따라서 제조사의 과실이 있다는 의미이다. 즉, 현재 시점을 적용한다면, 자동차 전기/전자 부문의 최신(State of the Art) 글로벌 설계 표준으로 인정받고 있는 ISO 26262를 준수하여 개발하지 않았을 경우, 제조사는 최신 기술 및 방법을 적용하지 않았기 때문에 제조사 과실로 판단될 수 있다는 의미이다. [4] [5]

[그림 3-2] 제조물 책임법과 소프트웨어 안전표준 적용



(2) 유럽

미국과 유사하게 유럽의 경우도 자동차 산업의 소프트웨어 안전에 대한 표준 준수 요구는 명확하게 법률적으로 표현되어 있지 않고, 자동차 / 자동차 시스템 / 자동차 부품 수준에서 안전을 준수해야 한다는 안전 요구 사항으로 구현되어 있다. 안전 표준 준수는 명확한 법률에 근거한 강제적인 준수보다는 포괄적인 법률 적용에 따른 자동

차 제조사들의 자발적인 준수가 핵심이다. 안전관련 법/제도 준수를 유도하는 활동도 크게 2가지로 볼 수 있는데, 1. 유럽 내에서 판매되는 자동차는 판매 전 안전 준수 관련 형식승인(Type Approval)을 통해 철저한 검사를 시행하여 EEC/ECE 법규에 따른 인가를 받은 후 다시 각국 법규의 인증을 받은 다음, 판매가 가능한 형태이며, 2. 제조물 책임법(Products Liability Law)에 근거하여, 제조사가 안전사고 발생 시 예상되는 소송에 대비하여, 안전 표준에 따라 자동차를 설계하고 제조하도록 유도한다. 제조물 책임법의 경우 제조사가 최신 기술 및 방법을 사용하여 자동차를 설계하고 제조해야 제조자 과실을 면책할 수 있어, 제조사가 자연스럽게 최신 국제 표준인 ISO 26262를 준수하여 개발하게 되었다. 제조물 책임법은 미국의 적용 사례와 유사하므로, 여기서는 유럽의 자동차 형식승인(Type Approval) 원칙을 적용한 안전 규정 및 표준 준수에 대하여 기술한다.

유럽의 통일법규는 유엔의 유럽경제위원회(ECE)에서 정한 ECE Regulation과 경제공동체(EEC)에서 제정한 EEC Directives의 두 형태가 있고 또 각국별로 국가형식승인(NTA : National Type Approval)이 있다. ECE Regulation은 협정서에 비준한 국가에만 적용되고 법규가 자발적이기 때문에 관계국에 강제력이 없고 자국의 법규에 일치시킨 가맹국에만 상호자동승인제도로 통용되고 있다. 이에 반해 EEC Directive는 회원국에 대하여 강제력을 갖고 있어 이 규정에 의한 형식승인을 회원국 주무당국이 인정한 차량은 모두 공동시장 내에서 판매가 가능하다. 모든 자동차관계 유럽법규는 형식승인원리(Type Approval)에 기초하고 있다. 즉, 유럽의 인증제도는 북미의 자기인증과는 달리 판매전에 철저한 검사를 시행하는 사전인증제도로 먼저 EEC/ECE 법규에 따른 인가를 받은 후 다시 각국 법규의 인증을 받아야 한다. 이 제도는 제조업자로 하여금 생산일치성과 판매된 각 차량에 대하여 법규와 일치한다는 것을 확인하는 증명서를 발행하도록 강제되어 있다. 주요법규내용은 형식승인(Type Approval), 제품책임(Product Liability), 정기검사제도(Periodic Inspection), 배출가스규제(Emissions), 연비(Fuel Consumption), 엔진력(Engine Power)등이 있다. EU 가맹국 대부분이 국가 기관 또는 사설 기관이 상기 형식승인을 수행하고 있다. (예. 영국의 경우 Vehicle Certification Agency, 독일의 경우 Kraftfahrt-Bundesamt (KBA): Federal Motor Transport Authority 등) 추가적으로, ECWVTA(Whole Vehicle Type Approval)라는 형식승인 제도가 있는데, 이 제도의 경우 한번 형식승인을 받을 경우, EU 가맹국별 추가적인 형식승인을 받을 필요가 없다. 최근 유럽 자동차 형식승인 지침인 2007/46/EC가 UNECE(United Nation Economic Commission for Europe)의 규정으로 대체되어 사용되고 있다. UNECE에서 규정한 자동차 관련 형식승인 규정은 총 133개로 구성되어 있으며, 자동차 주요 부품

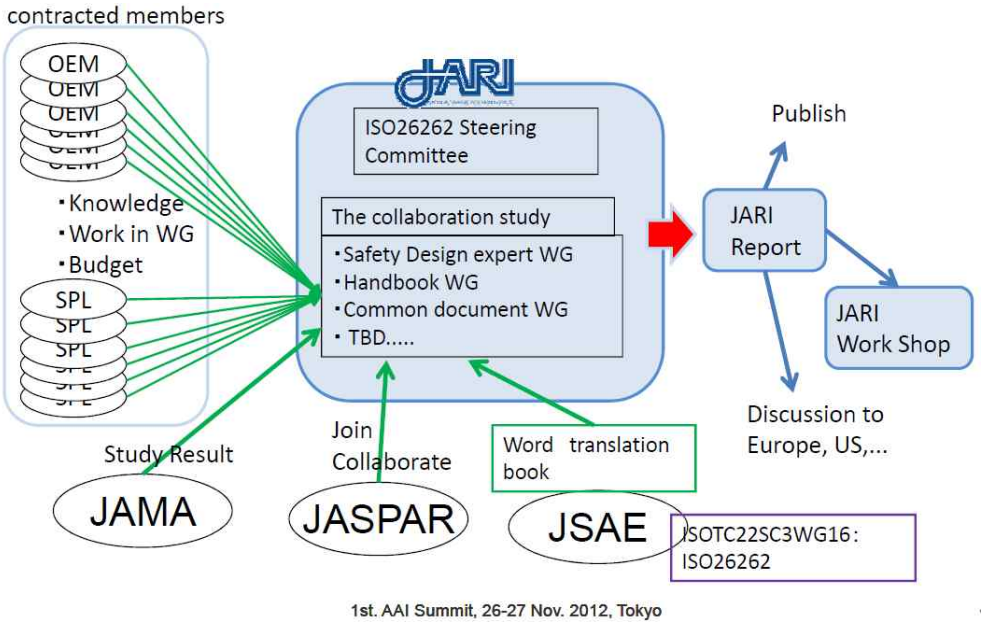
이나 시스템에 대하여 준수해야 할 규정을 제시하고 있다. 따라서 ISO 26262의 경우 별도의 규정으로 구별하여 구현되지 않고, 자동차의 전기/전자 부품 또는 시스템 제작 시 준수해야 하는 Underlying 표준으로 활용되어 적용되고 있다. 예를 들어, UNECE Regulation No.100 Electric Vehicle Safety의 경우, 준용해야할 Functional Safety 국제 표준으로 ISO 26262를 포함하고 있다. (자료. List of relevant regulations for Electric Vehicle Safety EVS-04-04e International (Europe) ECE Regulation No.100 (02 series, pp [3.) 6)]

(3) 일본

일본의 경우 정부 연구 기관과 자동차 및 부품 업체가 ISO 26262을 도입하면서, 발생한 주요 이슈 및 이를 극복하기 위한 노력을 통하여 표준을 적용한 사례를 조사하였다.

JARI(Japan Automobile Research Institute: 일본 자동차 연구기관)는 2005년도에 ISO 26262에 관심을 가지고, JSAE WG(Automotive Engineers of Japan Work Group)에 참여하였다. 그 후 JARI에서는 JAMA(Japan Automobile Manufacturers Association: 일본 자동차 제조사 협회)와 2008년까지 ISO 26262에 대한 연구를 계속하였고, 2009년 JARI가 주요 부품 업체를 대상으로 ISO 26262를 업무 프로세스에 적용하는데 따른 문제점을 조사하였다. 그 결과로 1. 회사 별로 ASIL 등급을 제정하는 의사 결정 프로세스의 상이, 2. 전반적인 ISO 26262 및 관련 안내서 상용화에 대한 번역, 3. 등급별 안전 관리 기술, 4. 안전 담당자들의 교육에 대한 문제가 도출되었다. 이 같은 문제를 해결하기 위해서 각 조직별로 담당 역할을 정하였으며, JAMA는 OEM 업체, JSAE는 ISO 26262 및 관련 안내서(Handbook) 번역 및 개발, JASPAR는 자동차용 소프트웨어를, 그리고 JAPIA는 공급자를 담당하였다. 2011년 4월에는 JARI가 OEM 및 공급 업체를 회원으로 하는 ISO 26262 운영위원회를 조직하였고, JAMA, JSAE, JASPAR가 참관자로 참여하였다. ([그림 3-2] 참조).

[그림 3-3] 일본의 ISO 26262 협력 시스템 및 회원사



Total: 26 companies 1 April, 2012

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

자료: Ryuji Osuga. Functional Safety (ISO26262) activities in Japan. 2012 [7]

ISO 26262 수행을 위해서는 추가적인 문서를 만들고 프로세스 활동을 향상시켜야 할 필요성이 있었는데 이는 업무량 및 소요시간의 증가로 이어졌다. 이를 위해 일부 항목의 경우 JARI 주도의 공통 활동으로 수행하였고, 그 결과를 공유할 수 있게 했다. JARI 안내서(ISO26262를 기술적인 부분을 고려하여 일본어로 번역한 다음, 기존 일본 Functional Safety Management System에 대한 공통 이해를 추가하여 제작)와 같은 공통 사용 영역(Common Use Area)에서 사용가능한 공통 문서(Common Document)를 제공함으로써, ISO 26262를 도입하는 기업에 추가 문서 작성에 부담을 해소하고자 노력한 것이다.

이처럼, 일본은 일본 정부 연구 기관과 완성차 및 자동차 부품 업체 등이 협력하여, ISO 26262 도입을 추진하였고, 특히 일본 정부 연구 기관은 각 업체들의 업무 부담을 경감하기 위해 표준 해석, 공통 활동 및 문서 제작 등에서 선도적인 역할을 하고 있었다.

2. 철도 부문

미국은 화물 및 저속 수송을 목적으로 하고 있고, 유럽연합은 승객 및 고속 수송을 목적으로 하고 있기 때문에, 유럽연합에서는 EN 50128을 적용하고 있으나 미국은 AREMA에서 제정한 AREMA 2011 C&S Manual을 De-facto 표준으로 적용하고 있다. 본 보고서에서는 철도 소프트웨어 안전 표준과 관련된 미국과 유럽연합 표준의 차이에 대하여 언급하고 실제 미국과 유럽연합의 표준 적용 방식을 제시한다.

1) 소프트웨어 안전 관련 주요 표준

(1) EN 50128 / IEC 62279

EN 50128는 철도 산업에 관련된 유럽의 안전 관련 소프트웨어 표준으로, 안전한 소프트웨어 개발을 위한 방법론, 원칙, 방안 등을 규정하고 있다. 주요 원칙으로는 하향식 디자인 방법(Top-Down Design Method), 모듈성(Modularity), 개발 단계 별 검증(Verification after each development step), 명확한 문서화(Clear documentation), 검증 가능한 문서(Verifiable Document), 해당 기기에서의 소프트웨어 확인 테스트(Test the software on the target hardware: Validation)가 있다. 주요 구성요소는 소프트웨어 보증 수준(Software Assurance levels), 소프트웨어 개발 프로세스(Software Development Process), 크로스프로세스 요구사항(Cross-Process Requirements), 기법 및 방법(Technique and Measures)이 있다. EN 50128을 기반으로 한 국제 표준으로 IEC 62279가 있으며, 서로의 내용은 동일하며 EC 50128의 경우 CENELEC에서, IEC 62279는 IEC에서 관장한다. [8)]

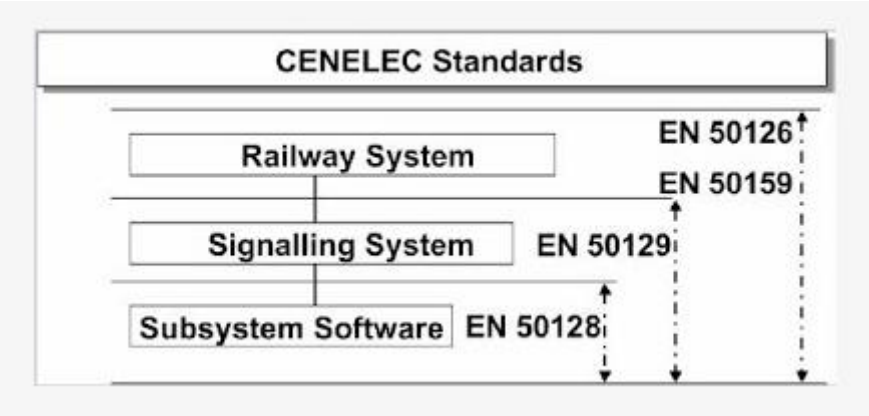
EN50128 / IEC 62279를 각 구성 요소 별로 간단히 살펴보자면,

<표 3-1> EN 50128/IEC 62279 구성요소

구성 요소	내용
Software Assurance Levels	소프트웨어 안전 등급에 따른 소프트웨어 안전 보증 수준(SSAS)을 구분하고, 등급에 적합한 개발 프로세스 적용 <안전 보증 수준> • SSAS 0: Non Safe Application • SSAS 1: Lowest Safety Request Level • SSAS 2: Medium Safety Request Level • SSAS 3: High Safety Request Level • SSAS 4: Highest Safety Request Level
Software Development Process	V 모델 기반의 개발 프로세스 사용. 각 단계별로 명확한 문서화 및 확인 절차(Documentation & Verification) 요구
Cross-Process Requirements	개발자에 대한 자격요건, 문서화, 품질 관리와 소프트웨어 유지 관리에 대한 요구 사항 포함
Techniques and Measures	SSAS 등급에 따른 차별화된 테스팅 기법 및 방법 제시

유관 표준으로 철도산업의 운영, 시스템, 유지관리, 안전에 관련된 규정인 EN 50126과 철도산업의 전기전자 시스템의 안전에 관한 규정인 EN50129가 있으며, 이들과의 관계는 EN 50126 > EN 50129 > EN 50128 이다. 즉, EN 50126은 철도 시스템 안전 규정을 정의하였다면, EN 50129는 관련 시스템(Communication, Signaling & Process System)의 안전을, 그리고 더 나아가서 EN 50128에서는 관련 시스템에서 사용되는 소프트웨어 안전에 대하여 규정한 것이다. 이들과의 관계는 아래와 같다.

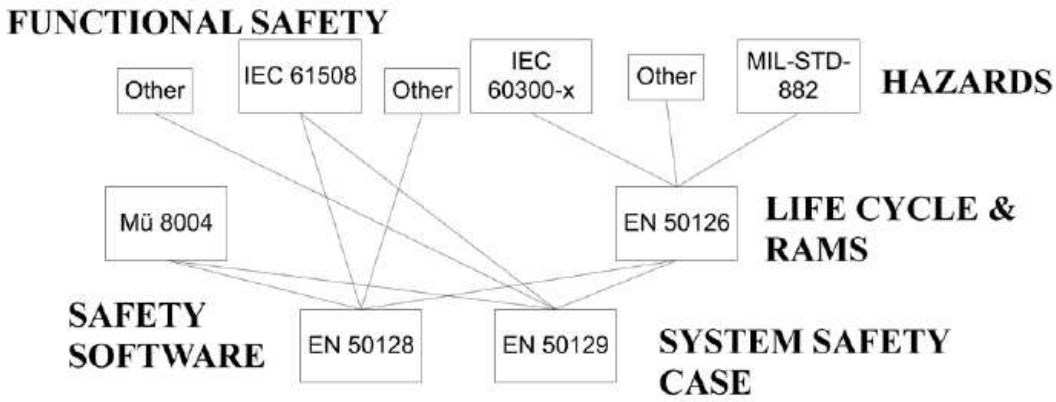
[그림 3-4] EN 50128과 유관 표준과의 관계



자료: Troels Winther. Quick quide to Safety Management based on EN50126 / IEC 62278. 2012 [9]

EN 50126, EN 50129, EN 50128는 기능 안전 표준(IEC 61508), 위험(IEC 60300-x, MIL-STD-882) 등 다양한 기존 표준을 기반으로 제정되었는데, 이들의 관계는 다음과 같다. ([그림 3-4] 참조).

[그림 3-5] EN 5012x와 관련 유관 표준들



자료: James B. Balliet. Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance . 2011 [10]

(2) AREMA C&S Manual

승객 운송 및 고속 운송 중심의 철도 환경을 고려한 유럽 표준에 비해, 화물 운송

및 저속 운송 중심인 미국은 유럽과 다른 표준을 제정하여 활용하고 있다. AREMA(American Railway Engineering and Maintenance of Way Association)에서 제정한 'The AREMA Communications and Signals Manual of Recommended Practices'(이하 AREMA C&S Manual)는 전기/전자/소프트웨어 안전 표준(De-facto Standard)으로 미국 및 캐나다 철도 산업에서 인정받고 있다. 2011년에 개정된 AREMA 2011 C&S Manual의 소프트웨어 및 시스템 안전 관련 주요 항목을 살펴보면, ‘ 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. AREMA C&A Manual의 경우, 포괄적이고 하향식 프레임워크 기반의 철도 안전 표준인 유럽과는 달리, 소프트웨어 기반의 필수 시스템에 대한 안전 보증을 위한 구조화된 프레임워크이다.

유럽과 미국 표준을 비교해 보면, 아래와 같다.

- 유럽 표준은 초기 디자인부터 종료까지 안전 시스템 라이프사이클 전반에 걸친 품질과 안전관리 강조
- 유럽 및 미국 표준 모두 시스템의 안전 등급 설정을 요구하고 있으나, 유럽의 경우 보다 형식적인 안전 등급 정의 사용(Safety Integrity Levels 0-4)
- 미국 표준 및 규정은 철도 시스템 개발에 적용되는 주 안전 보증 개념들을 식별하는데 유럽 표준과 차별화된 주요 부분은 Design Diversity and Self checking, Checked Redundancy, N-Version Programming, Numerical Assurance, Intrinsic Fail Safe Design 등이 있음
- 위험 유형(Hazard Classifications), 위해도 분석(Hazard Analysis), FTA(Fault Tree Analysis), 고장 유형(Failure Mode) 등의 활동은 두 표준 모두 동일

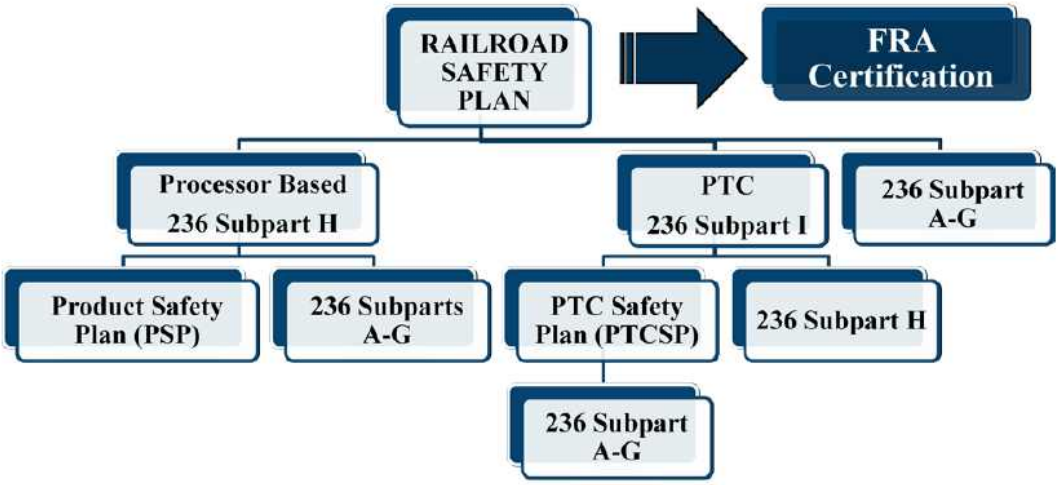
2) 주요 국가별 안전 표준 준수 활동

(1) 미국

미 연방철도국(Federal Railroad Administration: FRA)은 2010년 성과 중심의 안전 규정을 발표하였는데, 주요 내용은 1. 49 CFR Part 236 Subpart H: 프로세스 기반의 시그널 및 철도 통제 시스템 개발 표준과 2. 49 CFR Part 236 Subpart I: PTC(Positive

Train Control System) 이다. 이 규정들은 안전 시스템의 성능 표준 제정에 주안점을 두고 있지만, 필수 안전 제어 시스템의 안전 인증 획득을 위한 안전 개발 방법, 집행 기관, 공급자 프로세스 등을 정해 놓지는 않았다. 즉, 철도 사업자들은 자기들만의 프로세스, 절차, 분석 방법과 문서를 통해 FRA 규정의 요구사항을 만족하면 인증을 받을 수 있는 방식이다.([그림3-5] 참조).

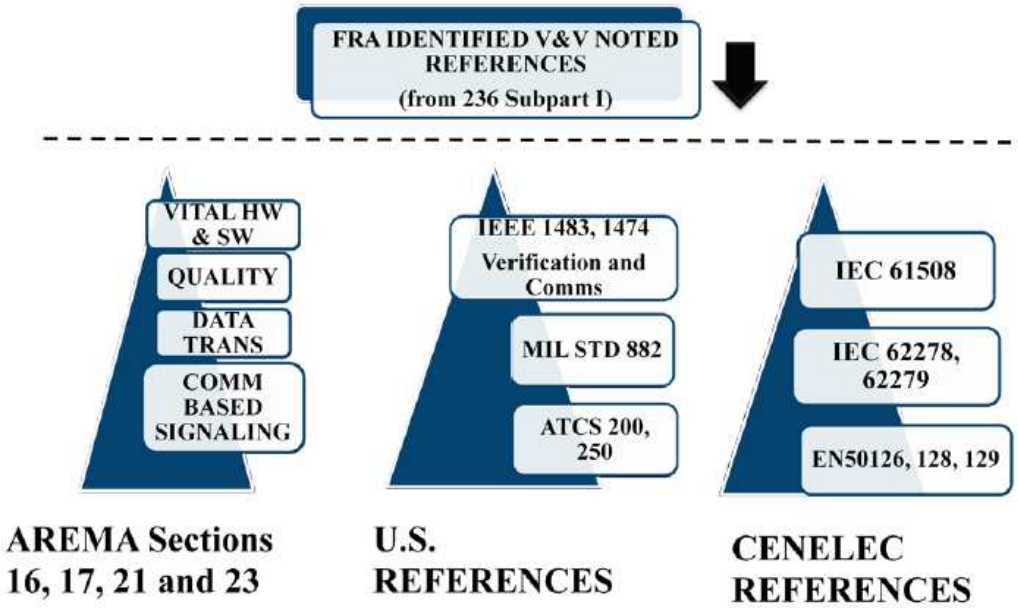
[그림 3-6] FRA 인증 구조



자료: James B. Balliet. Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance . 2011 [10)]

FRA 규정에는 철도 사업자들이 인증 획득을 위한 제품 및 시스템 안전 계획(Product & System Safety Plans) 수립 시 활용 가능한 검증 및 확인 표준들이 열거되어 있는데, 여기에는 AREMA를 포함한 미국 표준뿐만 아니라 유럽 표준(CENELEC)도 포함되어 있다.

[그림 3-7] 검증 및 확인(V&V) 활동 시 인정되는 주요 표준들



자료: James B. Balliet. Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance . 2011 [10)]

FRA 규정에서 명시된 미국 표준들은 크게 AREMA 2011 C&S Manual, IEEE 1483 & 1474, MIL STD 882C의 3가지가 있으며, 소프트웨어 및 시스템 관련 안전 보증 표준은 AREMA, 2011 C&S Manual Part 17.3.1, 17.3.2, 17.3.3 이다.

[그림 3-8] 미국의 철도 소프트웨어 안전 표준

236 Subpart H & Subpart I Appendix C Safety References	Safety Category
AREMA 2011 C&S Manual	Processor Based Verification and Validation
AREMA Manual Part 17.3.1	Recommended Safety Assurance Program for Electronic/Software based Equipment
AREMA Manual Part 17.3.3	Recommended Practice For Hardware Analysis for Vital Electronic/Software Based Equipment
AREMA Manual Part 17.3.5	Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software Based Equipment
IEEE 1483-2000	Verification of Vital Functions in Rail Transit
IEEE 1483-2000	Safety Assurance Concepts
IEEE 1474.1-2000	Performance and Functional Requirements
MIL STD 882C	Risk Assessment Processes
"Safety of High Speed Ground Transportation Systems", Luedeke 1995	Safety Validation

자료: James B. Balliet. Bridging the European and U.S. Rail Safety Assurance Gap: The Feasibility of Cross Acceptance . 2011 [10)]

미국 철도 산업의 경우 규정 및 제도의 기반 하에 이를 주관하는 기관이 존재하고, 관련 사업자들은 관련 규정을 준수하여 주관 기관의 인증을 득하여 제품 납품 및 사업을 수행할 수 있는데, 이를 위한 표준의 경우 규정에서 권고하는 여러 표준 중 하나를 사용하거나 사업자가 자체적인 절차 및 방법으로 충분히 규정을 만족할 수 있을 경우 자체적인 방법을 사용하여 인증을 받을 수 있는 것이 특징이다. 따라서 소프트웨어 안전의 경우도 AREMA C&S Manual Part 17.3.1~3 및 유럽표준인 EN 50128이 규정에 권고되어 있어 필요할 경우 사업자들이 사용하도록 유도하고 있으나, 규정에서 강제하지 않는다.

(2) 유럽

유럽은 유럽연합에서 철도 안전 및 상호운용 관련 지침(Directive 2004/49/EC, 2008/57/EC)을 제정하고, ERA(European Railway Agency)에서 유럽 철도 산업 및 관련 제조사들이 필수적으로 준수해야 할 요구사항들을 상호운용을 위한 기술 사양서(TSI: Technical Specifications for Interoperability) 형식으로 제공하며, 각 회원국은 관련 지

침에 의거해서 자국의 철도관련 법/제도를 개정하고 TSI를 근간으로 기술적으로 준수해야 할 요구사항을 제정하여 운영한다. 이를 통해, 유럽연합 가입국들은 점진적으로 자국 실정을 반영한 표준화된 철도 안전 법/제도 및 필수 준수 사항을 보유하게 되고, TSI에서 규정된 주요 표준 및 기술 사양 등을 자연스럽게 유럽 각 회원국 및 관련 철도 산업이 준수해야 하는 요구 사항으로 정착시켜 유럽 철도의 상호운용성을 보장한다. 자세히 살펴보면, 유럽연합 철도 안전 지침에 따라 정의된 철도 안전 관련 주요 역할자들은 Notified Body(정부에서 인증 받은 철도 인증 조직), Independent Safety Assessor(ISA: 독립 안전 평가자), National Safety Authority(정부 안전 관련 기관), Investigating Body(사고 및 사건 조사 조직), Infrastructure Manager(철도 인프라 및 안전 관리 조직), Railway Undertaking(철도 산업 종사자)등이 있다. 특히 독립 안전 평가자는 미국과는 차별화된 철도 안전 검증 단체인데, 이들은 정부 철도 기관 등에 고용되어 철도 관련 사업자들이 개발하는 안전 필수 시스템이 안전 필수 요구 사항 및 표준을 만족하는 지를 평가하는 역할을 한다. 즉, 철도 산업 종사자들은 철도 인증을 득하기 위해서는 TSI의 요구사항에 따라 개발해야 하며, 이를 독립 안전 평가자나 철도 인증 조직이 검사하는 체계로 운영된다.

EN 50128는 주요 시스템의 필수 기술 사양서(TSI)에 소프트웨어 관련 준수 표준으로 되어 있어서, 관련 사업자들은 TSI의 요구사항 준수에 대하여 평가를 받고 철도 인증을 받아야 하므로 EN 50128 표준은 법/제도적으로 강제 적용된다. 예를 들면, 'Applicable standards in CR Control-Command and Signaling TSI (2006/679/EC)' 의 Section 6.1.2 Index A2 Interoperability Constituents Modules 및 Section 6.2.2.3 Index A2, 'Applicable standards in HS Rolling stock subsystem TSI (208/232/EC)'의 Section 4.2.7.13 부분에서 소프트웨어 개발 시 EN50128 준수 항목이 명시되어 있다.

유럽 연합에서 규정한 지침(Directive) 및 TSI가 유럽 연합 회원국에 적용되는 방식을 간략히 살펴보자면, 독일의 경우 독일 교통부 산하 독립 조직으로 독일연방철도국(Eisenbahn-Bundesamt: EBA)이 있으며, 독일연방철도국은 유럽연합지침(Directive 2004/49/EC) 및 TSI에 따라 안전 규정을 제정하고 안전 인증을 수행하며, 소프트웨어 안전 표준에 대해서는, 철도 건설 및 운영 규정(Die Eisenbahn-Bau- und Betriebsordnung: EBO)에 철도차량용 안전 관련 소프트웨어 개발은 EN 50128을 준수하도록 강제되어 있다. (Verwaltungsvorschrift für die Abnahme von Eisenbahnfahrzeugen gemäß § 32 Abs. 1 EBO, Anhang 1: EBA-Anforderungen für die Abnahme von Regelfahrzeugen nach § 32 EBO : 철도 차량 승인을 위한 규정 중

별첨 1. EBA - 차량 승인을 위한 요건).

3. 항공 부문

항공 부문의 소프트웨어 안전은 자동운전과 결부되어 상당히 상세한 표준으로 발전하였으며 특히 항공이 발달한 미국의 정부 기관에서 여러 가지 표준을 적용하고 있었다. 항공기는 그 용도별로 우주항공용도, 국방용도, 그리고 민간상용으로 구분될 수 있으며 각각의 표준이 용도에 맞게 발전하였다. 여기에서는 미국의 사례로서 NASA(National Aeronautics and Space Administration, 미국우주항공국)와 FAA(Federal Aviation Administration, 미국연방항공청)에서 적용하는 소프트웨어 안전 표준에 대하여 설명하였다. FAA에서 사용하는 표준인 DO-178B는 미국의 RTCA(Radio Technical Commission for Aeronautics)와 유럽의 EUROCAE(European Organisation for Civil Aviation Equipment)에서 공동 작업한 표준으로서 미국과 유럽에 적용되는 표준의 명칭이 다를 뿐 동일한 내용을 포함하고 있으므로, 유럽 사례는 미국의 FAA에서 사용하는 DO-178B 표준 설명으로 대체한다.

1) 주요 항공 표준

미국 항공분야의 Safety-Critical 소프트웨어 개발 표준은 1. DFRC(Dryden Flight Research Center)와 같은 센터 특화된 표준을 포함하는 NASA (National Aeronautics and Space Administration, 미국우주항공국) 표준과 2. 민간 항공기 소프트웨어를 규제하는 FAA (Federal Aviation Administration, 미국연방항공청)에서 사용되는 RTCA DO-178B 및 3. 국방 표준인 MIL-STD 498의 3가지 부문으로 나눌 수 있다. 이 중, NASA 센터와 FAA 각각은 다른 타입의 소프트웨어 표준을 포함하고 있고 서로 다른 인증 절차를 보유하고 있다. 예를 들어서 우주선과 우주 정거장에 특화된 절차와 Onboard 비행 소프트웨어는 다른 인증 절차를 준수해야 한다. 또한 소프트웨어 등급(Mission-Critical 소프트웨어, Safety-Critical 소프트웨어)에 따라 각기 다른 인증 절차가 있으며, 영국과 유럽은 같은 인증 절차를 적용하고 있다.

- Mission-Critical: 미션 유효성을 감소시키는 기능의 손실을 의미
- Safety-Critical: 인명의 손실을 야기하는 장애 또는 설계의 결함을 의미

여기서는 국방부분을 제외하고 우주항공과 민간항공 부문에 적용되는 표준 정책에

대해서 다루었다.

2) 미국

(1) NASA의 소프트웨어 안전 표준 체계

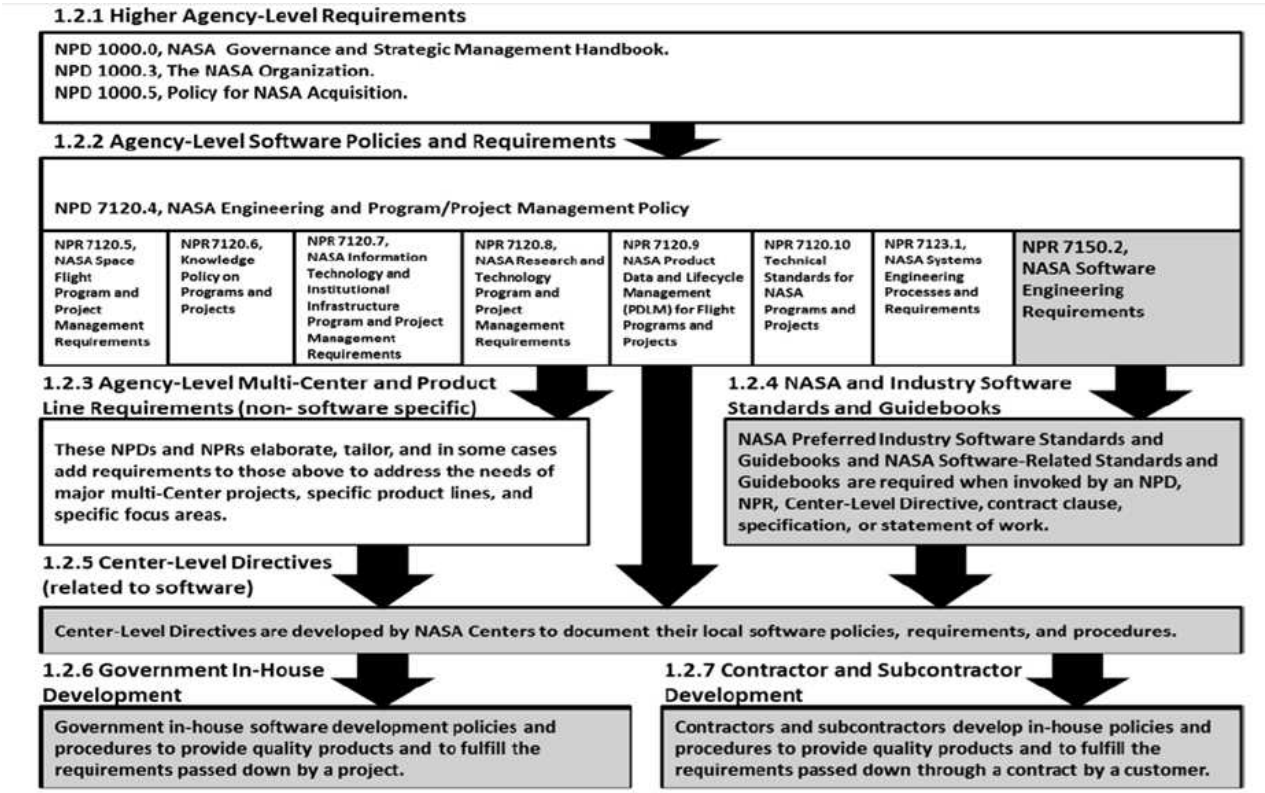
NASA의 소프트웨어 안전 규정은 상위 Agency-Level의 요건으로 시작하여 소프트웨어 안전에 관한 표준 및 가이드로 구체화되어 있다. NASA 소프트웨어 안전에 관해서는 NPR(NASA Processes and Requirements) 7150.2 소프트웨어 공학 요구사항에 명시되어 있는데, NPR 7150.2는 NASA의 임무와 지원 인프라의 핵심 역량과 핵심 가능 기술로서, NASA Policy Directive (NPD) 1000.0, 즉 NASA 거버넌스와 전략적인 경영 핸드북에 포함된 거버넌스 모델에 맞춰 소프트웨어 획득, 개발, 유지보수, 폐기, 운영 및 관리에 관한 요구사항을 설정하였으며, NASA의 NPR은 NASA Policy Directive (NPD) 7120.4의 구현하기 위한 방법으로서 사용된다.

그리고 NPR 7150.2의 소프트웨어 공학 요구사항에 대하여 NPR-STD-8719.13 소프트웨어 표준과 NPR-GB-8719.13 소프트웨어 가이드북으로 구체화하였으며, 센터 수준과 정부의 In-House 개발 및 외주 개발 수준까지 상세한 정책과 절차를 수립하여 전체적인 거버넌스 체계가 구축되어 있다.

[그림 3-9] NPR-STD-8719.13 체계

NASA 표준은 Safety-Critical 소프트웨어에 대하여 센터 수준 기관인 DFRC (Dryden Flight Research Center), ARC (Ames Research Center), JPL (Jet Propulsion Lab) 등에서 사용된다.

