

연구보고서 2016-022

소프트웨어 안전(Safety) 산업 동향 조사

Software Safety Industry Trends Study

박태형/진회승/정영철/송현이/송광섭/안태진/권용희

2017.04.

이 보고서는 2016년도 미래창조과학부 정보통신·방송연구
개발사업의 연구결과의 보고서 내용은 연구자의 견해이며,
미래창조과학부의 공식입장과 다를 수 있습니다.

목 차

제1장 서론	1
제1절 개요	1
1. 배경 및 필요성	1
2. 목적	1
제2절 연구방법 및 범위	2
1. 국내 소프트웨어 안전 현황 조사 연구방법	2
2. 선진사례 조사방법	6
제2장 해외 선진사례 분석	11
제1절 주요 산업도메인별 소프트웨어 안전 표준 및 안전 활동 조사	11
1. 자동차 부문	11
2. 국방 부문	22
3. 항공 부문	32
4. 의료 부문	44
5. 조사 결과 요약 및 시사점	76
제2절 해외 TIC 시장 현황 조사	78
1. 해외 TIC 선진사 현황	78
2. M&A 현황	86
3. TIC 시장 전망	88
4. 조사 결과 요약 및 시사점	90

제3장 국내 소프트웨어 안전 산업동향 분석	92
제1절 학계 및 공공기관	92
1. 개요	92
2. 인터뷰 상세내역	92
3. 조사 결과 종합 및 시사점	100
제2절 소프트웨어 안전 분야 사업 기업	102
1. 개요	102
2. 회사 일반 현황	102
3. 프로세스 분석	107
4. 소프트웨어 안전 인프라 현황 및 니즈(Needs)	110
5. 조사 결과 종합 및 시사점	112
제3절 End User 기업	114
1. 개요	114
2. 소프트웨어 안전 일반 현황	115
3. 소프트웨어 안전 예방점검 활동	117
4. 소프트웨어 안전 대응관리 활동	119
5. 소프트웨어 안전에 관한 정책 요구사항	123
6. 조사 결과 종합 및 시사점	127
제4장 비교 분석 및 SWOT 분석	131
제1절 비교 분석	131
1. 개요	131
2. 2015년 대비 2016년 국내 소프트웨어 안전 산업 비교 분석	131
제2절 SWOT 분석	134

1. 개요	134
2. SWOT 분석	134
제5장 국내 소프트웨어 안전 산업 개선 전략 및 과제	137
제1절 개요	137
제2절 개선 전략 및 개선 과제 도출	137
1. 정부 및 학계 부문	138
2. 소프트웨어 안전 컨설팅 부문	139
3. 소프트웨어 안전 개발·사용자 부문	140
제3절 미래모습: 범정부 소프트웨어 안전 플랫폼 구성(안)	142
제6장 결론	143

표 목 차

<표 1-1> 조사 대상별 조사 항목	4
<표 1-2> 상세 조사 대상 및 수행 결과	5
<표 2-1> 가이드라인 섹션 및 주요 내용	14
<표 2-2> 주요 표준별 안전 및 위험에 대한 정의	19
<표 2-3> 위험 평가 접근 방법 비교	20
<표 2-4> 심각도 등급	25
<표 2-5> 소프트웨어 통제 등급	27
<표 2-6> 소프트웨어 안전 중요도 매트릭스	28
<표 2-7> 소프트웨어 심각도 등급, 위험수준, 안전활동수준 업무, 위험과의 관계	29
<표 2-8> DO-178B 제정 과정	33
<표 2-9> DO-178C의 주요 변경 항목	38
<표 2-10> DO-278A와 DO-178C의 용어(예시)	39
<표 2-11> DO-278A의 Assurance Level	39
<표 2-12> 툴 자격 수준(Tool Qualification Level)	42
<표 2-13> 소프트웨어 안전 등급	47
<표 2-14> FFD&C Act, Provisions	51
<표 2-15> FDA의 의료기기 분류	52
<표 2-16> 우려수준 기반의 문서요구사항	56
<표 2-17> 규칙에 따른 의료기기 분류	64
<표 2-18> MDD의 부속서	70
<표 2-19> 미국과 유럽의 의료 규정 비교	75

<표 2-20> TIC 매출 상위 기업의 일반 현황 (단위: \$ millions)	79
<표 2-21> TIC 매출 상위 기업의 매출 현황 (단위: millions)	79
<표 2-22> TIC 매출 상위 기업의 직원 수 현황 (단위: 명)	80
<표 3-1> 소프트웨어 안전의 개념에 대한 주요 결과	93
<표 3-2> 국내 소프트웨어 산업 현황 관련 주요 답변	94
<표 3-3> 국내 소프트웨어 안전 산업 현황 관련 주요 답변	95
<표 3-4> 해결방안 - 법/제도/인증 관련 주요 답변	96
<표 3-5> 해결방안 - 표준/절차/가이드	97
<표 3-6> 해결방안 - 조직/기관	98
<표 3-7> 해결방안 - 교육	98
<표 3-8> 해결방안 - 業 환경개선	99
<표 3-9> 해결방안 - 프로세스	100
<표 3-10> 국내 선도 소프트웨어 사업자 강점	106
<표 3-11> 해외 소프트웨어 선진사 강점	107
<표 3-12> 업계에서 적용 중인 등급/수준 예	110
<표 3-13> End User 부문 조사 대상	115
<표 3-14> 산업도메인별 조사항목 비교	129
<표 4-1> 2015년 vs 2016년 국내 SW 안전 산업 현황 비교	132

그 립 목 차

[그림 1-1] 국내 소프트웨어 안전 현황 조사 프레임워크	2
[그림 1-2] 2015년 TIC 시장 점유율	7
[그림 1-3] 2015년도 주요 TIC 기업의 매출 현황 (단위, \$ millions)	8
[그림 1-4] 2015년 대비 2016년 조사 범위 및 대상	9
[그림 2-1] 자율등급에 따른 자율주행차 구분 기준	12
[그림 2-2] 자율주행 등급과 자율주행 주요 기능	13
[그림 2-3] 차량 성능 가이드 프레임워크	16
[그림 2-4] 시스템 안전 프로세스 8개 단계	24
[그림 2-5] 안내서 구성	30
[그림 2-6] 제4장 소프트웨어 시스템 안전 엔지니어링 프로세스	32
[그림 2-7] RTCA/EUROCAE의 DO-178C/ED-12C 관련 지침 관계	34
[그림 2-8] IEC 62304와 다른 표준과의 관계	46
[그림 2-9] IEC 62304와 IEC 82304-1 범위	49
[그림 2-10] FDA 공인 합의 표준 (소프트웨어)	58
[그림 2-11] Class III의 적합성 평가 절차	67
[그림 2-12] Class IIa의 적합성 평가 절차	68
[그림 2-13] Class IIb의 적합성 평가 절차	69
[그림 2-14] Class I의 적합성 평가 절차	69
[그림 2-15] 소프트웨어 시스템의 경계 및 구조	82
[그림 2-16] 기능안전 인증 프로세스	85

[그림 2-17] 기능안전 요구사항	85
[그림 2-18] 최근 5년 M&A 현황	86
[그림 2-19] Bureau Veritas의 TIC 미국 시장 전략	87
[그림 2-20] Bureau Veritas의 TIC 중국 시장 전략	88
[그림 2-21] TIC 시장의 구분	90
[그림 2-22] 아웃소싱 시장의 성장률	90
[그림 3-1] 학계 및 공공기관 대상 조사결과 분석 틀	92
[그림 3-2] 소프트웨어 안전 개념 유형	93
[그림 3-3] Governing 문제점 및 해결 방안	101
[그림 3-4] 소프트웨어 안전에 대한 인식 조사	103
[그림 3-5] 소프트웨어 안전(Safety) 관련 주요 제공 서비스	104
[그림 3-6] 주요 고객 산업군 분포 비중	105
[그림 3-7] 고객사 주요 요구사항	106
[그림 3-8] 소프트웨어 안전 사업 비중	108
[그림 3-9] 소프트웨어 안전에 필요한 활동 중요도	109
[그림 3-10] Supervising 문제점 및 해결 방안	113
[그림 3-11] 소프트웨어 안전에 대한 정의	116
[그림 3-12] 소프트웨어 안전 관련 업무 담당하는 부서의 속성	117
[그림 3-13] 소프트웨어 기능오류로 인한 안전사고 예방 활동	118
[그림 3-14] 안전성 강화 제품의 제조/판매할 계획이 있는 경우 그 이유	119
[그림 3-15] 제품(솔루션) 관련사고 대응 시나리오 보유 현황 및 보유 기업 속성	120
[그림 3-16] 사고 대응 시나리오 중 소프트웨어 관련 영역 적용 항목	121
[그림 3-17] S/W 관련 사고 발생 시 문제해결을 위하여 필요한 순위	121

[그림 3-18] SW안전에 관한 전반적인 검증활동을 관리하는 톨 보유 현황	122
[그림 3-19] SW안전 테스트 및 사고사례정보를 수집/축적 기간	123
[그림 3-20] 소프트웨어 안전 테스트 및 사고사례정보 활용 내역	123
[그림 3-21] 소프트웨어 안전 인증 관련 정부의 정책 지원을 받은 경험	124
[그림 3-22] 정부에 대한 지원 요구사항 : 단계별 요구내역 추진절차	125
[그림 3-23] End User 기업 문제점 및 개선 방향	130
[그림 4-1] 국내 소프트웨어 안전 산업의 SWOT 분석 결과	136
[그림 5-1] 국내 소프트웨어 안전 산업 개선 전략 도출	137
[그림 5-2] 소프트웨어 안전 개선 전략 및 과제	141
[그림 5-3] 범정부 소프트웨어 안전 플랫폼 개념도(안)	142

요 약 문

1. 제 목

2016년 국내 소프트웨어 안전(Safety) 산업 동향 조사

2. 연구 배경 및 목적

본 연구의 목적은 소프트웨어 안전(Safety)에 대한 개념 정립에 도움을 주고, 소프트웨어 안전 산업 활성화를 위한 국내 소프트웨어 안전 정책 수립에 필요한 신뢰성있는 현황 자료 및 개선 방향을 제공하는 것이다. 제공하는 자료는 1. 주요산업도메인별 해외 주요국의 소프트웨어 안전 활동 동향 및 표준 조사 자료, 2. 해외 TIC 선진업체 및 TIC 시장 동향 자료, 3. 2016년 국내 소프트웨어 안전 산업 동향 자료가 해당된다.

3. 연구의 구성 및 범위

본 연구는 첫 번째 주요산업도메인별 해외 주요국의 소프트웨어 안전 활동 동향 조사의 경우, 의료, 자동차, 항공, 국방의 4개 도메인에 대한 조사가 이루어졌다. 의료 부문에서는 소프트웨어 안전 표준과 이와 관련된 해외 선진국(미국, 유럽)의 소프트웨어 안전 활동을 조사하고, 자동차 부문에서는 미국의 자율주행차 정책 및 자동차 안전 관련 주요 표준을 비교 분석하였으며, 항공 부문의 경우 DO-178C 및 DO-330을 조사하였으며, 국방 부문은 미 국방 관련 시스템 안전 표준인 MIL-STD-882E와 Joint Software Systems Safety Engineering Handbook을 조사하였다. 두 번째, 해외 TIC 선진사 및 시장 동향 조사의 경우, 2016년 해외 주요 TIC(Testing, Inspection and Certification) 기업인 SGS, Bureau Veritas, Intertek, DEKRA, DNV GL의 서비스 활동을 조사하고, 2016년 해외 TIC 시장 동향을 조사하였다. 세 번째는 2016년도 국내 소프트웨어 안전 산업 현황을 조사하였으며, 이를 토대로 네 번째, 2015년 대비 2016년 국내 소프트웨어 안전 산업 현황을 비교 분석하고 SWOT분석(강점/약점/기회/위협 분석)을 수행하였다. 다섯 번째로 선진 사례, 국내 사례 조사 결과, 비교 분석/SWOT 분석 결과를 종합하여 개선 전략 및 개선 과제를 도출하고 미래모형(안)을 제시하였다.

4. 연구 내용 및 결과

첫 번째 전년도에 이어서 조사된 주요산업도메인별 소프트웨어 안전 활동 조사의 주요 시사점 중 하나는 전자시스템 및 소프트웨어 안전에 대한 중요성이 증대되고 소프

트웨어 안전 표준이 융복합화되고 있다는 것이다. 미 도로교통안전국(NHTSA)은 자율주행차 정책 가이드라인에서 자동차 생산 및 운행의 안전을 위해 ISO 26262 뿐만 아니라 필요에 따라 MIL-STD-882E, DO-178C 등의 안전 표준 활용을 권고하였다. 또한, 차세대 자동차 안전 규제를 위해 미 연방항공청 규제 제도를 연구하고 있었으며, 자동차 안전 신뢰성 향상을 위해 2016년 6월 전자 시스템 안전 관련 주요 표준 6개를 분석하였다.

두 번째는 소프트웨어 안전과 관련된 표준은 추상적인 수준에서 구체적인 수준으로, 시스템 기능 안전의 일부분으로 다루어지던 것이 독립적인 소프트웨어 안전 영역을 구축하여 다루어지고 있으며, 점차 상세화 되고 중요도는 높아지고 있었다. 그 일례로, 자동차부문의 MISRA C는 2004년 버전의 모호한 용어를 명확하게 정의하고, 코딩 규칙을 142개에서 159개로 증가하여 2012년 버전을 발표하였다. 그리고 2016년 4월 MISRA Compliance를 발표하여 MISRA C와 MISRA C++에 대한 적용 가이드라인의 종류, 시행 방법의 효과, 사용된 편차의 범위, 규율화된 소프트웨어 개발 프로세스의 사용, 프로젝트 외부에서 개발된 컴퍼넌트 현황 등을 밝히도록 준수 지침을 강화하였다. 항공부문은 새로운 소프트웨어 동향 및 기술 수용, 안전 프로세스 간 명확하고 일관된 연결 관계 제공을 위해, DO-178B를 잇는 표준으로 DO-178C, DO-278A와 기술 보충서를 발표하였다.

2016년에는 의료도메인의 동향을 신규로 추가하여 조사하였다. 먼저 의료부문의 기능 및 소프트웨어 안전 표준인 IEC 62304는 유럽과 미국에 채택된 의료제품 소프트웨어 설계에 대한 조화된(harmonized) 표준이다. 이것은 소프트웨어 안전 등급을 Class A, B, C로 구분하고 응용시스템을 분리(segregation)하여 소프트웨어 항목(item) 단위에서 안전 등급을 적용하도록 하며 의료기기 소프트웨어의 SOUP¹⁾ 사용을 식별하고 소프트웨어 설계 절차에 통합하여 검증하도록 하였다. 의료부문의 안전 인증 측면을 보면, 미국과 유럽은 각각 FDA인증과 CE마크를 통하여 각각 미국시장과 유럽시장 내 의료기기의 판매를 허용하고 있었다. 관할조직은 미국의 경우, FDA(미국식품의약국)의 CDRH²⁾에서 의료기기제품의 510(k) (premarket notification 510(k), 시판전통보)와 PMA (premarket approval, 시판전승인)을 담당하고, 유럽은 유럽연합의 조화된 의료관련지침(AIMDD, MDD, IVD)에 근거하여 각 EU 회원국의 규제당국에서 인증기관인 Notified Body와 CE인증을 담당하고 있었다.

두 번째 조사항목인 해외 TIC업체 및 시장 동향 조사 결과를 보면, 2015년과 동일하게 매출 상위 업체인 SGS, Bureau Veritas, Intertek, DEKRA, DNV GL이 전체 TIC 시장

1) Software of unknown provenance, 출처가 알려지지 않은 소프트웨어

2) Center for Devices and Radiological Health

을 주도하고 있었다. TIC 시장은 매년 5.15%의 지속적인 성장을 하여 2022년 약 1,132억 달러의 시장규모가 될 것으로 예측된다. 이러한 시장 성장의 이유로는 산업안전표준 기반의 규제 강화와 글로벌화로 인한 시장의 확대, 아웃소싱의 증가, 안전 및 품질 관리의 증가 등이 꼽혔다. 특히 아웃소싱 시장은 신규 규제의 증가로 인한 기업 내부의 비용 절감과 책임분산의 필요성이 대두되어 매년 5~6%의 높은 성장이 예상된다. TIC 시장은 유럽 중심에서 미국으로 이동 중이며, 향후 아시아(중국)지역이 가장 큰 시장이 될 것으로 전망된다. 특히 중국은 현재 TIC 시장 규모는 작으나 경제성장, 중산층 확대, 규제의 강화 등의 이유로 성장 향후 TIC 시장에서 중요한 지역이 될 것으로 예측되었다.

세 번째 국내 소프트웨어 안전 산업 동향 조사 결과를 토대로 비교분석/SWOT 분석, 그리고 선진사례를 반영하여 정부 및 학계, 소프트웨어 안전 컨설팅 업계, 소프트웨어 안전 개발·사용자로 구분하여 도출된 개선 전략 및 과제는 아래와 같다.