[그림 3-10] Relationships of Governing Software Documents



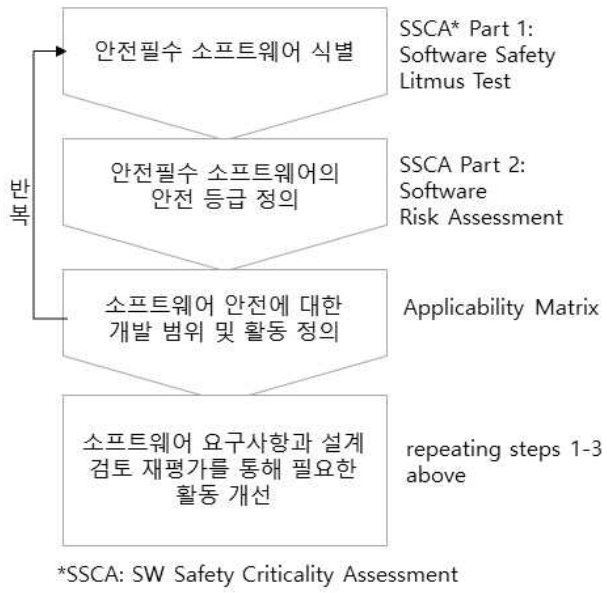
자료: NASA Software Engineering Requirements. 2014. [11]

NASA의 소프트웨어 레벨 정의는 센터마다 약간씩 차이가 발생하기도 하나, 기조는 동일하다. NASA Dryden에서 Class B는 Mission-Critical 소프트웨어를 의미하고 Class A는 Safety-Critical 소프트웨어를 의미한다. 즉, Class A 소프트웨어의 장애는 항공기와 파일럿을 위험에 빠지게 하므로 Class A 소프트웨어 인증에 필요한 테스팅은 Class B보다 더 엄격한 기준이 적용된다. [12]

소프트웨어 안전 표준 (NASA-STD-8719.13)은 Acquirer/Provider의 역할을 정의하고 소프트웨어 안전을 수행하기 위한 진단 단계 및 방법을 제시하여 소프트웨어 안전 활동에 적용하도록 한다. Acquirer(획득자 또는 구매자) 조직은 제공받거나 구매한 소프트웨어에 대하여 소프트웨어의 안전성을 높인 프로그램을 구현하고 이를 위한 충분한 자원을 제공해야 하는 책임이 있으며, Provider(제공자 또는 개발자) 조직 또한 제공하거나 개발하는 소프트웨어에 대해서 안전 프로그램을 구현하고 이를 위한 충분한 자원을 투입해야 하는 책임이 있다. 그리고 Acquirer and Provider SMA(Safety and Mission Assurance)는, 안전절차나 기술적인 구현에 있어서 평가를 하는 독립적인 조직이으로 소프트웨어 안전 라이프사이클에서 안전하지 못한 항목이 발생할 경우, 보고할

책임을 가지며, 개발 중 또는 소프트웨어를 인수하기 전에 상위 조직에 이슈를 상정하고 적절한 수준에서 합의를 받아야 하는 책임을 가지고 있다. 이러한 소프트웨어 안전 임계 평가를 위하여 SSCA(Software Safety Criticality Assessment)의 Part1. Software Safety Limus Test와 Part2. Software Risk Assessment로 소프트웨어 안전필수 여부를 식별하고 소프트웨어 안전에 대한 활동을 수행하고 개선한다. 먼저, Acquirer는 SSCA를 통하여 소프트웨어의 Safety Criticality를 결정하고 Provider는 소프트웨어 기능레벨에서 SSCA를 수행한 다음, 프로젝트 개발이 진행됨에 따라 위해도 분석, 조건 및 이벤트에 대해 적절한 수준에서 이를 수행한다. 시스템과 소프트웨어의 라이프사이클이 진행되는 동안 Provider는 표준 요건을 만족하는 어플리케이션이라는 것을 증명하기 위하여 재평가를 수행하며, Acquirer SMA에게 SSCA의 결과 (즉, Software Safety Criticality와 Software Risk Assessment)가 정확하다는 승인을 득해야 한다. Provider는 품질기록(요구사항)으로 승인받은 SSCA를 관리해야 한다.[13)]

[그림 3-11] 소프트웨어 안전 진단 단계



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

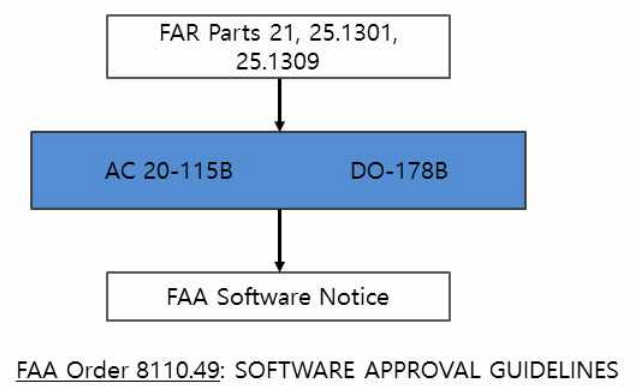
가. FAA 승인을 위한 DO-178B 표준 인증

RTCA 사에 의해 작성된 DO-178B (항공기 시스템과 장비 인증에 관한 소프트웨어

고려사항)는 항공기 시스템과 장비의 소프트웨어 부분이 감항성(airworthiness) 인증 요구사항의 준수 여부를 검증하는 소프트웨어 개발 표준이다. 이 표준은 RTCA와 EUROCAE에 의해 공동 개발되었고, 이를 FAA가 항공기 소프트웨어 인증을 위한 용도로 사용할 것을 승인하여 현재 항공기 소프트웨어를 위한 일반적인 표준 인증으로 자리 잡았다.

즉, FAA는 1993년 1월 11일에 AC 20-115B를 공시하여, 전자 설비 또는 시스템을 사용하는 디지털 컴퓨터 기술에 대하여 TSO (Federal Aviation Administration technical standard order), TC (type certification) 또는 STC (supplemental type certification)를 위한 요청에 대해서 규제 준수를 증명하기 위한 방법으로 RTCA의 DO-178B를 사용할 수 있으며, 이것은 FAR (Federal Aviation Regulations)의 Parts 21, 23, 25, 27, 29 and 33와 관련된다고 명시하였다. 그러나 DO-178B가 디지털 컴퓨터 소프트웨어에 대한 FAA 승인을 확인받는 유일한 수단은 아니라고 명시하였다. 또한 FAA Order 8110.49를 통하여 AIR (Aircraft Certification Service) 분야 사무소와 DER (Designated Engineering Representatives)을 대상으로 DO-178B 표준을 준수하는 소프트웨어에 대한 승인절차 가이드라인을 배포하였다.

[그림 3-12] Flow of FAA Regulations



FAA Order 8110.49: SOFTWARE APPROVAL GUIDELINES

나. RTCA/DO-178B의 소프트웨어 레벨 및 프로세스

DO-178B는 5단계로 소프트웨어를 구분하였으며 Safety-Critical 소프트웨어에 대해서는 더 견고한 인증 절차와 방법이 필요하다는 전체적인 사상은 NASA의 표준과 동일하다. 안전 평가 프로세스(Safety assessment process), 위해도 분석(Hazard analysis)으

로부터 결정된 레벨로서 시스템의 고장 영향성을 판단하는 기준으로 다음과 같은 단계가 있다. [14)]

- Level A: 비정상적인 동작으로 안전 비행과 착륙을 저해하는 치명적인 오류를 야기하는 소프트웨어
- Level B: 비정상적인 동작으로 위해하고 심각한 장애 상황을 야기하는 소프트웨어로서, 위해심각도란, 안전이 위태롭고 승무원의 육체적인 부하가 과도하며, 심각하거나 치명적인 상처를 입을 수 있을 정도로 불리한 운전 상태를 대처하기 위한 항공기 또는 승무원의 능력이 떨어져 있는 장애 상태로 정의함
- Level C: 비정상적인 동작으로 주요한 안전성을 감소시키는 주요한 장애를 야기하는 소프트웨어로서, 승무원의 부하가 가중되거나 승무원의 효율성 저하 또는 사용자의 불편이나 부상 등을 초래함
- Level D – 비정상적인 동작이 작은 장애를 야기하는 소프트웨어로서, 항공기의 안전성을 크게 감소시키기 않고 승무원의 활동의 손상되지 않으나 다소 불편함이 발생함
- Level E: 비행 조정 또는 승무원의 과부하에 영향을 미치지 않는 고장 수준의 소프트웨어

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

<표 3-2> 소프트웨어 레벨에 따른 독립성

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

소프트웨어 레벨(A에서 D까지, E의 경우에는 DO-178B 상 요건이 없음)에 따른 목표를 만족시키기 위해서는 프로세스가 필요하다. DO-178B에서 프로세스 자체가 구체적으로 명확히 기술되어 있지 않으며 추상적인 수준으로 기술되어 있고, 이를 구체적인

실제 프로젝트에서 실행하는 방법에 대해서는 각 프로젝트 계획 단계에서 이를 계획하도록 되어 있다. 그러므로 실제 프로젝트에서는 구체적인 프로세스를 만족시킨다기보다는 DO-178B의 각각의 요건(objectives)을 만족시키기 위한 활동들이 진행된다. 그리고 사실 그러한 활동이 계획 단계에서 수행된다.

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

다. DO-178B와 관련된 표준

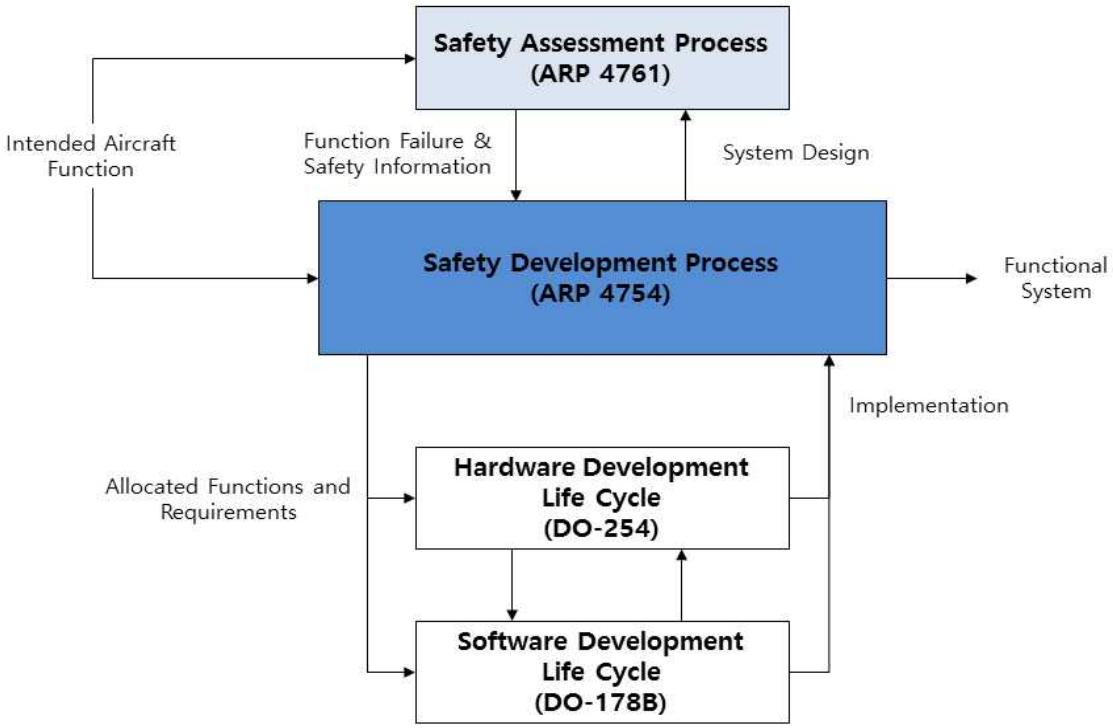
RTCA는 DO-178B를 명확하게 하기 위하여 다음과 같은 문서도 제작하였으며 이러한 문서들도 유럽에 동일하게 적용된다. (DO: RTCA, ED: EUROCAE의 표준을 의미함)

- DO-248B/ED-94B : DO-178B에 적용되는 베스트 프랙티스 설명 문서
- DO-278/ED-109 : 지상 시설, 비행용이 아닌 CNS/ATM (communications, navigation, and surveillance/air traffic management) 시스템에 대한 소프트웨어 표준 문서
- DO-254/ED-80 : DO-178B와 동일하나, 하드웨어에 적용되는 표준 문서

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

- ARP4761 : 항공기의 안전 평가 절차 수행 가이드
- ARP4754 : 항공기 시스템 개발 프로세스 가이드

[그림 3-13] DO-178B와 관련된 표준



자료: RTCA DO-178B Process visual Summary. [15)]

3) 유럽

유럽은 미국과 유사한 체계와 표준을 적용하고 있는데, 미국의 FAA에 대응되는, EASA, JAA 또는 CAA 기관에서 JAR 또는 CS 규정을 적용하고 있다. 다음은 미국과 유럽의 항공 표준의 대응관계를 표시한 것이다.

<표 3-3> 미국과 유럽의 소프트웨어 안전 표준

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

- EASA (European Aviation Safety Agency, 유럽항공안전기구)

- JAA (Joint Aviation Authorities, 유럽항공연합)
- CAA (Civil Aviation Authority, 민간항공기구)
- JAR (Joint Aviation Requirements)
- CS (Certification Specifications)

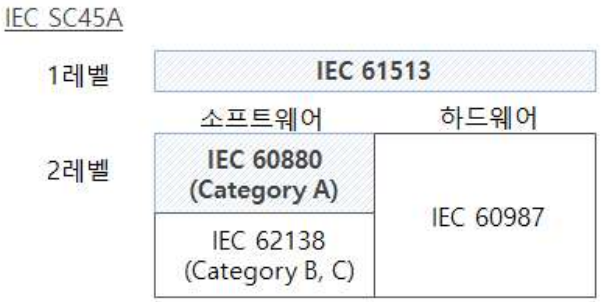
4. 원자력 부문

원자력 부문은 나라마다 원자력 부문의 상황이 다르기 때문에 자국에 맞는 표준을 설정하여 적용하고 있다. 따라서 여기서는 국제표준인 IEC 61513과 IEEE STD 7-4.3.2에 대해 조사한 다음, 미국, 영국, 독일의 소프트웨어 안전 표준 활동을 중심으로 조사하였다.

1) 소프트웨어 안전 관련 주요 표준

IEC 61513 (Functional safety-safety instrumented systems for the Nuclear Industries)은 IEC SC45A (Instrumentation and control (and electrical) systems for nuclear facilities) 표준 시리즈 구조의 첫 번째 레벨 문서로서, 원자력 발전소의 안전시스템에서 사용되는 높은 무결성의 컴퓨터 기반 I&C 시스템의 일반적인 요구사항에 대한 표준이다. IEC 61513은 SIL (Safety Integrity Level) 개념을 사용하고 있지는 않으나, 심각도에 따라 안전 기능을 A, B, C로 분류하고, 작동해야 하는 안전 기능 수준에 따라 시스템 클래스를 1, 2, 3으로 정의하였다. 이 표준은 안전 목표를 달성하고 일반적인 실패원인을 최소화하기 위한 다양한 방법으로 권장한다.

[그림 3-14] IEC SC45A와 하위 안전 관련 표준



IEC 60880은 IEC61513의 참고문서로서, Category A 기능을 수행하는 I&C (Instrucmented & Control) 시스템의 문제를 해결하는 두 번째 레벨의 SC45A 문서이다. 소프트웨어의 전체를 다루기 위해서는 Category B와 C에 대한 표준 문서인 IEC 62138을 같이 활용할 수 있다. 그리고 컴퓨팅 시스템의 하드웨어 SC45A의 표준은 IEC 60987에서 다루고 있다.

IEEE 608 (IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations)은 원자력 발전소 안전 시스템의 전력, 장비, 제어 부문에서 최소한의 기능적 설계 기준으로 수립되었다. 이러한 기준은 공공 보건과 안전을 도모하기 위하여, 설계 기준 이벤트의 영향을 완화하는 기능이 필요한 시스템에 적용된다. 이 표준의 목적은 안전시스템 성능과 신뢰성에 대한 설계 및 평가를 위한 안전한 방법을 향상시키는 것이다. 이 표준은 안전 시스템에 국한되지만, 표준에 포함된 원리들은 안전과 관련된 안전한 종료, 사고 후 모니터링 디스플레이 기기, 예방 연동 기능, 임의의 다른 시스템들, 구조 또는 장비들에 제공되는 장치에 적용가능하다.

IEEE STD 7-4.3.2 (Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations)는 IEEE STD 603의 기준과 요구사항을 보완하기 위하여 추가적으로 컴퓨터의 특정 요구사항을 명시하였다. 이 표준에서 컴퓨터라는 용어는 컴퓨터 하드웨어, 소프트웨어, 펌웨어 및 인터페이스를 포함하는 시스템을 지칭하며, IEEE STD 603의 기준과 함께 안전 시스템의 구성요소로 사용되는 컴퓨터에 대한 최소한의 기능과 설계 요건을 설정해 놓았다. [16)]

아래는 표준에 따른 다양한 안전성 등급을 표시하였다. 국제표준뿐만 아니라 국가마다 안전성 등급에 차이가 나타난다.

[그림 3-15] 표준에 따른 안전성 등급

National or international standard	Classifications
IAEA	Safety system Safety related system Systems not important to safety
IEC	Category A Category B Category C Unclassified
France N4	1E 2E Important for safety (unclassified)
EUR	F1A (Automatic) F1B (Automatic and Manual) F2 Unclassified
Russia	Class 1 (Beyond DBA) Class 2 (Safety system, DBA) Class 3 Class 4
UK	Category 1 Category 2 Unclassified
USA (IEEE)	1E Non-nuclear safety

자료: IAEA. Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants. 2009 [17]

2) 미국

원자력 안전은 NRC (Nuclear Regulatory Commission, 원자력규제위원회)에서 발의한 연방 규정에 의해서 관리된다. NRC는 해군군함의 동력 뿐 아니라 미국 내 모든 원자력발전소와 자재를 관리/감독한다. (미국정부에서 관할하는 원자력발전소와 자재는 제외)

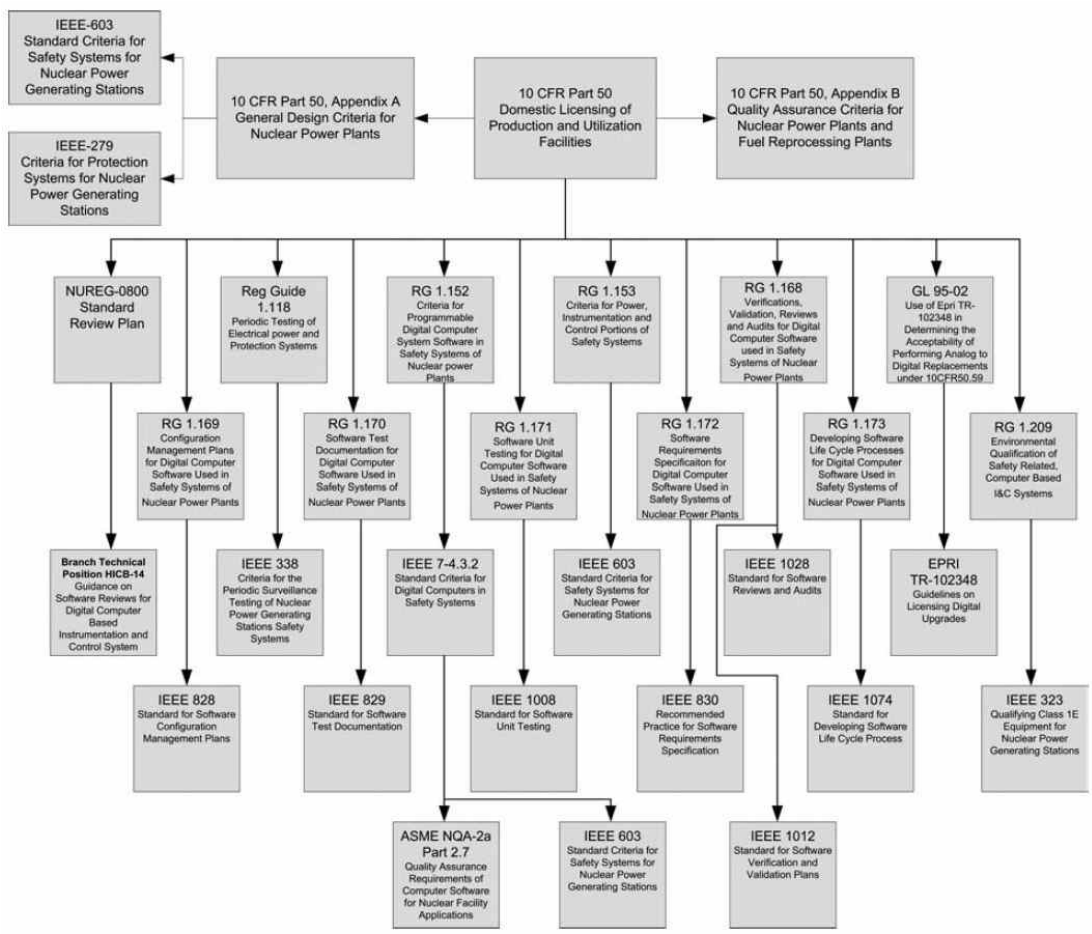
원자력 규제와 관련된 규정인, 10 CFR Part 50 (Domestic Licensing of Production and Utilization Facilities, 제조와 이용시설의 국내 허가)는 1954년 원자력법과 1974년 에너지 개편법 Title II에 따라 NRC에 의해서 발표되었고, 사용권자, 신청자, 계약자, 하청계약자, 사용권자나 신청자의 활동과 관련된 부품, 설비, 재료, 다른 상품 또는 서비스를 고의적으로 제공하는 모든 사람들에게 10 CFR Part 50.5 조항을 통하여 고의적 위법에 대해 NRC가 개별적으로 강제조치를 적용할 수 있다고 제정되어 있다.

NRC는 10 CFR Part 50의 Appendix B (Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants)에서 종합적인 QA 프로그램에 대한 기본적인 요

구사항을 설정하였고 Regulatory Guide 1.152를 통하여 컴퓨터의 기능과 설계 요구사항에 대한 규정 준수의 방법으로 IEEE Std 7-4.3.2를 적용할 수 있다고 발표했다.

“ IEEE Std 7-4.3.2-2003 (원자력 발전소의 안전 시스템에서 디지털 컴퓨터에 대한 표준 기준)의 요구사항 준수는 NRC 담당자가 원자력 발전소의 안전 시스템에서 사용되는 컴퓨터의 고기능 신뢰성과 설계 요구사항에 관한 NRC의 규정을 충족한다는 것을 허용하는 방법이다.”

[그림 3-16] 미국의 디지털 I&C 구현 및 라이센스 관련 문서



자료: IAEA. Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants. 2009 [17]

미국은 시스템을 단순하게 안전성 (Class 1E) 또는 비안전성으로 분류한다. 규제기관은 Class 1E로 분류된 시스템을 검토하는데 관여하고, 비안전성 시스템에서 디지털 장치는 자유롭게 설치가 가능하다.

원자력 산업과 규제기관이 NPP(Nuclear Power Plant, 원자력발전소)에서 소프트웨어

기반의 디지털 장치를 설치할 때 일어나는 문제를 더 많이 알게 됨에 따라, NRC는 보수적인 접근법으로 안전 시스템 (Class 1E)에서 소프트웨어의 사용은 해결되지 않은 안전 문제였다는 Generic Letter를 제출했다. 이에 대한 대응으로, EPRI (Electric Power Research Institute)은 NUMARC (Nuclear Management and Resources Council)와 NPP에서 디지털 업그레드를 허가하기 위한 가이드라인을 개발하는 프로젝트를 시작하였고, 산업 대표와 규제기관들의 검토 후에, 그 결과를 1993년에 EPRI TR-102348로서 발표했다. EPRI 보고서는 안전 시스템에서 디지털 시스템을 설치할 때 발생하는 설계와 라이선스 문제를 해결하기 위한 가이드이며 NSAC-125와 NSAC-105의 가이드를 보완하기 위한 목적을 가지고 있다. NRC는 공식적으로 이 가이드라인을 지정하지는 않았으나 사용을 권고한다. [18)]

3) 영국

영국의 원자력산업의 법률적인 프레임워크는 보건안전법 (HSWA, Health and Safety at Work etc. Act 1974), 에너지법 2013 및 원자력설치법 1965에 기초한다. 보건안전법 HSWA에는 원자력 산업에 종사하는 사람들을 포함하여 모든 고용주들에게, 근로자들과 공공의 건강과 안전을 돌보도록 의무를 부과한다고 명시하여 원자력 사용권자들의 공공 건강에 대한 책임을 부여하였으며, 특히 원자력 설치법 1965는 원자력 산업에 대해 규정하였고, 에너지법 2013 하위규정에 이온화 방사선 규정 1999 (IRR99)과 방사선 (비상사태대비와 공공정보) 규정들 (REPPIR)과 같이 원자력과 관련된 규정을 마련해 두었다. 원자력 규제 활동은 대표적으로 ONR(Office of Nuclear Regulation, 원자력규제사무국)이 원자력 발전소에서 원자력 시설의 안전성을 위한 일상적인 운영 활동과 잠재적인 사고에서 방사선 노출 위험을 제어하는 활동을 모두 규제하는 책임을 가지고 있으며, 이외에도 잉글랜드, 웨일즈와 스코트랜드에 있는 다양한 환경 규제기관들이 대기 속으로 방사선 물질이 방전되는 것을 규제한다.

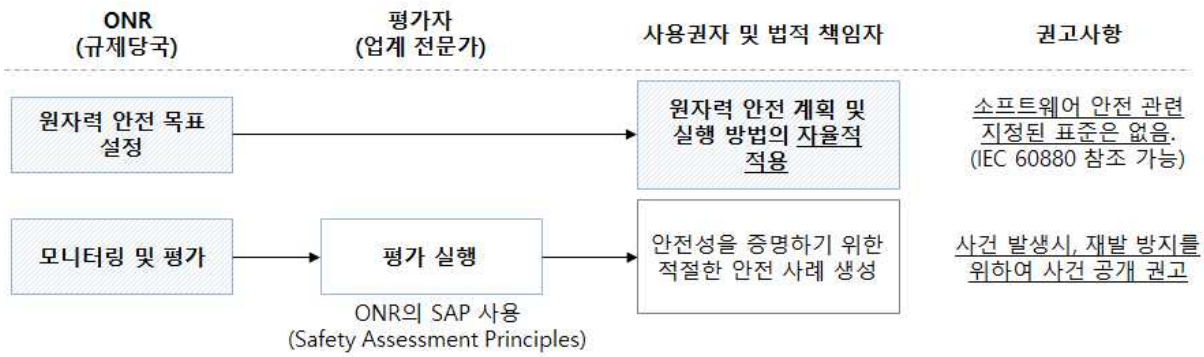
ONR은 영국에서 원자력 발전소를 규제하는 책임을 가지고 있으나, 원자력 안전을 보증하는 법적인 책임은 전적으로 사용권자에게 있다. 정부의 책무는 법적인 규제 프레임워크를 통해서 원자력 정책을 수립하는 것이며, 규정 표준을 설정하거나 규정을 결정하는 것은 아니다.

영국은 일반적으로 다른 국가에서 적용되는 권위적인 표준 기반 체계(Standard-based regime)보다는 목표설정체계(Goal-Setting regime)를 운영한다. 즉, ONR이 규정에 대한 기대치를 설정해 놓으면 사용권자들은 그것을 달성하기 위해 필요한 가장 좋은 방법

을 스스로 결정하고 판단한다. 이러한 접근 방법으로 운영자는 특정 환경을 충족하기 위한 실행방법을 적용함으로써 혁신적으로 높은 수준의 원자력 안전성을 달성하게 된다.

ONR의 안전 보장에서 중요한 부분은 사용권자들의 내부 레귤레이터나 보증 기능의 성능을 모니터링하는 것으로서 유용한 정보를 제공하고 현장 검사계획 개발 및 평가에 도움을 주는 것이다. 사용권자는 안전성에 영향을 끼치는 운전에 대해서 안전성을 증명하기 위한 적절한 안전 사례를 생성해야 하고, 전문적 자질과 원자력 발전소 또는 유사 업계에서 광범위한 경험을 소유한 전문가들로 구성된 평가자들이 ONR의 Safety Assessment Principles를 가이드로 사용하여 평가를 수행한다. 영국은 IEC 60880을 주요 레퍼런스로 사용하기는 하나, 원자력 발전소의 소프트웨어에 적용하는 특정 표준은 정해져 있지 않다. 원자력 발전소는 이상 현상, 사건 또는 심각도에 따라 사고라고 할 수 예상치 못한 이벤트가 발생할 수 있는데 그러한 사고의 재발을 방지하기 위해, ONR에서는 사용권자와 사이트의 법적 의무를 가진 사람들에게 사건을 공개하도록 권장한다. 영국은 보고된 사건을 평가하기 위한 방법으로 국제 원자력 및 방사선 이벤트 척도(INES)를 사용한다. 이 척도는 사고(Accident) 영역에 대하여 Level 4~7로 분류하고 사건(Incident) 영역에 대하여 Level 1~3으로 분류되어 있다. 2011년 후쿠시마 원전 사고와 1986년 체르노빌 사고는 Level 7로 지정되어 있으며, 영국에서는 1957년 Windscale 화재가 유일하게 Level 5로서 사고영역으로 분류되어 있다.

[그림 3-17] 원자력 규제 관련 목표 설정 체계



[그림 3-18] The IAEA International Nuclear and Radiological Event Scale

자료: ONR. A guide to Nuclear Regulation in the UK.. 2014 [19]

4) 독일

독일에서 원자력과 관련된 법규정 구조는 일반적 또는 관계당국에 대해 구속력을 가지는 상위법과 라이선스나 감독/조치 건에 대하여 구속력을 가지는 하위 규정의 피라미드 형태로 설명된다.

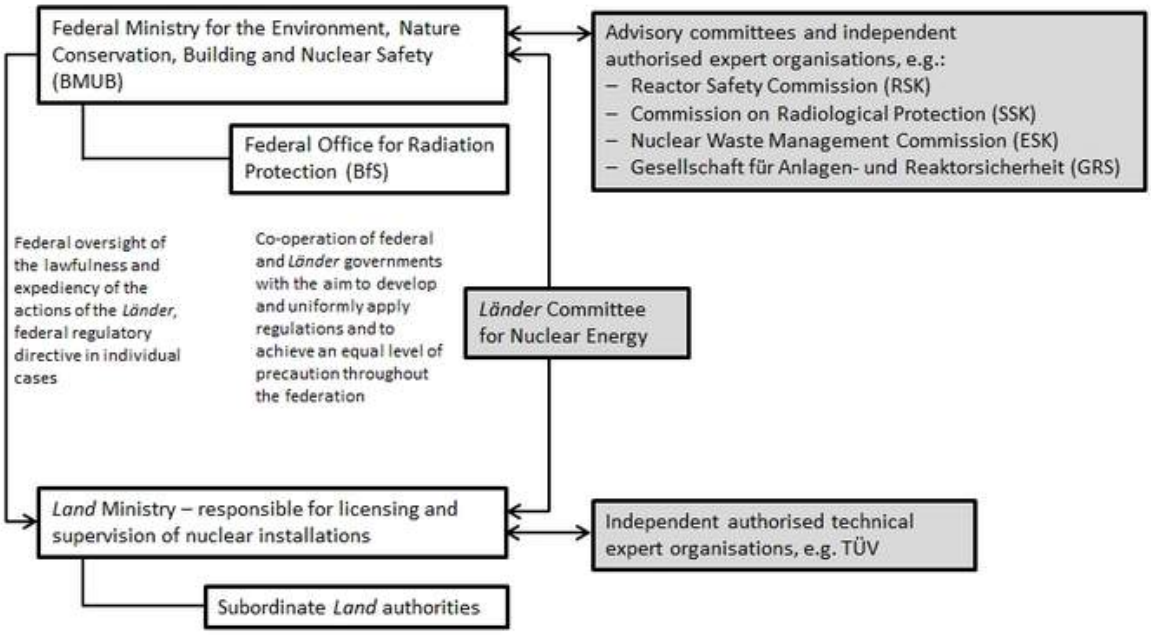
피라미드 규정의 상단에는 구속력이 있는 기본법, 원자력법 및 일련의 법령이 있으며, 일반적인 요구조항이 포함되어 있다. 기본법은 특히 생명과 신체의 완전성에 대한 기본적인 권리를 정의하여 원자력 시설에서 보호 및 예방 조치에 적용되는 규정을 결정하는 상위법이다. 원자력법은 보호 및 예방 조치, 방사선 보호 및 방사선 폐기물질처리와 소비연료에 대한 일반적인 규정으로서 관련법령의 기본이 된다. 법령은 연방의회의 승인이 필요하며 보호 및 예방 조치를 실체화하여 효력을 발생시킨다.

피라미드의 하위단에는 연방환경부의 출판물, KTA(Kerntechnischer Ausschuß , 원자력안전기준위원회) 표준 및 종래의 기술 표준이 있다. 이러한 규정은 일반적으로 구속력이 있지는 않으나, 구체적인 요구사항을 포함하고 있다.

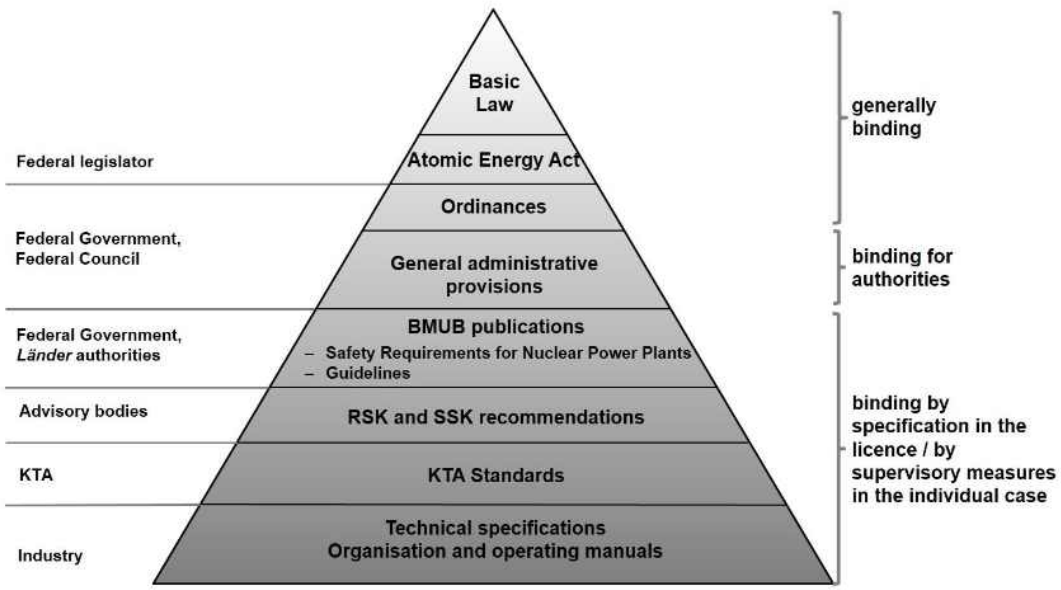
원자력규제기관은 BMUB (Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, 환경, 자연 보호, 건설 및 원자력 안전에 대한 연방정부부처)가 책임을 맡고 있으며, 그 하위 조직으로 BFS (Bundesamt für Strahlenschutz, 방사선보호연방사무국)에서 원자력관련 안전 및 보호에 대한 책임을 부여받고 있다. 각 주정부에서

는 원자력 설치에 대한 허가와 감독을 담당하며 연방정부와 주정부의 협업을 통하여 일관된 규정을 적용한다.

[그림 3-19] 원자력 법 규정에 관련된 조직



[그림 3-20] Nuclear regulatory pyramid



자료: Bundesamt für Strahlenschutz. Nuclear safety – legal bases, 2015. [20)]

독일의 I&C (Instrument and Control) 기능과 설비 안전 요구사항은 KTA의 KTA 35XX 시리즈 (원자력 기술 지침)에 명문화되어 있다. 그러나 컴퓨터나 소프트웨어에 특화된 지침을 없기 때문에 높은 수준의 소프트웨어 요구사항이 KTA 지침에서 나와야 한다. 좀 더 상세한 요구사항에 대해서 DIN (Deutsches Institut für Normung e.V., 독일표준연구소)은 국제표준인 IEC 880을 국가표준으로 채택하여, DIN IEC 880이 소프트웨어의 V&V에 사용되는 주요 표준이 되었다.

독일의 라이선스 절차는 유형평가와 적합성평가로 구분된다. 유형평가는 모든 발전소에서 아날로그에서 디지털 시그널로 변환되는 부품과 같이, 동일한 방식으로 적용되는 부품에 대한 평가이고, 적합성 평가는 발전소 특화된 시스템 특성을 고려한다. 분산된 I&C 컴퓨터 시스템에 소프트웨어로 구현된 I&C 기능들에 대하여, 구현 툴에 대한 구성요소들은 IEC 880과 IEEE 표준의 요구사항에 따라 정의되고 평가된다.

원자력 시설의 건설과 운영에 대해서 기존의 기술표준을 보조적으로 적용하고 있다. 표준은 DIN 국가표준과 ISO와 IEC의 국제 표준을 최소한도로 적용한다. 그러나 더 엄격하거나 다른 요구사항이 생성되거나 허용되었을 경우라도, 원자력법과 관련된 연방정부 또는 주정부의 규정은 이러한 표준에 영향을 받지 않는다.

독일의 표준 활동은 DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, DIN과 VDE의 전기/전자/정보기술 위원회)와 VDI (Verein Deutscher Ingenieure, 독일 엔지니어 협회)에서 수행되고 있다. (VDE: Verband der Elektrotechnik, Elektronik und Informationstechnik, 전기/전자/정보기술협회)

먼저, DKE는 전기, 전자, 정보기술 분야에서 표준과 안전규정을 개발하는 국가조직으로서, DKE 업무 결과물은 독일표준의 중요한 부분이다.

DKE Committee K132는 신뢰성 표준을 취급하는데, 신뢰성은 제품이나 장시간 동안 품질을 유지하기 위한 기술적인 시스템의 성능을 말한다. DKE는 신뢰성에 대한 소프트웨어 측면의 가이드라인인 DIN EN 62628 (2012)과 신뢰성 관리-시스템 신뢰성의 기술적인 구현을 위한 소개인 E DIN IEC 60300-3-15 (2006)을 해석하였다. 독일에서 전기공학, 기기 및 제어시스템 소위원회 (UK 967.1)은 소프트웨어 기반의 I&C 시스템의 요구사항을 포함한 표준을 다루고 있으며, 수정 및 초안에 대한 해석서는 점차적으로 표준을 개발하는 과정으로 이동되고 이들은 독일 표준 체계로 번역되어 통합된다. 단, 상위의 국가 차원의 원자력 지침과 규정에 대한 요구사항과의 일관성은 유지되어야 한다.

VDI, 독일 엔지니어 협회는 기술적인 가이드라인에 대한 종합적인 프로그램을 발표한다. 가이드라인은 전문가 위원회에서 개발되고 표준의 개발 또는 업그레이드의 기초로 주로 제공된다. 전문가 위원회 7.11 (원자력 발전소의 계측 및 제어)은 GMA (VDI/VDE 사회 측정 및 자동화 제어)의 부분으로서, GMA는 VDI와 VDE의 기술-과학 협회의 전문가 패널이다. GMA는 약 65개 이상의 전문가 위원회와 이사회에서 전문 업무를 다루고 이 분야의 경험을 교류한다. GMA 전문가 위원회 7.11은 원자력 발전소에서 안전 관련사용을 위한 산업의 연속적인 제품 적용성에 대하여 기술적 가이드라인을 개발 중에 있다. [21)]

5. 조사결과 요약 및 시사점

해외 산업 도메인별 소프트웨어 안전 관련 선진국의 활동 현황 조사 결과, 조사한 산업 도메인에서는 최소 한 개 이상의 소프트웨어 안전 표준이 존재하였다. 다만, 법/제도 및 정부의 안전 활동 측면에서 보면, 대부분의 소프트웨어가 실제로는 전자전기 시스템 內에서 동작되는 관계로 소프트웨어 안전 표준이 별도로 구별되어 법/제도 및 안전 활동 요구 사항으로 제시되어 있지 않고(Explicitly), 전기전자 부품/시스템 또는 제품 수준에서 안전한 부품/시스템/제품을 만들기 위해 준수해야할 법/제도 및 표준에 준수해야 할 항목으로 포함되어 규정화 되어 있었고(Implicitly), 정부 기관 및 인증기관 등을 통해 적용되고 있었다. 자동차 경우는 특이하게, 국제 표준(ISO 26262)이 존재하나, 법/제도적으로 명문화 되거나 정부차원에서 관리되지 않고, 사고 발생시 제조물 책임법 하에 사고를 유발한 부품/시스템이 최신 기법을 사용해서 개발 했다는 것을 증명하는 부분에서 소프트웨어 안전 최신 기법으로 ISO 26262가 인정받고 있어, 업체들이 자발적으로 준수하게 되어 있었다. 이 때문에, 모든 자동차 제조사가 일괄적으로 ISO26262를 준수하기보다는, 차량 판매가 높은 선도 기업부터 자발적으로 준수하고 차츰 중/하위 기업으로 범위가 확대되는 중이었다. 철도분야의 표준은 크게 미국과 유럽으로 구분이 되며 이것은 철도의 사용용도가 다르기 때문이었다. 미국은 화물 수송 중심의 저속 철도인 반면에 유럽은 승객 수송 중심의 고속 철도용도이므로 미국은 미국 실정에 맞는 AREMA 표준을 적용하고 유럽은 EN 50128을 사용하였다. 항공분야의 표준은 우주항공, 국방과 상용항공으로 구분되어 표준화가 되었고 상용항공의 경우는 미국의 RTCA와 유럽 EUROCAE의 공동연구를 통하여 개발된 표준을 적용하고 있었다. 원자력 분야는 국제 표준이 있기는 하나, 각 나라가 자국에 맞는 표준과 안전 등급을

정의하여 사용하고 있었다. 특히 영국은 대부분의 나라에서 적용되는 권위적인 표준 기반 체계(Standard-based regime)보다는, 사용권자가 설정된 목표에 도달하기 위한 방법을 스스로 결정하고 실행하는 목표 설정 체계(Goal-setting regime)를 운영하고 있었다. 자동차, 철도, 항공 및 원자력의 산업도메인별 국가별 소프트웨어 안전에 관한 주요 활동은 아래와 같이 요약된다.

<표 3-4> 산업도메인/국가별 소프트웨어 안전 표준 요약

<table>
<tr><th>산업도메인</th><th>미국</th><th>유럽</th><th>일본</th></tr>
<tr><td rowspan="3">자동차</td><td colspan="2">• 자동차 소프트웨어 안전에 대한 법적 요구사항은 표현되어 있지 않음
• 단, 자동차, 자동차 시스템, 자동차 부품 차원에서 안전표준 제시</td><td rowspan="3">• 정부 연구 기관과 완성차 및 자동차 부품 업체 등이 협력하여, ISO 26262 도입 추진
• 정부 연구 기관은 각 업체들의 업무 부담을 경감하기 위해 표준 해석, 공통 활동 및 문서 제작 등의 선도적 역할 수행</td></tr>
<tr><td colspan="2">• 제조물 책임법에 의한 현재 State of the Art인 ISO26262 표준을 준수하도록 간접적으로 유도하는 방식</td></tr>
<tr><td>• NHTSA의 자국 자동차 판매에 대한 안전 표준 준수 여부 검사를 통한 리콜이나 벌금형의 제재조치</td><td>• 자동차 판매 전, 형식인증을 통한 검사를 수행하고, EEC/ECE 법규의 인가를 받은 다음, 각 나라의 인증을 받아야 판매 가능</td></tr>
<tr><td rowspan="4">철도</td><td>• 화물 운송 및 저속 운송 중심</td><td>• 승객 운송 및 고속 운송 중심</td><td rowspan="4">• 문헌자료 부족</td></tr>
<tr><td>• AREMA C&S Manual Part 17.3.1~3 (규정)</td><td>• 철도 안전 및 상호 운용 관련 지침 제정 (Directive 2004/49/EC, 2008/57/EC)</td></tr>
<tr><td>• AREMA 2011 C&S Manual 표준</td><td>• EN 50128 / IEC 62279 표준</td></tr>
<tr><td>• 철도 사업자들은 자기들만의 프로세스, 절차, 분석 방법과 문서를 통해 FRA 규정의 요구사항을</td><td>• 철도 인증을 득하기 위해서는 TSI의 요구사항(EN 50128 포함)에 따라 개발, 검사하는 인증을 받</td></tr>
</table>

	만족하면 인증을 받을 수 있는 방식	는 강제화 방식	
항공	• 우주항공: NASA 표준체계 적용 • 상용항공: DO-178B/ED-12B 적용	• 상용항공: DO-178B/ED-12B 적용	• 문헌자료 부족
	• FAR (Federal Aviation Regulations)에 명시 • 전자 설비 또는 시스템을 사용하는 디지털 컴퓨터 기술에 대한 규제준수 증명 방법으로 DO-178B 사용가능 • FAA Order 8110.49 DO-178B에 대한 승인절차 가이드라인 배포	• 유럽은 미국과 유사한 체계와 표준 적용 • 미국의 FAA에 대응되는, EASA, JAA 또는 CAA 기관 있음 • FAR에 대응하는 JAR 또는 CS 규정	
원자력	• NRC는 10 CFR Part 50의 Appendix B (Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants)에 QA요구사항 설정 • Regulatory Guide 1.152에서 컴퓨터의 기능과 설계 요구사항에 대한 규정 준수 방법으로 IEEE Std 7-4.3.2의 적용 가능하다고 명시 • 시스템을 단순하게 안전성(Class 1E) /비안전성으로 분류	**[영국]** • 보건안전법 (HSWA, Health and Safety at Work etc. Act 1974), 에너지법 2013 및 원자력설치법 1965에 의하여 ONR 관리감독 • 목표설정체계 ONR:규제책임, 사용권자:안전보증책임 • ONR의 SAP(Safety Assessment Principle) 가이드로 평가 수행 • IEC 60880을 주요 레퍼런스로 사용하기는 하나, 원자력 발	• 문헌자료 부족

		전소의 소프트웨어에 적용하는 특정 표준 없음 **[독일]** • 원자력법/법령, KTA 표준 • 컴퓨터나 소프트웨어에 특화된 지침으로, DIN은 DIN IEC 880을 소프트웨어 V&V에 사용되는 주요 표준으로 사용 • 표준화활동은 DKE와 VDI에서 수행	

제2절 해외 시장 현황 조사

1. 해외 TIC (Testing, Inspection and Certification) 선진사 현황

1) 일반 현황 (Company Profile)

SGS, Bureau Veritas, Intertek, Dekra, DNV GL 5개 기업은 대략 100년 이상의 역사를 가지고 있는 회사로 구성되었으며 주로 유럽을 중심으로 활동을 하고 있다. 이들 기업의 2010년 이후 5년간 연간실적보고서를 조사해 본 결과, 매출 실적으로 살펴 본 성장세는 최소 5%에서 최대 22%까지 나타난다. 특히, DNV GL의 경우, 성장세가 상대적으로 큰 이유는 앞에서 언급했다시피 2013년 DNV와 GL의 합병에 의한 매출 및 인력의 확대에 의한 것이다.

인력 현황은 full time employee를 기준으로 산정된 것으로 보통 8.5% ~ 9% 정도의 안정적인 인력 증가 추세를 보이고 있다. 이러한 매출의 신장과 인력의 유입 증가세는 대체적으로 TIC 시장이 계속 확장될 전망이라고 예측해 볼 수 있겠다. 매출 부분에서 주목할 점은 2014년의 매출 기준 DNV가 5위로 부상한 것이다. 이것은 2011년 Intertek이 Moody를 합병하여 업계 3위 규모가 된 것과 마찬가지로 2013년 DNV가 GL을 합병하여 나타난 결과이다.

<표 3-5> TIC 매출 상위 기업의 일반 현황 (단위: $ millions)

TIC 상위 기업	본사	설립연도	2014 매출
SGS	스위스	1878년	6,233
Bureau Veritas	프랑스	1828년	4,601
Intertek	영국	1880년	3,236
DEKRA	독일	1925년	2,768
DNV GL	노르웨이	1864년	2,661

<표 3-6> TIC 매출 상위 기업의 매출 현황 (단위: millions)

TIC 상위 기업 (화폐단위)	2010년	2011년	2012년	2013년	2014년	CAGR (2010~2014)
SGS (CHF)	4,757.0	4,797.0	5,569.0	5,830.0	5,883.0	5.5%
Bureau Veritas (EUR)	2,929.7	3,358.6	3,902.3	3,933.1	4,171.5	9.2%
Intertek (GBP)	1,374.0	1,749.0	2,054.0	2,184.0	2,093.0	11.1%
DEKRA (EUR)	1,589.0	2,006.9	2,164.2	2,310.9	2,509.8	12.1%
DNV GL (NOK)	9,792.0	10,156.0	12,532.0	15,234.0	21,623.0	21.9%

<표 3-7> TIC 매출 상위 기업의 직원 수 현황 (단위: 명)

TIC 상위 기업	2010년	2011년	2012년	2013년	2014년	CAGR (2010~2014)
SGS	60,321	67,633	76,790	80,510	83,515	8.5%
Bureau Veritas	47,969	52,148	58,924	61,581	66,494	8.5%
Intertek	27,044	31,712	34,882	36,864	38,407	9.2%
DEKRA	24,869	27,321	28,340	32,591	35,021	8.9%
DNV GL	8,440	8,453	10,294	16,107	15,712	16.8%

2) 소프트웨어 안전 관련 주요 제공 서비스 및 활동

(1) SGS

SGS는 기능안전영역에서, 소프트웨어 안전과 관련된 국제표준 IEC 61508, ISO 26262를 적용하여 Automotive, Industrial Manufacturing, Consumer Goods and Retail 산업영역에서 테스팅, 컨설팅, 인증 및 교육 서비스 등을 제공하고 있다.

SGS의 기능 안전 전문가들은 구성품 및 제품과 관련한 국제표준을 준수하는 안전 프로세스 개발을 지원한다. SGS는 TUV와 단일 단위의 기능안전팀을 운영하는데, 이것은 기능 안전 공인 기관으로서, 제품이나 시스템의 안전성 확인, 제품안전에 대한 법적 증명 인증서 발행 및 관련 표준 요구사항에 대한 컨설팅을 제공한다. 기능 안전에 관한 서비스는 아래와 같이 교육훈련과 개인자격부문, 컨설팅, 안전성 분석 그리고 테스팅/인증으로 구분할 수 있다.

- 교육훈련과 개인자격: 기능안전 전문가, 품질, 개발자, 관리자 및 법률전문가 대상의 일반 과정 또는 기업 특화 과정 제공
- 컨설팅: 기능안전에 관한 개념부터 종결까지 전 범위 포함
- 안전성 분석: 안전성 극대화를 위해 아래의 도구를 이용하여 장애 및 솔루션 식별
  - Failure Mode and Effects Analysis (FMEA)
  - Failure Tree Analysis (FTA)
  - Markov Analysis
  - Reliability Block Diagram (RBD)
- 테스팅/인증: 개념, 체계, 제품 및 절차의 평가와 평가/감리보고서, 인증서, 시험인증 발행

또한, 신규 표준 작성 과정에 참여하여, ISO 26262와 관련된 ISO그룹 TC22/SC3/WG16나 IEC61508과 GK914 같은 많은 표준위원회에서 활동하고 있다. 그리고 SGS와 TUV가 단일 단위의 기능 안전팀을 운영함으로써 고객에게 TUV의 브랜드와 SGS의 노하우를 동시에 제공하고 있다.

SGS는 새로운 시장을 확장하고 다양한 서비스를 제공하고자 유능한 중소기업의 인수에 지속적인 관심을 기울이고 있으며, 2014년에는 자동차, 환경, 소비재서비스 분야에서 북미 3개 기업 (자동차, 환경), 유럽 6개 기업 (공업, 자동차, 환경, 소비재), 일본 1개 기업 (소비재) 등 총 10개 기업을 인수했다.

(2) Bureau Veritas

Bureau Veritas 또한 지속적으로 글로벌의 확장을 추진하고 있는데, 이미 캐나다에서는 글로벌 리더로 활동하고 있으며 Bureau Veritas의 중국 오피스는 직원수 측면에서 이미 No.1을 차지하고 있다. Bureau Veritas는 해외의 기술 원천 개발과 혁신적인 신규 서비스 론칭을 위한 노력을 계속적으로 추진하고 있으며, 특히 북미와 아시아 지역으로 확장하고 있다. 이의 결과로 2013년과 비교해 볼 때, Bureau Veritas의 지역별 매출비중은 북미지역이 3% 증가, 유럽은 2% 감소, 아프리카/중동/동유럽은 2% 감소, 아시아태평양은 1%가 증가된 것을 확인할 수 있었다. (<표 3-4> 참조)

<표 3-8> Bureau Veritas의 지역별 매출, 인력, 사무소 현황 비교

구분		북미	유럽	아프리카, 중동, 동유럽	아시아 태평양	비고
매출비중 (%)	2014년	**27%**	33%	12%	**28%**	북미: 성장세가 두드러짐. 아태: 점차 증가 추세.
	2013년	24%	35%	14%	27%	
인력 (명)	2014년	**20,100**	14,400	9,000	**23,000**	
	2013년	16,300	14,000	9,600	21,700	
사무소 & 실험실 수	2014년	**330**	400	260	**410**	
	2013년	270	380	290	390	

Bureau Veritas는 기능안전관련 검사, 테스팅, 인증과 더불어 업무와 관련된 가이드 작성에도 참여를 하고 있다. 최근에 진행하고 있는 것으로는 첫째, 임베디드 소프트웨어의 테스팅과 위험평가에 관한 가이드이다. 현대에 들어와서 임베디드 소프트웨어는 자동차, TV에서 심박조율기, 선박 및 비행기까지 제조된 제품의 하드웨어를 대체하고 있는데, 임베디드 소프트웨어는 장비와 통합되어 있으며 기계 인터페이스를 통하여 제어되는 부분이기 때문에, 성능과 실패 위험에 대한 평가가 어렵다. 그래서 프랑스 공공연구기관인 CEA LIST와 함께 화이트박스 접근에 기초한 임베디드 소프트웨어에 대한 인증 가이드라인을 발표할 계획이며, 이것은 소프트웨어의 구조와 코드를 분석하기 위한 방법을 설정한 것으로서, 시스템의 원래 사양에 대한 소프트웨어의 안전성과 성능을 테스트하고 중대한 위험을 평가하기 위해서 설계되었다.

두 번째는 철도 수송의 안전성에 대하여 전 프로젝트 라이프사이클동안 위험관리를 위한 10가지 황금률을 제시하는 국제 가이드를 출판했다. [23)]

Bureau Veritas의 소프트웨어 안전과 관련된 업무영역 중에서는 주요 도메인영역인 자동차와 항공부문의 기업 지원활동에 대하여 조사하였다.

자동차 분야에서는 전자/전기 자동차 시스템의 기능 안전 부합성을 입증하는 자동차 기능안전 평가와 지원업무를 수행하고 있다. 자동차 부문의 국제표준은 기능안전 문제를 다룰 때, 공통 위험 접근법에 기초하여 전체 공급망을 지원하는 구조이다. 그래서 기업은 국제표준에 따라 도로차량의 기능안전에 포함된 모든 엔티티를 고려하여, 차량 수준의 기능 또는 장비 수준의 아이템이 정의되면, 평가를 통하여 기능 안전이 달성되었다는 것을 증명해야 한다. 참고로, 차량 수준은 몇 개의 시스템과 공유하는 기능을 포함하고, 아이템 수준은 차량 수준의 기능을 구현하기 위한 시스템 또는 시스템의 집

합체를 의미한다. 이에 대하여 Bureau Veritas는 기술적, 방법론적인 전문성을 기초로 차량 수준 또는 아이템 수준으로 설계된 시스템의 기능 안전을 평가하고 ISO 26262에 따라 프로세스를 개발할 때, 기업 지원과 훈련까지 제공하며, BNA (Bureau of Automotive Standardization, 자동차 표준화국) 등의 국가 및 유럽 기술위원회에 적극적으로 참여하고 있으며, 이것을 통하여 규제의 진화를 예측할 수 있다.

[그림 3-21] 기능 안전 관리

자료: Bureau Veritas. ISO 26262 - Automotive Functional Safety Assessment & Support. 2013 [24]

상황과 필요에 따라 지원, 교육훈련 및 평가의 3가지 서비스를 수행할 수 있다. 기능 안전평가 절차는 4가지 단계로 수행된다. 1. 평가를 위한 안전 활동과 문서 정의. 2. 표준에서 요구하는 워크 제품 평가 3. 문서작성과 현장 감리 4. 평가결과가 담긴 기능 안전 보고서 발급.

[그림 3-22] 기능 안전 평가 절차

자료: Bureau Veritas. ISO 26262 - Automotive Functional Safety Assessment & Support. 2013 [24]

항공 분야에서는 EASA인증, EASA PART 21J 디자인 조직 승인(DOA)과 EASA PART 21G의 생산 조직 승인(POA)을 달성할 수 있는 설계와 생산영역의 인증 절차를 운영하고 있다. 그것은 Type-Certification (TC) and Supplemental Type-Certification Process (STC), Hardware & Software certification (DO 254, DO 178B), IAQG Quality and

Performance standards (AS/EN 9100 series), Supply chain process (SSCAM)까지 아우르고 있으며, 항공 규제와 표준의 이해를 증진시키기 위하여 Bureau Veritas 내 기업 교육 또는 다른 기업에서 사내교육 서비스도 제공하고 있다.

(3) Intertek

Intertek의 주요 기능 안전 관련 활동으로는, IEC 61508 표준에 기초한 온라인 가스 분석 시스템 (Online Gas Analyzer Systems) 분야의 프로세스 모니터링 서비스 시스템 설치 서비스와 전기차 관련 기능안전성 검증 활동이 있다. 온라인 가스 분석 시스템은 설계, 엔지니어링, 설치, 커미셔닝, 스타트업 및 운영의 전 주기 서비스와 프로젝트 관리, 기존 시스템의 대체, 트러블 슈팅(Trouble Shooting), 국내/국제적, 산업 특화된 표준에 대한 컨설팅 및 모니터링 시스템 설치 등의 서비스를 제공하며, 전기차 분야에서는 배터리 시스템의 안전성 검증, 실패 완화 및 ETL / CB / E-Mark 등의 인증 획득 및 ISO 26262 기반의 기능안전 테스팅 서비스를 수행한다.

Intertek은 다각화되고 있는 글로벌 시장에 대응하기 위하여 10여개의 다른 산업군을 망라하는 글로벌 플랫폼을 운영하고 있으며 국가 또는 산업 군의 고객별 요구사항을 충족하기 위한 로컬 수준을 지원하는 역량과 네트워크를 구축하고 있다. 그리하여 2014년에도 글로벌 오퍼링과 고객의 가치향상을 위하여 자체 능력을 상호보완하기 위하여, 석유&가스 분야의 국제적인 인스펙션 서비스 기업과 식품&농업 분야의 테스팅 기업을 인수하였다.

(4) DEKRA

전년도의 실적을 조사했을 때, DEKRA는 주력인 자동차 서비스 영역에서 2014년 7.4% 매출 성장을 이루어 왔으며, 주요 산업 서비스 영역에 있는 철도차량 (Rolling Stock) 검사, 전자제품 테스팅, 컨설팅 서비스 등에 해당하는 기업을 전략적으로 인수하여 서비스 영역을 확장해 왔다. [25)]

DEKRA의 기능 안전 서비스 활동으로는, 해당 장비에 필요한 기능 안전 및 안전 무결성 레벨 (SIL)을 정의하기 위한 위험 평가의 수행과 전체 제품 라이프 사이클을 포함하는 평가 계획 책정이 있으며, 이것은 하드웨어 및 소프트웨어 요건 리뷰, 설계 프로세스, 검증 테스팅, 문서 및 완전한 기술 구성 파일을 포함한다. 또한 기능안전에 대한 국제표준인 IEC 61508을 기본으로 하며, 의료장치 부문의 IEC 62304, 프로세스 산업부문의 IEC 61511, 도로차량 부문의 ISO 26262 등 특정 제품 표준에 맞추어 기능 안

전성을 평가하고 수행한다. [26]

DEKRA의 특이점으로는, 한국의 서울에 폭발 안전 (Explosion Safety) 사무소를 열었다는 것이다. 다른 지역으로의 사업 확장 시 중요한 것은 해당 지역의 진입과 제대로 된 포지셔닝을 하는 것이다. DEKRA는 한국어가 가능한 전문가를 활용하고 KC 인증을 근간으로 한국시장에 순조롭게 진입하였는데, 그 방법은 DEKRA의 현지 전문가들이 번역 또는 다른 모든 활동에서 발생하는 문서처리를 지원하고, KGS, KTS과 KOSHA 3개의 한국 인증기관과 연계하여 한국의 기관들에서 DEKRA 테스트 보고서를 인정받도록 하는 구조를 만들어 DEKRA의 이용에 불편이 없도록 하였다.

(5) DNV GL

DNV GL은 기술적 평가, 연구, 자문 및 위험관리 분야에서 전문성을 가진 국제적인 인증기관이며 선급협회로서, 2013년 9월에 이 분야의 선도기업인 노르웨이의 DNV (Det Norske Veritas)와 독일의 GL(Germanischer Lloyd)의 합병으로 설립되었다. 그 결과 DNV GL은 세계에서 가장 큰 선급협회가 되었고, 육상 및 해상 풍력, 파도, 조류, 태양 광 산업뿐만 아니라 글로벌 석유 및 가스 산업에서 세계 최대의 기술 컨설팅을 수행하고, 세계 해외 파이프라인의 65%가 DNV GL의 기술 표준으로 설계되고 설치되었다. [27]

DNV GL는 주요 서비스를 하고 있는 고객의 산업분야에 대하여 다음과 같은 비즈니스 과제를 고객들이 안고 있다고 분석했다. 주요 사업군인 해양, 석유, 에너지 산업 분야에서는 안전하고 견고한 운영 기능 요구에 따라 점차 Critical-Software의 의존성이 증가하게 되었고, 이에 따라 통합성과 복잡성이 계속 증가하고 있으며, 선박, 석유 및 가스 산업에서 복잡한 시스템의 제어기능은 전기/유압시스템에서 복잡한 소프트웨어 집약적인 시스템으로 이동되어, 현대의 모든 on-board 선박, 해양 설비 및 석유가스 시설들이 임베디드 소프트웨어에 의존하게 되었다. 또한 안전에 대한 공공적인 관심이 점차 증가하면서, 규제와 안전 표준에 대한 요구사항은 점점 늘어나게 됨에 따라, 기업은 소프트웨어를 검증하고 확인하고 통합하는 과제 (품질보증활동 수행, 실패 원인 식별, 요구사항과 변경사항 관리, 공급자/절차/개인의 자격 및 평가 등)를 해결해야 하는 숙제를 안게 되었다.

이러한 기업 과제에 대하여 DNV GL은 소프트웨어 집약적인 산업의 경험과 사례를 바탕으로, 맞춤화된 사례와 표준 및 방법론을 제공하고 있으며, 다음과 같은 서비스를 고객에게 전달하고 있다.

- 표준과 규제 부합성
- 소프트웨어 관련된 위험의 조기 식별 및 완화
- 시스템과 소프트웨어 공학기술 개선
- 안전 시스템의 표준(DNV OS-D203 ISDS and IEC 61508/11)과 관련된 서비스
- 소프트웨어 FMECAs, RAMS 워크샵 및 위험 평가의 촉진
- 독립적인 평가, 검증과 확인 활동 등

3) TIC 기업의 주요 당면 문제

Bureau Veritas의 경우, 그룹 운영 및 활동과 관련하여 14가지의 위험요소를 도출하였다. 거시 경제 환경, 지정학적인 사이트에서 발생할 수 있는 위험, 경쟁 환경의 위험, 자질 있는 직원 부족, 인건비의 증가, 주요 직원의 퇴사 등과 관련된 위험, 인/허가에 대한 비 재개/정지/손실에 대한 위험, 그룹의 인수 작업, 정부 서비스 산업의 전문성과 관련된 위험, 국제적인 경제 재개와 관련된 위험, 명성, 윤리위반, 이해당사자 구조 및 정보시스템과 관련된 위험요소들이다. 이러한 위험들은 TIC 산업의 기업들에게 일반적인 위험 군들로서, 각 기업들은 위험이 끼치는 영향과 위험을 경감하는 노력을 동시에 진행하고 있다.

예를 들어, 정치적으로 불안정한 국가에서는 갑작스런 서비스의 중단 요청, 전문가들의 안전 위험 등이 도사리고 있으므로 기업의 매출 하락과 직원 고용 및 이탈에도 영향을 줄 수 있다. 이에 대하여 해당 국가에 대하여 계속적으로 주시하거나 또는 주변 국가를 활용하여 위험을 분산하고 경감하는 방법을 강구하여 적용한다. [23) 28)]

2. TIC 시장 전망

1) TIC 시장의 특징

TIC 시장의 특징은 크게 4가지로 볼 수 있다. 첫째는 방대하면서도 분화된 시장이라는 것이며, 둘째는 장기적으로 지속가능한 시장이며, 셋째는 높은 진입 장벽이 있으며 마지막으로 통합과정에 있는 분화된 시장이라는 점이다.

(1) 방대하면서 분화된 시장

TIC (Testing, Inspection and Certification)은 실험실 또는 현장 테스팅, 관리프로세스 감리, 문서검토, 전체 공급망의 검사, 데이터 일관성 검증 등의 과업을 포함한다. 이러한 과업은 최종사용자, 구매자, 이해당사자 또는 공공기관이나 민간기관을 대신해서 수행되는데, 독립적인 제3자 업체를 사용하는 이유는 재정적인 목적 또는 행정당국에 의한 요구로 이루어질 수 있다. 전체적인 TIC 시장은 다음의 3가지 유형으로 구분되며, 일반적으로는 아웃소싱 시장과 내부 시장으로 크게 나눌 수 있다.

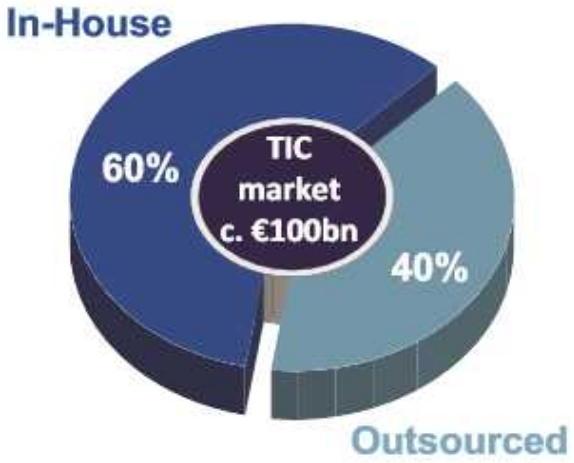
첫째, 아웃소싱 시장: TIC에 특화된 민간조직이나 회사가 서비스를 제공한다.

둘째, 내부(In-house) 시장: 기업의 사내 QC 또는 QA의 일부로 수행된다.

셋째, 퍼블릭 섹터: 공공단체, 세관, 경쟁당국, 항만당국, 산업안전당국 등에 의해 수행된다.

세 가지 시장의 상대적인 비중은 산업과 국가에 따라 다양하고, 정부의 정책이나 산업 군에 적용되는 실제적인 변화에 따라 매년 변동된다. 그리고 전체적인 TIC 시장은 제품, 자산가치, 제품이나 자산가치와 관련된 위험과 밀접하게 연결되어 있고, TIC 수행 또는 요구 수준 강도는 제조사나 운영사에서 부여하는 제품과 자산의 가치 비중과 일치한다. 일반적으로 TIC의 가치는 제품이나 자산 가치의 0.1% ~ 0.8% 정도로 예측된다. TIC 시장 규모는 인플레이션, 글로벌 경제 활동, 투자 및 국제 무역에 따라 달라지지만, TIC 시장의 아웃소싱 시장 규모는 근본적인 거시 경제 조건과 상관없이 국가의 행정 조직, 연방 수준과 활동 분야 등에 따라 크게 영향을 받는다.

[그림 3-23] 2012년 시장 유형별 시장 점유율



자료: Mergers and Alliance. Global Testing, Inspection and Certification M&A update. 2012 [22]

(2) 지속가능한 장기적 성장 동인

- 중국, 인도, 동남아시아, 남미와 같은 빠른 성장 국가의 중간계층의 확대로 안전성 관련 표준에 대한 요구가 지속적으로 증가하고 있다.
- QHSE (Quality, Health, Safety, Environment) 문제를 사전에 예방하고 관리하는 것이 기업의 가치를 부여하고 지속가능성을 유지하는 길이다. 그러나 광범위한 인터넷의 사용으로 제품과 회사 이슈는 즉석에서 공유될 수 있기 때문에 글로벌 브랜드의 보호 측면에서 QHSE 문제는 더욱 복잡해지고 있다.
- 공급망 개발에 의한 TIC 서비스 요구가 모든 산업에 영향을 끼치고 있다. 국제 무역의 확대로 여러 국가를 걸치는 생산, 제조, 조립 등 공급망이 개발되었으며 이와 함께 산업 안전, 규제, 품질, 성능 표준과 소비자의 기대에 부응하려는 요구 또한 증가되었다.
- 공공비용의 삭감으로 인해, 민간 사업자가 제어와 검사활동을 수행하고 있다. 즉, 공공기관들은 통제활동에 소요되는 비용을 절감하기 위하여, 시장의 제약조건에 유연하게 대처하는 전문 기업과 도급 계약을 맺고 전문 기업이 제어와 검사활동 업무를 대행한다.
- 제품이 더 정교해지고 더 빨리 시장에 출시된다. 시장 트렌드에 재빨리 대응하기 위하여 기업은 프로토타입 테스팅과 공급망 모니터링을 아웃소싱하고 있다. 제품에 많은 종류의 기술이 적용되면서 각 제품에 대한 테스팅과 관리해야 하는 협력업체는 점차 증가하고 있기 때문이다.
- 관리비용의 절감과 함께 자산의 신뢰성을 높이는 요구가 증가하고 있다. 규제 준수 문제를 떠나서, 자산의 유효기간 연장, 에이징 자산 관리, 유지관리 관행의 개선, 새로운 제어 체계 도입을 통해 자산의 유효성을 증가시키고자 한다.

(3) 높은 진입 장벽

새로운 플레이어가 진입하기에는 높은 장벽이 존재하며 이러한 문제에 대하여 다음과 같은 요건이 필요하다.

- 여러 국가의 허가(authorizations)과 인증(Certification)을 보유해야 한다.

- 지역적, 국제적으로 사무소/실험실과 지리적인 네트워크를 구축해야 한다. 서비스 포트폴리오를 확장하고자 할 때 현지 지역 네트워크가 필요하며, 동시에 글로벌 고객을 지원하기 위해서는 국제적인 네트워크가 구축되어 있어야 한다.
- 주요 고객에 대한 서비스, 대형 계약 체결, 지역 플레이어에서 부각되기 위해서는 넓은 서비스 오퍼링과 검사 서비스를 제공해야 한다.
- 고품질의 기술 전문가를 확보해야 한다. 기술 능력과 팀의 전문성으로 고부가가치 솔루션을 제공함으로써 차별화할 수 있도록 고품질의 기술 전문가를 확보해야 한다.
- 고객의 QHSE 관련 위험관리와 관련하여 장기적인 협력 관계를 맺을 수 있도록 무결성과 독립성에 대한 강력한 명성을 보유해야 한다.
- 국제적으로 알려진 브랜드를 보유해야 한다.

(4) 통합 과정에 있는 분화된 시장

TIC 시장에는 몇 개의 글로벌 플레이어와 액티비티나 서비스 타입에 특화되어 있는 수백여 개의 지역 플레이어들이 있다. 또한 일부 업체들은 국가 소유, 준 국영 기업 또는 단체에 등록된 업체들도 있다. 이렇게 분화된 시장에서 TIC 시장의 통합은 가속화되고 있으며, 주요 플레이어들은 지역 플레이어들의 통합을 통해 현지 시장에 진입하고 자신들의 포지셔닝을 늘리고 있다. [29)]

2) M&A 현황

앞에서 TIC 시장의 특징을 살펴보았듯이, 방대하고 분화된 시장이며 기업 간 통합이 진행되고 있는 시장이다. 이러한 통합이 발생하는 것은, 장기적으로 지속가능한 성장을 하고 있으나 진입 장벽이 높기 때문에, 현지 시장 진입을 위해서 해당 지역 또는 신규 서비스에 대하여 M&A를 통하여 기업을 확장하는 전략을 추진하기 때문이다. 이러한 이유로 TIC 시장에서 꾸준하게 진행되고 있는 인수합병 현황을 조사하였다.