- 정부 및 학계 부문

- ✓ 개선 전략: ‘소프트웨어 안전 생태계 조성을 위한 법/제도적 기반 및 지원 체계 마련’
- ✓ 개선 과제(총 9개): 소프트웨어 안전 개념 정립 및 확산, 소프트웨어 안전 관련 정책 수립, 소프트웨어 안전 관련 법/제도 제정, 소프트웨어 인증제도 개선, 소프트웨어 안전 자격 제도, 범정부 차원의 지원체계 수립, 전문인력 양성, 소프트웨어 안전 공통 산업 기반, 전문가 자문단 운영

도출된 9개 과제를 실행 순서에 따라 정리하면, 소프트웨어 안전 개념 정립 및 확산을 기반으로 한 소프트웨어 안전 관련 정책 수립 및 법/제도 제정하고 소프트웨어 안전 인증 및 자격 제도를 수립하여 안전 관련 인력이 유입될 수 있는 기반을 확보하고 범정부 차원의 지원 체계 수립을 통해 정책, 법/제도, 인증/자격 제도가 원활하게 운영될 수 있도록 지원하고, 안전 전문 인력 양성을 지원하며 산업계가 공통으로 활용할 수 있는 소프트웨어 안전 기반을 제공하고, 전문가 자문단을 운영하여 수시 활동을 통해 ‘소프트웨어 안전 생태계 조성을 위한 법/제도 기반 및 지원 체계 마련’ 개선전략을 달성하는 것이다.

- 소프트웨어 안전 컨설팅 부문

- ✓ 개선 전략: ‘소프트웨어 안전 기술 및 문화 주도’

- ✓ 개선 과제(총 4개): 소프트웨어 문화 민간분야 정착 주도, 소프트웨어 안전 표준 매뉴얼/가이드 작성, 소프트웨어 안전 관련 도구 개선, 소프트웨어 안전사고 및 해결 사례 공유

도출된 4개 과제를 실행 순서에 따라 정리하면, 소프트웨어 안전 컨설팅 업계는 소프트웨어 안전 문화 민간분야 정착 주도에 대한 인식 및 활동이 필요하며, 이를 위해 소프트웨어 안전 표준 매뉴얼/가이드 작성과 소프트웨어 안전 관련 도구(Tool) 개발 및 개선 활동이 필요하다. 또한, 소프트웨어 안전 지식 기반 확대를 위해 안전 컨설팅 업계 간 소프트웨어 안전사고 해결 사례가 공유되어야 한다.

- 소프트웨어 안전 개발·사용자 부문

- ✓ 개선 전략: ‘소프트웨어 안전 문화 정착’
- ✓ 개선 과제(총 3개): 기업의 자발적 안전체계 도입, 제3자 검증, 산업 도메인별 특성을 고려한 적용

도출된 3개 과제를 실행 순서에 따라 정리하면 기업이 자발적으로 안전 체계를 도입하기 시작하고 좀 더 객관적인 안전 검증을 위해 제3자 검증이 확대되며, 안전체계 및 안전 가이드 등이 산업도메인의 특성을 고려하여 업종별로 적용되어야 한다.

위에서 도출된 개선 전략 및 과제를 통해 미래모습으로 범정부 소프트웨어 안전 플랫폼(안)을 제시하면, 정부 차원에서는 소프트웨어 안전에 대한 정책, 법령, 지침, 가이드라인을 수립하고 관련 인증 지원, 해외 판로 지원 뿐 아니라 안전사고 해결사례에 대한 공유 데이터베이스 제공, 설계에 대한 안전 회피 메커니즘을 검토하는 시스템(범용적인 부분 중심, 업종별 특화 영역은 제외) 등을 제공하고, 이러한 정부서비스 기반하에, 각 산업 도메인별로 정부가 지정한 소프트웨어 안전 컨설팅 전문 업체가 안전 컨설팅 및 검증 작업을 지원하며, 이를 기반으로 제조 및 소프트웨어 개발 기업에서는 소프트웨어 안전이 강화된 제품을 생산하게 되는 구조이다.

SUMMARY

The purpose of the study is to help to form the definition of software safety and to promote software safety industry in Korea by 1. studying software safety trends and policies in advanced countries (eg. US, Germany, UK, Japan, etc), 2. studying world leading TIC(Testing Inspection and Certification) companies and TIC market, 3. surveying 2016' s software safety industry trend in Korea. It also intends to provide reliable basic data and the direction to improve domestic software safety policy.

1. Software trends and policies in advanced countries.

The study found the importance of electronic systems and software safety is increasing and safety standards are converging. In the autonomous vehicle policy guideline, NHTSA(National Highway Traffic Safety Administration) recommends the use of safety standards such as MIL-STD-882E, DO-178C, and ISO 26262 for the safety of automobile production and operation. NHTSA studied the Federal Aviation Administration regulatory system for the next generation automotive safety regulations and analyzed six electronic system safety standards to improve automobile reliability in June of 2016.

Software safety standards have evolved from the conceptual to the actual, and from in a subset of functional safety to a independent software safety.

2. World Leading TIC companies and TIC Market

Like in 2015, SGS, Bureau Veritas, Intertek, DEKRA, and DNV GL are the leading TIC companies in a golbal TIC market. The TIC market is expected to grow at an annual rate of 5.15%, resulting in a market size of approximately \$113.2 billion by 2022. The growth of this market is mainly due to strengthened regulation, expansion of market due to globalization, increase in outsourcing, and increase in demand for safety and quality control. In particular, the outsourcing market is expected to grow at a rate of 5~6% per year due to in demand for the cost reduction and the distributing responsibility.

3. Korea software safety industry trend in 2016

- Government and academic sectors
 - ✓ Improvement strategy: 'Establishing a legal / institutional software safety ecosystem'
 - ✓ Improvement Tasks: Establishing software safety concept and promoting software safety awareness, Establishing software safety policy, Establishing software safety law and regulations, Improving software certification system, Establishing software safety qualification system, Establishing government support system, Training Software Safety professionals, Operating advisory groups

- Software Safety Consulting Sector
 - ✓ Improvement strategy: 'Leading technology and culture for software safety'
 - ✓ Improvement Tasks: Establishing software-centric culture in private sector, making software safety standard manuals / guides, improving tools for software safety, sharing knowledge on software safety accidents and resolutions.

- Software Safety Developer / User Sector
 - ✓ Improvement strategy: 'Establishing a software safety culture'
 - ✓ Improvement Tasks: Establishing voluntary software safety system in industry, 3rd party inspection and verification, considering characteristics of industry domain upon applying software safety system.

제1장 서론

제1절 개요

1. 배경 및 필요성

2016년은 IT(Information Technology) 기술 및 산업에 있어 의미 있는 해이다. 구글의 알파고가 지금껏 불가능하다고 여겼던 바둑 분야에서 세계 최고수인 이세돌 9단에게 완승을 거두면서 인공지능의 신기원을 이룩하였고, 자율주행차가 핵심 화두로 떠올랐으며, 다양한 분야에서 사물인터넷을 활용한 제품이 상용화되기 시작하였다. 이러한 기술 모두 인간의 실제 생활에 밀접한 관련을 가지고 있고, 그 역할 또한 더욱 증가하여 향후 10-20년 내에 이러한 기술 없이 생활하는 것은 불가능해질 것으로 예상되는데, 특히 소프트웨어가 핵심 역할을 담당하고 있다. 이러한 특징으로 소프트웨어 안전은 더욱 중요한 부분으로 자리 매김하고 있으며, 특히 2016년 6월 30일 플로리다 주 월리스턴 고속도로에서 발생한 테슬라 S 자율주행차 첫 사망사고는 소프트웨어 안전이 대중의 일상생활에서 생명까지 영향을 미칠 수 있다는 것을 보여 준 중요한 사고였다.

2015년 국내 소프트웨어 안전 산업 동향 조사는 조사의 프레임워크 정의 / 조사 대상 정의 및 선정 / 주요 조사항목 정의 등의 기본 틀을 수립하여 불모지였던 국내 소프트웨어 안전 및 안전 산업에 대한 동향을 처음으로 파악하고, 이를 토대로 선진국과 국내 현황과의 비교 분석(Gap Analysis) 및 SWOT 분석 등을 통해 국내 소프트웨어 안전 정착을 위한 정책 수립 자료 및 아이디어를 제공하는 등의 성과가 있었다. 그러나 기간, 예산 및 범위 등의 제약으로 실제 제품 및 서비스를 제공하는 소프트웨어 개발·사용 기업(End User)의 소프트웨어 안전 활동에 대한 조사는 다소 부족하였다.

2. 목적

본 연구의 목적은 2016년 IT 트렌드를 반영하고, 2015년 국내 소프트웨어 안전 동향 조사에서 부족했던 소프트웨어 개발·사용 기업(End User) 부분에 대한 중점 조사를 통해 국내 소프트웨어 안전 산업의 구조적인 특성과 실태를 파악하고, 최신 해외 주요

국의 소프트웨어 안전 표준 및 관련 정책, 글로벌 시장현황을 조사하여 SW 안전성 제고를 위한 신뢰성 있는 정책 기초 자료를 제공하기 위함이다.

제2절 연구방법 및 범위

1. 국내 소프트웨어 안전 현황 조사 연구방법

2016년 조사는 2015년 조사 결과를 반영하여 1. 기존 프레임웍(Framework) 및 조사 항목을 수정/보완 및 현행화(Update)하고, 2. 조사 대상은 실제 제품 및 서비스를 제공하거나 활용하는 주체인 소프트웨어 안전 개발·사용자는 확대하고, 단순 소프트웨어 테스트만을 영위하는 TIC 업체는 조사 대상에서 제외하여 보다 정확한 국내 소프트웨어 안전 현황이 조사될 수 있도록 하였다.

1) 범위 및 대상

조사 범위는 2015년 기존 프레임웍을 준용하여, 소프트웨어 안전 학계·정부(Governing Sector), 소프트웨어 안전 컨설팅(Supervising Sector), 소프트웨어 안전 개발·사용자(End User Sector) 그룹으로 구분하여 동향조사를 실시하였다.

[그림 1-1] 국내 소프트웨어 안전 현황 조사 프레임웍



소프트웨어 안전 학계·정부는 소프트웨어 안전성 확보를 위한 정책적/학술적 역할을 수행하는 주체로써 주로 소프트웨어 안전 관련 법/제도 제정과 관련된 기관과 안전 연구 및 표준을 수행하는 기관으로 정의하였다. 소프트웨어 안전 컨설팅은 소프트웨어 테스트, 검사/인증 등의 활동을 통해 소프트웨어 안전을 점검하는 주체로써 TIC 기업(소프트웨어 안전 테스트, 검사 및 인증 산업 종사 기업)과 소프트웨어 안전 전문 기업(제품의 기능 안전 산업 종사 기업)으로 정의하였다. 소프트웨어 안전 개발·사용자는 소프트웨어 안전이 요구되는 제품/서비스/인프라 등을 제공하거나 사용하는 주체로 정의하였다.

2) 조사항목

각 그룹별 조사 항목은 2015년의 틀을 근간으로 해서, 2016년 소프트웨어 안전 이슈 반영, 유사 질문 통합, 모호한 질문 명확화, 실효성 없는 질문의 대체 및 삭제 등을 통해 소프트웨어 안전 중심으로 조사를 수행할 수 있도록 하였다. 특히, 이번 조사에서는 안전한 소프트웨어 및 제품 개발을 실제 담당하고 있는 소프트웨어 안전 개발·사용자(End User Sector)가 안전한 소프트웨어 개발 또는 도입을 가능하게 하는 전반적인 소프트웨어 안전 관련 체계(프로세스/매뉴얼, 인력/조직, 인프라 등) 보유 현황 및 준수 여부 조사에 주안점을 두었다.

소프트웨어 안전 학계·정부의 경우 거시적인 관점의 질문을 중심으로 하여 세계적인 소프트웨어 안전 개념의 변화 추이, 국내 소프트웨어 산업 및 안전 산업의 현황 및 문제점, 문제점을 해결하기 위한 국가 정책적/문화적 차원의 방안 등을 조사하였다. 소프트웨어 안전 컨설팅의 경우 각 인터뷰 대상 업체가 생각하는 소프트웨어 안전에 대한 개념, 소프트웨어 안전 확보를 위한 프로세스 및 인프라, 소프트웨어 안전 산업 활성화를 위한 지원요청 사항 등을 조사하였다. 소프트웨어 안전 개발·사용자의 경우는 제품/서비스를 개발 및 사용하는 과정에서 소프트웨어 안전을 담보하기 위한 인력/조직 체계, 프로세스 및 인프라, 정부 지원 요청 사항 등을 조사하였다. (<표 1-1> 참조).

〈표 1-1〉 조사 대상별 조사 항목

조사 대상	주요 조사 항목
소프트웨어 안전 학계·정부 (Governing Sector)	<ul style="list-style-type: none"> • 소프트웨어 안전 개념 • 소프트웨어 안전 산업 현황 및 문제점 • 해결방안: 법/제도/인증, 표준/절차/가이드 및 프로세스, 조직/기관, 교육, 業 환경개선 등
소프트웨어 안전 컨설팅 (Supervising Sector)	<ul style="list-style-type: none"> • 기업 현황 및 소프트웨어 안전 개념: 소프트웨어 안전 정의 및 개념, 주요 제공 서비스 및 고객현황, 소프트웨어 안전 사업규모 및 전문가 확보 현황 • 프로세스 측면: 예방, 탐지, 대응, 사후 활동 • 인프라 측면: 표준/매뉴얼, 인력/조직, 시스템 • 지원 요청 사항: 법/제도, 인력 및 시장 개발 측면
소프트웨어 안전 개발·사용자 (End User Sector)	<ul style="list-style-type: none"> • 인력/조직 체계: 소프트웨어 안전사고 예방/대응 관리 조직 및 역할, 내부 보유 전문 인력/자격요건 현황 • 프로세스 측면: 소프트웨어 개발/도입/변경 시 소프트웨어 안전 사전 점검 활동, 소프트웨어 안전사고 발생 시 대응 방안 및 사후관리 방안 • 인프라 측면: 소프트웨어 안전 관련 표준/매뉴얼 보유 현황 및 지원 요청 사항 • 지원 요청 사항: 법/제도, 인력 및 시장 측면

3) 조사방법 및 경과

앞에서 정의된 조사 그룹 및 조사 항목에 따라, 각 그룹별 특성에 맞는 조사 방법을 통해 조사를 진행하였다. 소프트웨어 안전 학계·정부 그룹의 경우, 그룹의 특성상 구조화된 설문보다는 주요 조사 내용 근간으로 해서 자유롭게 묻고 답하는 식으로 인터뷰가 진행되었고, 소프트웨어 안전 컨설팅 및 소프트웨어 안전 개발·사용자 그룹의 경우, 각 그룹의 특성에 맞는 구조화된 설문지를 통해 인터뷰 방식으로 설문을 진행하였다. 즉, 모든 설문은 일대일 대면 질의 조사 형식으로 진행되었고, 설문지 배포/작성/취합을 통한 조사는 수행하지 않았는데, 이는 본 연구 조사대상의 특성상 분야별로 전문화되어 있고 모수가 작으며 현재까지 국내에서는 소프트웨어 안전 개념이 정립 및 보편화되어 있지 않아서 단순 설문지 배포를 통한 설문은 효과가 없었기 때문이다.

각 그룹별 조사 대상을 파악 및 인터뷰 요청 후, 소프트웨어 안전 학계·정부는 3곳, 소프트웨어 안전 컨설팅 7곳, 소프트웨어 안전 개발·사용자 19곳에 대해 실제 방문 인터뷰를 수행하였다. 소프트웨어 안전 컨설팅 및 소프트웨어 안전 개발·사용자의 경

우 인터뷰 대상 대부분이 민간 기업으로서, 기업 정보 유출을 우려한 관계로 본 연구는 기업의 실명 및 원본 조사 데이터는 제공하지 않고 가공된 결과와 결과 분석을 통한 시사점을 제공한다.