(1) M&A에 대한 시각

“ Bureau Veritas는 중소규모 TIC 업체를 많이 인수해왔고 알맞게 자리 매김한 것으로 나타난다. 특히 상품 테스팅과 같은 더 작은 규모 분야에서 사업 영역을 성장시키

기 위한 기회를 지켜보고 있다." - Bureau Veritas

"뚜렷하게 규모의 경제를 보이는 산업분야에서, TIC는 상당히 분화되어 있다. 순환의 감속과 점점 성숙된 오너쉽 구조로, 거래활동은 가속화될 것으로 보인다." - Broker Research

"TIC 분야의 전문성, 지식과 기술은 지리적으로 다른 지역에 걸쳐 재활용될 수 있다. 새롭게 터득한 서비스와 기술은 국제적인 네트워크를 통하여 다시 배포될 수 있다." - Intertek [30)]

(2) M&A 동인

글로벌 플레이어들은 지난 몇 년 동안 기업 인수를 진행해 왔으며 여전히 진행 중에 있다. 특히 TIC 시장에서 활발한 M&A가 진행되는 동인은 첫째, 뚜렷하게 나타나는 규모의 경제와 잠재적인 시너지 효과이며, 둘째, 고객과 프로젝트에 근접한, 강력한 글로벌 네트워크 구축이며, 셋째, 서비스 포트폴리오의 확장을 위하여 추진되고 있다.

가. 규모의 경제와 잠재적인 시너지

효율성(Efficiency)과 확장성(Scalability)은 실험실 중심의 테스팅 사업에서는 뚜렷하게 나타난다. 그리하여 같은 수직적 시장 내에서의 활용률은 상대적으로 높게 나타난다. IT 시스템과 플랫폼의 단일화, 네트워크 최적화 (TIC 전문성, 지식, 기술의 타지역 간 활용), 다양한 포트폴리오에서 잠재적으로 여러 학문 분야에 걸치는 시너지 추출, 비용과 제경비의 합리화 등의 시너지 효과를 볼 수 있다.

나. 고객과 프로젝트에 근접한, 강력한 글로벌 네크워크

글로벌 네트워크 오퍼링, 대형 계약 수행, 지리적인 균형 확보 등에 의해 국제적인 네트워크를 강화하여 지역적인 포지셔닝을 확장하고 글로벌 고객의 사이트에서 글로벌 오퍼링을 제공한다.

다. 지역/서비스 포트폴리오 확장

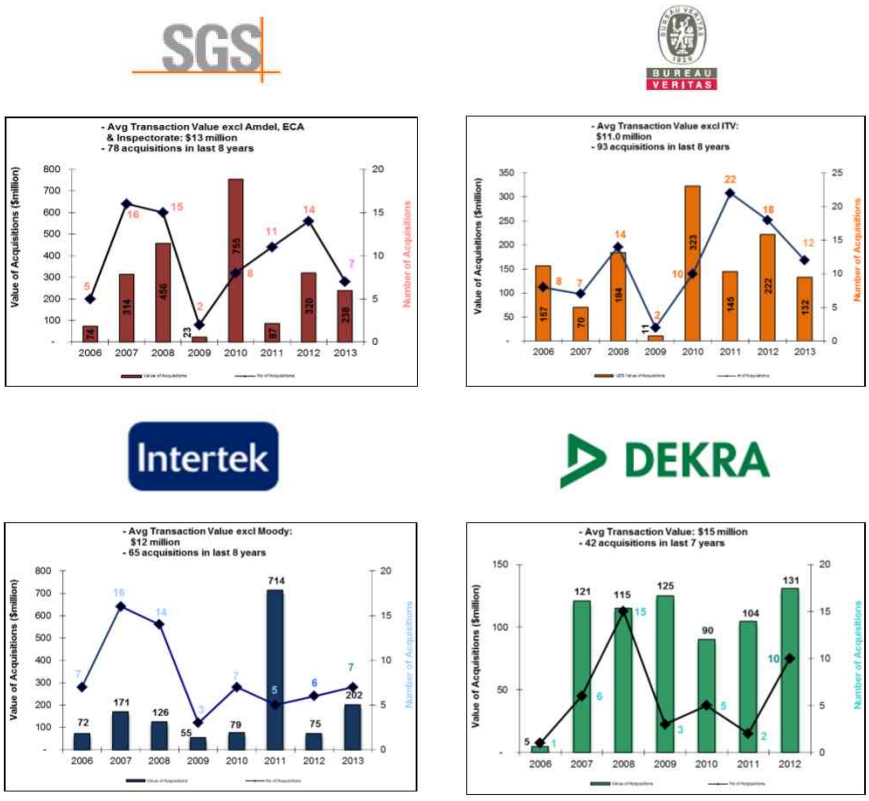
기업에서 부족한 기술력, 국제적인 인지도/브랜드, 인허가, 전문지식 및 사업 부문을 보충하여 서비스 포트폴리오를 확장하고 있다. 또한, 유럽이 주 사업기반이었던 글로벌 선진기업은 2006년~2013년까지 지리적 서비스 범위를 확대하기 위하여 다양한 지

역의 TIC기업을 인수하고 있었다.

(3) M&A 활동 현황

TIC 시장에서 기업의 글로벌화는 M&A 활동을 계속 촉진시키는 요소이다. 글로벌 TIC 산업은 유럽에 근거를 둔 다국적 기업에 의해서 지배되고 있으며, 상위 10개 기업의 전체 매출은 연간 매출 300억 달러를 초과한다. 이러한 기업들은 글로벌로 운영을 하고, 통일된 기반 하에서 글로벌 네트워크를 통하여 글로벌 고객이 어디에 있던지 지원 가능한 체제를 운영하고 있다. 따라서 지리적인 서비스 범위를 확대하기 위하여 기업 인수 작업을 계속하고 있다. 아래 그림에서 보듯이, 2006년에서 2013년까지 SGS는 78개의 기업을 인수했고, Bureau Veritas는 93개 기업을 인수했으며, Intertek은 65개 기업을 인수했다. DEKRA 또한 42개의 기업을 인수하여 지속적으로 사업 영역을 확장해 왔다. ([그림3-23] 참조) 두드러진 M&A건은 2012년 12월에 노르웨이의 DNV와 Germanischer Lloyd SE의 대형 합병으로서, DNV GL은 글로벌 석유가스 산업의 선도적인 기술 자문사가 되었다.

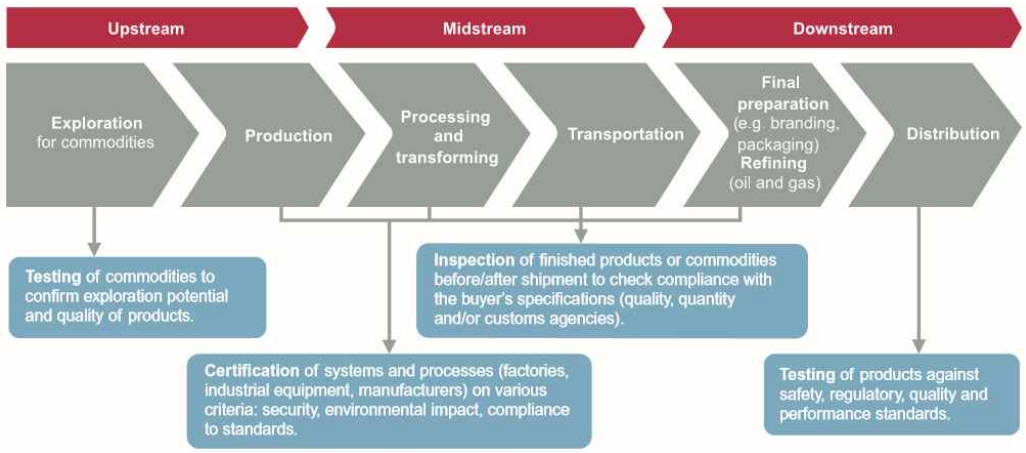
[그림 3-24] TIC 주요 기업의 8년간 (2006-2013) 인수 현황



자료: Industrial Capital Strategies. Testing, Inspection and Certification Industry: M&A Activity Remains High. 2014 [31]

또 다른 기업 인수의 특징으로 몇몇 기업들은 엔지니어링과 자산 무결성 관리 서비스로 확장하기 위하여 TIC의 가치사슬 범위를 확대하고 있다. 그리하여 제품의 설계-개발-양산 등의 직접적인 제조/서비스 산업과 검사-테스팅-인증의 TIC 산업의 경계가 모호해지고 있다. 예를 들어, Mistras는 석유가스산업의 Carmegen Engineering 인수, Applus+ RTD는 파이프라인 사업자에게 엔지니어링 서비스를 제공하는 Kiefner and Associates를 인수했으며, DNV는 GL과 합병하기 전, Noble Denton을 포함한 몇 개 기업을 인수하면서 우수한 석유가스 재생 엔지니어링 부문을 조직했다. 이러한 엔지니어링 기업의 인수는 설계/개발 기술을 확보하여 결과적으로 검사/인증 사업에 도움이 될 수 있을 것이다.

[그림 3-25] TIC 시장 구조



자료: Mergers and Alliance. Global Testing, Inspection and Certification M&A update. 2012 [22]

인수자들이 인수대상기업을 평가할 때의 중요한 요소로는 목표고객의 품질과 경제적인 회복력, 안전성 기록, 검사자의 자질, 직원의 재직 및 이직률, 정규 및 계약직 검사자, 고객 다양성, 표준 인증, 기술 수준, 문화적인 적합성 등이다.

3) TIC 시장의 향후 전망

TIC 시장은 주로 4가지 중요한 요인으로 작동이 되고 있다. 1. 규제와 산업표준의 증가, 2. 빠르게 일어나고 있는 글로벌화, 3. 제조의 품질과 안전에 관한 관심의 증가 등이 사업을 끌어내는 동인이 되고 전체적인 시장 성장에서 4. TIC 분야의 아웃소싱 증

가가 또한 중요한 역할을 수행할 것이다. 그러나 긴 리드타임과 규칙 및 규정의 변경은 시장에서의 주요한 제약요인이 될 것으로 예측한다.

최근 보고서에 따르면, TIC 시장은 2014년부터 2020년까지 CAGR (Compound Annual Growth Rate, 연평균 성장률) 5.8%의 꾸준한 성장과 2020년 말까지 약 504억 달러 정도의 시장 규모가 될 것이라고 한다. 이러한 시장의 성장은 주로 안전에 대한 관심이 높아진 신흥 시장과 중소규모 회사로부터 수요가 발생할 것으로 기대된다. 그리고 북미는 전체적인 시장을 점유할 것으로 예상되며, 글로벌화와 산업화로 인해 아태지역과 중동지역과 같은 신흥 시장에서 더 좋은 사업 기회가 생길 것이라고 전망한다. [32)]

3. 조사결과 요약 및 시사점

해외 TIC 시장은 아웃소싱(Outsourcing)과 내부(In-House) 시장으로 크게 분류가 되며, 전문 기업에 의한 아웃소싱 시장을 중심으로 문헌조사가 진행되었다. 전체 TIC 시장의 매출 상위 5위권 회사인 SGS, Bureau Veritas, Intertek, DEKRA 및 DNV GL은 전 세계의 글로벌 고객을 대상으로 각자의 서비스를 제공하고 있었다. 이들은 주력 도메인에서 고객 제품 및 자산가치에 대한 검사, 테스팅, 인증 서비스를 제공하고 있었으며, 국제 표준과 관련된 가이드 연구 및 배포, 국제 표준 기관 활동과 다른 TIC 업체와의 협업을 통한 서비스의 차별화 등의 노력을 하고 있었다.

특히나 두드러진 TIC 기업의 특징은, 모든 글로벌 회사들이 지난 몇 년간 기업의 인수합병을 계속 추진해 오고 있는 점이다. 이러한 인수합병을 일으키는 동인은, 같은 수직적 시장 내에서 활용률이 높게 나타나는 규모의 경제가 적용되고 여러 학문에 걸치는 잠재적인 시너지 효과를 볼 수 있고, 국제적인 네트워크를 강화하고 지역적인 전문서비스 품질을 강화하여 글로벌 오퍼링을 제공하며, 마지막으로 기업 내에 부족한 기술력, 인지도, 사업부문을 보충하여 서비스 포트폴리오를 확장할 수 있는 최선의 전략이기 때문이다. 그리하여, TIC 시장에서 글로벌 플레이어를 중심으로, 전문성 있는 중소기업을 대상으로 인수를 추진 중이며, 인수대상은 TIC 서비스 뿐 아니라 엔지니어링 부문으로 가치사슬 범위를 확대하여 진행되기도 한다.

[그림 3-26] 선진 TIC 업체별 제공 서비스 및 주요 활동

국가/ 국제표준	SGS	Bureau Veritas	Intertek	DEKRA	DNV GL
소프트웨어 안전 관련 서비스	• IEC 61508, ISO 26262 적용 • 자동차, 제조산업, 소비재&유통산업 • 테스팅, 컨설팅, 인증 및 교육 서비스 제공	• 자동차분야의 기능안전 평가 및 지원업무 수행 • 항공분야 인증을 위한 설계 및 인증 절차 운영 • 교육서비스 제공	• IEC61508 • 온라인가스분석 시스템 및 ISO26262 기반 전기차의 기능안전성 검증	• IEC61508 • IEC62304 (의료), IEC61511(프로세스), ISO26262 (자동차)를 적용한 기능 안전성 평가	• 해상부문의 인증기관 • 임베디드 소프트웨어 관련 안전성 검증, 평가, 기술개선 활동
특이 활동	• SGS / TUV와 기능안전팀 운영 • 표준위원회 활동 (ISO그룹, IEC61508 등)	• CEA LIST와 임베디드 SW에 대한 인증 가이드 진행 • 철도 수송 안전성 관련 가이드 배포		• 한국의 서울에 폭발 안전 사무소 설치 - 한국인 전문가 활용 및 한국 인증기관 연계	• 세계 해외 파이프라인의 65%가 DNV GL의 기술 표준으로 설계 및 설치
글로벌 확장	• 북미 3개, 유럽 6개, 일본 1개의 중소기업 인수 (2014년 기준)	• 전년 대비 북미와 아태지역 매출 증가 • 유럽, 중동 매출 감소	• 로컬 역량 및 글로벌 네트워크 구축으로 글로벌 플랫폼 운영 • 2014년 TIC 기업 인수	• 철도차량 (Rolling Stock) 검사, 전자제품 테스팅, 컨설팅 서비스 기업 인수	• 2013년 DNV과 독일의 GL의 합병으로 최고의 선급협회가 됨

제4장 국내 소프트웨어 안전 산업동향 분석

제1절 학계 및 공공기관

1. 개요

학계 및 공공기관 대상(Governing Sector) 소프트웨어 안전 동향 분석은 조사된 인터뷰 결과를 1. 개념정의, 2. 문제점 도출, 3. 해결방안 제시의 3단계 구조로 나누어 정리하고 결과를 분석한 다음, 도출된 문제점 및 해결 방안을 인과관계 별로 Mapping하였다. 특히, 조사된 해결 방안을 구분하여 유사한 항목 별로 Grouping 하여, 법/제도/인증, 표준/절차/가이드, 조직/기관 등을 포함한 6가지 부문으로 구분하였다. ([그림 4-1] 참조).

[그림 4-1] 학계 및 공공기관 대상 조사결과 분석 틀

2. 조사 결과

1) 소프트웨어 안전 개념

소프트웨어 안전(Safety) 개념은 현재 국내에서 정립된 개념이 아니므로 인터뷰 대상에 따라 소프트웨어 안전에 대한 개념 및 범위에 차이가 있었다. 특히, 1. 소프트웨어 안전을 품질 위주로 정의하는 의견과 2. 소프트웨어 안전은 소프트웨어로 인하여 발생하는 인명이나 재산의 사고를 회피하는 방안(Safety Mechanism)으로 정의하여 품질과 구별된다는 의견이 주를 이루었다. 본 조사에서 소프트웨어 안전에 대한 개념을 정의하지는 않으나, 주요한 2가지 의견을 종합하여, 소프트웨어 안전이란, ' 소프트웨어 품질에 기반하지만 감내하기 어려운 수준의 사고 발생시, 이를 회피하는 능동적인 방안(Safety Mechanism / Functional Safety)까지 포함한 개념' 으로 정리하였다. (<표4-1> 참조).

<표 4-1> 소프트웨어 안전 관련 주요 답변

주요 도출 결과	주요 답변
소프트웨어 안전은 품질임	• 소프트웨어 안전은 품질 또는 신뢰성으로 보고 있음. 즉, 소프트웨어 안전 = 품질임 • 결국 소프트웨어를 정확하게 만드는 것이 Key이며, 정확-안전-보안은 정확을 기반으로 같은 개념일 것임 • 소프트웨어 품질을 통해서 소프트웨어 안전을 추구해야 함
소프트웨어 안전은 안전사고 발생시, 이를 회피 할 수 있는 메커니즘까지 고려되는 부분임	• 품질과 안전은 다른 개념임 • 품질은 기본이고 소프트웨어 안전부분의 문제를 적절하게 회피할 수 있느냐 관점. 정보가 잘못되었을 때의 메커니즘도 구현이 되어 있어야 함 • Functional Safety 관련된 소프트웨어는 모두 하드웨어와 연결되어 있다. 그래서 국제표준은 소프트웨어 안전은 하드웨어와 함께 다루어지고 있음. 프로세스 측면: 예방, 탐지, 대응, 사후 활동 • 소프트웨어 안전은 기능요구사항 뿐만 아니라, 안전요구사항을 별도로 정의해야 함

2) 현황 및 문제점

(1) 국내 소프트웨어 산업

국내 소프트웨어 산업의 현황에 대한 문제점은 근원적으로 ‘ 소프트웨어 개발자들이 체계적인 절차와 방식에 따라 소프트웨어를 개발하고, 이를 문서화하는 문화가 부족 ‘ 에서 기인한다는 답변이 주를 이루었다. 즉, 체계적인 절차와 방식을 따르지 않고 개발되는 소프트웨어는 품질 문제를 내포하고 있고, 이로 인하여 소프트웨어 안전을 담보할 수 없다는 의견이었다. (<표4-2> 참조).

<표 4-2> 국내 소프트웨어 산업 현황 관련 주요 답변

주요 도출 결과	주요 답변
소프트웨어 개발자들이 체계적인 절차와 방식에 따라 소프트웨어를 개발하고, 이를 문서화하는 문화 부족	• 소프트웨어 산업 자체 기반이 미성숙 되어 있다 – 소프트웨어를 정확하게 개발하지 못하고, 이렇게 개발된 소프트웨어 품질은 낮은 수준임 • 국내 소프트웨어 개발 문제: 제대로 된 절차와 방식을 따라서 개발을 하고 있지 못함 • 국내 소프트웨어 개발자는 프로그래밍 능력은 뛰어나나, 구조화 및 문서화 능력이 낮은 편임 • 제대로 된 절차와 방식에 따라 개발이 안 되는 이유는 무엇보다 문화적인 기반이 미성숙 되어 있다고 봄

(2) 국내 소프트웨어 안전 산업

국내 소프트웨어 안전 산업의 현황에 대해 다양한 문제점 및 원인이 조사되었다. 특히, 소프트웨어 안전에 대한 개념 및 인식의 미성숙으로 인하여 나타난 문제점 등이 많이 조사되었다. 도출된 주요 시사점을 정리하자면, 소프트웨어 안전에 대한 개념 및 인식이 부족하여, 소프트웨어 안전에 대한 제도적인 기반 여건(법령, 평가가이드)이 조성되어 있지 않고, 이로 인하여 시장 여건이 미 조성됨 (전문인력 부족, 소프트웨어 안전을 담보할 수 있는 기간 및 비용 불인정) 으로 정리할 수 있다. (<표 4-3> 참조).

<표 4-3> 국내 소프트웨어 안전 산업 현황 관련 주요 답변

주요 도출 결과	주요 답변
소프트웨어 안전에 대한 개념 부족	• 공공부분의 소프트웨어 안전에 대한 인식 부족 • 소프트웨어 안전에 대해서 인식 수준이 낮음
소프트웨어 안전 법령 부재	• 국내 법령에 소프트웨어 안전에 대한 부분은 없음. 정보시스템이 많아지면서 소프트웨어 안전 및 품질에 대한 요구는 강해지고 있음
소프트웨어 안전 평가 가이드 부재	• 국가에서 안전 기준 및 가이드를 제공하지 않고, 진단을 수행하고 있음
소프트웨어 안전 전문인력 부족	• 소프트웨어 안전 관련해서 대부분의 기업은 전문인력이 없음
국내 소프트웨어 안전을 위한 기간 및 비용 불인정	• 국내 상황에서 소프트웨어 안전 테스트를 충분히 할 수 있는 기간 및 비용을 주지 않음

3) 해결방안

(1) 법/제도/인증

상기 문제점에 대한 법/제도/인증 측면에서 제시된 해결 방안으로는, 법/제도 및 자격증/인증 등을 활용한 소프트웨어 안전 인식 제고와 소프트웨어 안전관련 분리 발주를 통한 실질적인 시장 정착 방안이 조사되었다. 상세한 내용을 살펴보자면, 소프트웨어 안전에 대한 인식 제고를 위하여 소프트웨어 안전에 대한 법/제도 제정이 필요하나, 표준화 / 교육 등을 통해 어느 정도 기반이 구축된 후에 적용할 수 있도록 유예기간을 두고 적용하는 것이 좋다는 방안이 조사되었다. 또한, 자격증 / 인증 제도의 경우도 소프트웨어 안전 인식 및 안전성 제고를 위해 최소한의 규정으로 필요하나, 법적인 강제 인증보다는 민간 주도의 인증 제도를 운용할 수 있도록 하자는 의견이 조사되었다. 특히, 공공발주를 대상으로 소프트웨어 3자 검증을 포함한 소프트웨어 안전 관련 분리 발주 제도가 필요한데, 정부 예산 등을 감안하여, 단계적으로 적용해야 할 필요가 있다고 조사되었다. (<표 4-4> 참조).

<표 4-4> 해결방안 - 법/제도/인증 관련 주요 답변

주요 도출 결과	주요 답변
소프트웨어 안전 인식 제고를 위하여, 소프트웨어 안전 관련 법/제도 제정 필요. 단, 표준화 / 교육 등을 통해 어느 정도 기반이 구축된 후 적용될 수 있도록 유예기간을 두고 시행 하는 것이 바람직함	• 제도화를 통한 안전 인식 제고 필요 • 안전 인식확산이 필요하므로 제도화 필요 • 정부 산하 시설 부분은 소프트웨어 안전을 확보할 수 있도록 규제 필요 • 시장에서 소프트웨어 안전에 관한 요구를 할 수 있도록, 법/제도적 장치 필요. 발주기관에서 요구가 많은 상황임 • 법/제도는 바로 적용하는 것보다, 표준화 / 교육 등을 통해 어느 정도 기반이 구축되어진 후에 적용하는 것이 바람직
자격증 / 인증 제도는 소프트웨어 안전 인식 및 안전성 제고를 위한 최소한의 규정으로 필요하며, 법적인 강제 인증보다는 민간 주도의 인증 제도가 운영될 수 있도록 가이드	• 국제표준을 준수하라는 규정은 의미 있음 • 자격증은 필요함: 자격증 취득을 위한 활동이 개발자와 회사의 최소한의 수준 향상에 기여 • 소프트웨어를 정확하게 만들어 수출하기 위해서 인증이 중요함 • 공동인증제도 필요: 시험은 산업 도메인 민간수행기관이, 평가는 여러 기관이, 인증은 해당 도메인의 정부출연기관이 하는 구조. • 법적 강제 인증을 할 수 없음: 소프트웨어 자체만으로 피해가 발생하지 않는다. 즉, 소프트웨어의 문제로 인한 하드웨어 오작동으로 피해가 발생하기 때문임
공공발주를 대상으로 제3자 검증을 포함한 소프트웨어 안전 관련 분리 발주 제도가 필요함. 단, 정부 예산 문제를 감안하여 단계적으로 적용해야 할 필요가 있음	• 독립적인 제3자 검증 제도 필요 • 현실적으로는 제3자 검증을 활용한 소프트웨어 안전 관련 분리발주 필요. 단, 소프트웨어 안전 요건 적용을 위한 정부예산 문제 해결 필요

(2) 표준/절차/가이드

표준/절차/가이드를 통한 문제점 해결 방안의 주된 의견으로는 국제표준을 토대로 각 산업도메인별 소프트웨어 안전 관련 표준과 이를 Tailoring하고 활용하는 가이드, 그리고 Best Practice를 DB화하여 제공할 필요가 있다고 조사되었다. 또한, 국제 표준 활동에 국내 안전 및 품질 단체가 참여할 필요가 있다고 조사되었다. (<표 4-5> 참조).

<표 4-5> 해결방안 - 표준/절차/가이드

주요 도출 결과	주요 답변
국제표준을 토대로 각 산업 도메인별 소프트웨어 안전 관련 표준과 이를 Tailoring 하고 활용하는 가이드, 그리고 Best Practice를 DB화 하여 제공	• 해외 표준을 기본으로 하여 국내 각 도메인별 Best Practice (전문가가 알고 있는 꼭 해야만 하는 것)를 모아서 제공해야 함 • 주요산업의 국제표준이 존재하므로 공공차원에서 별도의 새로운 표준을 만들 필요가 없음. ISO26262는 자동차 도메인에서 그 표준을 따라야 함. 미국도 항공법은 DO-178을 준용하라고 되어 있으나, 상세한 지침은 없음. 국제표준이 있는 경우는 따로 표준을 만들 필요가 없으나, 정보시스템 중 관제시스템에 대해서는 표준이 존재하지 않음. 자동차, 의료, 항공, 원자력, 국방 등은 표준이 있으므로 이를 활용하고, 공공운영 시스템에 대해서는 어느 정도의 표준과 가이드가 필요함 • 소프트웨어 안전의 발전을 위해서는 각 분야마다 표준에 따라 핵심적으로 따라야 하는 부분에 대해서, 템플릿 / 수행 가이드 / Best Practice 등을 제공해서 업계 따라 오도록 이끌어야 함 • 정부기관의 경우, 안전 요구사항 분석 및 프로세스 설계에 집중하고, 안전 요구사항 분석 등을 만들어서 각 사업 군별로 적용 가능한 tailoring guide를 제공하는 식으로. 궁극적으로는 안전 요구사항 분석을 업계와 같이 협업하여, 각 사업 군별로 안전요구 사항 DB를 구축해야 함
국제 표준 활동에 국내 안전 및 품질 단체 참여	• 일본/독일/미국 등 소프트웨어 안전 관련 선진국과 포럼/협의 모색이 필요함

(3) 조직/기관

조직/기관을 통한 해결 방안으로는 관리/감독/인증기관이 분리되어야 한다는 의견과 다 부처가 참여한 소프트웨어 안전 협의체가 필요하다는 의견이 조사되었다. (<표 4-6> 참조).

<표 4-6> 해결방안 - 조직/기관

주요 도출 결과	주요 답변
관리, 감독, 인증기관 분리	• 관리, 감독, 인증기관이 분리되어야 함
다부처가 참여한 소프트웨어 안전 협의체가 필요	• 정부의 다부처가 참여하여 소프트웨어 안전문제를 해결해야 함.(미국의 백악관 산하에 소프트웨어 안전 관련 프로젝트에 10개 부처가 참여)

(4) 인력/교육

교육부분에서는 초기 교육 과정부터 체계적인 소프트웨어 개발 교육을 제공하고, 기업에 대한 소프트웨어 안전 교육/연구에 대한 지원이 필요하다고 조사되었다. (<표 4-7> 참조).

<표 4-7> 해결방안 - 교육

주요 도출 결과	주요 답변
초기 교육 과정부터 체계적인 소프트웨어 개발 교육을 제공하고, 기업에 대한 소프트웨어 안전 교육/연구에 대한 지원이 필요	• 국내 여건에 맞도록 교육 요구사항을 포함하여, 국내 산업 업계가 교육을 받도록 하는 것이 바람직 • 교육 및 연구 지원 필요 • 교육도 관련 담당별로만 별도로 수행하여 업체에 부담을 최소화해야 함, 또한 안전 분석기술 관련해서 이를 전수해 주어야 함 • 장기 차원의 교육 - 미국은 소프트웨어 교육을 초기 교육 과정부터 시작

(5) 業 환경개선

業 환경개선을 통한 소프트웨어 안전 제고 방안으로는 공공 영역에서 주도적으로 소프트웨어 안전 요구 사항을 포함하여 과제를 발주하고, 민간 영역에서 따라올 수 있도록 하되, 점진적으로 적용(예. 비안전계통에서 안전계통으로) 하는 것이 바람직하다는 의견이 주를 이루었다. (<표 4-8> 참조).

<표 4-8> 해결방안 - 業 환경개선

주요 도출 결과	주요 답변
공공 영역에서 주도적으로 소프트웨어 안전 요구 사항을 포함하여 과제를 발주하고, 민간 영역에서 따라 올 수 있도록 하되, 점진적으로 적용 (예. 비안전계통에서 안전계통으로)	• 강제성보다 공공부문에서 먼저 주도할 필요가 있음. 정부 및 공공기관에서 선도해서 이러한 요구사항을 정부 발주 사업 등에 명시하여 가는 방안이 있음 • 안전에 대한 부분은 공공이 푸는 게 맞고, 실제 실행은 민간에서 하는 것이 맞음 • 국내 기업에 참여 할 수 있도록 공공사업 발주를 통한 지원이 필요 • 국내 소프트웨어 안전 산업 육성을 위해, 공공사업 발주 시 국내 소프트웨어 안전 기업을 참여하게 해서 Track Record를 축적하게 지원하는 것이 바람직 • 선진국 사례를 보면, 공공이 먼저 시작함. 100% 민간에 맡겨서 제도를 시장논리에 맞춰두기에는, 안전요건과 자격을 명확하게 제시하는 것이 맞다고 봄 • 원전은 비안전계통부터 시작하여 물리적인 시스템은 물리적인 시스템을 적용(미국의 원전가이드를 적용하면서 비안전계통에서 안전계통으로 단계적으로 접근하여 표준/가이드를 적용하여 안전성을 갖춤)

(6) 프로세스

프로세스 측면에서는 소프트웨어 개발 초기부터 각 단계 별, 소프트웨어 안전 활동을 수행하도록 가이드 해야 한다는 방안이 조사되었다. (<표 4-9> 참조).

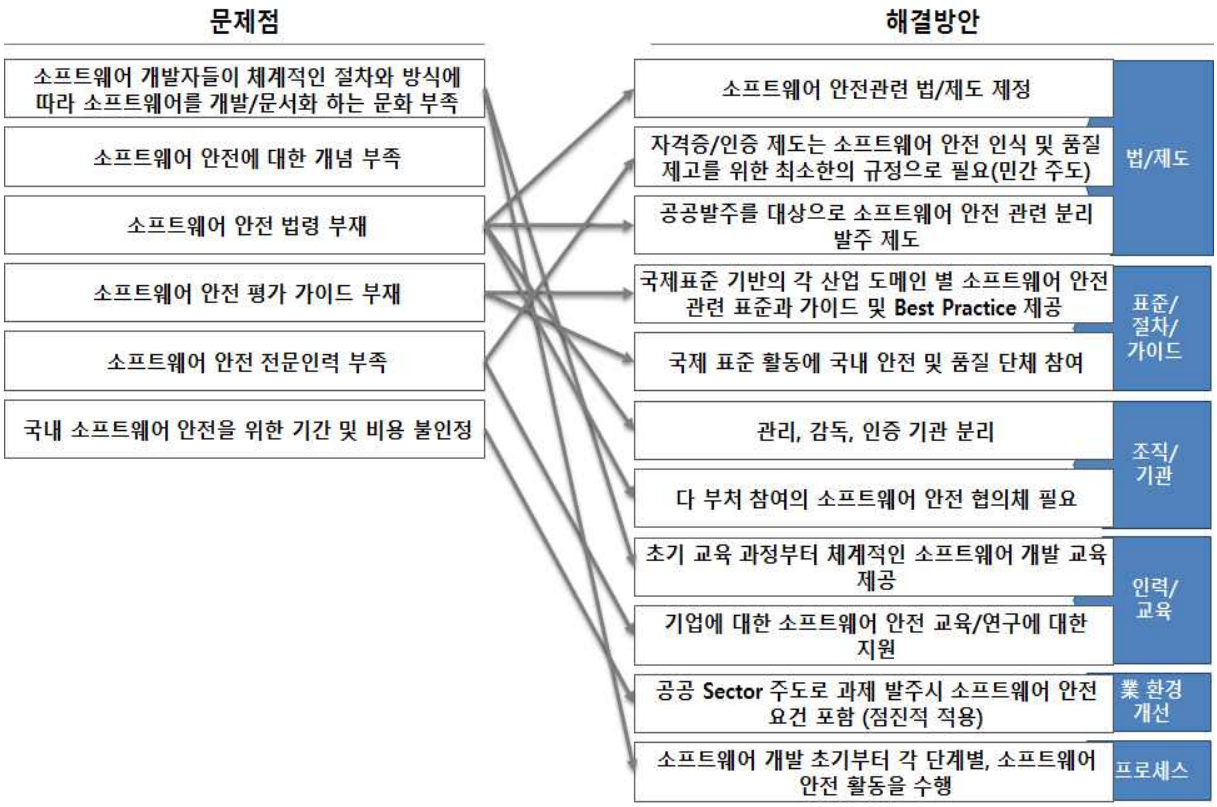
<표 4-9> 해결방안 - 프로세스

주요 도출 결과	주요 답변
소프트웨어 개발 초기부터 각 단계별, 소프트웨어 안전 활동을 수행 하도록 가이드 해야 함	• 소프트웨어 안전에서 테스팅만으로는 안전 확보가 안 된다고 본다. 시스템에서 위험발생 상황을 파악하고 영향도의 감소, 제거 등을 결정하여 시스템을 구현해야 하므로, 개발 초반부터 안전에 대한 설계가 필요함. SGS, TUV도 초반부터 컨설팅을 하여 매출을 올리는 구조임 • 소프트웨어 안전을 위해 개발 Process + 각 단계별 검증이 병행되어야 함

3. 조사 결과 종합 및 시사점

학계 및 공공기관 인터뷰 결과의 특징은, 직접적인 원인보다 근원적인 원인을 파악하고, 이를 해결하기 위한 방안도 보다 장기적인 차원에서 제시된 것이다. 제시된 해결 방안도 타 조사대상에 비하여 포괄적이었다. 즉, 법/제도, 표준/절차/가이드, 조직/기관 측면뿐만 아니라 業 환경 개선이나 인력/교육 등 시장 중심적인 방안도 다수 도출되었다. 도출된 방안을 6개 측면에서 정리하고 Grouping 한 후, 제시된 문제점을 만족하는지를 정리하였다. 특이한 점은, 소프트웨어 안전에 대한 개념은 조사 대상별 이해하고 있는 범위 및 방향이 상이하여, 본 보고서에서는 개념에 대한 정의를 하지는 않고 설문 결과를 종합/정리한 것으로 대신하였다.(소프트웨어 안전 개념: ‘ 소프트웨어 품질에 기반 하지만, 감내하기 어려운 수준의 사고 발생시, 이를 회피하는 능동적인 방안(Safety Mechanism / Functional Safety)까지 포함한 개념’) 하지만, 소프트웨어 안전 분야 사업 기업 및 소프트웨어 개발/사용 기업 대상 조사에서, 중복적으로 명확한 소프트웨어 안전 개념에 대한 요구가 도출되었고, 모든 법/제도, 표준/절차/가이드 해결 방안의 시발점이 되므로, 조속한 시간 내에 명확한 개념 정의가 필요한 것으로 분석되었다.

[그림 4-2] 학계 공공기관 문제점 및 해결 방안 Mapping



제2절 소프트웨어 안전 분야 사업 기업

1. 개요

소프트웨어 안전 산업 동향의 실태조사 대상은 소프트웨어 안전 및 품질 분야와 관련된 Player, 즉 TIC (Testing, Inspection and Certification, 안전사업포함) 시장에서 활동하는 기관 및 기업을 그 대상으로 하였다.

본 산업 실태조사를 위해, 먼저 회사의 일반현황, 소프트웨어 안전 프로세스 현황, 소프트웨어 안전 인프라 현황 및 니즈 등 각 영역에 대한 업체들의 현황을 조사하기 위한 구조화된 설문지를 개발하였으며, 조사방법 및 기간은 설문응답과 1:1 대면 인터뷰의 형태로 약 3주간 진행되었다. 국내 상당수 TIC 기업들이 소프트웨어 테스팅 협회에 소속되어 있어, 상당수의 인터뷰 및 설문조사를 협의의 지원을 받아 진행하였다. 인터뷰 중에 도출된 협의 소속이 아닌 소프트웨어 안전 전문 기업의 경우, 개별적으로 연락을 취하여 인터뷰를 진행하였다. 단, 기업의 기밀을 우려하는 업체에 대해서는, 해당 기업의 요청에 따라 설문응답 또는 대면 인터뷰를 수행하지 않았으며, 설문에 응답한 대상 중, 안전에 대해 전문적인 서비스를 수행하고 있는 업체에 대해서 추가적으로 1:1 대면 인터뷰를 병행하여 산업 현황과 니즈를 재확인하였다. 인터뷰 대상 기업들이 제공하는 주요 서비스로는 소프트웨어 기능안전(Functional Safety) 서비스와 소프트웨어 신뢰성(Reliability) 서비스로 구분할 수 있으며, 구체적으로, 기능안전 서비스는 시스템 소프트웨어 메카니즘 설계, 시스템 소프트웨어 구현, Safety 검증/인증 등이 있으며, 신뢰성 서비스는 정적 테스트, 동적 테스트 등이 있다. 국내 시장의 경우, 상기 서비스를 한 가지이상 복합적으로 제공하는 기업이 상당수 있었다. 여기서는 인터뷰 대상 전체 기업에 대한 조사/분석을 제시하고, 추가적으로 기능안전서비스 비중(기업 인터뷰 결과 기준)이 높은 기업(이후, ‘ 소프트웨어 기능안전 특화기업’)의 조사/분석 결과도 제시하였다.

국내 소프트웨어 안전 분야 사업 기업에 대한 설문 및 인터뷰 외에, 本 과제 수행을 위해, 설문 및 인터뷰 기업들을 대상으로 신용평가기관 및 각 社 홈페이지 등을 통해 공식적이고 객관적인 데이터를 수집하여 분석을 수행하였으며, 조사 내용은 국내 소프트웨어 산업 일반 현황, 기업 재무 현황 등이다.

본 대상에서 도출된 해결방안은 학계 및 공공분야와 마찬가지로 6가지 부문으로 구분하여 정리하고, 도출된 문제점과 Mapping 하였다.

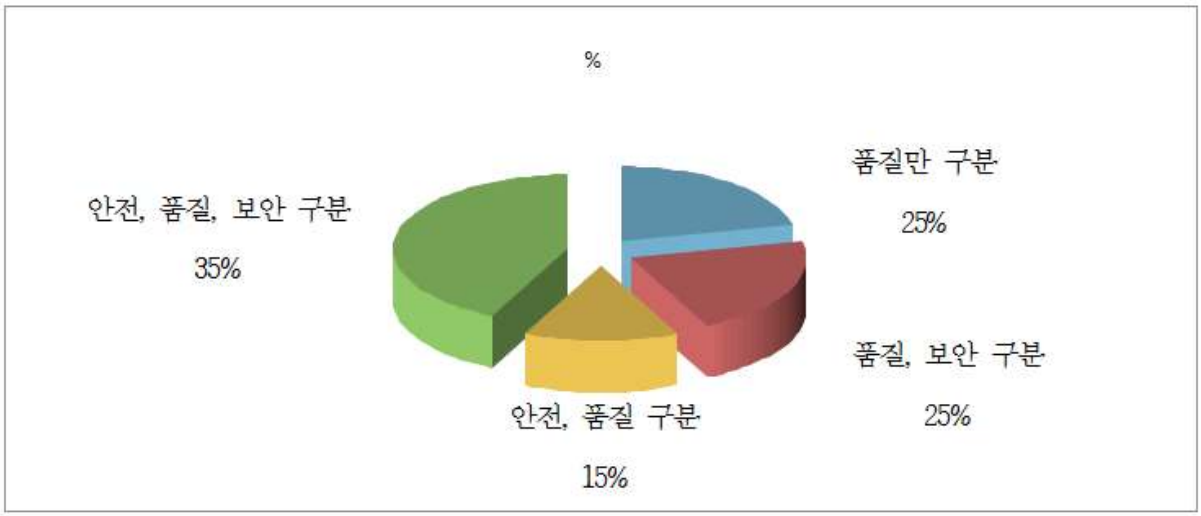
2. 환경 분석

1) 안전/품질/보안에 대한 구분

설문대상에 대해 안전, 품질 및 보안에 대한 개념적인 구분을 하고 있는지에 대한 조사결과, 대부분의 조사대상의 경우 품질을 안전이나 보안 개념과 구별하여 인식하고 있었는데, 이중 25%는 품질로만 구분하여 인식하고 있어 국내 TIC 업계가 현재 품질 중심의 인식 및 서비스를 제공하는 것으로 추정할 수 있었다.

50%의 조사대상이 안전을 품질 또는 보안과 차별화 된 것으로 인식하고 있었고, 이중 안전, 품질, 보안의 3가지 개념을 각각 구분하여 인식하고 있는 경우는 35% 수준이었다. 즉, 안전(Safety)을 보안(Security) 또는 품질로 인식하는 대상이 25%, 안전(Safety)을 품질(Quality)로 인식하는 대상이 25%로 조사되었다. 즉, TIC Sector에서의 소프트웨어 안전에 대한 인식도는 50%로 중간수준이었다.

[그림 4-3] 안전, 품질, 보안 구분 현황



업체에서 보는 ‘ 안전’ 에 대한 정의는 인명, 재산에 피해가 발생하는 경우를 의미하는 것으로서 추상적이고 일반적인 개념으로 인식하고 있었으며, 측정 가능한 수준의 명확한 소프트웨어 안전에 대한 개념 인식은 미미하였다.

<표 4-10> 소프트웨어 안전에 대한 개념 인식

❖ 품질 기반: 개발기간 전체의 품질확보에 따른 오류 최소화로 보고 있으며, 소프트웨어의 기능 및 성능의 품질요소가 인명/재산상의 피해를 야기하게 되는 부분을 안전이라고 봄 ❖ 하드웨어 기반: 안전영역은 하드웨어라고 인식하고 있으며 소프트웨어 분야는 무관함 ❖ 예측성 기반: 예상 가능한 위협으로부터 인적/물적 큰 피해가 발생하지 않도록 소프트웨어를 만드는 행위라고 봄

2) 소프트웨어 안전(Safety) 서비스 제공 사례

지금까지 전문적인 소프트웨어의 안전 서비스를 제공하고 있는 분야는 국내에서 원자력과 자동차 산업이 중심이며, 민간차원에서 자동차 산업에 집중되어 왔다. 자동차 분야에서는 기능 안전, 분석, 평가, 설계, 시험, 교육, 컨설팅 등이 수행되고 있으며 신뢰성 컨설팅을 수행하는 업체에서 이 중 일부를 수행하고 있다. 해당 전문 업체에서 수행하는 안전(Safety) 서비스는 소프트웨어 안전 메카니즘 설계와 교육, 기능 안전 서비스 등을 수행하고 있으며, 국내외 전문가를 활용하고 있다.

국내 소프트웨어 안전측면의 전문 서비스 사례가 희소한 근본원인은 크게 두 가지 측면으로 파악된다. 첫째는 최종고객-발주처에서의 안전에 대한 중요성이 낮은데 기인한다. 안전에 대한 기능적인 요건을 품질과 동일시하는 인식에 따라 대부분의 서비스는 품질차원에서 시험하고 평가하는 요청사항이 중심이다. 둘째는 산업도메인 지식이 있는 전문가 영입이 극히 어려운 관계로 일부 신뢰성 컨설팅 전문사만 해당 분야 전문가를 보유하는 등 전문 인력이 부족하기 때문이다. 일부 전문 업체에서 해외의 소프트웨어 안전 관련 전문가를 영입하여 국내 소프트웨어 안전 역량을 제고하려는 시도는 긍정적이나 아직 시장 전체 차원에서는 시험적인 단계에 머물러 있다.

<표 4-11> 안전(Safety) 전문 서비스 상세 내용

❖ 교육 서비스: IEC 61508의 안전관련 전문가를 초청하여 강의를 듣고 준비를 하고 있음 (Framework 측면에서 안전이 체계적으로 구성되어 있으며, 소프트웨어 품질 영역에서는 아직 국내에 준비가 되어있지 않는 현실임) ❖ 단, 발주처에서 안전/테스팅을 포괄하여 안전에 전문적인 요건을 요청하고 있지는 않음 ❖ 전문가 활용: ISO, IEC, IEEE 29119 공통의 표준 수립한 기관의장인 스튜어트 리드 (의장, STA CTO)가 full-time으로 업무를 수행하고 있음 (영국과 한국을 오가며 자문 활동) - 스튜어트 리드: 미사일 소프트웨어개발, 국방 특화 대학, 테스팅 교육과정 개발 및 방법론 개발, 사내 교육 전수, ISTQB 자격증 시험문제 출제 ❖ 기능 안전 측면: 시스템 레벨의 기능안전을 구현하는데 필요한 소프트웨어 안전 부분 수행 ❖ 전문인력: 신뢰성쪽 전문성을 가진 전담인력이 안전을 담당하고 있음

3) 관련자격 보유 현황

소프트웨어 안전에 관한 전문적인 자격증은 별도로 존재하고 있지 않은 상황이며, 업계에서는 품질기반의 테스팅 관련 자격이 일반적으로 사용되고 있다. ISTQB (국제소프트웨어테스팅자격), ISO 90001 (품질경영시스템 국제 인증), TS16949 (자동차 품질경영시스템 국제 인증), ISO 26262 (자동차 기능 안전성 국제 표준) 등 개인과 법인 차원에서 보유하고 있다.

각 Player는 품질테스트 서비스를 수행하기 위해 구성원이 ISTQB 등 개인 자격증을 보유하고 있으며, 해당 구성원의 1/3~1/2 이상이 관련 자격증을 보유하고 있는 것으로 파악되었다. 업체의 규모에 따라 차이가 있으나, 가장 많은 자격증을 보유하고 있는 업체는 100명 이상이 ISTQB 자격증을 보유하고 있으며, 업계에서 최소한의 자격증으로 인식되고 있다.

소프트웨어 안전 측면에서 업계에서는 단순한 시험 통과형식의 자격증보다는 실제적으로 안전에 대한 경험과 전문성을 검증할 수 있는 형태로의 자격증 혹은 제도가 효과적이라고 보고 있었다.

향후 소프트웨어 Safety에 대한 전문역량을 제고하기 위해서는 자격증에 대한 운영방법이 중요한데, 자격증 자체가 검증차원에서 필요하더라도, 자격증의 속성은 단기간에 준비하여 통과하는 시험형식의 내용보다는, 소프트웨어 안전에 대한 수행 경험과 이력에 대해 전문성을 부여하고, 부여된 전문성이 지속적으로 유지될 수 있도록 주기

적인 자격 관리가 수반되어야 할 것으로 분석되었다.

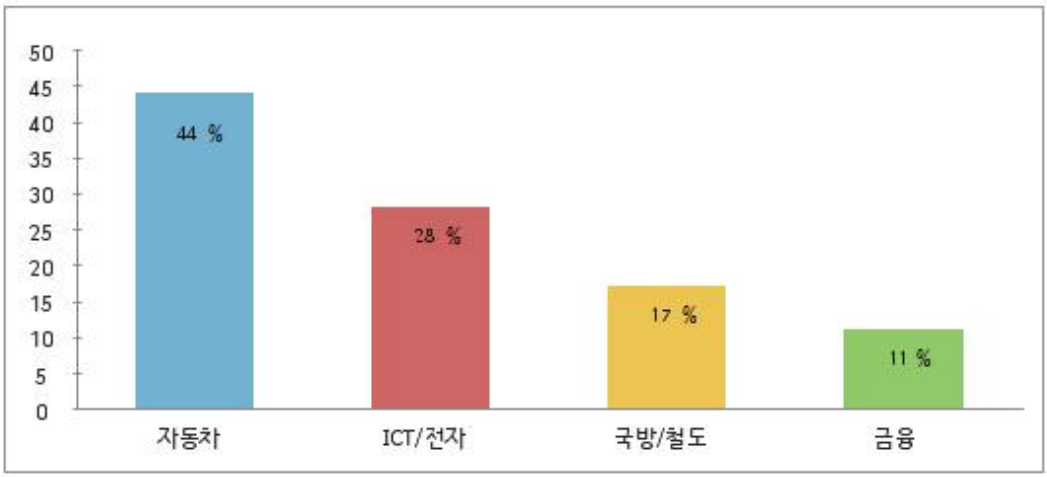
<표 4-12> Safety 전문 자격증에 대한 업계 견해

❖ 자격 요건: 경력중심의 자격 요건이 필요함 - 소프트웨어인증/검증 : 소프트웨어개발 최소 3년 이상 경력, Code Review 역량, 소프트웨어 테스팅의 이해, 산업별 기능안전 국제 표준의 이해 - 소프트웨어안전 : 신뢰성 분석 기법에 대한 기본적인 이해 (FMEA, FTA, HAZOP 등)
❖ 도메인 전문: 소프트웨어의 기본적인 안전 전문성과 함께 관련하는 도메인에 대한 전문성이 갖추어져야 함 예시) 테스팅 & 컨설팅을 하는 의료사업회사: FDA 인증을 받지 않으면 사업을 할 수 없는데, 장비에 대한 글로벌수준의 방법(요건 문서화) & 요건에 따른 테스트 수행 활동을 일치해야 하므로 해당 도메인 및 부품에 대한 이해가 선행되어야 함
❖ 소프트웨어 공학 지식과 도메인의 제품/부품에 대한 전문 지식이 필요함

4) 고객 현황

품질 측면을 포함하여 소프트웨어 안전 분야의 사업을 수행하는 기업의 해당 산업은 자동차 산업 등 특정 산업 중심으로 분포되어 있다.

[그림 4-4] 주요 고객 산업군 분포 비중



대부분 조사대상기업의 매출비중은 자동차 산업고객 - 제조사, 부품사 등이 전체 매출의 50%를 차지하고 있는 것으로 조사되었으며, 이들 기업은 자동차 도메인의 ISO 26262를 기준으로 한 표준화, 세부 분석도구 및 인프라 구축 등의 서비스를 제공하고

있었다.

고객사 및 프로젝트 규모에 따라 상이하기는 하지만 실제 안전에 특화된 프로젝트에 참여하는 인원의 규모는 10~12명의 규모로 6개월에서 1년 가까이 프로젝트를 수행하고 있었다.

민간부문에서는 자동차 산업이 소프트웨어 안전에 대해 가장 수요가 많은 것으로 파악되며, 공공부문은 항공 등 국가기반 산업을 모두 커버하고 있지 못해 향후 관련 산업 고객 확대가 필요한 것으로 분석되었다.

<표 4-13> 안전 전문 프로젝트 투입 상세 예시

❖ 소프트웨어인증/검증: 소프트웨어개발 최소독립검증, 안전, 보안까지 수행함 - 프로젝트에서 검증하기 위해서 6:2:2 비율로 검증/안전/보안을 진행하고 있음 ❖ 소프트웨어 설계부분: 안전 전문 프로젝트의 경우 설계까지 고객이 요구하는 경우는 많지 않음

5) 고객 요구 사항

소프트웨어 안전에 대한 고객의 요구사항은, 고객의 소프트웨어 안전 개념 및 중요성에 대한 인식이 낮아 안전에 특화되고 구체화되어 있지 않았다. 일부 고객의 경우, 제품 신뢰성에 대한 안정성 규격 준수여부를 지원하는 컨설팅 서비스 또는 제품 신뢰성에 대한 기능중심의 서비스를 요구하고 있었다. 또한, 시스템의 관리에 있어서도 일반적으로 고객은 안전에 대해서는 특화된 요청을 하고 있지 않으며, 안전을 일종의 ‘ 인증’처럼 형식적으로 갖추어야 되는 요식행위 수준으로 인식하고 있었다.

<표 4-14> 소프트웨어 안전/품질 분야 고객 요구 사항

구 분	대 상	내 용	비 고
신뢰성	정적 분석, 동적 시험	소프트웨어 프로세스 안정성 규격 준수여부	국방, 원자력, 자동차, 철도 분야 등
	기능/품질 테스트 서비스		
	내장형 소프트웨어	기본 동작 및 악의조건에 대한 신뢰성, 내구성, 호환성, 안정성 평가	자동차 분야 중심
기능	연구소 개발 영역	현업 QA팀과 테스팅 업무 선행 테스트, 양산 테스트	
	QA 영역	호환성 테스트, UI 테스트	
	자동화 영역	기능 검증 자동화, 성능측정	자동차 분야
	단계별 테스트 영역	단위시험, 통합 시험	상주 개념
컨설팅	시스템 부품	개발과정 전체 및 지원에 대한 모든 부분 컨설팅	엔지니어링 관점 수행
	시스템 제어	컨트롤 시스템, 모니터링 시스템	
기타	부품 제어	블루투스 기술을 이용한 차량용 장치 제어, 모바일 디바이스 발열 제어 등	전자산업 분야

6) 국내 경쟁사 및 해외 선진사

안전을 기반으로 하는 국내 소프트웨어 사업자는 대부분 규모가 비슷하고 기술력, 영업력 측면에서 대동소이하다고 업계에서는 인식하고 있으며, 매출규모, 서비스 종류 등에서 강점을 가지고 있는 일부 Player들은 안전에 대한 Total Process 관리 경험과 안전관련 Tool을 보유하고 있었다.

<표 4-15> 국내 선도 소프트웨어 사업자 강점

구 분	강 점	비 고
전문성	소프트웨어 수준에서의 안전성 분석, 설계, 구현, 검증 및 관리에 대한 노하우를 보유하고 있음	Total Process에 대한 관리 경험
	안전 관련 테스팅 서비스를 위한 자동화 Tool 자체 개발 및 유통	Tool의 보유 유무

국내 업계에서 보는 해외 선진사와의 가장 큰 Gap은 다양한 산업별로 보유하고 있는 Reference(Track Record)가 가장 크다고 느끼고 있으며 이러한 이유로 글로벌에 시장 진입이 어려우며, 국내 시장에서도 전문 경험 및 Reference를 보유하고 있는 해외 Player의 진입이 확대되고 있는 추세이다.(SGS 등 대형 글로벌 Player들의 국내 업체 인수를 통한 국내 시장진입 시도 등) 따라서, 국내 업체의 다양한 산업 군별 안전 수행 Reference 보유가 시급히 요구되고 있다.

<표 4-16> 해외 소프트웨어 선진사 강점

대 상	강 점	비 고
TUV SGS DMV 등	산업 도메인별로 각각 해당하는 메카니즘에 따른 소프트웨어 안전 컨설팅, 인증에 대한 경험/사례 보유	Hazard DB 등 사고 관련 데이터베이스 축적
	각 도메인별 Private Consulting 전문가에 대한 소싱 역량	각 산업 도메인 전문가 자문체계 강화
인도 위프로 등	규모면에서 국내 대형 SI업체보다 큰 규모로 테스팅뿐만이 아닌 Total Service를 제공하고 있음	산업별 Asset 보유
일본 ASTER 단체	단체 소속의 전문 기업들이 포진해 있으며, JaSST 주관으로 상시적인 테스트설계 콘테스트 등 수행	소프트웨어 품질관리에 대한 조직적인 역량

7) 해외 진출

소프트웨어 사업을 수행하는 업체의 약 60% 가까이 해외 진출에 대한 계획이 있음을 응답하였고, 1차적으로는 해외 진출한 국내 고객사의 현지 지원 서비스를 대상으로 하고 있다. 대부분 아직 계획 중인 내용으로 가시화되고 있지는 않지만, 서비스보다는

제품중심, 현지 고객보다는 해외 진출한 국내사를 대상으로 계획하고 있는 상황이다.

<표 4-17> 해외 진출 계획 내용

지 역	제품 및 서비스	비 고
유럽	소프트웨어 프로젝트에 특화된 전사적, 공학적 관리도구	소프트웨어 테스팅 글로벌리제이션 서비스
일본	일본 내 현지 대리점을 통한 소프트웨어 자동화 테스트 Tool 판매 및 서비스	Tool 제품 판매
	일본 진출한 국내 소프트웨어 솔루션 기업들을 대상으로 한 현지화 컨설팅 및 테스팅	솔루션과 테스팅 중 타겟 영역을 고민하고 있음
동남아	철도부문 대상으로 한 고장정보 자동수집 및 분석 시스템 개발 및 판매 등	
	베트남 등 진출한 국내 대기업과 협업하여 통신시장의 솔루션 및 테스팅 서비스 등	

조사대상 업체 중 유일하게 기존 제품/서비스가 아닌 부가가치 차원의 신사업을 통한 해외진출을 계획하고 있는 업체가 있었으며, 아직 계획 초기단계이나 향후 국내 소프트웨어 사업자의 해외 진출에 대한 방향성 측면에서 유의미한 시도라고 판단된다.

<표 4-18> 소프트웨어 신사업 내용

영 역	내 용	배 경
Tool	크라우드(집단지성) 소싱을 통해 테스팅 Tool을 개발하여 해외에 진출하려 함	해당사는 테스트 커뮤니티 기반의 테스팅 역량을 오랫동안 축적해 오고 있음

8) 국제 표준

모든 국내 소프트웨어 안전 사업 수행자는 국제표준은 해당 ISO 및 IEC 가이드를 근간으로 각 산업 도메인마다 특화된 국제표준의 존재를 알고 있으며 이를 준용하고 있었다.

<표 4-19> 전기전자 기능안전 규격군

레 벨	ISO	IEC
Guide	ISO Guide 51	IEC Guide 51
A규격 기본안전규격	일반설계 원칙: ISO 12100 리스크 평가 원리: ISO 14121	N/A
B규격 그룹안전규격	시스템 안전표준: ISO 13849-1	기능 안전표준: IEC 61508
C규격 제품안전규격	자동차기능 안전규격: ISO 26262	철도안전규격: IEC 62279 의료기기 안전규격: IEC 60601/62304 원자력 안전규격: IEC 61513 프로세스 산업 안전규격: IEC 61511

자료: KTL. (한국산업기술시험원) [33]

산업별로는 자동차 산업에서 ISO 국제표준이 명시되어 있고, 철도, 의료기기, 원자력 등 기반산업에 대해 IEC 국제표준이 명시되어 있으며, 그 밖에 항공분야의 DO 178B/C, 국방 분야의 무기체계 소프트웨어 개발 및 관리 지침 등이 있다. 대부분의 사업자들은 해당 산업에서의 국제표준을 준용하고 있으나, 일부 준용되지 못하는 경우는 고객의 특성에 기인한 것으로 조사되었다. 특히, 자동차 등 해외수출 주도형 산업에서는 고객의 요구로 국제표준을 준용하지만, 고객이 요구하지 않을 경우에 특별한 준용 가이드를 사용하고 있지 않았다.

<표 4-20> 국제표준 未 준용 사유

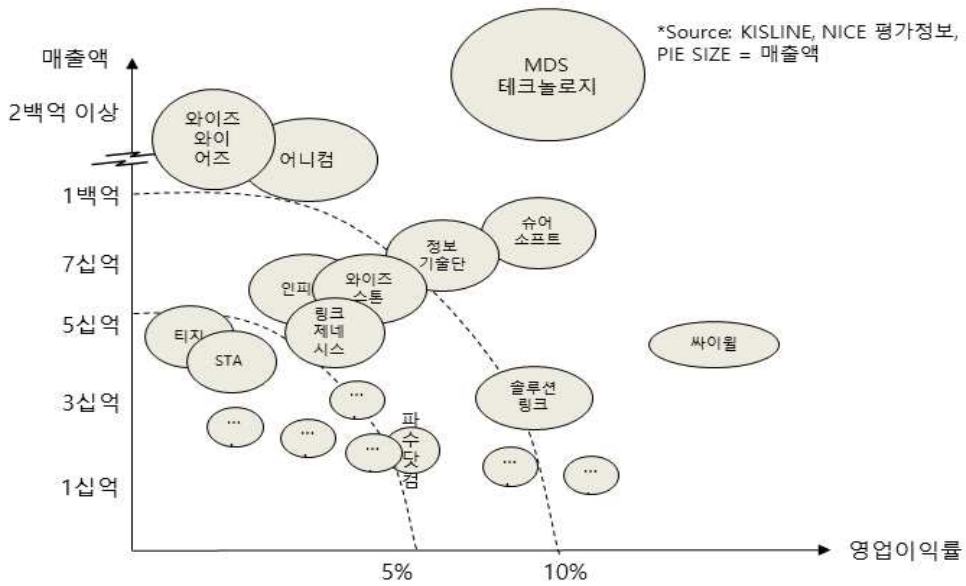
- ❖ 고객의 요구가 없거나, 고객사 요구에 따라 부분적으로 적용함
- ❖ 고객사 니즈도 크지 않고, 잘 모르기 때문, (소수) 해당 국제표준에 대한 정보 부재

9) 시장 규모 및 조사대상 기업 일반 현황

소프트웨어 안전 사업을 수행하는 기업 (자동화 툴 소프트웨어 개발, 안전 테스팅, 안전 관련 컨설팅 등 포함)을 대상으로, 소프트웨어 안전 및 제반 품질 서비스를 포함한 시장에 대한 재무 분석을 설문 및 인터뷰와 별도로 수행하였으며, 시장에 대한 주요 데이터 현황은 다음과 같다.

시장 규모의 경우 보수적으로 최소 2,600억 원 이상으로 추산되었는데, 이는 조사대상 30개 업체의 매출 합계 2,600억 원과 TIC분야가 별도의 산업 군으로 구분되어 있지 않아 조사대상에 포함되지 못한 업체가 많아, 이들 업체의 매출을 모두 포함해서 추정한다면, 2,600억 원을 크게 초과할 것으로 예상된다. (일부 2014년 매출 자료가 없는 6개 기업의 경우, 해당 업체의 2~3년 치 연평균 성장률을 적용해서 2014년 매출을 추정하였고, 일부 매출 100억 이상 업체의 경우, TIC 부분 外 매출이 클 경우, 전체 매출에서 TIC 부문의 매출만 추정하여 반영하였다)

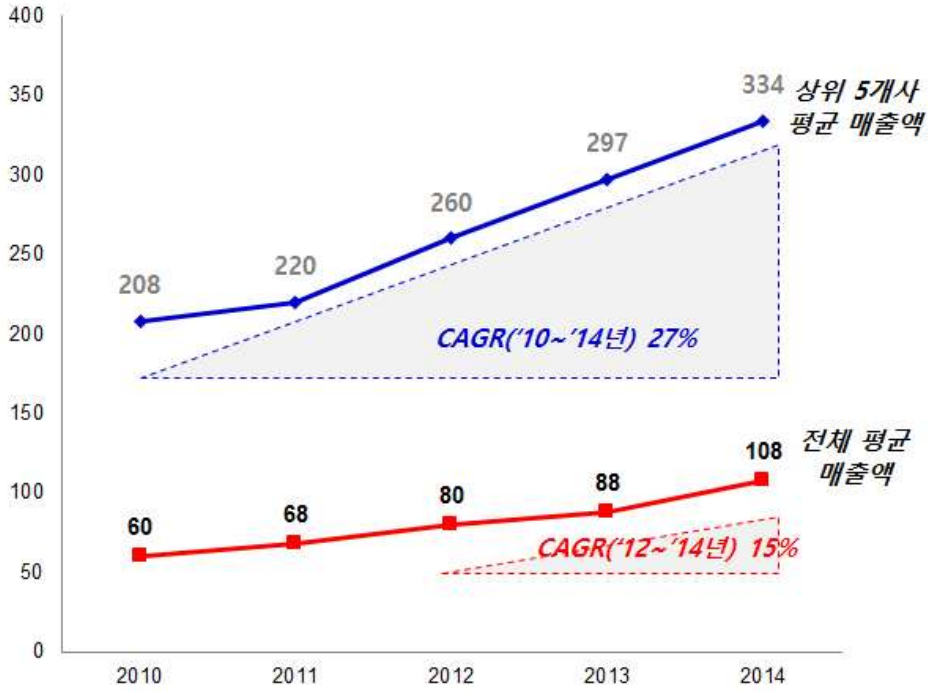
[그림 4-5] 30개 소프트웨어 안전 분야 사업 기업 매출 및 영업이익율



연평균 성장률(CAGR)의 경우 2012년 이후 2014년까지 소프트웨어 안전 분야 사업 기업은 CAGR 15%로 他 산업대비 고속성장을 지속하여 왔음을 확인할 수 있었고, 시장 전체적으로 동반 성장 중이지만, 그 중 특히 상위 5개사의 성장률이 두드러졌다. (상위 5개사 평균 CAGR 27%로 평균 대비 약 2배 수준) 따라서 현재까지는 시장 내 독보적인 독점이 존재하지 않고, 전체 시장이 지속적으로 타 산업대비 高 성장 중이며, 3 ~4년 후에는 시장 주도적 기업들이 등장할 것으로 예상된다. (조사 한계 및 기

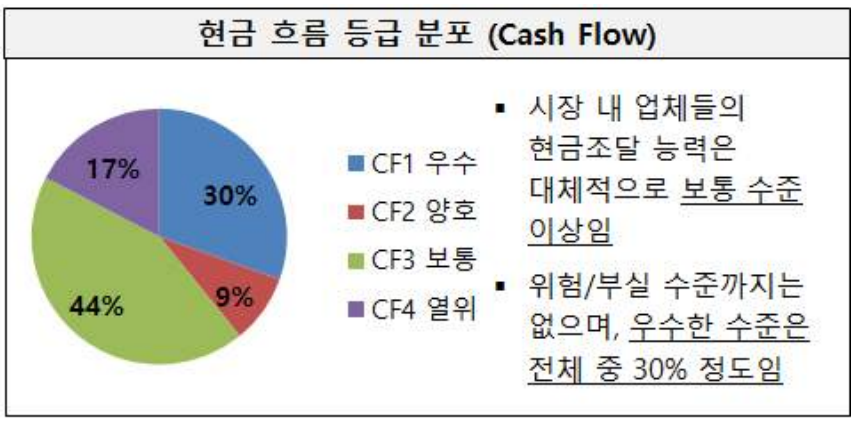
준: 상위 5개사의 경우, 업력이 오래되어 5년 치 CAGR 산출이 가능하였으나, 나머지 업체의 경우 업력이 짧거나 영세하여 해당년도 매출 파악이 되지 않는 경우가 존재하여 3년 치 CAGR을 산출하였다. 그리하여 전체 CAGR은 3년 치를 기준으로 산출하였다.)

[그림 4-6] 소프트웨어 안전 분야 사업 기업 연평균성장률



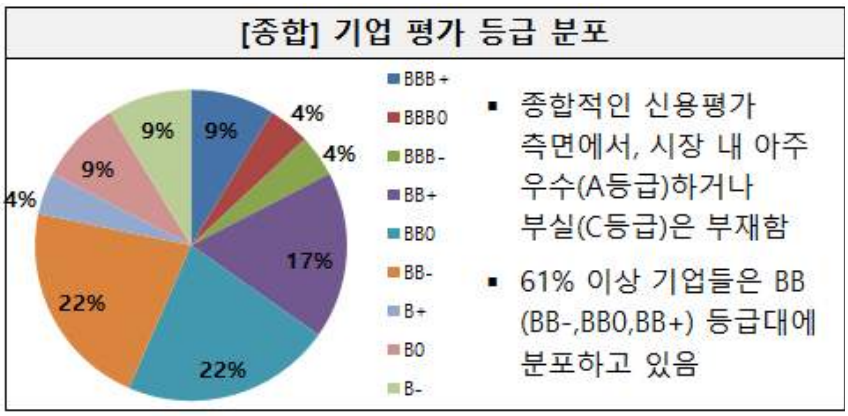
재무 현황의 경우, 소프트웨어 안전 분야 사업 기업들은 현재까지 내/외부적인 환경 변화에 부정적인 요인이 크지 않고 현금 흐름 측면에서도 보통 수준 이상으로 조사되었다.

[그림 4-7] 소프트웨어 안전 분야 사업 기업 현금 흐름 등급 분포



대부분의 조사대상 기업이 상거래를 위한 신용능력은 보통이며, 경영여건 및 환경 등 영향에 따른 거래안정성도 보통 수준으로, 최소한의 재무적인 여건을 보유한 것으로 판단된다.

[그림 4-8] 소프트웨어 안전 분야 사업 기업 평가 등급 분포



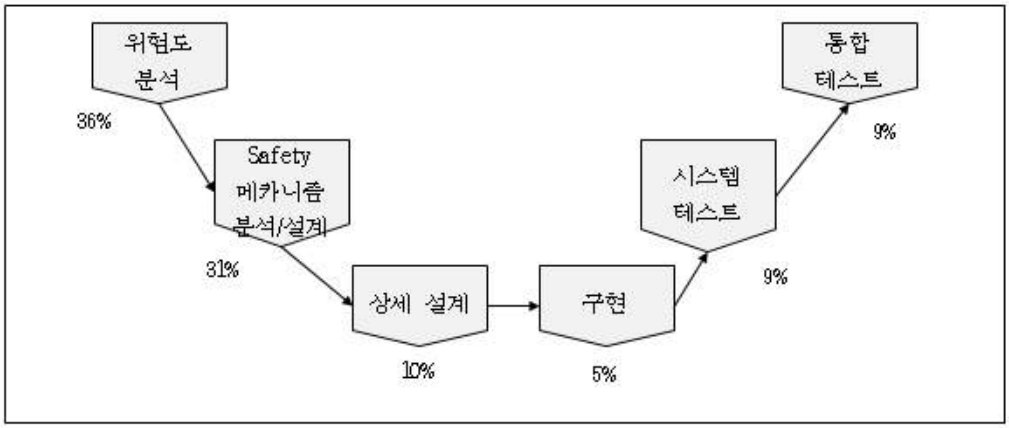
[그림 4-9] 소프트웨어 안전 분야 사업 기업 Watch 등급 분포

3. 프로세스 분석

1) 소프트웨어 안전 라이프사이클 中 중요 프로세스

조사대상이 인식하는 안전 프로세스의 각 단계별 중요도는 아래와 같다.

[그림 4-10] CMMI 기반 안전 프로세스 V 단계별 중요성



전체 업체 중 77%가 구현단계 이전 활동이 안전차원에서 가장 중요하다고 인식하고 있으며, 특히, 위험도 분석(36%) 및 안전 메카니즘 분석/설계(31%) 단계는 동등하게 중요하다고 인식하고 있었다. 이는 예방차원에서 상세 설계가 진행되기 전에 안전에 대한 요건이 정의되고 이를 반영하여 설계가 수반되는 것이 안전의 예방관리 차원에서 중요하기 때문으로 파악된다.

<표 4-21> 사전 단계 중요성에 대한 업계 견해

❖ 초기 위험분석을 통해 안전요건이 정의되고, 소프트웨어 테스팅 설계에 반영되어야 하며, 테스팅에서는 이를 Risk 기반 테스트라고 함
❖ 소프트웨어 개발 앞 단계에 투입되는 비용은 사후 오류/사고가 발생했을 때 발생하는 비용 대비 약 1:100 정도의 비중으로 중요하다고 할 수 있음
❖ 안전과 관련된 결함은 수정 및 변경에 많은 노력과 비용이 수반되기 때문임
❖ 그러나 현실은, 앞 단계에 대한 서비스 접근이 고객의 보안 이슈 때문에 어려운 상황임
❖ 안전 메카니즘 분석 및 설계를 통해 실제 회피 방안을 마련할 수 있음

2) 기존 인증제도 효과성

현재 국내에서 적용되고 있는 소프트웨어 관련 인증제도 (GS인증, SP인증 등)는 조사대상 중 76%가 소프트웨어 안전성 확보차원에서는 효과적이지 않다고 응답했다. 일부 기존 인증제도가 효과적이라고 보는 입장은, 전문적인 테스트를 받음으로써 품질이 제고되는 측면이 있음을 언급하고 있으며 중소기업 차원에서 도움이 될 것으로 보고

있다. 이는, 열악한 국내 중소 소프트웨어 개발 환경에서 필요한 최소한의 품질 활동 가이드를 제시하는 것에 대해 긍정적으로 보고 있다는 것을 의미한다. 대부분의 조사 대상 업체는 GS, SP 등 국내에서 적용되고 있는 인증제도는 소프트웨어 안전(Safety)을 제고하는 용도로는 적합하지 않다고 보고 있다. 이는 업체가 GS, SP인증 등의 품질 인증만으로는 안전에 대한 요구사항을 만족할 수 없다고 인식하고 있는 것으로 판단된다.