<표 1-2> 상세 조사 대상 및 수행 결과

구분	조사 대상 파악	수행 결과
소프트웨어 안전 학계·정부 (Governing Sector)	<ul style="list-style-type: none"> • 대학: 3개 • 주요 도메인별 연구/공공 기관: 15개 <ul style="list-style-type: none"> - 철도안전협회 - 철도기술연구원 - 한국원자력안전기술원 - 한국자동차안전학회 - 교통안전공단 자동차안전연구원 - 한국철도기술연구원 - 항공안전기술원 등 	<ul style="list-style-type: none"> • 총 3개 방문 인터뷰 수행
소프트웨어 안전 컨설팅 (Supervising Sector)	<ul style="list-style-type: none"> • 기능 및 소프트웨어 안전 컨설팅: 10개 • 시험/인증/평가: 7개 <ul style="list-style-type: none"> - 한국산업기술시험원 - 정보통신기술협회 - 한국의료기기 기술원 - 한국의료기기 검사원 - 지능형자동차부품진흥원 - 한국아이티평가원 등 	<ul style="list-style-type: none"> • 5개 기능 및 소프트웨어 안전 컨설팅 업체 방문 설문 인터뷰 • 2개 시험/인증/평가 기관 방문 설문 인터뷰 • 총 7개 방문 설문 인터뷰 수행
소프트웨어 안전 개발·사용자 (End User Sector)	<ul style="list-style-type: none"> • 정보통신 • 자동차 • 우주항공 • 금융 • 국가 기간 인프라 • 제조 	<ul style="list-style-type: none"> • 10개 정보통신 기업 • 2개 완성차 제조 기업의 자율주행 관련 부서 및 자동차 전자 부품업체 • 2개 금융 IT 기업 • 3개 우주항공 제조 기업 및 부품 기업 • 2개 국가 기간 인프라 및 제조업체 방문 인터뷰 • 총 19개 방문 설문 인터뷰 수행

2. 선진사례 조사방법

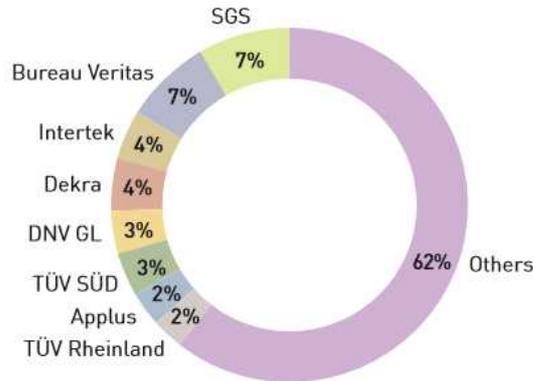
2015년 조사에서 수행하였던 주요 산업 도메인별(자동차, 철도, 항공, 원자력) 표준 및 선진국의 안전 보장을 위한 활동은 대부분 1년간 큰 변화가 없었기 때문에, 2016년 선진사례 조사에서는 2015년 조사에 포함되지 않았던 산업도메인에 대한 소프트웨어 안전 표준 정책 및 선진국 활동을 추가하고, 2015 ~ 16년 사이 변화가 많이 발생했거나 관심이 높은 산업도메인의 안전 표준 또는 안전 분야 정책 등을 조사하였다. 글로벌 TIC(Testing, Inspection and Certification) 시장 동향은 작년과 동일한 방법으로 수행하였으며 2016년 변경된 시장 동향을 조사하여 반영하였다.

1) 범위 및 대상

2016년 선진사례 조사에서는 1. 2015년 수행 시 포함되지 않았던 의료 부문 표준 및 주요국의 안전 활동 조사를 추가하고, 2. 최근 관심이 급증한 자율주행차 관련 미국의 정책 중 기능안전 관련 부문을 조사하고, 3. 항공부문 안전 표준에서 변경 및 추가된 내용을 조사하고, 4. 미국 국방 부문 소프트웨어 안전 표준 및 가이드를 조사하였다. 미국 국방 부문의 경우 타 산업 도메인 기능 안전 표준(자동차, 우주항공 등)에서 특정 부품이나 영역에 대해서는 미국 국방 부문의 표준 및 가이드를 참조하거나 지침 준수를 요구하는 사례가 늘어 본 연구 선진사례 대상에 추가하였다. 따라서 국방 부문의 경우는 타 산업 도메인과 달리 안전 부분 표준 및 가이드의 상세 내용을 조사하는 대신 안전 활동 조사는 범위에 포함하지 않았다.

해외 TIC 선진사의 경우 작년과 동일하게 TIC(Testing, Inspection and Certification) 시장의 Key Players 중, 2015년도 매출 상위 5개 기업을 선정하여 TIC 시장 현황을 조사하였다. 아래 [그림 1-2]를 살펴보면 주요 Players들의 TIC 시장 매출 비중이 40% 정도를 차지하고 있으며, 나머지 기업이 60% 정도를 차지하고 있다. 매출 상위 5개 기업의 활동을 통하여 전체 TIC 시장을 가늠해 볼 수 있으며, 특히 전체 시장의 14%를 점유하는 스위스의 SGS와 프랑스의 Bureau Veritas가 TIC 시장을 주도하고 있다.

[그림 1-2] 2015년 TIC 시장 점유율



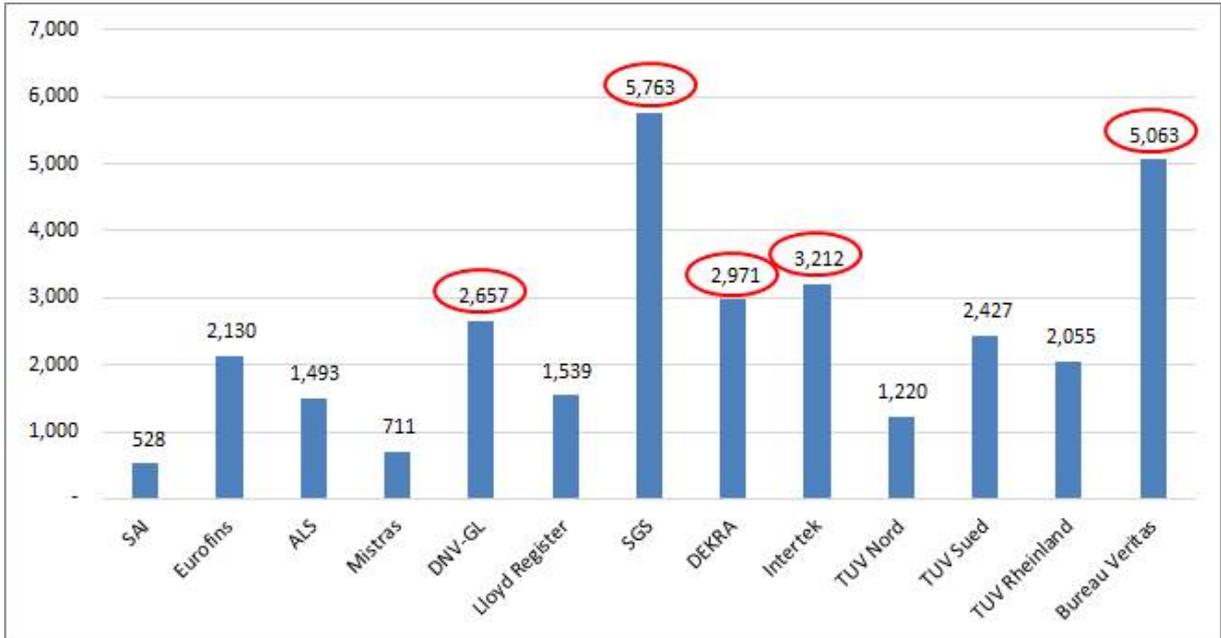
자료: Catalyst Corporate Finance LLP, 2016

이를 토대로 5개 기업 선정을 위한 주요 기업별 2015년도 매출을 조사하였다. 주요 Key Players는 작년의 선정기준과 동일한 업체를 대상으로 하였으며, 전체 대상 기업은 아래와 같이 구분된다.

- 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)

각 기업의 매출 규모는 2015년 Annual Report에서 참조하였고, 매출 규모의 비교를 위해 각 기업의 화폐단위는 US달러로 통합하였다(2015.12.31 환율적용). 2015년 매출 현황을 보면 SGS가 57억 달러로 TIC 시장 1위를 차지하였고, Bureau Veritas, Intertek 등이 그 뒤를 잇고 있었다. 조사된 매출 현황을 바탕으로 선정된 기업은 작년과 동일하며, 또한 [그림 1-2]의 주요 Players와 동일한 SGS, Bureau Veritas, Intertek, DEKRA, DNV GL의 5개 기업이며, 이들을 대상으로 사업 현황을 조사하였다.

[그림 1-3] 2015년도 주요 TIC 기업의 매출 현황 (단위, \$ millions)



2) 조사항목

자동차 부문의 경우, 최근 이슈가 되고 있는 자율주행차 관련 미국 도로교통안전국 안전 정책 중 기능 및 소프트웨어 안전 지침 및 정책을 조사하였고, 항공 부문은 DO-178B 표준과 신규로 작성된 DO-178C 표준에 대한 차이점에 대하여 조사하였다. 의료 부문에서는 IEC 62304 중심의 의료기기 관련 소프트웨어 표준과 미국 및 유럽연합 대상의 의료기기 및 소프트웨어 안전 활동에 관한 법/규정 또는 지침, 규제기관 및 안전 인증 활동을 조사하였다. 국방 부문의 경우, 미 국방 시스템 안전 표준(MIL-STD-882E)과 소프트웨어 시스템 엔지니어링 핸드북(Joint Software System Engineering Handbook)의 기능 안전 및 소프트웨어 안전 관련 가이드 및 지침 등을 조사하였다.

해외 TIC 선진사의 경우, 2015년 기준 매출 상위 5개사를 선정하고, 이들의 2015년 기준 회사 일반 현황, 매출 규모, 소프트웨어 안전 관련 주요 제공 서비스 등을 조사하였고, 해외 TIC 시장의 경우 2015년 시장의 주된 특징 및 M&A 활동, TIC 시장의 향후 전망 등을 조사 분석하였다.

[그림 1-4] 2015년 대비 2016년 조사 범위 및 대상

구분	대상	2016년	2015년
주요 산업 도메인	자동차	<ul style="list-style-type: none"> • 미 자율주행차 규정 중 안전(시스템/SW) • 차량전자제어시스템 안전표준분석 	<ul style="list-style-type: none"> • ISO 26262 中 SW 안전 부분 • 미국, 유럽, 일본의 SW안전 활동
	철도	-	<ul style="list-style-type: none"> • EN50128/IEC62279, AREMA C&S Manual of Recommended Practices • 미국, 유럽 SW안전 활동
	항공	<ul style="list-style-type: none"> • DO-178C 부분 상세 조사 	<ul style="list-style-type: none"> • DO-178, NASA-STD-8719.13 • 미국 SW안전 활동
	원자력	-	<ul style="list-style-type: none"> • IEC 61513, IEEE STD 7-4.3.2 • 미국, 영국, 독일, 일본 SW안전 활동
	의료	<ul style="list-style-type: none"> • IEC 60601, 62304 중 SW안전 • 유럽연합, 미국의 의료기기 SW안전 규정 및 활동 	-
	국방 (미국)	<ul style="list-style-type: none"> • MIL-STD-882E 중 SW안전 • Joint SW System Engineering Handbook 조사 	-
해외 TIC 시장		<ul style="list-style-type: none"> • 2016년 Global TIC Market 동향 • Global TIC 업체의 SW 안전 활동(업체는 2015년과 동일) 	<ul style="list-style-type: none"> • 2015년 Global TIC Market 동향 및 • Global TIC 업체 SW안전 활동 (SGS, DEKRA, Bureau Veritas, Intertek, DNV GL)

3) 조사 방법 및 경과

2015년과 마찬가지로 선진사례 조사 방법은 인터넷을 활용한 문헌 및 홈페이지 조사를 토대로 이루어졌는데, 자동차 부문의 경우 미국 교통부 (Department of Transportation) 홈페이지 및 산하 도로교통안전국 (NHTSA, National Highway Transportation Safety Administration) 홈페이지와 2016년 9월에 발행한 연방 자동 주행차 정책 (Federal Automated vehicles Policy) 및 자동차 전자 제어 시스템의 안전 표준 비교 분석 (Assessment of Safety Standards for Automotive Electronic Control Systems) 자료를 조사하였다. 항공 부문은 미국항공우주협회, 항공안전건설업체 등에서 발행한 백서 또는 발표자료 등을 기반으로 DO-178B와 DO-178C의 변화 및 차이점을 조사하였고 의료 부문은 표준제정위원회인 IEC(International Electrotechnical Commission)와 미국 FDA 홈페이지 및 유럽연합(EU) 헌법/법률/지침 홈페이지를 주로 조사하였다. 국방의 경우 미 국방성(DOD, Department of Defense) 홈페이지 및 국방성에서 발행한 시스템 안전 표준 실습(Standard Practice System Safety, MIL-STD-882E) 및 공동 소프트웨어 시스템 안전 공학 안내서(Joint Software Systems Safety Engineering Handbook)를 조사하였다. 또한 기타 주요 연구기관에서 발표한 자료 등을 수집 조사하였다.

해외 TIC 선진사의 경우, 회사 일반 현황 및 소프트웨어 안전 관련 제공 서비스 등

을 각 선진사의 홈페이지를 통해 조사하였다. 다만, 소프트웨어 안전 부분에 대한 상세 매출은 별도로 구분되어 있지 않아 소프트웨어 안전에 특화된 매출은 조사가 어려웠다. 세계 TIC 시장 동향의 경우, 2016년 CATALYST에서 출간한 TIC 자료(Global Testing, Inspection and Certification Summer 2016)와 다양한 TIC 시장 관련 자료 및 홈페이지를 통해 수집 조사하였다. 또한 TIC 시장은 크게 내부(In house)시장과 아웃소싱(addressable outsource)시장으로 나뉘며, 외부 전문 기업에 의한 아웃소싱 시장을 중심으로 문헌조사를 진행하였다.

제2장 해외 선진사례 분석

제1절 주요 산업도메인별 소프트웨어 안전 표준 및 안전 활동 조사

1. 자동차 부문

2016년 자동차 부문 중요한 화두 중 하나는 자율주행차였다. 최근 10여 년간 자동차의 많은 장치 및 부품이 기계식에서 전자식으로 대체되어 왔는데, 이것은 자동차 운행의 핵심적인 장비(엔진, 기어 등)에서부터 운행 보조 장비(내비게이션, 오디오 등)를 아우르는 전 분야에 걸쳐서 진행되어 왔다. 최근 2~3년 사이에는 이러한 추세를 토대로 점차 자동차 스스로 운행하는 자율주행차에 대한 시도가 증가하고 성숙되어 가고 있는 상황이다. 현재, 구글(Google)을 선두로 아마존, 우버(Uber) 등과 같은 주요 IT 기반 기업과 전통적인 완성차 업체(BMW, Mercedes Benz, AUDI, 테슬라 등)가 자율주행차 분야에 매진하고 있는 형국이다. 자율주행차의 핵심은 다양한 전자 장치와 이러한 전자 장치를 통해 취합되는 주변 및 운행 정보를 토대로 차량의 운행을 판단하고 제어하는 전자 장치, 그리고 이를 운영하는 소프트웨어이다. 따라서 자율주행 수준의 성숙도가 높아질수록, 운행 제어 장치와 이를 운영하는 소프트웨어에 대한 중요도가 높아지고, 이들에 대한 기능 안전 요건도 매우 높은 수준으로 요구된다. 이러한 추세에 따라 주요 선진국에서는 자율주행차 도입을 위한 다양한 노력을 하고 있는데, 특히 미국에서는 2016년 기준 캘리포니아(California), 플로리다(Florida), 미시건(Michigan) 등의 주에서 자율주행차 관련 법률을 제정하였고, 연방정부의 교통부 산하 도로교통안전국에서는 국가 차원의 자율주행차 정책 가이드라인(Federal Automated Vehicles Policy)을 2016년 9월 발표하였다. 앞서 밝혔듯이, 자율주행차는 다양한 종류의 전자식 장치가 주를 이루고 있어 기존 자동차 기능안전표준(ISO 26262) 외 다양한 기능 안전 표준(우주항공기능안전표준, 국방기능안전 표준 등)이 추가적으로 필요하게 되었다. 이러한 추세에 발맞추어 미국 도로교통안전국에서는 자동차 전자장치 신뢰성 연구 프로그램(Automotive Electronics Reliability Research Program)을 수행하고 있으며, 연구 중의 하나로 자동차 전자제어 시스템 관련 안전 표준 비교 분석 (Assessment of Safety Standards for Automotive Electronic Control Systems) 자료를 발간하였다. 본 연구에서는 미국 도로교통안전국에서 발행한 자율주행차 정책 가이드라인과 자동차 전자제어 시스템 관련 안전 표준을 조사하고 비교 분석하였다.