<표 4-22> 기존 인증제도 관련 문제 및 개선 방향

❖ GS는 전반적 품질에 대한 검증이고, 안정성에 대한 검증이 아니다. 안전 메카니즘에 대한 검증을 해야 함
❖ SP는 프로세스 수준의 인증이고 실제 분석/설계 등 산출물의 내용에 대한 검증은 아님
❖ 인증제도에 적용되는 표준 중, 안정성에 대한 기준은 없는 것으로 알고 있음
❖ 일부 기여하는 것은 맞는데, 안전이 높아지는 것은 아닌 것 같음
❖ GS인증, SP인증은 Safety를 전혀 반영하고 있지 않다. 기능안전 관련 국제표준 내용을 분석하여 품질 및 프로세스에 대한 내용에 Safety에 대한 내용들이 보완되어야 할 것임
❖ 단발성의 인증보다 지속적 모니터링이 중요함
❖ 산업 도메인에 일반적으로 적용되는 인증제도는 안정성 확보가 필요한 소프트웨어 프로젝트에서 특화시켜 적용해야 함
❖ 단발성의 인증보다 지속적 모니터링이 중요함
❖ (본 설문의 취지와는 다른 일부 의견) 기존 국내 인증제도의 인증 비용이 높다고 봄

3) 안전에 대한 등급/레벨 구분

IEC 61508 국제표준에서 안전 무결성 수준을 관리하기 위한 SIL(Safety Integrity Levels) 1~4단계의 기본 레벨을 부여하고 있으며, 주어진 조건하에 있는 안전관련 시스템이 주어진 시간 내에 요구되는 안전기능을 만족스럽게 수행할 수 있는 확률로 정의되고 있다. 국내에서도 각 산업별로 SIL 단계를 준용한 등급을 구분하여 안전 관리 및 서비스를 수행하고 있다. 업계에서는 대체적으로 형식적인 등급/레벨보다 실질적인 안전을 위한 운영을 강조하고 있다.

<표 4-23> 업계에서 적용 중인 등급/레벨

구 분	내 용	비 고
자동차	A-SIL 등급으로 명명됨 A (안전이 별로 중요하지 않은 레벨) B, C (안전이 중요한 레벨) D (안전이 가장 중요할 레벨)	A 레벨은 단순 품질 조건이 충족된 정도
전자	Defect Level 1~5 가장 위험한 것은 사이트다운 (Level 5) 간헐적으로 죽거나 결재가 안됨 (Level4), 하위기능이 간헐적으로 안되는 경우가나 UI 개선 등 (Level2)	사이트 오픈 전, Level별로 기능품질 조건을 90%, 98% 등 기준을 고객별로 협의, 테스트결과와 기준 비교 후 오픈 결정
일반	결함의 심각도를 기준으로 1~5 등급 시스템 다운 (1등급), 오동작 (2등급) 등	

<표 4-24> 등급/레벨 방향에 대한 업계 견해

❖ 소프트웨어 안전을 위해서는 임베디드 소프트웨어에 대한 이해가 필요하며, 등급/레벨도 순수 소프트웨어만으로 구성된 시스템만이 아닌 전체적인 차원에서 정의되면 좋을 것임
❖ 산업별로 국제표준에 따른 안전등급 방식이 일부 상이하지만, 안정등급의 성격은 내용적으로 동일하며, 이러한 등급 체계 및 방식을 이해하고 적용해야 함
❖ 국내에서 별도 등급체계를 만드는 것보다, 각 산업별로 국제표준을 따라야 함

4) 법/제도 방향성

업계에서는 소프트웨어 안전을 위해 크게 세 가지 차원에서 방향성을 언급하고 있다. 첫째는 기본법적인 상위차원의 안전으로서 법/제도 차원에서의 강제화이며, 둘째는 소프트웨어 안전 산업자체에 대한 산업 군으로서의 지정 필요성이다. 마지막으로 분리발주에 대한 부분도 제도적으로 강조되고 있는데 이 부분은 별도로 정리하였다.

일부 법/제도 필요성에 대해 부정적인 견해는, 국제표준은 정해져 있고 각 산업별로 적용할 표준을 민간에서 요구하면 국가에서 지원할 수 있는 부분은 아니라고 보는 시각이다. 이러한 의견은 법/제도를 국제표준 자체와 상응하는 것으로 인식한 내용으로 이해되며, 안전제고를 위한 법/제도가 무용하다고 주장하는 것은 아니다.

소프트웨어 안전에 대한 Ground Rule이 될 수 있는 소프트웨어 안전법 같은 기본법이 필요한 것으로 조사되었다. 구체적으로는, 산업 군별 안전계통과 비 안전계통 시스템에 대한 분류 기준이 정해져야 하고, 안전계통 시스템의 경우 해당 도메인의 국제표준에 준하는 안전성 표준을 준수하라는 수준의 법이 필요한데, 정부가 품질/안전차원에서 최소한의 가이드 및 규정을 만들고, 민간에서는 필요한 것을 만들어 쓰도록 하는 것이 적합하다고 분석되었다. 소프트웨어 안전 문화를 정착시키기 위해서는 시간과 비용 등 Cost가 수반되기 때문에 시장원리에만 맡겨놓을 경우 작동하지 못할 위험성이 있으므로, 법/제도 측면에서 징벌적 성격을 가지는 일종의 강제화가 필요하다고 조사되었다. 현재는 예방 조치에 대한 규제는 거의 없기 때문에 최소한 ‘ 제조물 책임법’ 수준의 포괄적인 규정 정도로도 효과가 있을 것으로 예상하였다. 이는 본 연구의 선진사례 자동차산업 도메인에서 조사되었듯이, 미국/유럽의 경우 별도로 법/규정에 명확한 안전표준 준수를 명문화 하지 않아도, ‘ 제조물 책임법’ 에 의하여 포괄적으로 안전표준 준수가 강제화 되는 효과가 발생하기 때문이었다. 일반법 측면 외에 구체적인 규정의 제정 필요성도 언급되었다. 예를 들어, Mission-Critical한 소프트웨어는 위해도 분석, 정적분석 및 동적시험을 반드시 하도록 규정하는 것 등이다.

또한, 현재까지 소프트웨어 안전이라는 산업 군이 존재하지 않아, 소프트웨어 안전에 대한 시장 조사 및 해당 정책이 수립되기 어려운 실정이므로, 산업 군이 선행되어야 소프트웨어 안전 산업이 활성화될 것으로 조사되었다. 특히, 분리발주에 대한 이슈도 공론화되고 있지만, 실행이 어려운 이유로서 소프트웨어 안전이 별도의 산업 군으로 지정 되어 있지 않기 때문이라고 보는 측면도 있었다.

5) 관련 매뉴얼/Tool

산업 내에서 소프트웨어 안전에 대한 서비스가 활성화되어 있지 않은 만큼, 관련 매뉴얼이나 Tool도 안전 부분보다 소프트웨어 품질 측정을 위해 필요한 Tool 중심으로 이루어져 있었다. 안전에 대한 Tool은 전체 조사대상 중 일부의 소프트웨어 안전 컨설팅社 정도가 보유하고 활용하고 있는 실정이나, 안전 요건이 강화되면 Tool에 대한 수요도 높아질 것으로 예측된다.

<표 4-25> 소프트웨어 안전/품질 관련 Tool 사용 현황

구 분	내 용	비 고
안전	• 안전 프로세스 관리, 안전성 분석을 위한 Tool (일부 존재) • SIL 프로세스 관리 시스템 운영 Tool	안전을 위한 전문 분석 Tool 기반 미약
품질	• 소프트웨어 성능, 신뢰성에 대한 시험항목과 측정도구 • 소프트웨어 자동화 테스팅 Tool • 소프트웨어 요구사항/형상/변경/이슈/빌드/배포 관리 Tool • 소프트웨어 개발 생명주기 영역에 대한 테스트, 리스크 Tool • 프로세스 매니지먼트 Tool • 소프트웨어 개발/테스트 주체 커뮤니케이션 Tool: 버그 트래킹 시스템 Tool 등	품질 측면에서 다양한 Tool이 활용되고 있으며, 테스팅 자동화 Tool에 대한 수요가 많음

또한, 소프트웨어 안전 제품 및 서비스 확대를 위해 업계에서는 소프트웨어 안전 관련 데이터에 대한 축적 및 관리와 국제표준 매뉴얼의 국내 적용에 대한 정부 지원이 필요하다는 의견을 주었다.

<표 4-26> 향후 필요한 매뉴얼/Tool에 대한 업계 의견

❖ 소프트웨어 위험, 재난, 사고 데이터들에 대한 축적 관리 매뉴얼이 필요함
❖ 해외의 규제 지침이나 표준이 모호하게 되어 있으므로 국내에 적용하기 어려우며, 소프트웨어 안전 차원에서 이를 해석하고 적용할 수 있는 매뉴얼이 새롭게 만들어져야 함

6) 인력 현황

소프트웨어 안전 및 품질에 종사하는 인력의 규모는 공개된 현황자료와 업체 인터뷰에서 확인된 바로는, 한 업체당 평균 약 90여명의 규모를 보이고 있다. 그러나 인원 규모는 상위 매출업체와 일반 매출업체간 차이가 크므로 평균보다는 중앙값(Median)을 기준으로 약 30명 정도의 규모가 일반적이었다.

<표 4-27> 조사대상 중 소프트웨어 안전/품질 Player 인력 현황

구 분	규 모	Reference
매출 상위5개사	평균 인력은 약 315명 수준, 중간값은 약 243명 수준	KISLINE, NICE 평가정보
전체 조사대상	평균 인력은 약 93명 수준, 중간값 약 36명 수준	
생산성	매출 상위5개사: 매출액 대비 인당 약 1억1천4백만 원 생산	
	전체 조사대상: 매출액 대비 인당 약 1억1천4백만 원 생산	
시사점	소프트웨어 안전/품질 인당 생산성은 약 1억 원대로 중소기업 평균 생산성 0.9억과 비슷한 수준임	
	가장 많은 업체가 분포하고 있는 업체 당 30명 수준으로는 전문성이 확보되지 않으면 지속적인 성장이 어려울 수 있음	

인력 관련 주요 이슈는 산업도메인별 업무 전문성을 가진 소프트웨어 전문가 확보가 어렵다는 것이다. 즉, 소프트웨어 엔지니어링 측면도 중요하지만 고객의 업무를 이해하고 안전 컨설팅을 수행할 수 있는 산업도메인 전문가가 없다는 것이고, 이를 양성 및 확보가 어렵다는 의견이 많았다. 원인으로는, 전문가를 양성하기 위해 교육체계를 수립한다고 해도 교육을 수행할 전문가가 없으며, 사회/문화적인 측면에서 소프트웨어 안전에 대한 중요성 인식이 사회적으로 낮고, 산업적인 측면에서 보상이 부족한 현실에서 산업도메인 전문가의 영입이 어려운 것 등으로 분석되었다. 또한, 사내 전문가를 육성하는 차원에서 업체별로 진행하고 있는 교육은 그 자체로 필요성 및 효과성이 있으나, 아직까지 소프트웨어 안전에 대한 교육을 체계적으로 수행하고 있는 곳은 부족하다.

해외 인력에 대한 소싱 여부는 대부분의 업체에서 니즈가 없으며, 그 원인은 고객정보에 대한 해외 유출 및 커뮤니케이션상의 이슈로 부담을 가지고 있는 부분이 가장 크다고 할 수 있다.

7) 지원 요구사항

(1) 법/제도 측면

제품이나 서비스를 제공하고 있는 기업이 소프트웨어 안전에 대한 중요성 및 파급효과에 대한 인식은 하고 있으나, 투자가 수반되지 못하고 있다. 대기업은 그나마 가능하나 중견기업은 안전에 대하여 투자하기 어려운 상황이다. 예를 들어, 일부 중견기업 등으로부터 안전에 대한 요구 사항이 있으나, 가격적인 이유로 진행되지 못하는 경우가 대부분이었다. 또한, 소프트웨어 안전 사업을 수행하는 개발 및 담당자들의 문화도 보수적이다. 선진국의 경우 소프트웨어 개발 후, 소프트웨어 인스펙션(Inspection) 시, 관련자들이 Line by Line을 검토하는 것이 당연한 협업 문화로 정착되어 있는 반면, 국내에서는 개발 담당자가 본인이 수행한 업무에 대하여 타인이 검토하는 것을 꺼리는 경향이 많다. 따라서 소프트웨어 안전에 대한 인식 제고뿐만 아니라, 소프트웨어 안전에 대한 사회/산업적인 기반이 성숙되어야 해결될 것으로 분석되었다. 또한, 중장기적 차원에서 단순한 경제적인 지원보다 소프트웨어 안전을 중시하는 사회/문화측면의 성숙이 동반되어야 할 것으로 분석되었다.

업계에서는 소프트웨어 안전을 위한 법/제도적인 지원 방향은 1차적 국제표준에 대한 국내 적용 및 이해를 제고할 수 있는 매뉴얼의 한국화, 보급화를 언급하고 있으며, 2차적으로 국제표준이 준용될 수 있도록 제도적으로 발주요건에 소프트웨어 안전성 기능항목을 의무화하는 방향, 마지막으로 이와 관련하여 분리발주 제도화를 통한 소프트웨어 안전의 독립성 강화의 필요성을 제시하였다.

<표 4-28> 소프트웨어 제3자 분리발주 관련 의견

❖ 감사와 마찬가지로 개발과 안전/품질 테스트는 분리가 되어야 하며, 전문업체가 객관적인 시작을 가지고 테스트를 해야 함
❖ SI 프로젝트의 경우 개발자가 테스팅 평가를 하는 것은 맞지 않으므로, 테스팅 평가는 제3자 테스팅 업체가 참여해야함. 발주처가 개발평가 결과를 제대로 알 수 있어야 함
❖ 분석/설계와 개발/테스트 간에는 분리발주가 되어 있으나, 개발/테스트 간에도 분리발주가 되어 제3자 테스트가 가능해야 함

(2) 인증제도 측면

소프트웨어 신뢰성 개발/검증 사업자들은 소프트웨어 안전 관련 인증 체계에 대한 이슈를 제기하고 있으며, 국내 인증시장이 글로벌 선진사에게 잠식되고 있는 현황을 우려하고 있었다. 또한, 업계에서는 인증 시장에 대해 글로벌 선진사에 지불하는 高인증 비용을 지양하고, 아직 영세한 국내 소프트웨어 안전 관련 기업들의 사업 안정성

확보를 위해, 국내 소프트웨어 안전 인증 제도 수립 및 시장 육성 방안이 필요하다고 보고 있었다.

<표 4-29> 국내 SIL 인증 시장 현황

구 분	내 용	비 고
선박	전체적으로 높은 인증비용을 지출하고 있음 수행비용에 인증비용을 포함하여 약 30여년간 지출됨	글로벌社 지출 (로이드)
자동차	현대/기아차가 자체적인 수행을 통해 외부 인증 비용 억제 중. 또한, 완성차 약 30만 협력사가 SIL 인증을 받기 어려운 현실임	글로벌社 진입 가능성
철도	SIL 인증비용을 지출하고 있음 글로벌사가 안전성 인증을 독점하고 있음	글로벌社 진출 (리카르도 레일-로이드)
원자력	인증비용을 지출하고 있지 않으며, KINS에서 검사를 수행 중임	-
의료	해외에서 인증을 받지 않으면 수출을 하지 못함	인증비는 높지 않음
항공	국내에서 인증에 대한 지출을 아직까지 한 적 없음	

<표 4-30> 국내 안전 인증제도 관련 업계 견해

❖ 국내인증 표준은 국제표준 준용
❖ 시험 역량, 컨설팅 역량, 시험도구 필요
❖ 내수용으로 사용하는 제품보다, 해외 수출을 위한 대상에 대해 국내 인증기관 활용 필요

(3) 인적/교육 측면

소프트웨어 안전이 중요한 산업도메인의 지식을 보유한, 소프트웨어 안전 전문가 육성이 필요한 것으로 조사되었다. 이를 위해서는 자격제도는 의미가 크지 않으며, 단순한 인력의 數적인 증가가 중요한 것이 아니라, 해당 산업도메인별(제품/부품 포함) 소프트웨어 안전 전문가가 필요한 것으로 조사되었다. 전문가 역량 측면에서도 현재 우리나라는 신뢰성, 개발 프로세스 및 테스팅 측면에서 글로벌과 비교하여 역량적인 Gap이 크다고 업계에서 느끼고 있었다. 이를 극복하기 위한 방안으로, 상시적인 교육

도 수행되어야 하지만, 근본적으로 기초 교육측면에서 소프트웨어 안전의 중요성이 인식되어야 한다는 시각을 가지고 있었다. 정규교육 과정에 소프트웨어 안전 분야를 신설하고, 이를 통해 소프트웨어 안전 분야 직군에 대한 국내 인식이 제고될 수 있도록 하는 방안도 제시되었으며 전문적인 소프트웨어 안전 교육체계 및 기관이 필요하다는 의견도 많았다. 또한, 지금은 소프트웨어 안전 교육관련 매뉴얼도 없는 상황이므로, 사전에 이를 위한 매뉴얼 제정이 필요하다고 조사되었다.

<표 4-31> 주요 선진국 소프트웨어 교육 현황

구 분	내 용	비 고
영국	초/중/고 소프트웨어 코딩 필수과목 도입 운영 중	필수 교육 차원
미국	유치원/초/중/고 소프트웨어 코딩 수업 도입 - 연방 차원 2만여 명 교사들이 코딩 수업 리드 뉴욕/시카고 등 대도시 약 30개 학군 코딩수업 개설 합의 컴퓨터 수업을 선택 아닌 기초 수업化 - 9개주 교육 당국	기초 교육 확대

자료: 한국경제, 2014

소프트웨어 안전 산업의 활성화 및 전문가 양성을 위해 제도적인 보상이 필요하다는 의견이 많이 제시되었다. 현재, 소프트웨어 개발 단가체계는 있으나, 안전(위해도 분석, 안전 메카니즘 설계, 분석, 테스팅 등)을 위한 단가체계는 없으며, 중요성에 대한 인식도 낮은 편이었다. 따라서 소프트웨어 안전에 대하여 차별화된 단가 체계 마련과 안전공학을 전공한 소프트웨어 안전 전문가에 대한 인센티브 지원 등의 소프트웨어 안전 산업 활성화를 위한 환경 조성이 필요한 것으로 분석되었다.

(4) 시장 측면

업계에서는 소프트웨어 안전의 속성상 비자발적인 시장이라고 보고 있다. 즉, 고객이나 산업에서 요구하지 않으면, 추가적인 비용을 들여 소프트웨어 안전에 대한 활동을 수행하는 것을 꺼려한다는 것이다. 품질의 경우 인증을 받으려면 품질 테스팅을 하지 않을 수 없으므로 품질 테스팅 시장이 조성된 측면이 있다. 그러므로 안전의 경우도 제도적으로 강제화 되거나 보장되지 않으면, 자생적으로 성장할 수 있는 시장이 아니라고 보고 있었다.

소프트웨어 안전부문은 품질부문과 구분되어 강조될 필요가 있는 것으로 조사되었다. 소프트웨어 안전 시스템은 납품으로 완료되는 것이 아니라, 지속적인 유지 활동까지 관리와 지원이 필요하므로, 高 안전이 요구되는 시스템에 대해서는 발주부터 다른 체계로 적용되어야 하며, 산업적인 활성화를 위해서는 시장에서 소프트웨어 안전과 관련하여 발주처의 기능/요건 요구를 의무화해야 할 필요가 있는 것으로 조사되었다. 구체적으로 보자면, 소프트웨어 안전 관련 인증된 Tool로 검증했는지를 의무화하는 것도 필요하다는 것이다 (예, 5억 이상의 소프트웨어에 대해 인증된 Tool을 사용하여 테스팅을 하라는 요건). 또한, 국내는 구현 단계의 테스트에 집중되어 있으나, 개발 초기 단계에서부터 안전 요건 정의 및 안전 활동 수행 의무화가 필요하다고 조사되었다.

비자발적인 시장 성격을 고려하여, 소프트웨어 안전 산업 활성화를 위해서는 공공 주도의 산업 활성화 방안이 필요하다고 조사되었다. 즉, 안전과 밀접한 관련이 있는 국가기반시설 발주 시, 요구사항에 소프트웨어 안전요건을 포함함으로써, 민간업체들이 자발적으로 소프트웨어 안전 요건을 강화하도록 유도하여 자연스럽게 국내 안전 산업이 활성화되도록 하자는 의견이 많았다.

(5) 요구사항 종합

주력 제품/서비스를 기준으로 국내 안전 분야 사업 기업의 실태조사 대상이 된 업체들의 요구사항을 앞서 도출한 해결방안 6가지 부문을 활용하여 Grouping하면, 법/제도 측면, 표준/절차/가이드 측면, 인력/교육 측면, 業 환경개선 측면의 4가지 부문으로 정리할 수 있었다. (<표4-34> 참조).

소프트웨어 사업 수행 주체들의 입장을 반영한 다양한 건의가 있었으나, 특히 안전 사업 종사 기업의 특성상 業 환경개선에 대한 요구 사항이 많았는데, 특히 소프트웨어 안전을 위해서는 공통적으로 ‘ 소프트웨어 안전 기능성에 대한 발주요건 의무화’ 와 ‘ 소프트웨어 안전 활동 및 안전 전문 인력에 대한 적정 대가 체계’ 를 중요하게 언급하고 있었다. 법/제도 측면에서는 안전을 위하여 규정화가 필요하다고 요구하였고, 표준/절차/가이드 측면에서는 체계적인 안전 매뉴얼 제정의 필요성을, 인력/교육 측면에서는 안전 전문가 육성이 요구되었다.

<표 4-32> 업체 요구사항 종합

구 분	건 의 사 항	비 고
법/제도	• 안전을 위해서는 법/제도 측면의 강제성이 필요	
표준/절차/가이드	• 국제표준을 준용할 수 있는 한국형 매뉴얼 등의 제도 지원 필요 • 소프트웨어 안전 관점에서 창조적 시장 창출이 필요하며, 이를 위한 Think Tank가 필요함	
인력/교육	• 소프트웨어 전문 안전 QA가 필요함 • 소프트웨어 품질 인력에 대한 교육 강화 및 인식수준 제고 필요	
業 환경개선	• 소프트웨어 안전 기능성에 대한 발주요건 의무화 • 제3자 검증을 위한 분리 발주 의무화 필요 • 소프트웨어 안전 기능성에 대한 발주요건 의무화 • 소프트웨어 안전 기능성에 대한 발주요건 의무화 • 소프트웨어 품질 직군에 대한 단가체계 정의 필요 • 소프트웨어 안전 활동에 대한 적정 MM(Man Month) 및 기간 인정 • 시장측면에서 개발 항목 內, 소프트웨어 안전에 대한 항목을 구별하여 차별화된 대가 확보 필요 • 공공부문 주도의 소프트웨어 안전 산업 활성화 • 소프트웨어 안전 Reference(Track Record) 확보 지원	중복된 건의사항의 경우 강조를 위해 통합/정리하지 않고 모두 기술하였음

4. 소프트웨어 기능안전 특화 기업

국내 TIC 시장 사업기업의 경우, 한 가지 서비스만을 제공하기 보다는 두 가지 이상의 서비스를 복합적으로 제공하고 있으며, 각 업체 별 주력 제공 서비스는 매출로 구분하거나 고객에게 제공하는 서비스를 세부적으로 분석하여 객관적인 기준을 가지고 주력 사업을 구분하기가 어렵다. (기업별 매출을 세분화 하여 제공하지 않으며, 상세 내역은 기업 비밀이라 공개 불가) 따라서, 본 조사에서는 업체 인터뷰 결과(주요 업무 및 구체적인 서비스)를 기준으로 소프트웨어 기능안전 특화 기업으로 구분하여 별도의 조사결과를 제시하였다.

이들 기업의 주요 업무는 시스템 진단/분석과 시험평가이며, 주요 제공서비스는 서비

스는 Safety 검증/인증, 시스템 소프트웨어 메카니즘 설계, 소프트웨어 테스팅 등이 있었다. 상기 업무 및 서비스를 위해 필요한 자격증이나 자격요건은 일부 인증 및 테스팅에 대한 부분을 제외하고는 대부분 없었는데, 이는 이들 서비스 대부분이 매우 깊은 산업 도메인 지식(Industry Domain Knowledge)를 보유하고 있어야 수행할 수 있어, 단순 자격증보다는 서비스 제공 인력의 해당 산업 도메인에서의 실제 업무 수행 경험이 더 중요한 요소로 인정되기 때문이었다. 따라서 이러한 업무를 수행 할 수 있는 핵심 인력은 국내 기업 여건상 확보하거나 육성하기가 매우 어려운 실정이었다.

주요 고객군은 Private Sector로는 자동차, 중공업 등이 있고, Public Sector로는 철도, 원자력, 항공, 국방 등이 있었다. 특히, 자동차 부분의 경우 타 산업 군과 달리 소프트웨어 안전 표준(ISO 26262) 요구 사항이 강제화 되어 있지 않고 인증 또한 요구되고 있지 않음에도 불구하고 자동차 부분(완성차, 부품 포함)에 대한 비중이 높았는데, 국내 자동차 산업 비중이 크고, 해외 수출시 해외 선진국 등에서 제조물 책임법 등을 통해 소송 발생 시 소프트웨어 안전 표준 준수 여부 확인하고 있어 자발적으로 표준을 준수하고 있는 것으로 분석되었다. 고객이 원하는 주요 서비스로는 소프트웨어 분석, 안전 및 테스트, 소프트웨어 프로세스 안정성 규격 준수, 신뢰성시험(소프트웨어 정적 분석, 동적 시험) 등이 있었다. 서비스를 위한 주요 표준으로는 자동차의 경우 ISO 26262, 중공업 IEC 61508, 철도 RAMS, EN 50128, IEC 62279, 항공 DO-178B/C, 원자력 KINS 등 이었다.

이들 기업 중 절반이상이 소프트웨어 기능안전을 담보하기 위한 활동 중 중요 단계로 ‘ 위험도 분석 단계’ 를 꼽았고, 이는 예방 차원에서 위험도 분석을 통해 안전 기능을 도출하여 Safety Requirement를 정의하고 개발하는 것을 가장 중요하기 생각하고 있기 때문으로 분석되었다.

이들 기업의 요구 사항을 법/제도, 표준/절차/가이드, 인력/교육, 業 환경개선의 4가지 측면에서 별도로 정리하면 아래 표와 같다.

<표 4-33> 소프트웨어 기능안전 특화기업의 요구사항

구 분	요 구 사 항
법/제도	• 소프트웨어 안전법 마련 (예, 제조물 책임법과 소프트웨어 안전과 결부한 징벌적 과징금제도 확산) • 안전전문가의 엔지니어링부문 상시 점검 체계 제도화 • 주요 안전 도메인별 Hazard DB 구축 강제화 • 안전 전문업을 소신 있게 할 수 있는 제도적 장치 (예, 독일의 안전관련 부문의 고용 보장) ※제도적인 규정이 없을 경우, 자생적인 성장 어려움
표준/ 절차/ 가이드	• 산업별 상이한 소프트웨어 안전등급을 표준화 • 소프트웨어 안전 매뉴얼 구비 (해외 규정은 모호하므로 보수적으로 해석하여 적용) • 소프트웨어 소스코드 품질지표에 대한 기준/검사 매뉴얼 필요 • 소프트웨어 테스팅 툴 필요 ※소프트웨어 개발 프로세스 준수가 선행되면 소프트웨어 안전 이슈는 감소될 수 있음
인력/ 교육	• 제품/부품별 현장인력을 안전전문가로 육성 또는 안전공학 전공자의 유입 - 소프트웨어 개발자 역량 향상부터 선행되어야 함 - 소프트웨어 안전 프로세스 컨설턴트 양성 - 소프트웨어 안전성 테스팅 툴 전문가 양성 • 소프트웨어 안전 교육기관 및 교육체계 구비 - 시스템의 안전에 대한 이해가 선행되어야 함 - 소프트웨어 안전성 프로세스 국제규격, 실사례를 통한 안전 교육 강화 ※소프트웨어 안전교육은 법적 근거를 통한 생태계 최고 발주자를 통해 교육체계를 진행해야 효과 큼
業 환경개선	• 소프트웨어 안전 중요성 부각 및 안전문화 확산 필요 • 발주 시 제품이나 기능에 안전메커니즘 반영 의무화 • 소프트웨어 고안전 확보를 위해 납품~완료뿐 아니라 지속적인 유지활동까지 관리/지원 필요 • 소프트웨어 안전 전문가에 대하여 인센티브 지원 등 환경 필요 ※시장측면에서 인위적으로 안전전문가의 단가를 높게 책정하는 것은 시장원리측면에서 비현실적이므로 안전설계 항목의 의무화 등을 통하여 자연스럽게 안전생태계를 구축해야 함

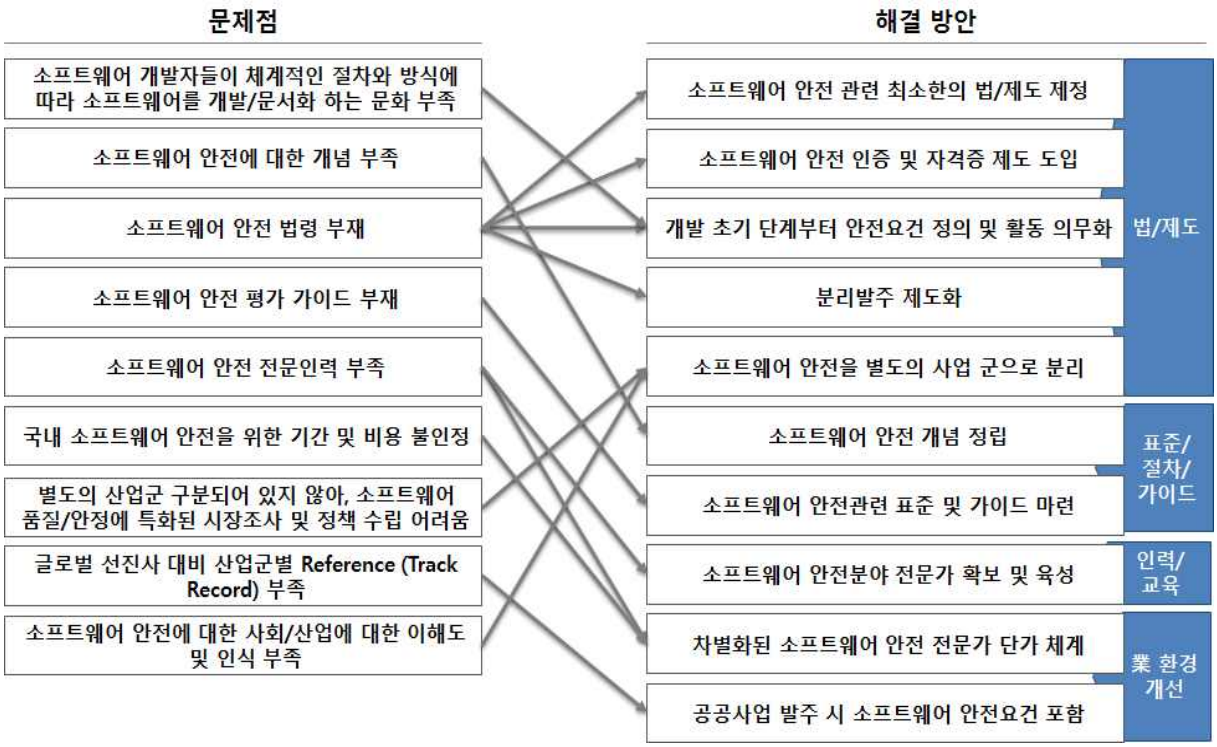
5. 조사 결과 종합 및 시사점

국내 안전 분야 사업 기업 분석 부문은 시장 현황, 문제점, 해결방안 및 요구사항으로 정리하였다. 시장 현황에서의 중요 시사점은 시장 규모를 보수적으로 추정하더라도 최소 2,600억 원대 정도이며, 연평균 성장률이 16%에 달하는 고성장 산업임에도 불구하고, 아직까지 제대로 된 산업으로 인정을 받지 못하고 있다는 것이다. 심지어, 표준 산업분류에서 소프트웨어 안전 산업이 구분되어 있지 않아, 안전에 특화된 통계 및 현황 분석이 이루어지기 어려운 현실이었다. 사회/문화적인 측면에서는 소프트웨어 안전에 대한 인식이나 이해가 낮아, 안전 활동을 할 수 있는 여건이 미성숙되어 있어 체계적인 안전 활동을 수행할 수 있는 기간 및 예산이 보장되어 있지 않고, 안전 활동이 간소화되거나 형식적으로 행해지는 경우도 많았다. 이로 인하여, 국내 업체는 산업 군별 Reference(Track Record)가 부족하여, 글로벌 선진사가 국내 시장 진입을 꾀할 때 제대로 된 경쟁을 하기 어려운 실정이었다. 또한, 안전의 특성상 비자발적인 성격이 강하여, 고객 및 시장의 요구 등의 일정의 강제성을 갖지 못하면, 제대로 소프트웨어 안전 활동이 준수되거나 이행되는 것이 어려워 보였다.

문제점 및 해결 방안의 경우 대부분 학계 및 공공기간에서 제시한 안과 유사한 안들이 많았고 산업 현장의 입장을 고려한 구체적인 항목들이 많았다. 학계 및 공공기관에서 제시된 문제점 외에 도출된 문제점 중, 주목할 만한 것으로는 표준산업분류표에서 소프트웨어 안전 산업이 별도의 산업 군으로 분리되어 있지 않아, 특화된 시장 조사 및 정책 수립이 간과되고 있다는 것이었다. 또한, 기존 Reference를 중시하는 보수적인 산업 특성상, 선진사 대비 각 산업 군별 안전사업 Reference(Track Record)가 부족하여, 보유 기술력과 상관없이 경쟁에서 배제되는 문제가 있었다.

해결방안 및 요구사항의 경우 소프트웨어 기반이 미 성숙된 단계이기 때문에 총 조사된 10개의 주요 해결 방안 중, 7개 부분이 법/제도(5개), 표준/절차/가이드(2개)로 정부나 학계/공공기관에서 능동적인 역할을 통해, 기반 정립을 요구하는 방안이 많았다. 또한, 조직/기관 및 프로세스에 대한 요구 사항 대신, 안전 사업 및 인력에 대한 적정한 대가가 보장되는 業 환경개선을 요구하였다. 도출된 해결방안 및 요구사항을 법/제도, 표준/절차/가이드, 조직/기관, 인력/교육, 業 환경개선, 프로세스의 6개로 구분하여 정리한 다음 문제점과 Mapping해 보면 아래와 같다. 그리고 국내 소프트웨어 안전 산업 기업의 문제점은, 학계 및 공공기관 조사에서 도출된 문제점에 추가적으로 3개의 문제점이 덧붙여졌다.

[그림 4-11] 소프트웨어 안전 사업 기업 문제점 및 해결 방안 Mapping



제3절 소프트웨어 개발/사용 기업

1. 개요

조사대상은 정보통신, 전기/기구제조, 금융, 방위산업 부문의 기업을 대상으로 하여 1:1 대면 인터뷰 방식으로 진행되었다. 인터뷰는 기업 내의 소프트웨어 안전 또는 품질 담당자를 대상으로 진행되었다.

조사영역은 소프트웨어 개발/운영 규정, 안전/품질 관련 조직, 소프트웨어 예방활동, 소프트웨어 사고대응/사후관리 활동 및 정책에 대한 지원 사항으로 구분하였고, 이러한 영역에 대한 설문을 기반으로 인터뷰를 수행하였다. 또한 소프트웨어 안전의 대상은 어플리케이션, 소프트웨어 탑재 부품, 소프트웨어 탑재 제품으로 구분하여 설문을 구성하였다. 인터뷰 대상 기업은 2.소프트웨어 안전 분야 사업 기업을 활용하는 기업이기 때문에, 소프트웨어 안전 뿐 아니라 소프트웨어 품질 및 테스팅의 범주에서 인터뷰가 수행되었다. 그리고 방위사업부문은 산업의 특성상 안전을 신뢰성이라는 용어로 이해하고 있었다. 본 조사 대상이 작아 의견이 각 산업의 대표성을 띄지는 않으나, 주요 조사대상인 소프트웨어 안전 분야 사업 기업을 활용하는 업체로서의 의견이라는 점에서 의미를 가진다.

<표 4-34> 소프트웨어 개발/사용 부문 조사 대상

업종	기업체	규모	조사방식	완료여부
정보통신	ICT사	매출 1조 이상	대면 인터뷰	완료
정보통신	정보통신사	매출 1조 이상	대면 인터뷰	완료
금융	금융증권사	매출 1000억 이상	대면 인터뷰	완료
전기/기구제조	전기장치사	매출 1000억 이상	대면 인터뷰	완료
방위산업	방위사업 전문업체	매출 1조 이상	대면 인터뷰	완료

2. 조사 항목별 현황 요약

각 기업의 소프트웨어 관련 규정 및 조직은 CMMI, ISO20000 등과 같은 국제인증에 따라 규정, 절차, 역할이 수립되어 있으며, 전체 안전/품질 비용은 정보통신업종 내에서도 시스템의 중요성에 따라 통상 2%에서 25%까지 할당하고 있었다. 소프트웨어의 테스팅 활동은 5개 기업 중 4개 기업이 테스팅 Tool을 도입/사용하고 있으며 외부 테스팅 전문업체를 활용하여 테스팅을 수행하고 있었다.