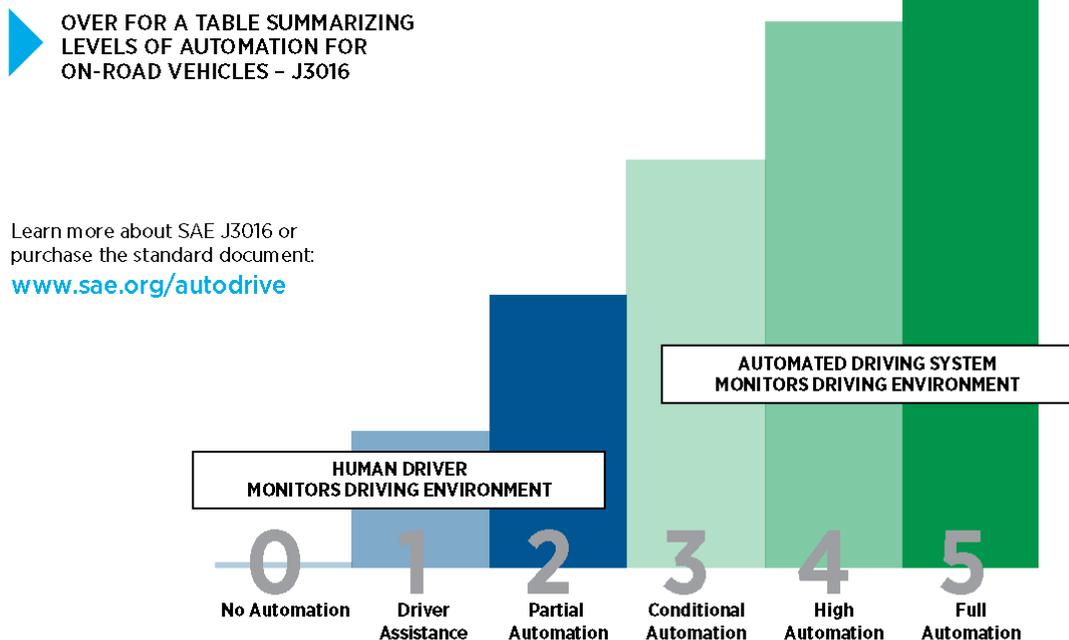
1) 미 연방 자율주행차 정책 (Federal Automated Vehicles Policy)

미국 도로교통안전국(NHTSA)의 자율주행차 관련 정책 가이드라인은 1. 자율주행차의 안전 운영을 조장하고, 2. 자동차 제조사 및 설계자들이 자율주행 차량 개발을 위해 다양한 기술적 시도를 할 수 있게 하면서도 적절한 안전 조치를 포함하도록 차량 설계 가이드라인을 제시함으로써, 자동차 제조사가 규제 당국과 협업을 통해 자율주행차량 제조 및 판매에 필요한 안전 요구 사항을 충족시키는 적절한 기대 수준을 제공하기 위해 2016년 9월 작성되었다. 이 가이드라인은 서두에 자율주행에 대한 설명 및 자율주행 등급에 대해서 간략히 설명하였다.

미국 자동차기술학회(SAE, Society of Automotive Engineers)에서 정의한 자율주행 수준 등급(SAE J3016)은 0단계에서 5단계까지 총 6단계가 있으며, 이 중 자율주행시스템(HAV System)이라고 함은 자율주행 수준 등급 3단계 이상을 뜻하는데 이는 운전자 또는 자동화된 운전 시스템이 운전 환경에 대해 주시(Monitoring) 가능한지에 따라 구분된다.

[그림 2-1] 자율등급에 따른 자율주행차 구분 기준

dynamic driving task while a driving automation system is engaged.



자료: Automated Driving Levels of Driving Automation are defined in new SAE international standard J3016

자율주행 등급을 간단히 살펴보면, SAE Level 0은 운전자가 모든 작업을 하는 것이며, SAE Level 1은 자동차의 자동화 시스템이 때때로 운전자를 대신해서 운전 기능을 자동화하는 것이며, SAE Level 2는 자동차의 자동화 시스템이 실제로 운전 기능 일부를 대신하여 실행하지만 운전자는 운전 환경 주시 및 나머지 모든 운전 기능을 직접 수행하는 것이며, SAE Level 3은 자동차의 자동화 시스템이 실제 일부 운전 기능을 수행하고 운전 환경을 때때로 주시하지만, 운전자는 필히 자동화 시스템 요청 시 자동차를 제어할 준비를 하고 있어야 하며, SAE Level 4는 자동차의 자동화 시스템이 운전 기능 수행 및 운전 환경을 주시하며, 운전자는 자동화 시스템의 요청 시 자동차를 제어할 준비를 하지 않아도 되나, 자동화 시스템은 특정 환경 및 조건하에서만 자동차 운영이 가능하며, SAE Level 5는 자동차의 자동화 시스템이 모든 조건하에서 운전에 대한 모든 기능을 수행하는 것으로 정의되어 있다.

[그림 2-2] 자율주행 등급과 자율주행 주요 기능

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/Deceleration	Monitoring of Driving Environment	Fallback Performance of Dynamic Driving Task	System Capability (Driving Modes)
Human driver monitors the driving environment						
0	No Automation	the full-time performance by the <i>human driver</i> of all aspects of the <i>dynamic driving task</i> , even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the <i>driving mode</i> -specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the <i>driving mode</i> -specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	System	Human driver	Human driver	Some driving modes
Automated driving system ("system") monitors the driving environment						
3	Conditional Automation	the <i>driving mode</i> -specific performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> with the expectation that the <i>human driver</i> will respond appropriately to a <i>request to intervene</i>	System	System	Human driver	Some driving modes
4	High Automation	the <i>driving mode</i> -specific performance by an automated driving system of all aspects of the <i>dynamic driving task</i> , even if a <i>human driver</i> does not respond appropriately to a <i>request to intervene</i>	System	System	System	Some driving modes
5	Full Automation	the full-time performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> under all roadway and environmental conditions that can be managed by a <i>human driver</i>	System	System	System	All driving modes

자료: Automated Driving Levels of Driving Automation are defined in new SAE international standard J3016

자율주행차 정책 가이드라인은 자율주행차 성능가이드라인, 주(State) 정책 모델, 현대도로교통안전국의 규제 수단, 최신 규제 수단 및 규제 당국의 총 4개의 섹션으로 구성되어 있으며, 주요 내용은 아래와 같다.

〈표 2-1〉 가이드라인 섹션 및 주요 내용

섹션	주요 내용
자율주행차 성능 가이드라인 (Vehicle Performance Guidance for Automated Vehicles)	<ul style="list-style-type: none"> • 자율주행차 판매 전, 안전한 차량개발을 위한 디자인, 개발, 테스트 모범사례 및 가이드 제시
주 (State) 정책 모델 (Model State Policy)	<ul style="list-style-type: none"> • 주(State) 별 일관된 자율주행차 관련 법, 규정 제정을 위한 국가적인 프레임워크(Framework) 제공
현 도로교통안전국의 규제 수단 (NHTSA's Current Regulatory Tools)	<ul style="list-style-type: none"> • 현 도로교통안전국이 보유한 자동차 관련 규제 수단과 이를 토대로 한 자율주행차 관련 정보, 실행 지침 및 지원 내용을 포함한 가이드 문서 제공 • 자율주행차 관련 해석 및 면제 요청에 대한 판단 간소화
최신 규제 수단 및 규제 당국 (New Tools and Authorities)	<ul style="list-style-type: none"> • 안전하고 효율적인 자율주행차 개발을 위한 새로운 규제 수단 및 규제 주체 검토

상기 내용을 간략히 살펴보자면, ‘자율주행차 성능 가이드 라인’은 자율주행차 테스트 및 운행³⁾을 위해 자동차 제조업체, 부품업체, 기타 업체들이 단기간 내 준수해야 할 합리적인 사례 및 절차 제시를 통해 자동차 산업계에 대한 미 교통부의 기대치 설정한 것으로 안전 분석 항목을 제시하였다. ‘주 정책 모델’은 각 주별 차량 허가 및 등록, 교통 법규 및 집행, 보험 및 책임 제도에 대한 기존 권한 유지됨을 확인하고, 국가 차원의 일관성 있는 관련 법 규정 프레임워크를 유지하는 것을 목표로 하였다. ‘현 도로교통안전국의 규제 수단’에서는 도로교통안전국은 기존의 규제 수단인 해석, 면제, 입안통보절차(notice and comment rulemaking), 결함 및 집행을 통해 자율주행 차량에 대한 규제를 수행하고 있고, 연방 자동차 안전 표준(FMVSS, Federal Motor Vehicle Safety Standard)이 없는 차량 및 차량 장치에 대해서도 안전에 문제가 있을 경우 기관이 리콜 할 수 있도록 안전 결함에 대한 식별 권한을 보유하고 있다고 밝혔다. 이러한 규제에 대한 이해를 돕기 위해 새로운 정보와 가이드 문서를 제공하는데, 가이드 문서에는 이러한 규제를 이해하고 활용하려는 업체에게 유용한 설명, 실행 지침 및 지원 내용을 포함하고 있다. 또한, 도로교통안전국은 심사 과정을 간소화하여 60일 내에 단순 자율주행차 관련 해석을 발표하고, 6개월 내에 단순 자율주행차 관련

3) 여기서 운행은 차량제조 및 개발 관련자가 아닌 일반 대중이 자율주행차량을 운행함을 말한다.

면제 요청에 대한 가부를 판단한다고 밝혔다. ‘최신 규제 수단 및 규제 당국’에서는 오래전 규제가 신속히 변화하는 기술의 속도를 따라가지 못하므로, 규제 기관을 보다 민첩하고 유연하게 하여, 신기술의 안전하고 신속한 적용을 위해 도움이 가능하도록 새로운 규제 수단, 규제 당국, 규제 구조에 대한 가이드를 제시하였다.

이 중, ‘자율주행차 성능 가이드라인’에서 제시한 시스템 및 소프트웨어 안전 가이드라인에 대한 상세 내용을 아래와 같다.

- 자율주행차 성능 가이드라인

상기에 제시된 4가지 섹션 중, 자율주행차의 기능 및 소프트웨어 안전에 대한 가이드라인은 ‘자율주행차 성능 가이드라인’의 차량 성능 가이드라인 프레임워크에 포함되어 있다. 차량 성능 가이드라인 프레임워크는 ‘범위 및 프로세스 가이드(Scope & Process Guidance)’, ‘차량의 모든 자율주행 시스템에 적용 가능한 가이드(Guidance Applicable to All HAV Systems on the Vehicle)’, ‘각 자율주행 시스템에 대한 개별 가이드(Guidance Specific to Each HAV System)’의 3대 가이드로 구성되어 있다. 이 프레임워크는 테스트 및 생산중인 자동차와 기존 자동 장치(Original) 및 교체 자동 장치(Replacement), 업데이트(Update)⁴⁾에 적용되는데, 자동차 제조사 및 기타 업체는 우선 기존 FMVSS에서 제시된 모든 요구 사항을 확인해야 한다.⁵⁾

‘차량의 모든 자율주행 시스템에 적용 가능한 가이드’에 포함된 ‘시스템 안전’ 항목은 전자/전기, 기계의 오작동, 소프트웨어 오류를 방지하여 안전한⁶⁾ 자율 주행 시스템을 설계하기 위한 설계 및 확인 프로세스 준수를 강조 한다. 이 프로세스는 자동차 기능 안전 프로세스 표준⁷⁾ 및 차량 디자인 관련 모든 영역을 포함해야 하며, 위험 분석(Hazard Analysis) 및 안전위험평가(Safety Risk Assessment)를 포함해야 한다. 자동차 제조사 및 기타 업체는 가이드, 모범 사례, 설계 원칙 및 차량 기능 안전 표준과 필요할 경우 우주항공표준(DO-178C), 국방표준(MIL-STD-882E) 및 기타 관련 표준을 모두 준수해야 한다.⁸⁾ 또한, 이 프로세스에서 소프트웨어 개발, 검증, 확인 절차를 중요시 하도록 요구하는데, 이러한 소프트웨어 개발 프로세스는 예기치 못한 소프트웨어 오류를 발견하고 수정하기 위해 잘 계획되고, 관리되고, 문서로 기록되어야 한다. 그리

4) 소프트웨어 업데이트 및 업그레이드 포함

5) 필요에 따라 미 도로교통안전국에게 해석/면제 요청

6) Free of unreasonable safety risks

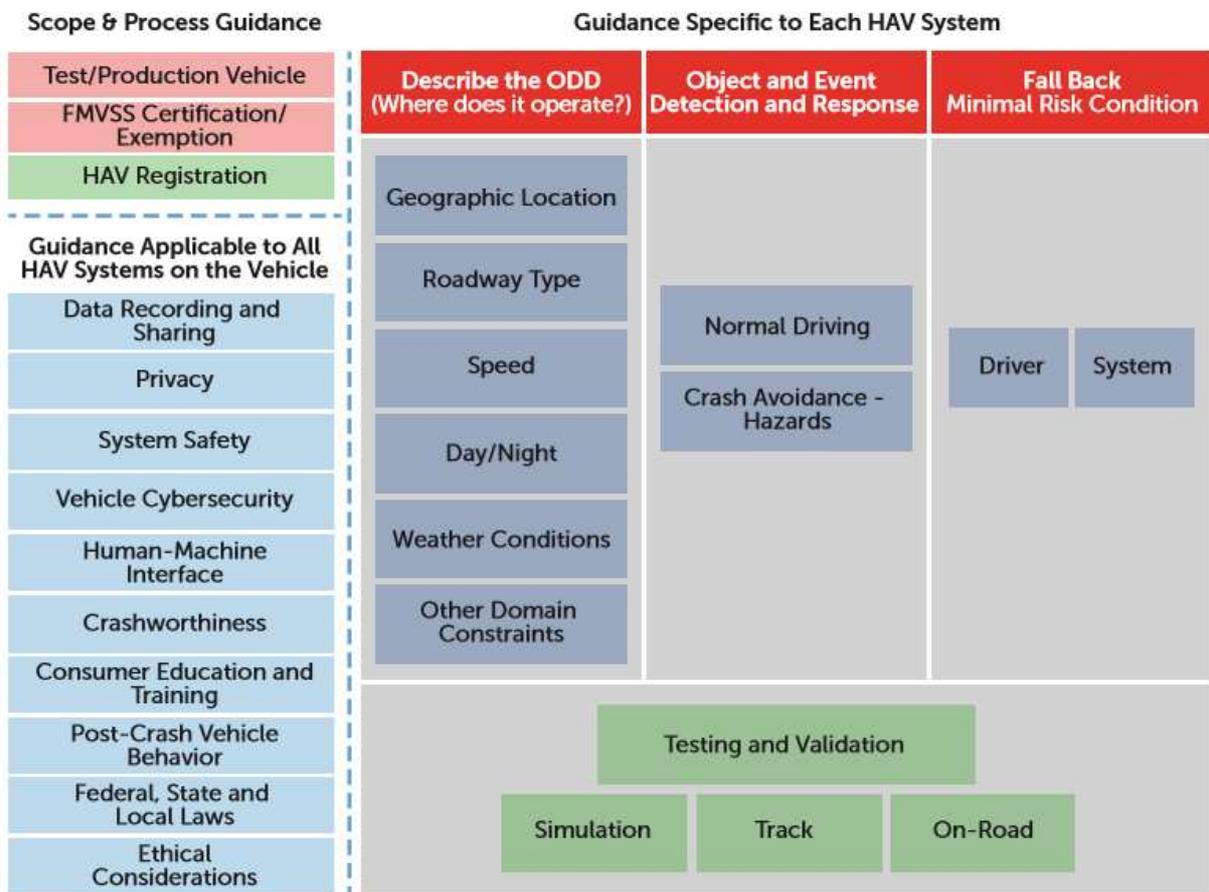
7) ISO 26262

8) 미 도로교통안전국에서 2016년 6월 발행한 ‘차량전자제어시스템 안전표준 분석(Assessment of Safety Standards for Automotive Electronics Control Systems)’에서 적용 가능한 다양한 안전 표준에 대해 분석하였다.

고 자동차 제조 관련 업체들은 인공지능(AI, Artificial Intelligent), 머신 러닝(Machine Learning) 및 기타 관련 소프트웨어 기술과 알고리즘의 발전, 적용, 안전 분석(Safety Assessment)을 지속적으로 모니터링 해야 한다.

모든 설계는 개별 하위 시스템(Individual Subsystems) 및 자동차 전체 아키텍처의 일부로 테스트, 검증, 확인된 후 결정되어야 하며, 이러한 모든 변화, 설계 결정, 분석, 테스트 및 관련 데이터는 확인 가능하도록 모두 기록되어야 한다.

[그림 2-3] 차량 성능 가이드 프레임워크



자료: Federal Automated Vehicles Policy, NHTSA, U.S. Department of Transportation

2) 차량전자제어시스템 안전표준 분석 (Assessment of Safety Standards for Automotive Electronics Control Systems)

안전 필수 자동차용 전자 제어 시스템이 지속적으로 확대 적용됨에 따라, 이들 장비의 안전 및 신뢰성을 담보할 수 있는 방법을 찾기 위한 일환으로 미 도로교통안전국

(NHTSA)은 ‘전자 신뢰성 연구 프로그램(Electronics Reliability Research Program)’ 을 수행하고 있다. 이 프로그램은 자동차 산업계 내/외부를 포괄하여 자동차 설계에 전자 장치 및 제어 시스템 적용이 증가됨에 따라 발생하는 새로운 위험을 분석, 식별, 방지 하는 표준 및 방법을 포함하고 있다. 이 프로그램의 일환으로 수행된 ‘차량전자제어 시스템 안전 표준 분석’ 연구는 자동차 전자 제어 시스템의 전자 신뢰성 관련 업계 및 정부의 6가지 주요 안전 표준을 평가 비교 분석하여, 각 표준별 강점, 한계 및 향상의 기회를 조사하여 향후 높은 기능 안전을 보장하는 자동차 전자 제어 시스템 개발 지원을 목표로 하고 있다.

이 연구는 6개의 자동차 안전 관련 주요 표준을 대상으로 하여,

- ISO 26262 : 자동차의 기능 안전
- MIL-STD-882E: 미 국방부(DOD) 표준관행 - 기능 안전
- DO-178C: 항공 시스템 및 장비 인증 관련 소프트웨어 고려 사항
- FMVSS(Federal Motor Vehicle Safety Standard): 연방 자동차 안전 표준
- AUTOSAR(Automotive Open System Architecture): 개방형 자동차 표준 소프트웨어 아키텍처
- MISRA C: 안전 필수 시스템에 활용되는 C 언어 사용에 대한 가이드라인

이들 표준을 11개의 항목으로 분석하였다.

1. 표준 유형(Type of Standard)
2. 안전 및 위험에 대한 정의(Definition of Safety and Hazard)
3. 안전 요구 사항 식별(Identification of Safety Requirements)
4. 위험요소 및 안전 분석 방법(Hazard and Safety Analysis Methods)
5. 안전 요구 사항 관리(Management of Safety Requirements)
6. 위험 평가 접근방법(Risk Assessment Approach)
7. 안전 접근을 위한 설계(Design for Safety Approach)
8. 소프트웨어 안전(Software Safety)
9. 시스템 수명주기 고려사항(System Lifecycle Consideration)

10. 인적 요소 고려사항(Human Factors Consideration)
11. 검토, 감사, 인증 관련 접근 방법(Approach to Review, Audit, and Certification)

이 연구에서 발견한 10가지 주요 내용은 다음과 같다.

1. 시스템 엔지니어링 접근법을 따르는 프로세스 안전 표준 또는 가이드라인은 FMVSS의 가이드라인과는 다르며 기존의 안전 보증에 대한 표준 보완
2. 자동차 안전 맥락에서 “부당한 위험“에 대한 명확한 정의를 제공함으로써 기존 프로세스 표준 향상
3. 위험에 대한 정의는 안전 표준에 따라 다름
4. 심각도만으로 DO-178C의 접근법과 유사하게 소프트웨어 위험 척도로 사용 가능. 또한, 통계적으로 유효한 실패 확률 또는 사고 발생 확률이 없을 경우, 심각도가 유일한 척도로 사용 가능
5. ISO 26262 표준에 정의된 업계에서 사용하는 노출 및 제어 가능성 평가는 특정 실험 설계를 통한 추가 데이터 수집으로 향상 가능
6. 소프트웨어 설계에 대한 기존 프로세스 표준은 전반적인 제어 시스템 및 소프트웨어 안전 인증의 전반적인 안전성, 그리고 설계 솔루션의 특정 측면(우수한 아키텍처 및 코딩 표준)을 고려하여 향상 가능
7. MIL-STD-882E의 안전 설계 접근법은 일반 시스템 요구 사항, 보다 단순한 위험 분석, 보다 강조된 인적 요인으로부터의 위험추적 및 안전요구를 개별 관리할 수 있는 프레임워크제공
8. 운전자와 서비스 기술자에 대한 건강 위험 분석 부분을 프로세스 표준에 포함하는 것이 적절한 지는 차후 평가
9. 테스트, 제조, 작동, 유지 보수 등에 대한 기존 프로세스 표준이 차량 수명주기 전반에 미치는 환경적 영향은 언급하지 않음
10. 인적 요인 연구는 포괄적 기능 안전 접근법에 통합이 용이함

주요 내용 및 소프트웨어 안전 관련된 항목을 상세히 조사하였는데, 조사한 항목은 안전 및 위험의 정의, 위험도 평가, 소프트웨어 위험도 평가, 소프트웨어 안전이다.

- 안전 및 위험 정의

MIL-STD-882E와 DO-178C의 안전 정의는 사람과 사회에 미치는 영향에 직접 초점을 두고 ISO 26262와 AUTOSAR은 ‘불합리한 위험’ 이 없으므로 정의하고 있으나, ‘불합리한 위험’ 에 대한 상세 정의는 제공하고 있지 않다.

MIL-STD-882E는 위험을 안전한 상황을 상실할 수 있는 시스템 상태라고 정의하였는데, 이는 자동차 전자 제어 시스템의 부품 오작동 및 안전하지 않은 시스템 상호 작용을 모두 포함하고 있다. ISO 26262는 위험의 정의를 제조자의 설계 의도를 충족시키지 못한 제품의 오동작으로 인한 영향으로 제한하며, 이는 MIL-STD-882E의 정의와 맥락이 같다. 하지만, MIL-STD-882E의 위험 정의는 자동차 운전자의 안전 요구 및 대중의 안전 관심을 충분히 반영해야 한다는 관점에서 보면 보다 포괄적이다.

<표 2-2> 주요 표준별 안전 및 위험에 대한 정의

표준	안전	위험
ISO 26262	<ul style="list-style-type: none"> 불합리한 위험의 부재 	<ul style="list-style-type: none"> 주요 항목의 비정상적인 작동으로 기인한 잠재적 피해 비정상적인 작동 : 작동 불량 및 설계 의도와 다른 작동
MIL-STD-882E	<ul style="list-style-type: none"> 사망, 상해, 직업병, 장비 또는 재산의 손상/손실/환경파괴를 초래할 수 있는 조건으로 부터의 자유 	<ul style="list-style-type: none"> 사망, 부상, 직업병, 장비 또는 재산의 파손 또는 손실, 환경 손상을 초래하는 계획되지 않은 사건 또는 일련의 사건(사고)을 초래할 수 있는 실제 또는 잠재적 상태
DO-178C	<ul style="list-style-type: none"> 명확한 정의 없음 고장 조건에 따르면 MIL-STD-882E와 유사 	<ul style="list-style-type: none"> 명확한 정의 없음
FMVSS	<ul style="list-style-type: none"> 규칙 제정 과정(자동차 안전 필요성에 대한 법적 정의에 따른)은 발생 가능한 잠재적 위험과 안전에 대한 영향 고려 표준 수립 후, 잠재적 위해 요소 및 안전에 대한 영향 분석보다 수립된 성능 요구 사항을 충족하는 기준 준수 	
AUTOSAR	<ul style="list-style-type: none"> ISO 26262와 동일 	<ul style="list-style-type: none"> ISO 26262와 동일
MISRA C	<ul style="list-style-type: none"> 명확한 정의 없음 	<ul style="list-style-type: none"> 명확한 정의 없음

자료: Assessment of Safety, Standards for Automotive Electronic Control Systems, 2016년 6월

• 위험도 평가

ISO 26262는 자동차 안전 무결성 수준(ASIL⁹⁾)을 사용하여 위험을 평가하는데, 심각

도(S, 안전 목표 미충족시 발생하는 사고의 심각도), 사고 확률(E, 위험 운영 상황에 노출되는 확률), 통제성¹⁰⁾(C, 위험 상황에 대한 통제 가능성)의 3가지 범주를 조합하여 평가한다. MIL-STD-882E는 하드웨어 시스템의 경우 사고의 심각성과 위험 발생 가능성을 결합하여 위험 지수를 도출하며, 소프트웨어의 경우 심각도 및 소프트웨어 통제 범주(Software Control Category)를 사용하여 위험 지수를 도출한다. 소프트웨어 통제 범주란 자율성, 명령 및 제어 권한, 소프트웨어 기능의 다중 내고장성에 대한 수준을 시스템의 동작과 관련지어 지정하는 것을 의미한다. DO-178은 전반적인 시스템 안전성에 대한 소프트웨어 오작동으로 인한 심각도(Severity)만으로 소프트웨어 레벨을 지정한다.

DO-178C는 위험 심각도(Hazard Severity)를 하드웨어 및 소프트웨어 시스템 위험 평가에 필요한 항목으로 정의하고 있다. 위험 심각도는 사고로 인한 상해 및 손실을 통해 상대적으로 쉽게 정의가 가능하다.

<표 2-3> 위험 평가 접근 방법 비교

구분	ISO 26262 Hardware and Software	MIL-STD-882E for Hardware	MIL-STD-882E for Software	DO-178C (Software only)
심각도 ¹¹⁾	√	√	√	√
운영 시나리오 확률 ¹²⁾	√			
비정상적인 동작발생 확률 ¹³⁾		√		
통제성 ¹⁴⁾	√			
소프트웨어 통제성 항목 ¹⁵⁾			√	

자료: Assessment of Safety Standards for Automotive Electronic Control Systems, 2016년 6월

9) Automotive Safety Integrity Level

10) Controllability

11) Severity

12) Probability of operational scenario(Exposure)

13) Probability of mishap occurrence

14) Controllability

15) Software Control Category

- 소프트웨어 위험도 평가

ISO 26262는 자동차 안전 무결성 수준(ASIL) 분해 프로세스를 통해 자동차 안전 무결성 수준(ASIL)을 소프트웨어 요구 사항에 지정하는데, 소프트웨어 요구 사항은 관련된 안전 목표 보다 낮거나 동일한 수준의 ASIL 등급으로 지정될 수 있다.

MIL-STD-882의 경우, 소프트웨어 오작동 확률은 산출하기 어렵고 과거 발생 이력에 무관하기 때문에 소프트웨어 오작동 확률을 사용하지 않는 대신 ‘소프트웨어 관련 위험 심각도(Severity)’와 ‘소프트웨어 통제 범주(Software Control Category)’를 사용한다. 주의해야 할 점은, 소프트웨어 통제 범주의 경우, 반자동 시스템의 위험도가 전자동 시스템의 위험도에 비해 항상 낮다고 할 수 없다는 것이다.¹⁶⁾ 소프트웨어의 경우 가장 보수적인 위험도 평가 접근법은 심각도 평가만을 사용하는 것일 수 있다.

DO-178C에서는 소프트웨어 오작동 확률 산정 방법은 임의의 하드웨어 오작동 확률(Random Hardware Failures) 산정 방법과 다르다고 강조한다. DO-178에서의 위험 평가는 영향의 심각도(Severity of Impact)만을 고려한다. 또한, 소프트웨어 신뢰성 모델 및 계산은 임의 오작동 확률(Random Failures)에 근거하고 있어, 표준으로 인정되지 않는다. DO-178C는 심각도(Severity)만을 사용한 가장 보수적인 소프트웨어 위험 평가 접근법을 제공하고 있다.

- 소프트웨어 안전

ISO 26262, MIL-STD-882E, DO-178C는 시스템 엔지니어링 프로세스를 따름으로써 소프트웨어 안전을 보장한다. AUTOSAR 및 MISRA C는 소프트웨어 안전을 달성하기 위한 방안으로 좋은 아키텍처¹⁷⁾(Good Architecture)와 좋은 코딩 표준¹⁸⁾(Good Coding Standard)을 요구하고 있다.

시스템 엔지니어링 프로세스 외에도 ISO 26262는 아키텍처 설계, 유닛 설계 및 테스트 단계에서 우수한 소프트웨어 설계 방법을 제시¹⁹⁾하지만, 아키텍처 속성이 만족스러운 수준으로 달성되었는지를 측정하는 방법에 대한 가이드는 제공하지 않는다.

16) 항공기의 반자동 운행이 오히려 위험을 초래한 경우가 있다.

17) AUTOSAR

18) MISRA C

19) 예를 들면, 아키텍처 설계 고려 사항에는 검증 가능성, 테스트 가능성, 모듈성, 최소 복잡성 등이 포함되어 있다.

좋은 소프트웨어 설계 방법²⁰⁾을 따르면 안전상의 이점이 있는데, 이때 고려해야 할 영역은 포괄적인 안전 관련 소프트웨어 요구 사항 목록을 작성하는 것이다. 코딩 표준, 아키텍처 고려 사항, 테스트 방법과 같은 소프트웨어 설계 방식은 설계 요구 사항을 만족하기 위한 수단이다. 소프트웨어 시스템은 소프트웨어 개발을 최대한 모듈화하고, 테스트 가능하며, 유지보수가 쉽고, MISRA C와 같은 코딩 표준을 준수한다고 하더라도 설계 요구 사항보다 더 좋게 만들 수는 없다. 최종적인 제품에 대한 시스템 엔지니어링 프로세스 효과는 결국 요구사항 정의²¹⁾에 주로 영향을 받는다.

ISO 26262 및 DO-178C는 모두 소프트웨어 오작동²²⁾ 해결에 중점을 두고 있다. ISO 26262는 결함을 ‘부분 또는 항목이 오작동을 일으킬 수 있는 비정상적인 상태²³⁾’로 정의하고 있으며, 오작동은 ‘항목이 의도된 기능을 수행하지 못하는 것²⁴⁾’으로 정의하고 있다. DO-178C는 모든 위험은 소프트웨어의 비정상적인 동작으로 발생한다고 가정하고 있는데, 여기서 비정상적인 동작이란 ‘특정 요구 사항과 일치되지 않는 동작²⁵⁾’로 정의되어 있다. 따라서 ISO 26262의 소프트웨어 결함(Software Fault)과 DO-178C의 소프트웨어 이상(Software Abnormalities)은 모두 소프트웨어 오작동에 따른 결과(Consequential Software Failures)에 주안점을 두고 있다.

소프트웨어 오작동은 소프트웨어 관련 안전 문제의 원인 중 일부일 뿐이며, 실제 소프트웨어 관련 사고는 소프트웨어 코딩 및 기타 구현에 대한 오류가 아닌 요구 사항의 결함²⁶⁾(즉, 불완전하거나 불충분한 요구 사항)에 기인한 것이 대부분이다. 요구 사항이 정확하게 식별되지 않거나 누락된 경우 발생하는 소프트웨어의 안전하지 않는 동작은 소프트웨어 오작동 및 신뢰성에 대한 접근 방법으로 해결할 수 없다. 소프트웨어 요구 사항을 포괄적으로 최대한 식별하기 위해서는 추가적인 노력이 요구된다. ISO 26262 및 DO-178C는 안전 요구 사항과 제안된 엔지니어링 프로세스 간의 연계를 명확히 함으로써 더욱 강화될 수 있다.

2. 국방 부문

20) Good software design practices

21) Definition of requirements

22) Software Failures

23) Abnormal condition that can cause an element or an item to fail

24) Termination of the ability of an element to perform a function as required

25) Behavior that is inconsistent with specified requirements

26) Incomplete or insufficient requirements

미 국방 안전 관련 표준 및 가이드는 미국 뿐 아니라 타 국가의 국방 표준에 참조되거나 인용되고 있다. 특히, 인명과 재산에 장비에 전자 장치가 광범위하게 사용되고 통합·복잡화됨에 따라 기존 관련 산업 도메인의 안전 표준뿐만 아니라 높은 수준의 안전 등급이 요구 되는 장치 및 부품에 대해 안전 등급 수준이 높은 항공 및 국방 표준 적용을 추가적으로 요구하고 있다.

본 연구는 미 국방부에서 발행한 시스템 안전 표준인 MIL-STD-882E와 소프트웨어 안전 가이드인 Joint Software Systems Safety Engineering Handbook의 소프트웨어 안전 부분 주요 내용을 조사하였다.

1) 미 국방부 시스템 안전 표준 (MIL-STD-882E)

이 표준은 미 국방부에서 제정한 시스템엔지니어링²⁷⁾ 안전 표준으로 위험에 대한 식별, 분류, 회피에 대한 표준 및 일반적 방안을 제시하였는데, 최근 2012년 개정된 MIL-STD-882E 에서는 소프트웨어 시스템 안전 기법 및 실무 등이 추가되어 소프트웨어 안전 영역이 강화되었다. 이 표준은 일반적인 경우 섹션 3²⁸⁾과 섹션 4²⁹⁾의 내용을 최소한의 강제 항목으로 요구하고 있는데, 섹션 3은 주요 용어에 대한 정의이며, 섹션 4는 일반 요구사항으로 시스템 안전 요구사항, 안전 프로세스, 위험 식별/평가/완화/축소/확인/검증/수용 및 각 단계별 문서화, 수명 주기 위험 관리, 소프트웨어 안전 관련 사항들을 기술하고 있다.

• 시스템 안전(System Safety) 주요 내용

시스템 안전 프로세스는 시스템 안전 접근법 문서화(1 단계), 위험요소³⁰⁾ 식별 및 문서화(2 단계), 위험³¹⁾ 평가 및 문서화(3 단계), 위험 완화 조치 식별 및 문서화(4 단계), 위험 경감(5 단계), 위험 경감 확인/검증 및 문서화(6 단계), 위험 수용 및 문서화 (7 단계), 수용 주기 위험 관리(8 단계)의 총 8단계로 구성되어 있으며 필요에 따라 단계가 반복될 수 있다.