소프트웨어 사고 대응 활동 부문에서는 사고대응규정, 책임과 역할 및 대응 시나리오가 마련되어 있고, 사업부 또는 서비스 별로 차이가 있기는 하나 정기적인 모의훈련과 교육을 실시하고 있으며, 사고사례는 자료화하여 문서나 시스템 형태로 축적하고, 이를 소프트웨어의 개선, 테스트케이스 설계 및 교육 자료로 활용하고 있었다. 각 기업의 주요 조사 항목별 현황은 아래와 같이 요약된다.

<표 4-35> 조사 항목별 현황 요약

조사항목	ICT	정보통신	전기장치	금융증권	방위산업
전사 품질 규정	있음	있음	있음	있음	있음
품질/안전조직 체계	있음	있음	있음	있음	있음
품질비용	25% (보통10%)	~2.5%	-	-	-
테스팅 점검 및 업체 활용	테스팅 Tool 사용 (외산)	테스팅 Tool 사용	없음	테스팅 Tool 사용 (국산)	테스팅 Tool 사용 (외산)
	국내업체 활용	국내업체 활용	없음	국내업체 활용	국내업체 활용
사고대응체계 (규정 및 시나리오 보유)	보유 (정기적 훈련수행)	보유 (정기적 훈련수행)	보유 (정기적 훈련수행)	보유 (정기적 훈련수행)	보유 (정기적 훈련수행)
사고사례축적 및 활용	축적함 (서비스별 문서형태)	축적함 (10년)	축적함	축적함 (15년)	축적함
	테스트 설계, 교육 및 소프트웨어 개선	테스트 설계, 교육	테스트 설계, 교육 및 소프트웨어 개선	테스트 설계, 교육 및 소프트웨어 개선	테스트 설계, 교육 및 소프트웨어 개선

3. 항목별 인터뷰 결과

1) 표준/매뉴얼 현황

조사 기업들은 전사차원의 소프트웨어 운영 관리 규정과 절차를 수립하고 이에 따라 체계적인 소프트웨어 개발 및 운영 업무를 수행하고 있었으며, 이러한 규정과 절차를 준용하는 업무체계가 소프트웨어 안전의 기초가 된다는 의견이 있었다. 또한 각 기업들은 CMMI, ISO20000 등과 같은 국제표준인증을 취득했거나 준비 중에 있었으며, 소프트웨어 기업의 국제표준인증은 해외 진출 시 제품에 대한 최소한의 신뢰성을 제공하여 해외 업체 경쟁에 유리하게 작용할 수 있다고 하였다. 이미 해외 수출을 하고 있

는 기업에 대하여, 해외 고객이 국제인증을 요구하는 경우도 발생하고 있었다.

<표 4-36> 소프트웨어 국제표준인증 현황

도출 내용	인터뷰 내용
전사 규정과 절차를 준용하는 업무체계가 소프트웨어 안전 확보의 기초	• IT서비스 규정과 절차 수립 및 이에 따른 업무 수행 • 3년 주기 재인증 및 매년 2회 샘플링 검사를 통한 권고/부적합 사항에 대한 시정 조치를 실시함 • 서비스별 소프트웨어 개발 스타일은 다르겠으나, 규격과 기준을 준수한다면 소프트웨어 안전 확보는 따라오게 됨
국제표준인증은 해외 진출 시 제품에 대한 신뢰성을 제공하여 해외 업체 경쟁에 유리하게 작용할 수 있음	• CMMI, TMMI 국제표준인증을 취득하여 절차에 따라 업무를 수행함 • 해외 고객의 국제표준인증 요구로 소프트웨어 개발 부문 CMMI 인증을 준비 중임 • 해외 수출 시, 국제표준인증은 해외 업체 경쟁에 유리함

2) 소프트웨어 품질 조직 현황

기업의 품질조직은 체계적으로 조직화되어 있으며, 안전사고 발생을 대비하여 외부기관과 협력 채널을 구비한 곳도 있었다. 기업의 규모에 따라 전사-사업부-프로젝트 단위로 세분화시켜 품질기준의 적합성 여부를 점검하는 활동을 수행하고 있었고, 소프트웨어 안전을 포함한 안전사고의 대응이나 수습은 대외채널을 가진 안전관리조직에서 수행을 하기도 하였다.

기업 내부적으로 개발과 테스팅을 전문화하여 역할을 분리하는 것이 이상적이라고 인지하고 있으며 테스트 전담 조직을 운영하는 방향으로 추진하고 있다. 테스팅 인력을 조직화하여 운영하고 있는 기업도 있고, 테스팅 조직을 만들기 위해 역량을 확보중인 기업, 그리고 개발자가 테스팅을 동시에 전담하고 있는 기업도 있었으나, 전반적으로 개발/테스트가 독립적으로 운영되어야 한다는 인식과 테스트 전담 조직의 필요성에는 공감하고 있었다.

<표 4-37> 품질/테스팅 조직 현황

도출 내용	인터뷰 내용
품질조직은 체계적으로 조직화되어 있으며, 안전사고에 대한 별도의 채널을 구비하고 있음	• 품질담당조직은 전사-사업부-프로젝트로 조직화함 - 전사품질: 소프트웨어 개발의 분석, 설계, 개발, 구현 및 테스트, 인수인계 단계에서 품질기준의 적합성 점검 - 사업부품질: 사업부내 프로젝트의 샘플링 검사 실시 - 프로젝트품질: 단계별 Open Checklist를 통한 자체 QC(Quality Control)활동 수행 • 품질관리 담당자는 10년 이상의 경험을 가진 도메인 전문가로 구성 (총20명 중 10명), 사내 인력 뿐 아니라 국내/외 인력이 참여하여 검증활동을 수행함 • 기업 내 별도의 소프트웨어품질관리팀을 운영함 • 품질조직은 기술연구소 산하에 품질관리부서를 두고 있고 소프트웨어결함에 의한 사고, 메르스질병, 대테러, 천재지변 등의 사고로 인한 장애발생 대응활동에 대하여 리스크위기관리 전담부서를 두고 대/내외 업무를 수행함 • 전사내 소프트웨어 신뢰성 담당 인력을 보유함
기업 내부적으로 개발과 테스팅을 전문화하여 역할을 분리하는 것이 이상적이라고 인지하고 있으며 테스트 전담 조직을 운영하는 방향으로 추진하고 있음	• 사내 인력으로 구성된 테스팅 조직에서 시스템 구축의 테스트를 지원함 • 내부 테스팅 인력의 양성과 이를 조직화하여 단계별 테스트 수행 체제로 전환할 계획임 • 테스팅 인력의 부족 또는 부재로 인하여 외부 전문업체를 활용함 • 개발자와 테스터의 역할을 분리하는 것이 이상적이라는 것을 인지하나, 개발담당자가 테스트를 수행함

3) 안전 관련 비용 현황

통상 소프트웨어 품질 비용은 조직 인력 또는 프로젝트 비용의 10%정도를 차지하고 있으나, 기업에 따라 2.5% 정도가 할당되는 경우도 있었다. 그러나 인명의 손실을 유발할 수 있는 소프트웨어 안전 및 신뢰성과 관련된 소요비용은 20~25% 정도로 조사되었다.(전체 개발 인력 대비 안전 인력의 비중, 전체 개발 비용 대비 안전 비용 기준)

<표 4-38> 안전 관련 비용 현황

도출 내용	인터뷰 내용
일반적인 품질비용은 조직 또는 프로젝트 비용의 2~10%까지 할당이 되나, 소프트웨어 안전 및 신뢰성과 관련된 소요비용은 20~25% 정도 할당 되는 경우도 있음	• 해당 프로젝트에 대하여 품질비용은 50억 정도를 할당하나 총 구축비용의 2.5% 수준임 • 인명과 관련된 안전 분야의 정보시스템임을 고려하여 안전 비용은 총 구축비용의 약 25%를 할당하고 있으나, 통상적인 품질비용은 10%임. 즉, 안전성을 요구하는 중요 정보시스템의 안전비용은, 일반적인 품질인력 및 품질점검기간의 2.5배를 투입하는 것임 • 20~25% 정도의 신뢰성 인력을 보유함

4) 소프트웨어 개발 비용 현황

소프트웨어 산업의 제대로 된 業환경을 갖추기 위해서는 소프트웨어 개발의 적정 사업대가 책정을 통해 소프트웨어 인력이 대우받는 환경을 조성함으로써 구현될 수 있다고 조사되었다. 소프트웨어 단가 압력은 개발 업체에 전가되므로 결국 소프트웨어 부실을 야기하고 소프트웨어 산업 인력의 개선 의욕 상실로 이어진다.

또한 소프트웨어 신뢰성 테스트 강제화에 대응하여 소프트웨어 신뢰성 테스트에 소요되는 적정 MM 투입과 적정 테스트 기간 확보가 필요하다. 소프트웨어 사업대가의 적정성 검토는 발주처의 소프트웨어 전문가가 제출된 WBS(Work Breakdown Structure)와 체크리스트의 적정성 여부를 검토/평가함으로써 확인이 가능할 것이라고 조사되었다.

<표 4-39> 소프트웨어 개발 비용 현황

도출 내용	인터뷰 내용
소프트웨어 개발의 적정 사업대가 책정을 통해 소프트웨어 인력이 대우받는 환경 조성 필요	• 제대로 된 業환경을 갖추기 위하여 적정 원가를 투입할 수 있는 사업대가가 책정되어야 함 • 소프트웨어 전문성에 대한 인식과 소프트웨어 인력이 대우받는 환경 조성이 필요함 • 개발자들이 교육을 받거나 새로운 것에 도전하는 자기 개선 마인드가 부족함
신뢰성 테스트에 대한 적정 MM 투입과 신뢰성 테스트 기간 확보 필요	• 소프트웨어의 신뢰성 테스트가 강제화 되었으나 해당 예산은 미 반영됨 - 하드웨어 중심 가격체계로 인한 소프트웨어 적정 예산 미반영으로 소프트웨어는 부실 - 소프트웨어 신뢰성 테스트를 위한 적정 투입 인력 및 적정기간 또한 확보 필요
소프트웨어 예산의 적정성은 제출된 WBS와 체크리스트의 적정성 여부 검토/평가로 확인 가능	• 소프트웨어 예산의 적정성은 수행 사에서 상세화 된 소프트웨어의 WBS / 체크리스트 제출, 제출 건에 대하여, 발주처의 소프트웨어 전문가에 의한 적정성 여부 검토/평가로 확인 가능함

5) 테스팅 현황

소프트웨어의 테스팅을 강화하는 노력으로 도메인전문(현업), 개발자 및 테스팅 매니저의 3자 공동이 참여하는 테스팅을 수행하고 있었다. 소프트웨어 분석/설계 단계부터 3자 공동이 참여하여 테스팅을 수행하기도 하는데, 이것은 초기단계에서 각 부문 담당자의 참여로 정확한 요건을 분석/설계하는 것이 구현 단계의 오류를 최대한 감소시키고 품질 비용 절감과 기간 연장을 방지할 수 있는 방법이기 때문이다. 한편으로는, 단계별 테스팅 Tool 사용을 사내 규정화하여 직원의 테스팅 의식 수준을 제고하고자 하였다.

<표 4-40> 테스팅 현황

도출 내용	인터뷰 내용
도메인전문(현업), 개발자 및 테스팅 매니저의 3자 공동 참여 테스팅 수행	• 구축 초기 단계부터 테스팅 인력(업무전문성)과 개발자(통찰력), 현업(도메인 전문)의 3자가 공동 참여한 테스트 요건 분석 및 설계 업무를 수행함 • 최종 검증 시 현업(발주처), 테스터(수행사), 개발(협력업체) 간 3자 검증을 실시함 (최근, 발주처 참여) • 임베디드 소프트웨어에 대하여, 프로젝트 착수 단계부터 소프트웨어 부문의 안전 검사 계획 수립, 테스트 계획 등 별도의 계획서를 작성함 (이전에는 하드웨어부문만 작성)
테스팅 Tool 사용에 대한 사내 규정화하여 테스팅 의식 수준 제고	• 테스팅 Tool 사용을 사내 규정화하여 테스팅 생활화를 꾀하여 직원들의 테스팅 의식 수준을 제고하고자 함

6) 외부 전문업체 활용 현황

외부 전문업체는 기밀사항의 해외유출 방지 및 민첩한 업무 대응을 위해 전문기술력을 가진 국내 전문 업체를 주로 활용하고 있으나, 회사 기술 유출 문제에 민감한 경우 외부 업체를 선호하지 않았다. 이들 외부 전문 업체는 테스트 계획 수립, 관리 및 통제, 테스팅 업무를 지원하는 업무를 수행하며, 실제 테스팅은 사용자의 접점에 있는 사내 인력 또는 실제 사용자가 직접 테스트를 담당한다고 조사되었다.

<표 4-41> 외부 전문업체 활용 현황

도출 내용	인터뷰 내용
기술전문성과 업무대응력 및 기밀사항의 해외유출 방지의 이유로 국내 전문업체를 주로 활용함	• 국내 전문 업체는 해외 전문 업체에 비하여 기술 전문성이 높고, 책임감과 신뢰가 확보되어 사고 발생 시 빠른 업무 정상화가 가능함 • 기밀사항의 해외유출을 우려하여 해외업체를 활용하지 않음
회사 기술력 유출 문제로 인해 외부 전문업체 미활용	• 개발자가 직접 테스팅을 수행하고 별도의 외부 전문업체를 활용하지 않음 - 특정 구매품은 해당 테스트 전담팀이 체크리스트로 작성된 스케쥴에 따라 테스트 실시 - 코드 공유 등으로 인한 회사 기술력의 유출 경험과 금액적인 이유로 외부 전문업체 미활용
외부 전문 업체 활용 용도는 테스팅 계획 및 관리, 통제 역할, 테스팅 업무 지원 등 다양함	• 외부 전문 업체는 테스트 계획수립, 테스트 분석/설계, 관리 및 통제 역할을 수행하고 실제 사용자가 테스트를 직접 수행함 • 외부 전문 업체의 전문 인력을 지원받아 품질 교육 및 테스팅 업무를 지원함

7) 사고수습 및 대응 활동 현황

조사 대상 기업은 소프트웨어 사고수습 및 대응절차에 대한 규정과 시나리오를 보유하고 있었으며 정기적인 모의훈련을 수행하는 것으로 조사되었다. 각 담당자 및 전문가는 명확하게 규정된 책임과 역할에 따라 수습 및 대응활동을 수행하고 업종이나 서비스에 따라 월, 분기, 반기 등 주기적인 모의 훈련을 실시한다고 조사되었다. 기업 외부 사고처리에 대해서는 내부 사고처리에 추가적으로 대외채널 및 담당조직을 구성하여 대응체계를 마련해 두고 있었다.

8) 소프트웨어 사고사례 정보 축적 및 활용 현황

대부분의 기업은 양산 이후 소프트웨어 결함 또는 사고에 대한 사례 및 조치정보를 문서나 시스템으로 관리하고 있지만, 개발 단계의 결함이나 사고 정보의 수집은 부족하며, 일부 근본적인 사고 대책 마련 및 개선 활동이 미흡한 경우도 있었다.

<표 4-42> 소프트웨어 사고사례 정보 축적 및 활용 현황

도출 내용	인터뷰 내용
조사 대상 양산 후 발생한 결함 또는 사고사례 정보를 문서 또는 시스템을 DB화 하여 수집/축적하고 있었다. 다만, 개발 단계의 결함 및 사고정보 수집은 부족하였고, 사고에 개선 활동은 일부 미흡함	• 15년 이상으로 사고사례정보를 문서 또는 시스템 DB화하여 수집/축적함 • 제품의 양산 후 소프트웨어 결함 및 사고 대상으로 수집하고 있으나 개발단계의 결함이나 사고정보 수집은 부족함 • 사고사례정보는 소프트웨어의 개선과 요건 설계, 인력의 교육 자료로 활용함 • 사고에 대한 근본적인 대책 수립 마련 및 개선은 일부 미흡함

9) 교육 현황

기업은 협력업체에 가이드, 매뉴얼 제공을 통한 운영 및 테스트 교육을 실시하여 업체 역량을 개선하고 있다. 그러나 실제 기업의 개발자들은 소프트웨어 사업 환경이나 향후 직종에 대한 성장가능성에 대한 기대가 낮기 때문에 자기 개선 마인드가 부족한 것으로 조사되었다.

<표 4-43> 교육 현황

도출 내용	인터뷰 내용
협력업체에 운영정의서 및 테스트 교육을 통한 역량 강화 지원. **반면 개발자들의 경우 직종에 대한 낮은 성장가능성 등으로, 자기 개선 마인드 부족**	• 가이드, 매뉴얼 등이 포함된 운영정의서를 협력업체와 공유, 사용 Tool 및 정적/동적 테스트 교육을 무료로 연간 4회 실시함 • 소프트웨어 사업 환경 및 직종에 대한 성장가능성에 대한 낮은 기대치로 인하여, 개발자들은 업무 개선에 대한 적극적이지 않으며, 교육을 통한 자기 개선 마인드가 부족함

10) 주요 개선 의견

인터뷰에서 지원 요청 및 개선 의견으로는, 1. 소프트웨어 業 환경개선을 위한 소프트웨어 적정 사업 대가 책정과, 2. 개발자를 위한 업종/업무 사례 중심의 교육 지원과 3. 규정과 절차에 따라 업무 수행이 중요하다는 의견이 있었다. 또한, 4. 최소한의 자

격요건을 보유한 소프트웨어 안전 및 테스팅 업체가 사업에 참여하여야 한다는 의견도 있었다.

<표 4-44> 인터뷰의 주요 의견

도출 내용	인터뷰 내용
소프트웨어 개발의 적정 사업대가 책정을 통한 업 환경 개선	• 제대로 된 業환경을 갖추기 위하여 적정 원가를 투입할 수 있는 사업대가 책정 필요 • 신뢰성 확보를 위한 소프트웨어안전 부문의 적정 예산 반영 • 소프트웨어 인력에 대한 전문성에 대한 인식과 소프트웨어 인력이 대우받는 환경 조성
소프트웨어 업종의 사례 중심 교육 필요	• 개발자를 위한 기술 교육이 아니라, 업종에 맞는 사례 중심의 교육 지원이 필요
규정이나 절차에 따른 업무 수행 필요	• 규정 및 절차 준수로도 충분히 직원의 안전/품질 인식 수준 향상과 소프트웨어 안전성 확보 가능
사업 참여 업체와 인력은 최소한의 자격 요건을 구비해야 함	• 최소한의 자격 요건을 갖춘 업체 및 인력에 대하여 사업참여가 가능해야 함 - CMMI, TMMI, SP, SPICE 등 인증을 보유한 업체 참여 - 업종 경험은 뛰어나지만, 소프트웨어 공학, 구조화 능력이 부족하므로 개인의 자격 구비도 필요

4. 조사 결과 종합 및 시사점

소프트웨어 개발/사용 기업은 주로 사용자 관점에서의 안전 활동, 문제점 및 해결방안 등이 조사되었는데, 조사 대상의 모수가 많지 않은 관계로 조사 대상 업체에 국한된 답변 등은 가능한 배제하고, 보편적인 측면에서 제시된 해결 방안 및 문제점을 정리하였다. 특이점으로는 법/제도, 표준/매뉴얼/가이드보다는, 실제 사업 수행에 도움이 될 수 있는 인력/교육, 프로세스 및 業 환경개선 부분에 대한 요구가 도출되었다. 특히, 業 환경개선에 대한 요구사항이 많았는데, 이는 국내 소프트웨어 개발 및 안전 業 환경 자체가 상대적으로 열악하다고 추정할 수 있었다.

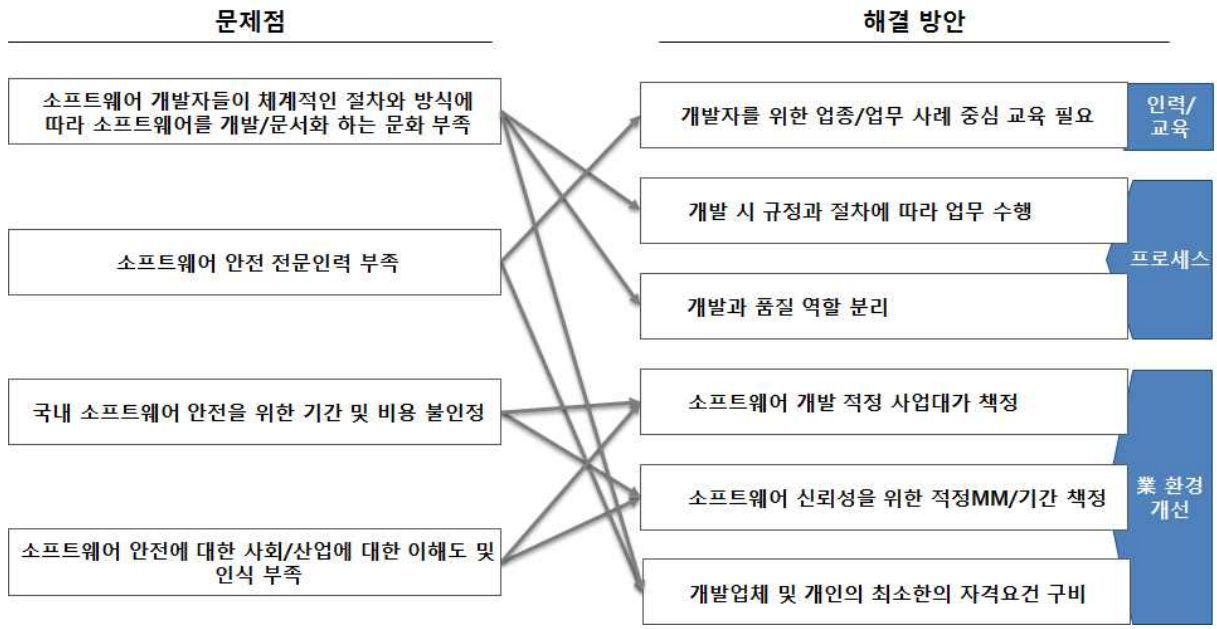
또한, 소프트웨어의 신뢰성 향상을 위해, 외부 전문 업체를 사용하기도 하였으나, 보안 및 업종 지식 부족 등의 문제로 적용 분야가 대부분 단순 테스팅에 국한되었다. 이

때문에, 사용기업(End-User)에서는 업종 지식을 보유한 개발 담당자가 안전/품질 역량도 함께 보유할 필요가 있는데, 이를 위해 업종/업무 사례 중심의 구체적인 개발자 교육이 필요한 것으로 분석되었다.

소프트웨어 신뢰성 테스트에 적정 MM 투입 및 기간이 확보되어야 한다는 방안은 소프트웨어 개발의 적정 사업대가 책정과 일부 일맥상통하는 면이 있었다. 소프트웨어 개발의 적정 사업대가는 단순히 신뢰성 테스트에 대한 비용 보장뿐만 아니라, 시장 차원에서 사업 개발 대가 및 안전 관련 인력에 대한 대가 및 비용이 개선되어야 한다는 의미를 포함한다.

구현 단계에서 발생할 수 있는 품질비용을 최소화시키고 안전성을 향상하기 위해, 안전/품질 테스트 설계 단계부터 현업, 안전/품질 테스트 매니저와 개발자의 3자가 공동 참여해야 안전성/품질과 비용 효율성을 제고할 수 있다고 조사되었다. 종합적으로 소프트웨어 안전성을 제고하기 위해 안전/품질 테스트 Tool, 전문 업체의 활용, 자체 역량의 개선 등이 필요하며, 프로젝트 초기 단계부터 현업(발주처), 안전/품질 테스트 엔지니어와 개발자의 3자가 공동 참여하는 검증 절차가 필요하다고 조사되었다.

[그림 4-12] 소프트웨어 개발/사용 기업 문제점 및 해결 방안 Mapping



제5장 GAP 분석 및 SWOT 분석

제1절 GAP 분석

1. 개요

GAP분석은 통상 현재의 현황(As-Is)과 선진 현황(To-Be)의 차이점(GAP)을 비교분석하여 개선전략을 도출하는 방식으로 진행되나, 본 연구에서는 국내 현황 분석 시 조사 대상별(학계 및 공공기관, 국내 소프트웨어 안전 산업의 기업과 소프트웨어 개발/사용 기업) 문제점 및 해결방안(개선과제)들이 대다수 도출되어, 각 대상별 도출된 문제점을 종합/정리한 9개의 문제점을 선진사례와 비교하여 개선 전략을 도출하였다.

2. 국내 소프트웨어 안전 산업과 해외 사례 비교

1) 체계적인 절차와 방식에 따른 소프트웨어 개발 및 문서화하는 문화 부족

해외 주요 산업 도메인별 소프트웨어 개발 표준 및 소프트웨어 안전 표준과 상세 수행 가이드들이 존재하는데, 이들 표준에서 요구하는 주요 사항은 개발 초기부터 최종 완료단계까지, 단계별 상세 수행 절차에 따라 업무를 수행하고, 문서화하라는 것이었다.

철도산업의 유럽 표준인 EN 50128의 주요 특징으로, 개발 단계별 검증(Verification after each development step)과 명확하고 검증가능한 문서화(Clear documentation, Verifiable document) 기본 원칙으로 강조하고 있다. 또한, 소프트웨어 안전 평가나 인증에 있어, 정부기관 또는 인증평가 기관이 소프트웨어 개발 시 절차 준수 및 문서화 부분을 주요 평가 항목으로 포함하여 확인함으로써 이들 요구사항이 준수될 수 있도록 되어 있었다.(예. 미국/유럽 철도 산업, 미국/유럽 항공 산업 등)

GAP분석을 통해 도출된 개선 전략으로, 개발 절차에 대한 표준 및 상세 가이드 제공과 이를 강제화 하는 법/제도 제정 및 조직/기관의 설립 또는 지정을 통해, 제대로 개발하는 소프트웨어 개발 문화가 뿌리 내릴 수 있을 것으로 분석되었다.

2) 소프트웨어 안전에 대한 개념 부족

현재 국내는 소프트웨어와 관련된 안전(Safety), 품질(Quality), 보안(Security) 간의 개념이 명확하지 못하다. 특히 소프트웨어 안전, 품질, 보안 사이의 개념 구분이 모호하여, 소프트웨어 안전에 대한 연구 범위 및 정책 방향 설정이 이루어지고 있지 않았다. 해외 사례의 경우, 주요 산업도메인별 소프트웨어 안전에 대한 명확한 개념 및 안전 등급(SIL) 등이 정의되어 있었다.

자동차 분야의 경우 SIL 1,2,3,4 등급으로 구분하고 있으며, 철도 분야에서는 SSAS 0,1,2,3,4의 5개 등급을 적용하고, 항공 분야는 DO-178B에서 Level A/B/C/D/E로 구분하여 적용하고 있었다. 같은 원자력 분야라고 하더라도, IAEA에서는 Safety System/Safety Related System/Systems not important to safety의 3개 등급을, IEC는 Category A,B,C, Unclassified의 4개 등급으로 구분하고 있었고, 미국은 1E, Non-nuclear safety의 2가지로만 소프트웨어 안전 등급을 정의하고 1E 등급에 규정을 적용하고 있었다.

국내에서도 주요 산업 도메인별로 해외 표준을 도입하여 적용하려는 노력이 진행 중이므로, 학계/국가기관 또는 해당 산업도메인별 주도 업체를 중심으로 소프트웨어 안전 표준이 국내 정착 될 수 있도록 해외 표준 번역 및 해석, 국내 현황을 반영한 상세 수행 가이드 제정 등의 다양한 노력을 해야 할 것으로 분석되었다.

3) 소프트웨어 안전 법령 부재

해외 선진국에서는 주요 산업 도메인별 소프트웨어 안전 표준이 준수될 수 있도록, 직/간접적으로 법/규정을 제정하고, 관리감독 기관에서 감독하고 있었다.

미국의 경우 철도 소프트웨어 관련 표준 및 가이드인 AREMA C&S Manual of Recommended Practices(소프트웨어 안전의 경우 part 17.3.1, 17.3.3, 17.3.5)를 미국 연방철도국(FRA)에서 준수해야할 표준 중의 하나로 선정한 다음, 안전 승인 제도를 수행하여 이들 표준이 준수되도록 규정(49 CFR Part 236 Subpart I & H) 되어 있었다. 미국 항공 분야도 유사한 구조를 가지고 있었는데, 민간 항공 분야의 경우 FAA(미국연방항공청)는 FAR(Federal Aviation Regulations)에 표준을 준수하도록 명시해 두었으며 DO-178B에 대해서는 AC 20-115B를 통하여 전자 설비 또는 시스템을 사용하는 디지털 컴퓨터 기술에 대하여 TSO (Federal Aviation Administration technical standard order), TC (type certification) 또는 STC (supplemental type certification)를 위한 요청

에 대해서 규정 준수를 증명하기 위한 방법으로 RTCA의 DO-178B를 사용할 수 있다는 지침이 있었다. 철도 및 항공 분야 관련 미국 제도의 공통된 특이점은, 사용가능한 표준을 제시하되 그 표준만이 승인을 위한 유일한 방법이 아니라는 것이다. 즉, 해당 분야에 사용가능한 표준을 몇 가지 제시하고 있으며, 심지어 기업이 자체적으로 보유한 방법 및 절차로 안전 요구사항을 충분히 만족할 경우 이들이 사용하는 방법 및 절차로도 승인이 가능하게 되어 있어, 산업계의 역량 및 수준에 대해서 OPEN된 정책을 가지고 있었다. 이미 아마도, 이들 산업 분야에 종사하는 기업의 역사 및 역량이 충분하여, 오히려 국제 표준을 선도하고 있는 경우가 많아, 이들의 역량을 고려한 정책으로 추측된다. 자동차의 경우는 자동차 제조물 책임 법에서 최신 기술 및 기법을 활용해야 한다는 포괄적인 법/규정을 통해서 점진적으로 업계가 ISO 26262를 준수할 수 있도록 간접적으로 강제화하고 있었다. 또한, 법/제도에서 표준 준수 여부를 정부 기관이 관리/감독하거나, 허가 받은 업체가 인증을 수행함으로써, 표준이 준수될 수 있도록 제도화하고 있었다. 우주항공의 경우, NASA가 제정한 표준을 하위 기관 및 관련 업체들이 준수하도록 NASA Policy Directives인 NPD 7120.4(NASA Engineering and Program/Project Management Policy)를 통해 규정하고 있었다. 원자력 부문에서 미국의 NRC(Nuclear Regulation Commission, 원자력규제위원회)는 10 CFR Part 50의 Appendix B에서 종합적인 QA 프로그램에 대한 기본적인 요구사항을 설정했으며, Regulatory Guide 1.152에서 컴퓨터의 기능과 설계 요구사항에 대한 규정 준수의 방법으로 IEEE Std 7-4.3.2를 적용할 수 있다고 명시하고 있다. 영국은 보건안전법(HSWA, Health and Safety at Work etc. Act 1974), 에너지법 2013 및 원자력설치법 1965에 기초하여, 일반적으로 다른 나라에서 적용되는 규범적인 표준 기준 체계보다는 목표 설정 체계를 운영하고 있다. 정부는 원자력 발전소를 규제하는 책임을 가지고 있으나, 원자력 안전을 보증하는 법적인 책임은 사용권자에게 있고 사용권자는 안전성에 영향을 끼치는 운전에 대해서 안전성을 증명하기 위한 적절한 안전 사례를 생성하고 시험하도록 하고 있으며, 영국 정부는 업계 전문가를 활용하여 이에 대한 평가를 하고 있다. 영국은 원자력 부문의 소프트웨어 안전에 관한 표준으로 IEC 60880 (Category A 기능을 수행하는 I&C (Instrumented & Control) 시스템의 문제를 해결하기 위한 표준)을 주요 레퍼런스로 사용하기는 하나, 소프트웨어에 적용하는 특정 표준은 정해져 있지 않다. 또한 이벤트 발생 시, 사고의 재발을 방지하기 위해 원자력 사용권자와 법적 의무를 가진 사람들에게 사건을 공개하도록 권장한다.

국내에서도 산업도메인의 특성을 고려해서 직/간접적으로 법/제도를 통한 표준 준수 규정을 제정하고, 이들이 준수될 수 있도록 관리/감독하는 기관 또는 단체를 지정해야

할 필요가 있다. 다만, 국내 산업도메인의 현황 및 특성을 고려해서 단일 표준 준수 또는 복수 표준 및 그 외 방법의 허용여부 등, 규정 내용 및 수준 그리고 규정을 관리/감독 방법을 특화하여 적용할 필요가 있을 것으로 보인다.

4) 소프트웨어 안전 평가 가이드 부재

1)번 문제에서 언급하였듯이, 해외 선진국의 경우 산업도메인별 사용가능한 소프트웨어 안전 표준을 제시하고, 이를 수행할 수 있는 상세 수행 가이드 등을 해당 국가 기관 또는 연구 단체에서 제공하고 있었다.

미국의 경우 철도관련 기술자 단체인 AREMA에서 소프트웨어 안전 표준 및 상세 수행 사이드를 제작 배포하고 있었고(AREMA C&S Manual of Recommended Practices 중 소프트웨어 안전의 경우 part 17.3.1, 17.3.3, 17.3.5), 우주항공 부문의 미국 NASA에서는 NPR 7150.2의 소프트웨어 공학 요구사항에 대하여 NASA-STD-8719.13 소프트웨어 표준과 NASA-GB-8719.13 소프트웨어 가이드북을 제작 배포하고 있으며, 인증업무를 허가 받은 선진 TIC 업체에서도 안전관련 가이드를 직접 작성하여 배포하기도 하였다.(예. Bureau Veritas) 일본은 자동차 안전표준인 ISO 26262를 자국에 적용할 당시, 정부연구기관과 민간 업체 및 엔지니어들이 ISO26262 표준과 관련 안내서를 번역 및 개발하여 회원사들에게 배포를 하였다. 또한 독일은 DKE(독일의 DIN (독일표준연구소)과 VDE (전기, 전자, 정보기술 협회)의 전기, 전자, 정보기술 위원회)와 VDI (독일엔지니어협회)를 통해 표준 활동을 수행하고 있다. DKE는 신규 또는 국제표준의 초안 또는 수정본을 해석하여 검토를 한 다음, 독일의 표준 체계와 통합하는 과정을 진행하고, VDI는 기술 가이드라인을 개발하여, 이를 표준의 개발/업그레이드의 자료로 활용할 수 있도록 제공한다.

국내는 현재 소프트웨어 안전 산업 기반이 약하므로, 정부나 연구단체 또는 산업도메인별 선도 업체에서 주도적으로 소프트웨어 안전 평가 및 가이드를 제정하여 배포해야 할 필요가 있다.

5) 소프트웨어 안전 전문인력 부족

국내 소프트웨어 분야 산업 기업의 경우, 업체가 대부분 300억 미만의 중소규모이며, 저부가가치 사업인 신뢰성 중심의 컨설팅 및 테스팅 서비스가 주 매출원(전체 매출의 65%)이었다. 또한, 소프트웨어 안전 관련 사회/산업적인 기반이 미 성숙되어 있어, 소프트웨어 안전 관련 적절한 대가를 받지 못하고, 충분한 교육 기회도 제공되지 못하고

있었다. 상기의 세 가지 이유로 인하여, 수준 높은 안전 전문 인력 유입과 전문 인력 육성이 어려워서 전문인력 부족 문제가 해결되지 못하고 있다.

해외 TIC 기업을 살펴보면, 소프트웨어 안전 표준 및 가이드에 계획, 설계, 개발, 구현, 운영, 유지보수의 전 과정에 대하여 검사/테스팅/인증 업무 서비스를 제공하며, 고가의 비용을 청구하고 있었다. 전문인력 육성의 경우 선진 TIC 기업은, 1. 일반적인 TIC 교육 또는 기업 특화된 교육을 실시하여 전문 인력을 육성하거나(ex. SGS, Bureau Veritas 등), 한편으로, 2. TIC Value-Chain을 확장하여 엔지니어링 업체 인수를 통하여 인력 역량을 보강하고 있는 기업도 있었다. (ex. Mistras는 석유가스산업의 Carmegen Engineering 인수, Applus+ RTD는 엔지니어링 서비스를 제공하는 Kiefner and Associates 인수, DNV의 석유가스 재생 엔지니어링 부문 조직 등)

국내의 경우, 전문 인력 확보를 위해서는 소프트웨어 안전 관련 사회/산업적인 기반 성숙이 선행되어야 한다. 소프트웨어 안전 산업에 대한 인식 제고, 소프트웨어 안전 서비스에 대한 대가의 현실화 등이 이루어지고, 이를 통해 수준 높은 전문 인력의 유입 또는 육성되는 선순환 구조를 마련해야 할 것으로 분석되었다.