27) SE, Systems Engineering

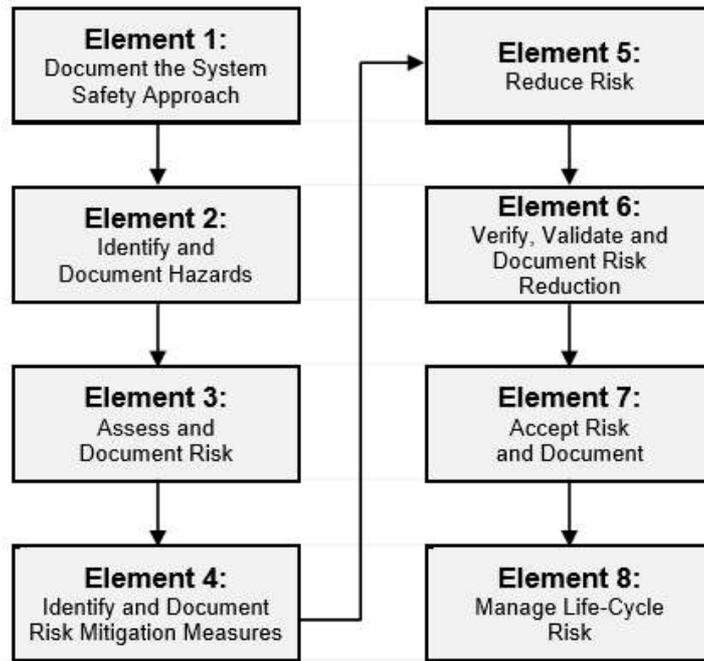
28) 3. Definitions

29) 4. General Requirements

30) Hazard

31) Risk

[그림 2-4] 시스템 안전 프로세스 8개 단계



자료: MIL-STD-882E Standard Practice System Safety, U.S. Department of Defense, 2012

1 단계(시스템 안전 접근법 문서화)에서는 프로젝트 관리자와 계약자는 필수적으로 위험요소 관리를 위한 시스템 안전 접근법을 문서화해야 한다. 2 단계(위험요소 식별 및 문서화)에서는 체계적 분석 프로세스를 통해 위험 식별 시, 시스템 하드웨어와 소프트웨어, 시스템 인터페이스³²⁾ 및 사용 목적, 운영 환경을 고려해야 한다. 이때, 사고 데이터, 관련 환경 건강 데이터와 직업 건강 데이터, 사용자의 물리적 특성, 사용자 지식, 기술, 능력 및 기존³³⁾ 시스템과 유사한 시스템을 통해 습득한 교훈을 함께 고려해야 한다. 위험요소 식별 프로세스는 시스템의 전체 수명 주기뿐만 아니라 인력, 인프라, 방위 시스템, 대중 및 환경에 미치는 잠재적 영향도 고려해야 한다. 3 단계(위험 평가 및 문서화)에서는 모든 시스템 모드 별 위험에 대한 잠재적 사고 확률과 심각도 범주를 측정한다. 주어진 위험 요소에 대해 적절한 심각도 범주를 결정(〈표 2-4〉 참조)하려면 사망 또는 상해, 환경 영향 또는 금전적 손실 가능성을 식별해야 한다. 4 단계(위험 완화 조치 식별 및 문서화)에서는 가능한 경우 위험 요소를 제거하는 것을 목표로 하고 있으나, 위험 요소를 제거 할 수 없는 경우 우선순위의 시스템 안전 설계 순서를 적용하여 위험을 비용, 일정 및 성능의 제약 내에서 가장 낮은 허용 수준으로 낮추어야 한다. 5 단계(위험 경감)에서는 수용 가능한 위험 수준을 달성하기 위한 완화 조치

32) 인간 인터페이스(Human Interface) 포함

33) Legacy

를 선택하고 실행한다. 6 단계(위험 경감 확인/검증 및 문서화)에서는 적절한 분석, 테스트, 데모 또는 검사를 통해 구현을 확인하고 선택한 모든 위험 완화 조치의 유효성을 검증한다. 7 단계(위험 수용 및 문서화)에서는 시스템 관련 위험을 사람, 장비 또는 환경에 노출시키기 전, DoD 5000.02에 정의된 해당 기관에 의해 승인을 받아야 한다. 공식적인 위험 수용 결정 관련된 시스템 구성 및 관련 문서는 시스템 수명 기간 동안 정부에 제공되어야 한다. 8단계(수용 주기 위험 관리)에서는 시스템 도입 후, 시스템 프로그램 부서는 시스템 안전 프로세스를 사용하여 위험을 식별하고 시스템 운영 기간 동안 위험관리시스템(HTS)³⁴⁾을 통해 유지 관리해야 한다. 유지 관리 업무는 사용자, 하드웨어 및 소프트웨어, 사고 데이터, 시스템 상태 데이터 등을 포함하는 모든 변경 사항을 관리해야 한다.

<표 2-4> 심각도 등급

심각도 등급	설명	사고결과 수준
1	재앙적수준 ³⁵⁾	다음 중 하나 이상을 유발 가능: 사망, 영구적 완전 장애, 회복 불가능 중대한 환경 영향 또는 \$10M 이상의 금전적 손실
2	치명적수준 ³⁶⁾	다음 중 하나 이상을 유발 가능: 영구적 부분 장애, 3명 이상의 입원을 유발할 수 있는 직업병이나 상해, 회복 가능한 중대한 환경 영향 또는 \$1M ~ \$10M의 금전적 손실
3	보통수준 ³⁷⁾	다음 중 하나 이상을 유발 가능: 1일 이상 결근을 유발하는 직업병이나 상해, 회복 가능한 중간정도의 환경 영향 또는 \$100K ~ \$1M의 금전적 손실
4	낮은수준 ³⁸⁾	다음 중 하나 이상을 유발 가능: 결근을 유발하지 않는 직업병이나 상해, 최소한의 환경 영향 또는 \$100K 이하의 금전적 손실

자료: MIL-STD-882E Standard Practice System Safety, U.S. Department of Defense, 2012

• 소프트웨어 안전(System Safety) 주요 내용

34) Hazard Tracking System

35) Catastrophic: 사망, 영구장애, 영구 환경 피해, 100억 이상의 피해

36) Critical

37) Marginal

38) Negligible

소프트웨어 및 소프트웨어에 의해 운영되거나 소프트웨어의 의존도가 높은 시스템에 대한 위험 평가는 위험 심각도와 확률에만 의존해서는 안 된다. 단일 소프트웨어 기능 고장 확률을 추정하는 것은 어려우며 과거 데이터를 기반으로 할 수 없다. 소프트웨어는 일반적으로 응용프로그램에 특화되어 있어 여기에 관련된 신뢰성 요소는 하드웨어와 동일한 방법으로 추정할 수 없다. 따라서 시스템 리스크에 대한 소프트웨어의 기여도 평가는 기존과 다른 접근법을 사용해야 한다.

소프트웨어 통제 등급은 소프트웨어가 안전이 중요한 시스템 및 하부 시스템에서 문제 발생시, 소프트웨어가 어느 정도까지 자율적인 권한을 행사하느냐에 따라 1 ~ 5등급까지 구분된다. (<표 2-5> 참조)

‘소프트웨어 안전 중요도 매트릭스(SSCM)³⁹⁾’는 일반적인 경우, ‘소프트웨어 통제 등급(SCC)⁴⁰⁾’, ‘소프트웨어 심각도 등급⁴¹⁾’를 통해 평가한다. ‘소프트웨어 심각도 지수(SwCI)는 소프트웨어 안전 중요도 매트릭스를 통해 정해지며, 지수에 따라 ‘안전 활동수준(LOR)⁴²⁾이 결정된다.

소프트웨어 심각도 지수 등급이 높을수록 소프트웨어 안전 활동 업무(테스트 → 요구사항/아키텍처 분석 + 테스트 → 요구사항/아키텍처/설계 분석 + 테스트 → 요구사항/아키텍처/설계/코드 분석 + 테스트)가 확대되며, 추가적인 소프트웨어 분석 가이드는 Joint Software Systems Safety Engineering Handbook을 활용하도록 권고한다.

39) Software Safety Criticality Matrix

40) Software Control Category

41) Software Criticality Index

42) Level of Rigor

〈표 2-5〉 소프트웨어 통제 등급

소프트웨어 통제 등급(SCC)		
등급	명칭	설명
1	자율 (AT, Autonomous)	<ul style="list-style-type: none"> 잠재적으로 안전에 중요한 하드웨어 시스템, 하위 시스템 또는 구성 요소의 재난 및 위험 발생을 방지하기 위해 사전 정의된 안전 감지 및 개입 없이 자율적인 통제 권한을 행사하는 소프트웨어 기능⁴³⁾
2	반-자율 (SAT, Semi-Autonomous)	<ul style="list-style-type: none"> 잠재적으로 안전에 중요한 하드웨어 시스템, 하위 시스템 또는 구성 요소의 재난 및 위험 발생을 방지하기 위해 사전 정의된 안전 감지 및 개입을 위한 시간을 확보하기 위한 제어 권한을 행사하는 소프트웨어 기능⁴⁴⁾ 사고 발생 또는 위험을 완화하거나 제어하기 위해 운영자가 조속히 사전 정의된 조치를 취하도록 요구하는 안전 관련 정보를 표시하는 소프트웨어 항목. 소프트웨어 예외, 오류, 결함 또는 지연은 사고 발생 또는 예방을 수행하지 못함
3	중복적인 내결함성 (RFT, Redundant Fault Tolerant))	<ul style="list-style-type: none"> 안전 기능이 중요한 하드웨어 시스템, 하위 시스템 또는 업무 수행을 위해 지시 기능이 필요한 구성요소에 명령을 지시하는 소프트웨어 기능. 시스템 탐지 및 기능적 반응은 기 정의된 각 위험 상태에 대한 중복적이고 독립적인 내결함성 포함 중요한 결정을 내리는 데 필요한 안전에 필수적인 정보를 생성하는 소프트웨어. 이 시스템은 위험한 조건, 탐지 및 디스플레이에 대한 다수의 중복적이고 독립적인 내결함성 메커니즘 포함
4	영향 있음 (Influential)	<ul style="list-style-type: none"> 소프트웨어는 운영자의 결정을 지원하기 위한 안전 관련 정보를 생성하지만, 사고 회피를 위해 운영자의 조치를 요구하지 않음
5	안전 영향 없음 (NSI, No Safety Impact)	<ul style="list-style-type: none"> 소프트웨어 기능이 안전에 중요한 하드웨어 시스템, 하위 시스템 또는 구성 요소에 대해 명령 또는 제어 권한이 없으며 안전에 중요한 정보를 제공하지 않음 소프트웨어는 안전 관련 또는 시간에 민감한 데이터 또는 제어 기기의 상호 작용에 필요한 정보를 제공하지 않음. 소프트웨어는 안전에 중대한 또는 시간에 민감한 데이터를 전송하거나 해결하지 않음

43) 이 정의는 여러 서브 시스템, 상호 연관된 병렬 프로세서, 다중 인터페이스, 시간이 중요한 안전 중요 기능을 포함한 복잡한 시스템/소프트웨어를 포함한다.

소프트웨어 기여도 평가를 위해 <표 2-6>⁴⁵⁾의 안전활동수준(LOR)의 업무 수행이 요구된다. 안전활동수준 업무의 결과는 안전이 중요한 소프트웨어에 대한 신뢰 수준을 제공하고 완화가 필요한 인과 요인 및 위험 요소를 문서화한다. 이러한 모든 활동은 위험 관리 시스템(HTS)에 저장되어야 한다.

<표 2-6> 소프트웨어 안전 중요도 매트릭스

소프트웨어 통제 등급	심각도 등급			
	재앙적	치명적	보통	낮음
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	필요 업무
SwCI 1	요구사항, 아키텍처, 설계, 코드를 분석하고, 심도 있는 SW안전 테스트 수행
SwCI 2	요구사항, 아키텍처, 설계를 분석하고, 심도 있는 SW안전 테스트 수행
SwCI 3	요구사항, 아키텍처를 분석하고, 심도 있는 SW안전 테스트 수행
SwCI 4	SW안전 테스트 수행
SwCI 5	안전성 검증을 통해, 안전과 무관하다고 판단되면, SW안전 관련 분석 및 확인 불필요

필요한 안전활동수준 업무가 수행되지 않는 경우, 불특정 또는 불완전 안전활동수준 업무와 관련된 시스템 위험 기여도는 <표 2-7>⁴⁶⁾에 따라 문서화되어야 한다.

44) 이 정의에는 다소 복잡한 시스템/소프트웨어 기능, 병렬 프로세싱이 아니거나 인터페이스의 제어를 포함하지만, 다른 안전 시스템/메커니즘이 이를 부분적으로 완화 될 수 있다.

45) 자료: MIL-STD-882E Standard Practice System Safety, U.S. Department of Defense, 2012

46) 자료: MIL-STD-882E Standard Practice System Safety, U.S. Department of Defense, 2012

〈표 2-7〉 소프트웨어 심각도 등급, 위험수준, 안전활동수준 업무, 위험과의 관계

소프트웨어 심각도 지수(SwCI)	위험 등급	소프트웨어 안전활동수준(LOR) 업무 ⁴⁷⁾ 및 위험 평가/수용
SwCI 1	매우 높음 (High)	<ul style="list-style-type: none"> SwCI 1 LOR 업무가 지정되지 않았거나 불완전한 경우 시스템 위험에 대한 기여도는 매우 높음(High)으로 문서화하고, PM⁴⁸⁾이 결정. PM은 SwCI 1 LOR 업무를 수행하는 데 필요한 자원을 투입할지 매우 높은(High) 위험을 수용할 지에 대한 결정 후 이를 문서화 함
SwCI 2	심각함 (Serious)	<ul style="list-style-type: none"> SwCI 2 LOR 업무가 지정되지 않았거나 불완전한 경우 시스템 위험에 대한 기여도는 심각함(Serious)로 문서화하고, PM이 결정. PM은 SwCI 2 LOR 업무를 수행하는 데 필요한 자원을 투입할지 심각한(High) 위험을 수용할 지에 대한 결정 후 이를 문서화 함
SwCI 3	보통 (Medium)	<ul style="list-style-type: none"> SwCI 3 LOR 업무가 지정되지 않았거나 불완전한 경우 시스템 위험에 대한 기여도는 보통(Medium)으로 문서화하고, PM이 결정. PM은 SwCI 3 LOR 업무를 수행하는 데 필요한 자원을 투입할지 보통(Medium) 위험을 수용할 지에 대한 결정 후 이를 문서화 함
SwCI 4	낮음 (Low)	<ul style="list-style-type: none"> SwCI 4 LOR 업무가 지정되지 않았거나 불완전한 경우 시스템 위험에 대한 기여도는 낮음(Low)으로 문서화하고, PM이 결정. PM은 SwCI 4 LOR 업무를 수행하는 데 필요한 자원을 투입할지 낮은(Low) 위험을 수용할 지에 대한 결정 후 이를 문서화 함
SwCI 5	안전 관련 없음 (Not Safety)	<ul style="list-style-type: none"> 안전 관련 분석이나 테스트가 불필요

2) 합동 소프트웨어 시스템 안전 공학 안내서 (Joint Software Safety Engineering Handbook)

47) LOR Tasks

48) Program Manager

미 국방성(DOD, Department of Defense)이 주관이 되고, 육군, 해군, 공군, 미 항공우주국(NASA, National Aeronautics and Space Administration), 미 해안경비대, 민간 및 학계가 참여하여 제작한 소프트웨어 시스템 공학 안내서로서 1. 업무 정의서(SOW)를 통해 합리적인 소프트웨어 시스템 안전 업무 범위 설정하고, 2. 구매 라이프사이클 각 단계별로 정의된 소프트웨어 시스템 안전 업무를 엔지니어링 및 관리 프로세스에 통합하고, 3. 계약자의 시스템 안전 준수 여부 모니터링을 위한 데이터 식별하며, 4. 개발 라이프사이클 전반에 걸친 계약자 성과 평가를 수행할 수 있도록 시스템 안전 관리자 및 소프트웨어 개발 관리자에게 정보 및 가이드를 제공하여, 시스템 내에서 소프트웨어가 허용 가능한 안전 위험 수준 이내로 실행될 수 있도록 합리적인 수준의 보장을 달성하기 위한 관리 및 엔지니어링 지침을 제공하는 하는 것을 목적으로 제작되었다.

이 안내서는 소프트웨어 안전 이해에 도움이 되는 소프트웨어 설계와 기능의 일부 기술적인 측면까지도 다루고 있다. 전체적인 구성은 제1장 개요(Overview), 제2장 안내서 소개(Introduction to the Handbook), 제3장 위험 관리 및 시스템 안전(Introduction to Risk Management and System Safety), 제4장 소프트웨어 시스템 안전 엔지니어링(Software System Safety Engineering), 제5장 별첨(Appendices)의 총 5장으로 구성되어 있으며, 제4장 소프트웨어 시스템 안전 엔지니어링 부분이 소프트웨어 안전 주요 내용을 다루고 있다.

[그림 2-5] 안내서 구성



자료: Department of Defense, Joint Software Safety Engineering Handbook, version 1.0 2010.09.

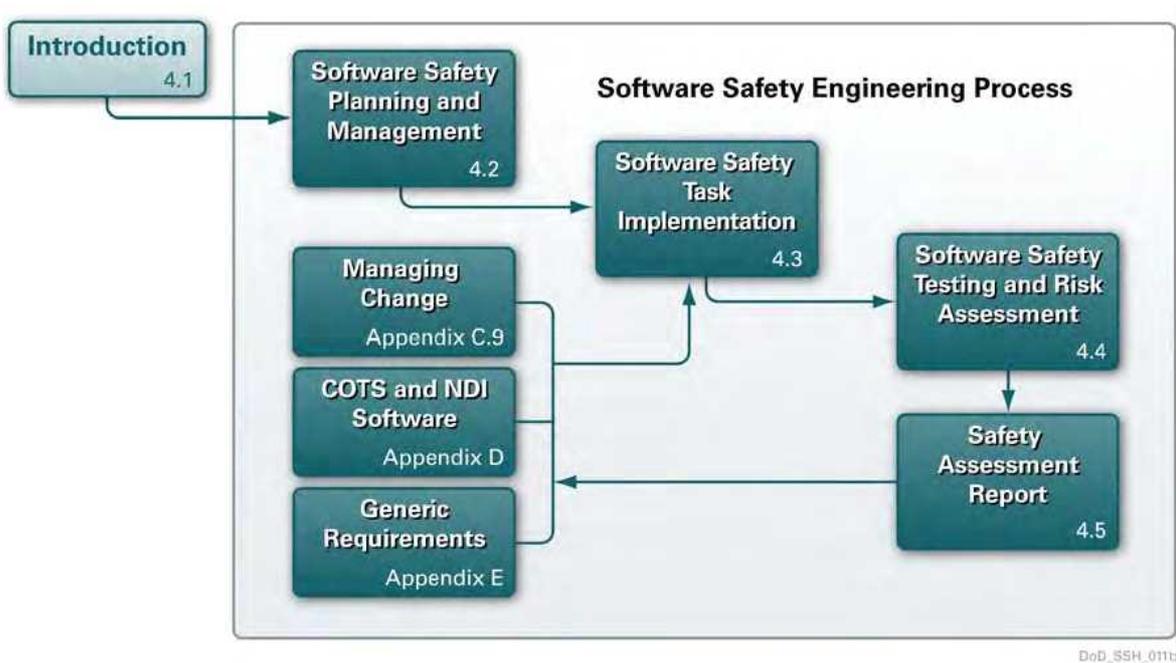
제4장 소프트웨어 시스템 안전 엔지니어링 부문에서는 효과적인 시스템 소프트웨어 안전⁴⁹⁾ 프로그램을 수립, 조정 및 구현하는데 필요한 면밀한 계획과 사전 고려 사항에 대한 지침 제공하고 있다. 주요 목적으로는 1. 추출/맞춤화/실행 가능한 소프트웨어 안전 엔지니어링 프로세스 정의, 2. 소프트웨어 보증 및 무결성 프로세스 정의, 3. 소프트웨어 안전성/보증 및 무결성 작업에 할당 된 각 전문 분야별 필수 수행 업무 기술, 4. 소프트웨어 시스템 안전팀에 할당된 개별 업무와 전문 분야간 인터페이스 관계 식별, 5. 소프트웨어 안전성/보증 및 무결성 프로세스를 완성하기 위한 모범 사례 제시, 6. 사용자 요구 사항을 식별하기 위한 맞춤화된 권장 업무 제공이다.

그리고 제4장은 엔지니어링 프로세스의 흐름으로 구성되어 있는데, 1. 개요(Introduction), 2. 소프트웨어 안전 계획수립 및 관리(Software Safety Planning and Management), 3. 소프트웨어 안전 업무 수행(Software Safety task Implementation), 4. 소프트웨어 안전 테스트 및 위험 평가(Software Safety Testing and Risk Assessment), 5. 안전 평가 리포트(Safety Assessment report)와 별첨⁵⁰⁾ 으로 구성되며, 2절에서 5절까지는 수행 프로세스로서 단계별 수행을 요구한다. 소프트웨어 안전 프로세스는 개념 설계부터 시스템 폐기까지의 전체적인 소프트웨어 안전 프로세스를 다루고 있으며, 프로그램 관리(계획부터 실행까지), 요구 사항 도출(교훈을 통한 일반 요구사항 도출, 시스템 수준 분석을 통한 시스템 특화된 안전 요구사항), 요구사항 확인 및 검증(상세 분석, 안전 테스트), 안전 분석 업무를 포함하고 있다.

49) SSS, System Software Safety

50) 변화관리(Managing Change), 상용 및 비개발 소프트웨어 COTS and NDI Software), 일반 요구 사항(Generic Requirements)

[그림 2-6] 제4장 소프트웨어 시스템 안전 엔지니어링 프로세스



자료: Department of Defense, Joint Software Safety Engineering Handbook, version 1.0 2010.09.

3. 항공 부문

1992년 RTCA⁵¹⁾와 EUROCAE⁵²⁾에서 “항공기시스템과 장비인증에 관한 소프트웨어 고려사항(Software Considerations in Airborne Systems and Equipment Certification)”으로서 DO-178B/ED-12B를 공동 개발하였으며, 이 지침은 1993년 1월 FAA문서인 AC 20-115B에서 FAR에 부합하기 위한 지침으로 채택되었고 대부분의 항공업계에서 채택되어 사용되고 있다.

51) RTCA(Radio Technical Commission for Aeronautics, 1935년 설립): FAA, NASA, 국방부, 기타 정부 기관, 항공기 제조업체, 항공기 운영 업체, 항공기 장비 공급 업체 등 250 개 이상 항공 조직이 포함된 사설 협회

52) EUROCAE(the European Organisation for Civil Aviation Equipment, 1963년 설립): 유럽 및 기타지역의 항공기 및 장비 제조업체, 서비스 제공업체, 국내/국제 항공 당국 및 사용자 등 항공관련 이해당사자로 구성된 비영리 기관

〈표 2-8〉 DO-178B 제정 과정

규격	주요 내용	년도
DO-178	기본적인 절차	1980
DO-178A	소프트웨어 엔지니어링 관련 원칙 강화. Verification 및 Validation 개념 적용	1985
DO-178B	“어떻게” 보다는 “무엇을” 에 중점, Validation 개념은 제외	1992
DO-248	DO-178B 관련 FAQs 및 명확화	2001
DO-278	지상용 CNS/ATM ⁵³⁾ 소프트웨어에 대한 DO-178B 적용 관련	2002

DO-278은 “Guidelines for CNS/ATM Systems Software Integrity Assurance” 로서, DO-178B를 기초로 CNS/ATM 시스템 중 지상장비 운용 소프트웨어의 개발 목적으로 2002년 3월에 제정되었다. DO-278은 DO-178B에 비하여 하나의 소프트웨어 레벨이 더 있는데, DO-178B 목표(objective) 중 일부를 수정하였으며, 일부 목표(objective)들에 대하여 독립성을 추가로 요구하였고, 지상용임을 고려하여 이에 적합하도록 용어(Terminology)를 수정하였다. DO-248B는 추가 인증 지침을 제공하지는 않았지만 소프트웨어 인증에 관한 FAQ, DO-178B 주요 토론 문서, DO-178B 및 DO-278 지침을 개발하는데 사용된 근거가 포함되어 있다.⁵⁴⁾

1) 항공기 관련 신규 지침 개발 배경

DO-178B는 하드웨어 표준, 항공기 안전관련 개발 또는 평가 절차 가이드와 연결되어 기능시스템을 구축하는 요건으로 사용되었다. 이는 목표(Objectives)를 충족하기 위하여 다양한 대체 방법을 수용하는 요구사항기반의 개발/검증 방법론이며, 검증 가능한 고신뢰성 소프트웨어를 개발하기 위한 소프트웨어 개발 프레임워크로 활용되어 왔다. 그러나 객체 지향 프로그래밍, 모델 기반 설계 및 자동 코드 생성 등 새로운 소프트웨어 기술에 대한 대응, DO-178B에 내재된 에러 수정 등, 시스템과 안전 프로세스 간 명확하고 일관된 관계를 제공하고 이머징 소프트웨어 동향 및 기술을 수용할 수 있는 검증 가능한 접근방식을 구현하기 위하여 DO-178B의 변경이 필요하게 되었다. 2004년 12월 RTCA와 EUROCAE는 항공기에서 사용되는 소프트웨어에 관한 규정을 개정하도록 Special Committee 205/Working Group 71 (SC-205/WG-71, SCWG)의 후원을

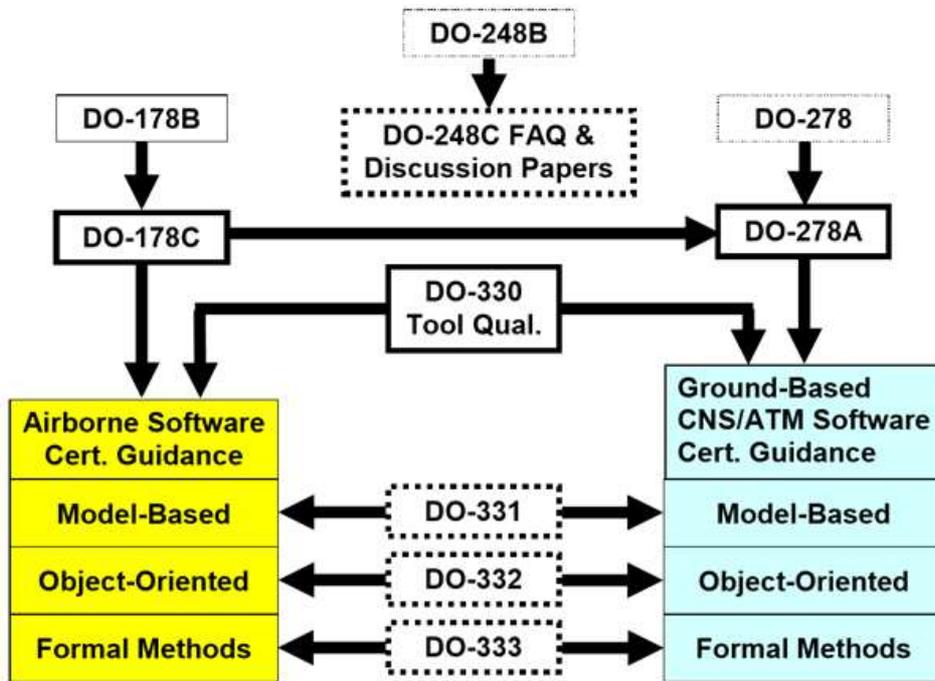
53) 위성항행시스템 Communications, Navigations, and Surveillance/Air Traffic Management

54) 자료: 항공용 소프트웨어 개발 및 인증 기술동향, 한국항공우주연구원, 2007

했으며, 개정 작업의 방향성은 DO-178B의 기본 원칙 및 하위 호환성을 유지하면서 시스템 안전을 지원하는 소프트웨어 개발에 대해 최신기술을 다루고, 기술의 변화를 수용하기 위해 기존 텍스트를 변경하는 방향으로 개정이 진행되었다.⁵⁵⁾

그리하여 2011년 새로운 인증 기준으로 DO-178C/ED-12C와 6개의 관련 지침이 발표되었으며 관련 지침 간의 관계는 [그림 2-7]과 같다.

[그림 2-7] RTCA/EUROCAE의 DO-178C/ED-12C 관련 지침 관계



자료: Certification of Safety-Critical Software Under DO-178C and DO-278, AIAA, 2012

위의 그림에서 DO-178C/ED-12C는 항공기 시스템과 장비에 관한 소프트웨어 인증에 관한 개정 지침이고 DO-278A는 지상 기반 CNS/ATM* 소프트웨어 인증을 위한 신규 지침이다. DO-278A는 원래 DO-178B와 DO-278을 병합하고 추가 고려사항이나 전용 보충 자료를 통해 모든 특정 토픽을 처리하고자 했으나, DO-278을 사용하여 진행 중인 프로젝트에서 발생할 수 있는 부작용에 대해 일부 업계에서 우려가 있었으므로, DO-178C와 일관적 목표를 가지지만 독립적인 활동으로 분리하여 신규 지침으로 생성되었다.

DO-248C는 DO-178B/ED-12B의 설명을 제공하는 DO-248B의 개정문서로서, 일부 정보가 사용되지 않거나 핵심문서에 포함되었고 DO-178C에서 새로 추가/변경된 정보를

55) DO-178C/ED-12C versus DO-178B/ED-12 Changes and Improvement, ACG, Sept 2012

추가하고 지상 기반 도메인인 DO-278A까지 범위가 확장되었다. 또한 DO-178C/ED-12C의 목표(Objective)에 대한 이론적 근거가 포함되어 있으며, 이것은 관련 지침을 이해하는데 도움이 될 수 있다.

SCWG는 주요한 지침인, DO-178C와 DO-278A는 유용한 기술을 포함하고 있으나, 두 지침의 핵심내용을 확장하는 것은 실제적인 개정 작업의 접근방식이 아니었기 때문에 별도의 보충서를 제작하여 몇 가지 새로운 특정 기술을 다루었다. 이러한 보충서는 DO-178C와 DO-278A에서 목적의 추가, 변경, 삭제를 식별하여 필요한 추가 지침을 제공하여 DO-178C와 DO-278A를 보완한다. SCWG는 DO-331, DO-332, DO-333의 3개 보충서를 제작하였다.

- DO-331/ED-216: Model-Based Development and Verification supplement
- DO-332/ED-217: Object-Oriented Technology and Related Techniques supplement
- DO-333/ED-218: Formal Methods supplement

향후에 다른 기술 보충서가 필요할 경우, 핵심 지침이나 기존 보충서의 변경없이 필요한 보충서가 추가될 수도 있다.

DO-178B/ED-12B의 툴 자격(Tool Qualification) 지침은 툴의 세부사항을 적용하기에 불필요하게 어려우며 상세하게 다루어지지 않았기 때문에 개정이 필요했다. 툴 자격 지침은 핵심지침을 개정할 뿐 아니라 완전하고 독립적인 권고, 목적 및 지침으로 구성되기 때문에 보충서의 개념이 아니었고 항공기 영역에만 국한되어서는 안된다는 인식이 있었으므로, 도메인에 독립적인 DO-330이라는 새로운 지침으로 개발되었다. DO-330은 항공기, 지상기, 소프트웨어의 지침에 참조될 수 있으며 우주, 자동차, 의료와 같은 다른 도메인에서도 사용될 수 있다.

2) DO-178C의 유지 및 변경 항목

DO-178C는 DO-178, DO-178A, DO-178B에서 수립된 원칙을 기반으로 제작되었다. 그래서 DO-178C의 기본 철학 역시, 테스트를 통하여 소프트웨어 오류가 없음을 결코 증명할 수 없기 때문에, 오류 생성을 최소화하기 위해 소프트웨어 개발 프로세스의 품질을 처음부터 끝까지 증명하는 것이다. DO-178C는 광범위한 요구사항기반의 소프트웨어 테스트를 수행하도록 요구하지만, 동등하게 중요한 점으로 시스템 안전분석, 소프트웨어 분석/검토, 공식적 증명을 강조한다. DO-178B와 동일하게 적용되는 항목은 다음과 같다.

먼저, 첫 번째, DO-178C는 DO-178B와 동일한 소프트웨어 수준 항목(SL-A to SL-E)을 사용한다. Level A는 소프트웨어 치명도가 가장 높은 수준이며 Level A, B에 대해 광범위한 검증 커버리지 테스트를 요구한다. 커버리지는 2가지 유형으로 구분하는데, 첫 번째 요구사항 기반 커버리지는 소프트웨어 테스트케이스들이 모든 요구사항을 충족한다는 증거를 제공하는지를 확인하기 위해서 분석하는 것이고, 두 번째 구조 커버리지는 테스트케이스가 모든 코드 명령문을 실행하고 모든 데이터 결합 및 제어 경로가 테스트되었다는 것을 증명함으로써 충족된다.

두 번째, 소프트웨어 개발 계획은 소프트웨어 개발 방법을 식별하는 것으로 코딩 표준, 프로그래밍 언어, 소프트웨어 테스트, 디버깅 툴, 소프트웨어 개발 절차 및 소프트웨어를 개발/실행에 사용되는 하드웨어를 명시한다. 소프트웨어 개발 계획을 준수한다는 것을 보증하기 위하여 소프트웨어 개발동안 정기적으로 검토가 수행된다.

세 번째, 이전 버전의 DO-178에서와 마찬가지로, DO-178C는 소프트웨어 개발 프로세스를 소프트웨어 요구 사항의 계획 및 개발부터 시작하여 소프트웨어 개발 및 테스트를 통해 계속되고 소프트웨어 배포 및 유지 관리로 끝나는 생명주기로 간주한다. 소프트웨어 개발 프로세스에서는 먼저 소프트웨어를 더 큰 시스템의 일부로 인식하여 시스템으로부터 소프트웨어 요구사항을 분해한다. 이러한 요구사항은 소프트웨어의 성능 사양뿐 아니라 시스템 안전성 평가 및 관련 문서에서 파생된 요구사항도 포함한다. 소프트웨어 개발 프로세스는 상위 레벨 및 파생된 상위 소프트웨어 요구 사항을 순차적인 절차를 통해(상위레벨 요구사항 -> 소프트웨어 아키텍처 개발 -> 하위레벨 및 파생된 하위레벨 요구사항 도출 -> 소스 코드 생성 -> 오브젝트 코드 생성) 코드로 변환한다. DO-178B와 같이, DO-178C에서도 요구사항부터 코드까지 추적성을 요구한다.

네 번째, 소프트웨어 검증(Verification) 프로세스는 소프트웨어의 정확성을 확인하는 절차로써, 요구사항 검토, 코드 검토, 분석 및 테스트로 구성되어 있다. DO-178B와 DO-178C에서는 상위수준 시스템 요구사항부터 오브젝트 코드까지의 각 단계마다 적용하고 소프트웨어 정확성을 확인하고 에러를 찾기 위해 모든 결과물을 검토할 것을 요구한다. 하위 코드는 하위레벨 또는 상위레벨 요구사항까지 추적 가능해야 하고 그러한 요구사항을 준수해야 한다.