6) 국내 소프트웨어 안전을 위한 합리적인 기간 및 비용 책정 필요

국내에서는 현재 소프트웨어 안전에 대한 사회/산업적인 기반이 성숙되어 있지 않은 관계로, 소프트웨어 안전을 개발의 한 부분인 단순 품질 테스팅 정도로 보는 시각이나 개발의 추가 서비스 정도로 여기는 시각이 많았고, 이로 인해 소프트웨어 안전 활동에 소요되는 기간 및 비용을 추가적인 기간이나 비용으로 인식하여, 최소한의 기간 및 비용을 책정함으로써 적절한 기간 및 대가를 인정받지 못하고 있었다. 해외의 경우 산업 도메인별로 소프트웨어 안전 요건을 법/제도 차원에서 규정되어 있으며, 특히 제도적 차원에서 인증 부분에 대한 영역을 민간영역에서 수행할 수 있게 보장함으로써(유럽 철도의 Independent Safety Assessor), 소프트웨어 안전의 중요성 및 민간영역에서의 역할이 사회/산업적으로 확보되고 있었고, 이를 통해 충분한 기간 및 적절한 비용을 산정할 수 있었다.

따라서 소프트웨어 안전 표준 준수, 평가 및 인증에 관련된 교육기회를 제공하고, 법/제도적인 규정이 마련되어 소프트웨어 안전을 습관처럼 준수하는 사회/산업적인 기반 구축이 자발적/강제적 측면에서 마련되어야 할 것으로 분석되었다. 또한, 민간영역에서의 안전 활동을 제도화하여 보장함으로써, 안전 인식의 제고와 함께 안전산업도 발전하는 방향으로 나아가야 할 것으로 보인다.

7) 소프트웨어 안전 산업을 별도의 산업 군으로 분류 필요

국내는 현재 TIC 산업에 대한 별도의 산업 구분 및 시장 정보 자체가 전무한 상황이다. 해외는 TIC 산업(Testing, Inspection and Certification)안에 소프트웨어 안전이 포함되어 있으며, TIC 산업이 주요 산업으로 구분되어 주요 시장 조사 기관(Marketsandmarkets, Rearch and Markets 등)에서 시장조사 보고서 및 시장 동향 정보를 제공하고 있었다. 또한, 세계 전체 TIC 시장은 2020년에 504억 달러(약 55조) 규모가 될 것이라고 추정하며, 국내도 마찬가지로 CAGR 15%대로 고속 성장하는 시장으로서, 현재 보수적으로 추산하여도 최소 2,600억 원 이상의 시장 규모이다.

따라서 국내 소프트웨어 안전 산업 육성을 위하여 이러한 TIC 산업을 별도의 산업 군으로 구분하여 특화된 시장 분석 및 정책 사업을 수립할 필요가 있는 것으로 분석되었다. 단, 소프트웨어 안전 산업만 별도의 산업 군으로 분류하는 것보다, 품질, 테스팅 등을 포괄하여 TIC 산업 군으로 구분하는 것이 바람직할 것으로 사료된다.

8) 글로벌 선진사 대비 국내 산업 군별 Reference (Track Record)의 확보 미흡

소프트웨어 안전 산업의 중요한 성공요소로 경험과 노하우를 들 수 있는데 후발 주자인 국내 업체는 산업 군별 Reference (Track Record)가 부족하여, 글로벌 선진사가 국내 시장 진입을 꾀할 때 제대로 된 경쟁을 못할 우려가 있다.

글로벌 플레이어들은 자신들의 Value-Chain이나 지역별 서비스 등 서비스 포트폴리오를 확장하기 위하여 전문기술, 인허가, 지리적인 이점 등을 보유한 중소기업을 인수하여 짧은 기간 내에 경쟁력을 강화하는 전략을 추진하고 있었다. 예를 들면, SGS의 경우 자동차, 제조 산업, 소비재 및 유통 분야에 역량을 보유하고 있으나 2014년 미국 3개(자동차, 환경), 유럽 6개(공업, 자동차, 환경, 소비재), 일본 1개(소비재) 등의 중소 TIC 기업 인수를 통해 업종/지역별 역량을 강화하고 있었다. Intertek의 경우, 2014년 석유&가스 분야 기업과 식품&농업 분야 기업을 인수 합병하였다. DNV GL의 경우 해양, 석유, 에너지 산업 분야에서 세계 최고의 역량을 보유하고 있는데, 이는 2013년 노르웨이 DNV와 독일의 GL이 합병하여 설립된 기업이다.

따라서, 국내 기업의 경쟁력 확보를 위해 주요 산업 군별 Reference (Track Record)를 확보할 수 있는 기회가 제공되어야 하며, 업계 스스로 필요에 따라 인수합병을 통해 빠르게 변화하는 해외 TIC 시장에 적극적으로 대응할 필요가 있는 것으로 분석되었다.

9) 소프트웨어 안전에 대한 사회/산업적인 이해도 및 인식 제고 필요

국내의 소프트웨어 안전에 대한 낮은 사회/산업적인 이해도 및 인식은 이미 상기 문제점(5)번, 6)번)들에 대한 근본 원인으로 분석되었고, 이에 대한 방안이 제시되었으므로 별도의 논의를 하지 않는다.

<표 5-1> 국내 소프트웨어 안전 산업 현황과 해외사례 비교

문제점	해외 사례	개선 방향
1. 체계적인 절차와 방식에 따른 소프트웨어 개발 및 문서화하는 문화 부족	• 산업도메인(자동차, 철도, 항공, 원자력)별 소프트웨어 안전 표준 및 가이드 존재 - 개발 초기~완료단계까지 단계별 수행절차 및 문서화 [예시: 절차 및 가이드 원칙] • EN 50128 (철도표준)은 개발 단계별 검증과 문서화 기본 원칙으로 강조 - Verification after each development step - Clear documentation, Verifiable document • 미국/유럽 철도 및 항공 부문은 소프트웨어 안전 평가&인증 시, 절차 준수 및 문서화를 주요 평가 항목으로 포함	• 개발 절차에 대한 표준 및 상세 가이드 제공 • 이를 강제화 하는 법/제도 제정 • 조직/기관을 통한 평가 및 인증으로 요구사항의 준수 여부 확인
2. 소프트웨어 안전에 대한 개념 부족	• 소프트웨어 안전에 대한 명확한 개념 및 안전 등급(SIL) 정의 [예시:소프트웨어 안전 등급] • 자동차: SIL 1, 2, 3, 4 등급 구분 • 철도: SSAS 0, 1, 2, 3, 4 등급 구분 • 항공 DO-178B: Level A, B, C, D, E 구분 • 원자력: - IAEA: Safety System, Safety Related System, Systems not important to safety의 3개 등급 - IEC: Category A, B, C, Unclassified 4개 등급 - 미국: 1E, Non-nuclear safety 2개 등급	• 소프트웨어 안전 관련 해외 표준 번역 및 해석, 국내 현황을 반영한 상세 수행 가이드 제정 및 배포 필요 • 학계/국가기관 또는 해당 산업도메인별 주도 업체 중심의 활동 필요

3. 소프트웨어 안전 법령 부재	• 직/간접적으로 법/규정 제정 • 관리감독 기관에 의한 준수여부 점검 • 사용가능한 표준을 제시하되, 특정표준을 강제하지 않음 [예시: 국가/도메인별 법제도화] • 미국 철도: 안전 승인제도로 49 CFR Part 236 Subpart I & H - AREMA C&S Manual of Recommended Practices(소프트웨어 안전의 경우 part 17.3.1, 17.3.3, 17.3.5)를 사용가능 표준으로 선정 • 미국 상용항공: FAA에서 FAR(Federal Aviation Regulations) • 우주항공: NASA Policy Directives 인 NPD 7120.4(NASA Engineering and Program/Project Management Policy) • 자동차: - 자동차 제조물 책임법을 통한 포괄적인 법 규정 - 정부기관의 표준 준수 여부에 대한 관리/감독 업무 또는 허가 받은 업체의 인증 업무에 대해 제도화 • 영국 원자력: 보건안전법(HSWA, Health and Safety at Work etc. Act 1974), 에너지법 2013 및 원자력설치법 1965	• 산업도메인별 특성을 고려하여, 직/간접적인 법제도 마련 • 표준 준수 규제 필요 - 단일/복수 표준 준수 및 허용 여부 - 규정 내용 및 수준 그리고 규정을 관리/감독 방법 고려
4. 소프트웨어 안전 평가 가이드 부재	• 주요 도메인별 소프트웨어 안전 표준 이외에 상세 수행 가이드 및 평가 가이드 배포 [예시: 평가 가이드 배포 및 활동] • 미국 철도: AREMA에서 소프트웨어 안전 표준 및 상세 수행 사이드를 제작 배포 - AREMA C&S Manual of Recommended Practices 중 소프트웨어 안전의 경우 part 17.3.1, 17.3.3, 17.3.5) • 미국 우주항공: NASA에서 제작 배포	• 정부나 연구단체 또는 산업도메인별 선도업체에서 주도적으로 소프트웨어 안전 평가 및 가이드의 제정 및 배포 필요

	- NPR-STD-8719.13 소프트웨어 표준 - NPR-GB-8719.13 소프트웨어 가이드북 • 일본 자동차: 정부연구기관과 민간단체의 협업을 통하여 ISO26262 표준과 안내서의 번역 및 개발하여 회원사에 배포 • 독일: DKE와 VDI의 표준 활동 - DKE: 신규표준, 수정본을 해석하여 독일 표준체계와 통합하는 활동 - VDI: 기술 가이드라인 개발 • 선진 TIC 업체: Bureau Veritas의 안전관련 가이드 제작	
5. 소프트웨어 안전 전문인력 부족	• 선진 TIC기업의 전문인력 양성 교육 및 Value-Chain 확장을 통한 전문성 강화 [예시: 전문인력 육성] • SGS, Bureau Veritas 등: 일반적인 TIC 교육 또는 기업 특화된 교육 실시 • 엔지니어링 업체 인수를 통한 인력 역량 및 서비스 보강 (ex. Mistras는 석유가스산업의 Carmegen Engineering 인수, Applus+ RTD는 엔지니어링 서비스를 제공하는 Kiefner and Associates 인수, DNV의 석유가스 재생 엔지니어링 부문 조직 등)	• 소프트웨어 안전 관련 사회/산업적인 기반 성숙이 선행되어 소프트웨어 안전 산업에 대한 인식 제고, 소프트웨어 안전 서비스에 대한 대가의 현실화 등이 이루어지고, 이를 통해 수준 높은 전문 인력이 유입 또는 육성되는 선순환 구조 마련
6. 국내 소프트웨어 안전을 위한 합리적인 기간 및 비용 책정 필요	• 산업도메인별 소프트웨어 안전 요건에 대한 법/제도적 규정이 존재하여 안전에 대한 인식 정착 • 소프트웨어 안전의 중요성이 사회/산업적으로 인정되며, TIC 서비스에 대한 충분한 기간 및 적절한 비용 확보 가능 [예시: 합리적 비용 책정] • 유럽철도 ISA: 제도적 차원에서 인증 부분에 대한 영역을 주요 TIC업체가 수행할 수 있게 보장	• 법/제도적으로 소프트웨어 안전 표준 준수, 평가 및 인증에 관련된 규정 마련 선행되어야 함 • 상세 가이드에 근거하여 업무 수행에 필요한 기간과 비용의 합리적인 책정이 가능
7. 소프트웨어 안	• 해외는 크게 TIC 시장으로 분류 • 해외 시장조사 기관 및 M&A 기업 등	• 국내 소프트웨어 안전 산업 육성을 위하

전 산업을 별도의 산업 군으로 분류 필요	은 TIC 전반에 관한 자료 제작 • 소프트웨어 안전이 TIC에 포함되어 있으나, 별도의 시장규모, 동향 및 재무 성과를 공시하지는 않음 • 향후, 2020년 TIC시장 규모는 504억 달러(약 55조)로 추정 [예시: TIC 산업의 분류 및 시장 규모] • 시장 조사 기관의 TIC시장 자료 배포 - Marketsandmarkets, - Rearch and Markets 등	여 이러한 TIC산업을 별도의 산업 군으로 구분 필요 • TIC산업의 국내시장 분석 및 정책 수립 용이 • 단, 소프트웨어 안전, 품질, 테스팅 등을 포괄하여 TIC 시장으로 그룹핑할 것을 권고
8. 글로벌 선진사 대비 국내 산업 군별 Reference (Track Record)의 확보 미흡	• 해외 선진사들은 Value-Chain이나 지역별 서비스 등 서비스 포트폴리오를 확장하고 다양한 Reference를 확보하기 위한 전문기술, 인허가, 지리적인 이점 등을 보유한 중소기업을 인수하여 짧은 기간 내에 경쟁력을 강화하는 전략 추진 中 [예시: TIC 산업의 분류 및 시장 규모] • SGS: 자동차, 제조산업, 소비재 및 유통 분야에 역량 보유, 2014년 미국 3개(자동차, 환경), 유럽 6개(공업, 자동차, 환경, 소비재), 일본 1개(소비재) 등의 중소 TIC기업 인수을 통한 업종/지역별 역량 강화 • Intertek: 2014년 석유&가스 분야 기업과 식품&농업 분야 기업 인수 • DNV GL: 해양, 석유, 에너지 산업 분야 역량 보유, 2013년 노르웨이 DNV와 독일의 GL이 합병하여 가장 큰 선급회사가 됨	• 국내 기업의 해외 선진사에 대응할 수 있는 경쟁력 확보를 위한 주요 산업군의 Reference 확보 기회 제공 필요
9. 소프트웨어 안전에 대한 사회/산업의 이해도 및 인식 제고 필요	• 5번, 6번 항목의 내용과 동일	• 5번, 6번 개선사항과 동일

제2절 SWOT 분석

1. 개요

국내 소프트웨어 안전 분야 산업의 국내시장환경 및 내부역량에서 강점과 약점을 도출하고, 해외 TIC (Testing, Inspection and Certification) 시장의 동향에 의한 국내 기업들의 기회와 위협요인을 파악하고, 개선 전략을 제시하였다.

2. SWOT 분석

1) 강점

소프트웨어 품질 차원에서는 테스팅 중심의 다양한 고객군을 보유하고 있으며, 타 산업대비 높은 성장률 및 생산성을 가지고 있다. 국내 소프트웨어 안전 분야 사업은 산업도메인이나 서비스영역에서 상호배타적으로 사업을 추진하고 있었기 때문에 서로의 강약점을 보완하여 서로 상생할 수 있는 業 분위기가 조성되어 있었고, 장기적으로 고객과의 신뢰관계를 구축하고 있었다. 제한적이기는 하나 기능안전의 서비스 영역에서 전문적인 역량을 보유하고 국제적인 기술 교류를 통한 전문성 확보에 기여하고 있었다. 이에 대하여 국내 소프트웨어 안전 산업 발전을 위하여 산업도메인과 서비스에 걸쳐서, 업계의 기술 및 전문가 활동을 강화하여 해외 경쟁력과 자생력을 키워야 될 것으로 분석되었다.

2) 약점

소프트웨어 개발 및 설계에 대해서는 글로벌 선진 수준대비 차이가 존재하고 있으며, 아직까지 품질차원의 서비스 수행에 따라 안전 서비스에 대한 경험이 부족하다. 이러한 안전에 대한 Reference 부족으로 인하여, 해외 글로벌 업체와 비교할 때 경쟁력 차이가 존재하고 있었다. 예를 들어, 해외 글로벌 업체의 경우 다양한 국가와 다양한 산업 군에 걸쳐서 많은 Reference가 있지만, 국내 기업의 경우 이러한 사례가 매우 부족한 실정이다. 또한 소프트웨어 안전에 관한 검사/테스트/인증관련 서비스 및 교육 등의 종합적인 서비스 포트폴리오를 가지고 있는 국내업체는 여전히 소수이며, 고부가

가치의 솔루션을 제공하는 고품질의 기술 전문가 확보도 시급한 상황이다. 이것은 국내 소프트웨어 산업의 환경 및 사회적인 인식과도 연결되어 있는 문제로서, 열악한 대가 체계의 소프트웨어 산업을 기피하는 현상으로 인해 고급인력의 수급, 전문 인력의 보유를 어렵게 만들고 있다. 이에 대한 약점을 보완하기 위해서는, 소프트웨어 개발 및 안전 산업의 중요성과 미래 핵심 산업의 비전을 부각하고, 적절한 대가 체계가 마련될 필요가 있다.

3) 기회

해외시장 측면에서 생활수준 향상에 의한 중간계층의 성장과 생산지역 / 제조지역 / 조립지역 등 여러 국가에 걸쳐지는 공급망 개발 등의 글로벌화 및 산업화로 인하여 안전에 대한 요구사항은 점차 증가하고 있으며, 2014년 북미 시장의 안전 시장 활성화에 이어 앞으로는 중국 또는 아시아태평양 지역의 안전 사업이 가속화될 것으로 예상된다. 또한 TIC 시장의 아웃소싱이 증가하면서, 산업 저변에 펼쳐져 있는 소프트웨어 안전에 대한 요구도 지속될 것으로 예측된다. 그러므로 글로벌화 된 국내기업(예. 삼성, 현대, LG 등)을 대상으로 하는 내수시장과 지리적으로 근접한 중국이나 동남아 등지의 해외시장에서 사업기회를 찾을 수 있을 것으로 전망한다.

4) 위협

글로벌 TIC 선진 기업은 산업도메인별로 100여년에 걸친 다양하고 풍부한 레퍼런스와 전문화된 인력 등을 보유하고 있고, 이러한 역량을 가지고 서비스 및 지역 포트폴리오 확장을 위해 중소규모의 기업을 인수하면서 중국 및 아시아태평양 지역으로 진출하고 있었다. 국내 인증시장 또한 주요 산업도메인 별로 글로벌 선진 기업이 진출 중에 있으므로, 국내 낮은 인건비 기반의 단순 테스팅 기업 또는 중소규모의 전문성을 갖춘 기업의 경우, 글로벌 선진업체와의 경쟁으로 인하여, 고사하거나 인수될 가능성이 있을 것으로 예측된다. 이는 중장기 적으로 국내 소프트웨어 개발 산업 전체에 영향을 줄 수 있으므로 국내 기업의 글로벌 수준의 전문성 확보와 경쟁력을 갖출 수 있는 방안이 마련될 필요가 있다.

[그림 5-1] 국내 소프트웨어 안전 산업의 SWOT 분석 결과

강점 / 약점 / 기회 / 위협		강점 (Strength)	약점 (Weakness)
		• 소프트웨어 안전 관련 다양한 고객군 보유 • 장기적인 고객신뢰관계 형성 • 서로의 강/약점을 보완하는 상생의 業 분위기 • 타 산업대비 높은 성장률	• 글로벌 업체 대비 안전 사업 Reference 부족 • 소프트웨어 개발 및 안전에 대한 낮은 사회/산업적 인식 수준 • 고품질의 기술 전문가 부족
기회 (Opportunity)	• 2020년까지 글로벌 TIC 시장 매년 5.8% 성장 전망 • 중국 또는 아시아태평양 지역의 안전 사업이 가속화 • TIC 시장 Outsourcing 증가	SO전략 • 지속적인 고객 신뢰 관계를 통한 국내 소프트웨어 안전 시장 수성 • 지리적으로 근접한 중국, 동남아 등지의 해외시장 사업기회 발굴	WO전략 • 산업도메인과 서비스에 걸쳐서, 업계의 기술 및 전문가 활동을 강화 • 삼성, 현대, LG 등 국내 글로벌 기업을 대상의 내수시장 확보
위협 (Threats)	• TIC 선진사의 국내 및 아시아 태평양권 진출에 따른 국내 기업의 경쟁 심화 예상 • TIC 시장의 중소기업 대상의 M&A 활동	ST전략 • 국내 소프트웨어 안전 산업 기업의 자생력을 강화하기 위한 기업 간 상호 보완 및 개선 활동 추진 • 관련 전문 기술, 지식 교류 및 전문가 양성	WT전략 • 소프트웨어 개발 및 안전 산업의 중요성과 미래 산업의 비전 필요 • 소프트웨어 개발 및 안전 산업의 적절한 대가 체계 마련

제3절 국내 소프트웨어 안전 산업 개선 전략 도출

1. 개요

GAP분석을 통해 도출된 개선 전략과 SWOT분석을 통해 도출된 개선 전략을 비교/종합한 후, 개선 전략과 현황분석 결과 도출된 개선방안 Mapping을 통해 유효성 검증을 수행한 후, 최종 개선 전략을 확정하였고, 확정된 개선 전략에 기 도출된 개선 방안을 Grouping하여 최종 개선 전략 및 개선 방안을 수립하였다.

2. 개선 전략 도출

1) 소프트웨어 안전 산업의 제도적 기반 구축

산업도메인의 특성을 고려해서 직/간접적인 법/제도를 통한 표준 준수 규정을 제정하고 이들이 준수될 수 있도록 관리/감독하는 기관이나 단체를 지정할 필요가 있다. 또한 안전 산업의 육성을 위하여 TIC 산업을 별도의 산업 군으로 분류하여 특화된 시장 분석 및 정책을 수립할 수 있도록 해야 한다.

세부 개선 방안은 아래와 같다.

- 소프트웨어 안전 관련 최소한의 표준 준수 규정 제정
- 관리, 감독하기 위한 기관 또는 단체 지정
  (단, 독립성, 무결성을 위한 관리, 감독, 인증기관 분리 필요)
- 다 부처 참여의 소프트웨어 안전 협의체 필요
- TIC 산업을 표준 산업 군으로 분류
- 개발 초기 단계에서부터 안전 요건 정의 및 안전 활동 요건 의무화

2) 소프트웨어 안전 표준 및 가이드 제정

소프트웨어 안전이 실제 사회/산업적으로 적용되기 위해, 체계적인 절차와 방식에 따라 소프트웨어를 개발할 수 있도록 개발 절차의 표준 및 가이드를 제공할 필요가 있으며, 정부나 연구단체 또는 산업도메인별 선도 업체에서 주도적으로 소프트웨어 안전

평가 및 가이드를 제정하고 배포하며, 소프트웨어 안전 표준이 국내에 정착할 수 있도록 해외 표준 번역 및 해석, 국내 현황을 반영한 상세 수행 가이드의 제작이 수반되어야 한다.

세부 개선 방안은 아래와 같다.

- 정부/연구단체/산업도메인 선도업체 주도의 소프트웨어 안전 표준/가이드 제작
  (표준 번역 및 해석, 상세 수행 가이드, 측정가능한 수준의 명확한 소프트웨어 안전 개념 정립)
- 국제 표준 활동에 국내 안전 및 품질 단체 참여

3) 소프트웨어 안전 인적 기반 구축

국내 소프트웨어 안전 산업의 발전을 위한 도메인/서비스에 걸쳐서, 업계의 기술 및 전문가 활동을 강화하여 해외 경쟁력과 자생력을 키울 필요가 있으며, 수준 높은 전문 인력을 유입하고 육성하기 위한 글로벌 수준의 전문성 확보 방안이 마련되어야 한다.

세부 개선 방안은 아래와 같다.

- 초기 교육 과정부터 체계적인 소프트웨어 개발 교육 제공
- 개발자를 위한 업종/업무 사례 중심 교육 필요
- 기업에 대한 소프트웨어 안전 교육/연구 지원
- 소프트웨어 안전 분야를 정규 교육 화하고 전문 양성기관 신설
- 인증 및 자격증 제도 도입
  (자격증/인증 제도는 소프트웨어 안전 인식 및 신뢰성 제고를 위한 최소한의 규정으로 필요하며 민간 주도 권고)

4) 소프트웨어 안전 業 환경 개선

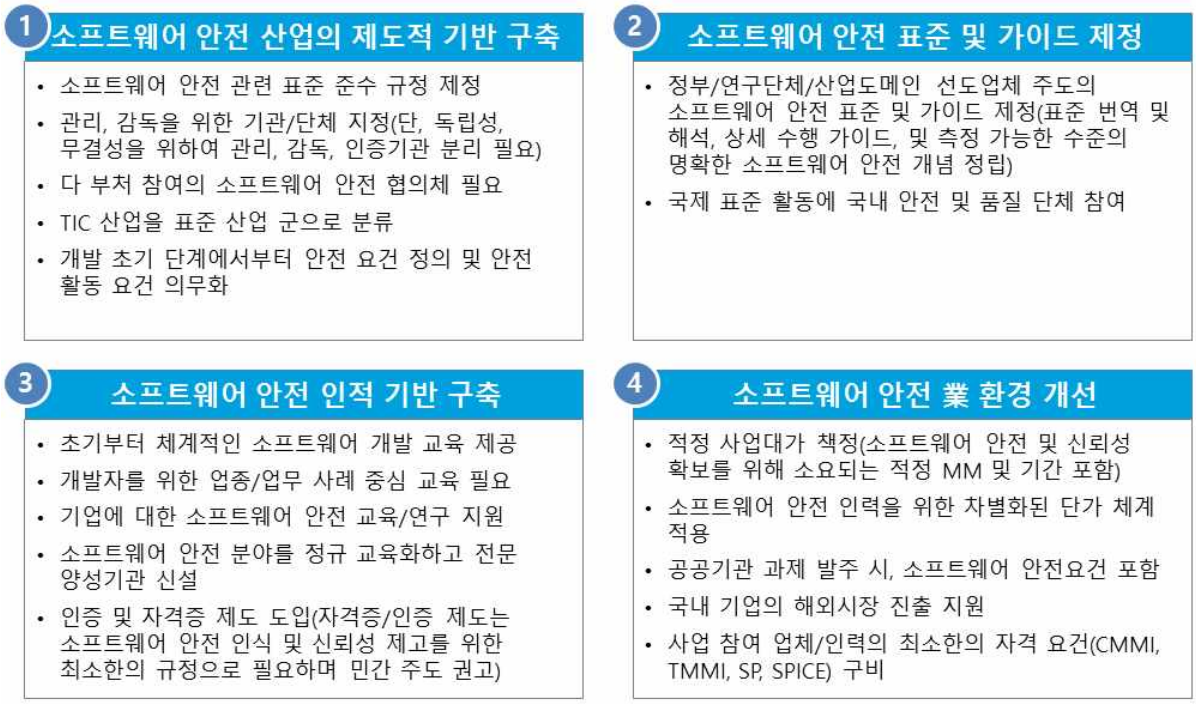
소프트웨어 안전 관련 業 환경 개선을 위해서는 무엇보다 소프트웨어 안전 관련 사회/산업적인 기반 성숙이 선행되어야 한다. 이를 위하여 소프트웨어 개발 및 안전 산업의 중요성과 미래 핵심사업의 비전을 부각하여 소프트웨어 안전 산업에 대한 인식을 제고하고, 소프트웨어 안전 서비스에 대한 대가의 현실화 등이 이루어져야 한다. 또한, 국내 기업의 경쟁력 확보를 위해 주요 산업 군별 Reference(Track Record)를 확보할 수 있는 기회가 제공될 필요가 있으며, 삼성, LG, 현대와 같은 글로벌 국내기업

대상의 내수시장과 지리적으로 근접한 중국, 동남아 등지의 해외시장진출 판로를 구축하기 위한 지원도 필요하다.

세부 개선 방안을 아래와 같다.

- 소프트웨어 개발 적정 사업대가 책정
  (소프트웨어 안전 및 신뢰성에 소요되는 적정 MM 및 테스트 기간 포함)
- 소프트웨어 안전 인력에 대하여 차별화된 단가 체계 적용
- 공공기관 과제 발주 시, 소프트웨어 안전 요건 포함
  (공공 주도로 시작하여 민간 부문으로 점진적 적용)
- 국내 기업의 중국, 동남아 등지의 해외시장 진출 지원
- 사업 참여 업체와 인력에 대하여 최소한의 자격 요건(CMMI, TMMI, SP, SPICE 등) 구비 필요

[그림 5-2] 4대 개선전략 및 세부 개선방안



제6장 결 론

최근 20년간 IT 기술 및 산업의 급격한 발전으로 인해 단순 기기들은 IT와 접목된 기기로 변화되었고, 이를 운영(Operate)하는 소프트웨어의 중요도가 증가하게 되었다. 이러한 사람들의 삶과 밀접한 IT 기반의 기기들이 증가하면서, 소프트웨어는 개인의 생활에 직접적인 영향을 미치는 수준으로 그 영향력이 증대되었다. 특히, IT 기반의 기기 중 안전과 직결된 기기의 경우, 문제 발생 시 사람의 인명에까지 영향을 끼칠 수 있게 되면서, 소프트웨어는 단순한 중요성을 넘어 소프트웨어 안전 부문으로 구분되어 논의되기 시작하였다. 이러한, 소프트웨어 안전 부문은 현재 초기 단계인 한국과 달리 해외, 특히 선진국에서는 매우 활발하게 논의되고 있으며 주요한 산업의 하나로 인식되고 있다.

한국의 경우, 소프트웨어 안전 부문은 제도적, 사회적, 산업적 기반이 빈약하여 아직 별도의 산업 군으로 조차 인정받지 못하고 있다. 근본적인 이유는 현재까지 소프트웨어 안전에 대한 명확한 개념이 정립되어 있지 못하여 이를 정착하기 위한 제도적인 기반이 미흡하고, 사회적인 인지도가 낮아 수준 높은 전문 인력 유입이 어려우며, 소프트웨어 안전이 소프트웨어 개발의 부록 정도로 인식되어 안전 활동에 소요되는 적절한 기간 및 대가를 인정받지 못하여, 이를 영위하는 업체들의 수익성 및 매출이 낮아 대부분 영세성을 벗어나지 못하고 있는 실정이었다. 반면, 글로벌에서 한국 산업 비중은 나날이 높아져 세계 일류 제품을 만들고 수출하는 국내 기업들이 증가하고 있는데, 이러한 기업들이 해외 시장에 진출하기 위한 주요 요건으로 소프트웨어 안전 표준을 준수하라는 요구가 많아지고 있다. 이러한 이유로 국내에서도 소프트웨어 안전에 대하여 산업도메인 전문적이고 수준 높은 서비스를 요구하는 수요가 증가하고 있는 추세이다. 이러한 시장 수요로 인하여, 해외의 주요 산업도메인에서 소프트웨어 안전 관련 많은 Reference(Track Record)를 보유하고 있고, M&A를 통한 규모의 경제 및 도메인 전문가를 확보하고 있는 글로벌 선진 TIC 업체의 국내 시장 진출도 진행되고 있다.

따라서 국내 소프트웨어 안전을 담보하고 국내 TIC업체의 경쟁력 강화를 위해, 국내 소프트웨어 제도적 기반을 구축하는 일이 시급하다고 판단되며, 우선 소프트웨어 안전 개념을 정립하고 이를 토대로 주요 산업도메인별 소프트웨어 안전 표준을 준수하게끔

직/간접적으로 규정하는 법/제도를 제정하고, 이들 규정이 준수될 수 있도록 관리/감독하는 기관의 지정이 필요하다. 이러한 제도적 기반을 마련한 후, 정부/학계/선도업계 주도로 각 산업도메인별 표준, 가이드 등을 제정하여, 실제 산업에서 활용할 수 있는 Tool을 제공하고, 전문 인력 육성을 위한 다양한 교육, 자격증 등의 정책을 마련해야 할 것이다. 또한 소프트웨어 안전 산업 활성화를 위하여 공공 Sector 주도의 소프트웨어 안전 요건을 포함한 사업 발주, 소프트웨어 안전 부문 분리 발주, 안전 부문 적정 대가 체계 등을 통해 산업 환경의 개선이 이루어져야 할 것이다.

결론적으로, 소프트웨어 안전에 대한 제도적 기반을 통해 사회 인식 제고 → 인적 기반 강화 → 산업 기반 강화의 선순환 체계를 조성하여, 안전 산업 기업의 경쟁력을 달성하고, 동시에 국내 소프트웨어 안전이라는 주요 명제를 달성할 수 있을 것으로 연구되었다.

본 연구는 앞서 언급했듯이, 미약한 산업 기반 하에서 처음으로 수행된 연구로써 소프트웨어 안전 산업 종사기업의 경우, 안전 또는 TIC관련 산업 분류체계가 존재하지 않는 관계로 기업 List를 확보하는데 어려움을 겪었고, 따라서 모든 소프트웨어 안전 종사 기업을 조사 대상에 포함시키지 못하였다. 또한, 소프트웨어 도입/개발/사용 기업의 경우, 안전 문제가 기업 기밀 사항으로 구분되어, 극히 일부의 기업만 인터뷰에 응하여, 대표성 있는 충분한 조사가 이루어지지 못하였다. 차후, 소프트웨어 안전 산업 기반이 마련되고, 성숙됨에 따라 보다 많은 조사 대상과 정교화 된 조사 항목을 통해, 더욱 포괄적이면서 구체성을 띄는 수준으로 연구되어야 할 것이다.

참 고 문 헌

국내 문헌

3) 위키백과, 『Misra C』, (2015). https://ko.wikipedia.org/wiki/Misra_c (2015-8 방문)

6) 최인정. 『자동차 법규』 http://dwcij.com.ne.kr/study/study_app2.htm (2015-8 방문)

33) 한국산업기술시험원. 『전기전자 기능안전 규격군』

해외 문헌

1) "ISO 26262", 『Wikipedia』. https://en.wikipedia.org/wiki/ISO_26262 (accessed July, 2015)

2) Hommes, Qi Van Eikema. (2012). "Assessment of the ISO 26262 Standard. "Road Vehicles-Functional Safety".

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

5) "Federal Motor Vehicle Safety Standards", 『Wikipedia』, https://en.wikipedia.org/wiki/Federal_Motor_Vehicle_Safety_Standards (accessed July, 2015)

7) Osuga, Ryuji. (2012). "Functional Saftey (ISO26262) activities in Japan". 1st Asia Automobile Institute Summit 26-27 November 2012, Tokyo.

8) "EN 50128.kr". 『Wikipedia』, https://de.wikipedia.org/wiki/EN_50128.kr (accessed July, 2015)

9) Winther, Troels. (2012). "Quick guide to Safety Management based on EN 50126 / IEC 62278".

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

11) NASA. (2014). "NASA Software Engineering Requirements". NPR 7150.2B-Chapter1.

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

13) NASA. (2013). "NASA-STD-8719.13C, Software Safety Standard"

14) "DO-178B", 『Wikipedia』, https://en.wikipedia.org/wiki/DO-178B (accessed July, 2015)

15) "RTCA DO-178B Process Visual Summary". https://upload.wikimedia.org/wikipedia/commons/4/4f/DO-178B_Process_Visual_Summary_Rev_A.pdf

16) Kim, Charles. "Standards of IEC related to safety-critical application of computers". Howard Universtiy. http://www.mwftr.com/cneF11/WK09_IECstandards.pdf

17) IAEA. (2009). "Implementing Digital Instrumentaion and Control Systems in the Modernization of Nuclear Power Plants". IAEA Nuclear Energy Series. No.NP-T-1.4.

18) IAEA. (1999). "Verification and Validation of Software Realted to Nuclear Power Plant Instrumentation and Control". Technical Reports Series No. 384.

19) ONR(Office for Nuclear Regulation). (2014). "A guide to Nuclear Regulation in the Uk".

20) Bundesamt für Strahlenschutz. (2015). "Nuclear safety-legal bases". http://www.bfs.de/EN/topics/ns/safety/law/law.html

21) Bundesamt für Strahlenschutz. "Committees developing nuclear safety standards". http://www.bfs.de/EN/topics/ns/safety/committees/standards/standards.html

22) Mergers Alliance. (2012). "Global Testing, Inspection and Certification".
23) Bureau Veritas. (2014). "Annual Report & Activity Report".
24) Bureau Veritas. (2013). "ISO 26262-Automotive Functional Safety Assessment & Support". http://www.bureauveritas.com/41d88bd5-5a77-4594-8eea-dce8e7045f6c/ISO26262-0913+JS+Final+11.9.13.pdf?MOD=AJPERES&CACHEID=41d88bd5-5a77-4594-8eea-dce8e7045f6c
25) DEKRA. (2014). "Annual Report".
26) DEKRA. http://www.dekra-certification.com/en/industry
27) "DNV GL". 『Wikipedia』, https://en.wikipedia.org/wiki/DNV_GL (accessed July, 2015)
28) Intertek. (2014). "Annual Report".
29) Bureau Veritas. (2014). "Annual Report & Registration Report".
30) CEOC. (2012). "TIC sector: a corporate finance perspective". ABN AMRO.
31) Weyers, Chirs. "Testing, Inspection and Certification Industry: Merger & Acquisition Activity Remains High".
32) Marketsandmarkets. (2015). "Summary in the TIC Market Report".