다섯 번째, 소프트웨어 인증(Certification)은 인증기관의 Plan for Software Aspect of Certification (PSAC) 충족성 동의의 결과로 발행된다. 미국은 FAA가 항공기소프트웨어 인증 책임을 가진 기관이며, PSAC는 FAA와 DER⁵⁶⁾의 협업으로 개발되었으며,

56) DER: Software Developer's Designated Engineering Representative

Certificaton Liaison⁵⁷⁾(인증지원) 프로세스 또한 DO-178B와 동일하다.

그 외 소프트웨어 생명주기에 포함된 DO-178C의 소프트웨어 형상관리, 소프트웨어 품질보증계획, 소프트웨어 개발표준, 소프트웨어 설계표준 및 전체적인 검증 활동 등은 모두 DO-178B에 설명된 것과 동일하다.

DO-178C에는 사소한 변경들이 많이 있었지만 대부분이 사실상 편집이나 DO-178B 개념을 더 이해하기 쉽도록 만들어진 설명들로서, 핵심적인 구조와 내용은 DO-178B와 동일하기 때문에 DO-178B와 호환이 가능하다. 이것은 DO-178B에서 승인된 기존 소프트웨어에 대해서 DO-178C 하에서도 승인이 가능하다는 것을 의미한다. DO-178C 지침 셋트의 신규 지침, 추가, 보완 항목은 보충서에 포함되어 있고 이것은 다음 섹션에서 설명되므로, 여기에서는 DO-178C에 포함된 몇 가지 변경 항목에 대해서만 <표 2-9>에서 제시하였다.

57) Certification Liaison Process(CLP, 인증지원프로세스): 인증 신청자와 인증기관간에 인증 진행의 방법을 정의/협의를 하는 것으로서 수행되는 검토 유형에 대한 정의, 검토일자/장소, 인증기관 담당자(DER), 신청자 정보, 제출 산출물 등을 PSAC에 정의하고 인증기관의 합의를 얻는 것임

〈표 2-9〉 DO-178C의 주요 변경 항목

주요 변경 항목	내용
Activities, Guidance, and Guidelines 용어 대체	Activities: 소프트웨어 개발자가 수행해야하는 활동 목록과 관련하여 프로세스를 설명하므로 DO-178B의 guidance 용어를 activities로 대체 Guidance: 인증기관의 가장 중요한 단계 지침 Guideline: 지원정보목록(list of supporting information)지침
Parameter Data Item Files	매개변수 데이터항목을 실행가능한 오브젝트 코드를 수정하는 것 없이 소프트웨어 동작에 영향을 주는 데이터로 정의 “executable object code” 를 “executable object code and parameter data items” 로 대체하여, 실행 가능한 개체 코드에 대해 수행 된 것과 동일한 매개 변수 데이터 파일 항목에 대해 동일한 확인 프로세스를 준수해야 함
Bi-directional Software Traceability	양방향으로 검증, 개체 간 검증 가능한 추적 데이터 존재를 강조 <ul style="list-style-type: none"> • system requirements and high-level requirements • high-level requirements and low-level requirements • Low-level requirements and source code • software requirements and test cases • test cases and procedures • test procedures and test results
Product Service History	대체 방법 (12.3절) 하에서, DO-178C는 제품 서비스 이력을 인증 크레딧을 얻기 위한 수단으로 사용하기 위하여 확장된 지침 제공 일정 기간 서비스되고 있고, 실행 가능한 오브젝트 코드가 제어되지 않은 방식으로 수정되지 않은 소프트웨어에 대하여 인증 크레딧 부여가 가능.
Tool Qualification Levels	검증 프로세스의 일부분을 자동화하는 데 사용되는 도구와 소프트웨어를 자동으로 생성하는 데 사용되는 도구를 구별. TQL(Tool Qualification Level)을 5개의 소프트웨어 레벨에 따라 3가지 Criteria를 적용하여 5가지 툴 자격 수준으로 구분.
Formal Methods and Assurance Cases	DO-178C 의 목적을 충족시키는 대체 방법으로 공식적인 방법 사용을 언급하지는 하지 않으나, 보증 사례(assurance case)를 제품이나 프로세스가 안전 요구사항을 준수한다는 증거를 명시적으로 제시하는 한 가지 기법으로 정의

3) DO-278A (Software Integrity Assurance Considerations for CNS/ATM Systems)

이전의 DO-278은 DO-178B의 보충서로 사용되었으나, DO-278A는 DO-178C와

DO-278의 결합으로 제작된 단독적이고 독립적으로 구성된, 지상 기반 CNS/ATM* 소프트웨어 제품 인증을 위한 새로운 인증 지침이다. 이전 지침과는 다르게, DO-278A는 DO-178C의 참조 없이 사용될 수 있으며, DO-178C와의 차이점 예시는 아래와 같다.

〈표 2-10〉 DO-278A와 DO-178C의 용어(예시)

DO-178C	DO-278A
Software Level	Assurance Level
Certification Authority	Approval Authority
Aircraft, Airborne System	CNS/ATM System
Plan for Software Aspects of Certification (PSAC)	Plan for Software Aspects of Approval (PSAA)

(1) Assurance Level Definitions

DO-178C는 5개의 Software Level로 구분하고, DO-278A는 6개의 Assurance Level로 구분한다. AL-3(엄격한 수준)과 AL-5(관대한 수준)사이의 CNS/ATM 시스템 수준으로 AL-4가 개발되었다.⁵⁸⁾

〈표 2-11〉 DO-278A의 Assurance Level

Software Failure Effect Category	DO-178C Software Level (Airborne Software)	DO-278A Assurance Level (CNS/ATM Software)
Catastrophic	SL-A	AL-1
Hazardous	SL-B	AL-2
Major	SL-C	AL-3
Less than major, more than minor	Not used	AL-4
Minor	SL-D	AL-5
No Effect	SL-E	AL-6

(2) Tool Qualification

DO-278A도 본질적으로 DO-178C와 동일한 툴 자격 가이드를 포함한다. DO-178C와 마찬가지로, DO-278A는 소프트웨어 개발 및 검증 툴은 DO-278A에서 사용된 프로세

58) Certification of Safety-Critical Software Under DO-178C and DO-278, American Institute of Aeronautics and Astronautics(AIAA)

스가 소프트웨어 툴을 사용함으로써 제거, 감소, 자동화될 때 자격을 필요로 한다. 주된 차이점은 DO-278A는 CNS/ATM 시스템에 추가된 Assurance Level을 고려한 것이다.

(3) COTS(Commercial Off-The-Shelf) 소프트웨어

DO-278A는 COTS 소프트웨어 신뢰수준이 DO-278A에서 제공하는 기준 지침에 따라 개발된 다른 소프트웨어와 동일한 수준이라는 것을 보증한다는 COTS 소프트웨어에 관한 지침 목표에 따라, CNS/ATM 시스템에 COTS 소프트웨어를 구현하기 위해서는 DO-278A의 모든 요건을 충족하는 방식으로 개발되어야 승인이 가능하다. COTS 소프트웨어 개발의 약점을 식별하기 위하여, DO-278A는 DO-278A 요건들이 증명될 수 있는 범위를 식별하기 위하여 비교 분석을 수행하도록 권고하며 차이점들이 목표하는 보증수준을 어떻게 충족할 것인지를 구체화하기 위하여 보증계획이 수립되어야 한다.

(4) 추가적인 시스템 고려사항

DO-178C에서 다루지 않은 지상 소프트웨어 검증에 관한 추가적인 주제, 소프트웨어 커뮤니케이션, 보안, 적응성, 컷오버(hot-swapping)등을 다룬다. 지상기반 소프트웨어는 다양한 시스템 요소로 구성되어 있는데, 낮은 보증 수준을 가진 소프트웨어와 높은 보증 수준의 소프트웨어가 충돌했을 때 우려가 발생할 수 있다. 이러한 경우 일반적인 해결방법은 하위레벨 소프트웨어의 보증 수준을 올리기 위해 추가 검증활동을 지정하는 것이다. 그리고 hot-swapping 항목에는 1일 24시간 가동, 실시간 업데이트가 필요한 소프트웨어의 완전성을 보증하기 위한 추가적인 고려사항을 명시해 놓았다.

4) DO-248C (DO-178C와 DO-278A에 대한 설명서)

DO-248C는 항공기 또는 지상 기반 CNS/ATM 소프트웨어에 대한 어떠한 추가적인 인증이나 승인 지침을 제공하지는 않지만, 방대한 양의 설명 자료, 논쟁 기록 및 새로운 지침을 제작하는 동안 개발된 근거를 포함한다. DO-248C는 DO-178C와 DO-278A에 대한 FAQ, 토론 보고서 및 이론적 근거의 키워드 검색을 통해 관심 주제별로 가장 적합한 자료를 찾을 수 있도록 구성되어 있다.

5) DO-330 (Software Tool Qualification Consideration)

DO-330은 툴 자격이 언제 필수적이고, 어떤 검증 활동이 권고되는지를 판단하기 위한 지침을 알려주는 독립적인 문서이며 소프트웨어 개발에 사용하는 툴과 검증에 사

용하는 툴에 대한 지침을 제공한다. 이 지침의 목표는 소프트웨어가 생성/검증되는 것과 동일한 보증 수준으로 이러한 툴들이 개발된다는 것을 보증하는 것이다. 툴 자격 고려사항 문서는 도메인 관련 문서와 함께 사용되는데, 툴 자격 고려사항 문서를 적용하기 위하여, 도메인 관련 문서에서 툴 자격 고려사항의 적용여부 식별, 툴 자격 기준 정의, 툴 자격 수준을 정의해야 한다.

DO-178B의 2가지 툴 자격 기준은 소프트웨어 수준과 관련하여 세 가지 기준(Criteria)로 대체되어, 적용 가능한 툴 자격 수준 (TQL: Tool Qualification Level)을 결정했다. 기존의 “개발툴” 과 “검증툴” 로 분류되는 자격 기준은 아래와 같다.

- 결과물을 검증하지 않은 결과소프트웨어에 에러를 주입할 수 있는 툴을 개발툴로 분류하고, 결과소프트웨어와 동일한 목표를 적용한다.

- 에러를 감지하는데 실패할 수 있는 툴을 “검증툴” 로 분류하고, 자격기준은 툴이 정상적인 운영조건에서 운영요구사항을 준수한다는 것을 증명하는 것이다.

이러한 두 가지 분류가 대체된 이유는, 툴 분류(개발, 검증)를 정의하기 위해 사용되는 용어가 올바르지 못한 툴에 기능을 전가했을 수도 있다는 것, 개발툴을 검증하기 위하여 항공기 소프트웨어 목표를 적용하는 것이 무관한 사항인 경우도 있고 여러 가지 해석을 야기시키는 등 이슈가 발생했기 때문에, 아래와 같이 기준#1(개발툴), 기준#3(검증툴) 외에 기준#2가 추가되었다.

- 기준(Criteria) #1: 항공기 소프트웨어의 일부분, 에러를 유발할 수 있는 툴
- 기준(Criteria) #2: 검증 프로세스를 자동화를 통해 비록 오류를 감지하지 못할 수는 있으나 다음의 작업을 하는데 합당한 근거가 될 수 있는 툴;
 1. 툴에서 자동화된 절차 이외에 검증 절차 제거/감소
 2. 항공기 시스템에 영향을 주는 개발 절차 제거/감소
- 기준(Criteria) #3: 의도된 용도 범위 내에서 에러를 찾는데 실패할 수 있는 툴

툴의 목적은 인공결과물의 개발 및 검증이며, 인증 신용클레임은 이 인공결과물에 적용할 수 있는 목표선까지이다. 즉, 테스트케이스로부터 툴 절차를 생성하는 툴의 경우, 인증 신용은 테스트절차의 정확성까지로 제한되고, 소스코드의 코드표준 준수여부를 검증하는 코드체커에 대한 인증 신용은 소스코드가 표준에 부합한다는 목표까지로 제한된다.

〈표 2-12〉 툴 자격 수준(Tool Qualification Level)

Software Level		Criteria ⁵⁹⁾		
		#1	#2	#3
Level A	Catastrophic	TQL-1	TQL-4	TQL-5
Level B	Hazardous	TQL-2	TQL-4	TQL-5
Level C	Major	TQL-3	TQL-5	TQL-5
Level D	Minor	TQL-4	TQL-5	TQL-5
Level E	No Effect	-	-	-

자료: DO-178C/ED-12C versus DO-178B/ED-12B Changes and Improvements, ACG, Sept 2012

TQL-1은 가장 높은 자격 수준이고 가장 많은 요건과 검증 활동이 있다. TQL-1은 DO-178C의 SL-A(소프트웨어 수준 A등급) 또는 DO-278A의 AL-1 (보증수준 1등급) 소프트웨어 툴에 대해 적용된다. TQL-2는 SL-B와 AL-2 소프트웨어를 만드는데 사용되는 소프트웨어 툴, TQL-3은 SL-C와 AL-3 소프트웨어를 생성하는데 사용되는 소프트웨어 툴에 적용된다. TQL-4와 TQL-5는 소프트웨어를 검증하는데(생성하지 않음) 사용되는 소프트웨어 툴에 적용된다. DO-330은 코드를 검증하는데 사용되는 툴보다 코드를 생성하는데 사용되는 툴에 좀 더 엄격한 검증 요건을 적용한다.

툴 검증 절차는 2개 파트로 구분된다. 첫 번째 파트는 검토, 분석 및 테스트케이스의 조합으로 구성되는데, 요구사항의 정확성, 툴아키텍처의 요건충족성, 하위레벨 요건의 소프트웨어 아키텍처요건 준수, 상위레벨/하위레벨 요건에 대한 소스코드의 충족성 등을 검증한다. 두 번째 파트는 소프트웨어 툴이 소프트웨어 개발 및 검증 툴로써, 의도한 요건을 충족하는지를 보증하는 것이다. 툴 운영 검증 절차는 툴의 결과물과 기능이 의도한 운영 환경에서 툴 운영 요건에 부합한다는 신뢰성을 제공하기 위해 수행되며, 툴의 사용으로 인해 제거, 감소, 자동화되도록 의도된 소프트웨어 생명주기의 전체 범위를 입증하기 위한 검토, 분석 및 테스트의 조합으로 구성된다.

6) 기술 보충서

모델기반 개발/검증을 다루는 DO-331, 객체지향 관련 기술 사용을 다루는 DO-332, 공식적 방법에 관한 DO-333, 3가지 특정 기술에 관한 보충서가 새로운 소프트웨어 개발 지침으로 사용된다. 이 보충서는 DO-178C와 DO-278A에 대한 지침과 목표를 제공하고 기술 특화된 해석, 목표 수정, 추가 목표 등을 포함하여 각 목표들이 특정기술에

59) DO-178C/ED-12C versus DO-178B/ED-12B Changes and Improvements, ACG, Sept 2012

대해서 어떻게 변경되는지를 설명해 두었다. 보충서 내의 목표는 DO-178C와 동일한 구조를 따른다.⁶⁰⁾

(1) DO-331 (Model-Based Development and Verification Supplement)

DO-331은 모델⁶¹⁾ 기반의 개발 및 검증이 소프트웨어 생명주기의 일부로 사용될 때, DO-178C와 DO-278A의 목표, 활동, 주석 및 소프트웨어 생명주기 데이터에 변경 및 추가를 포함한다. 본질적으로 모델은 요구사항이나 아키텍처를 모호하지 않은 표현하고, 자동 코드 생성 지원, 자동 테스트 생성 지원, 요구사항이나 아키텍처의 분석 툴로써 사용되고, 요구사항이나 아키텍처, 또는 실행 가능한 오브젝트 코드의 부분적인 검증을 위한 시뮬레이션에서도 사용된다. 이것은 도출된 검증 증거뿐 아니라 모델을 사용하면서 표현된 결과물을 포함한다. DO-331은 또한 소프트웨어 요구사항 또는 소프트웨어 아키텍처를 정의하는 시스템 절차 내에서 개발된 모델에도 적용된다.

(2) DO-332 (Object-Oriented Technology and Related Techniques Supplement)

DO-332는 객체지향 기술 또는 관련 기술이 소프트웨어 개발 생명주기의 일부로 사용되고 추가 지침이 필요할 때, DO-178C와 DO-278A 목표들에 추가, 보완, 삭제항목들을 식별한다. DO-178C와 합하여 객체지향 기술과 관련 기술기반의 시스템을 평가하고 수용하는데 동일한 프레임워크를 제공할 목적을 가지고 있다. 객체지향 기술은 중요하지 않은 소프트웨어 개발 프로젝트에 넓게 채택되어 왔다. 항공 전자 공학에서 중요한 소프트웨어 응용시스템에 이 기술을 적용하는 것이 증가되어 왔지만 안전과 무결성의 목적을 충족시키기 위해 고려되어야 하는 많은 문제가 있다. 이러한 문제들은 언어 특성 및 잘 정의된 안전 목표들을 충족할 때 발생하는 복잡성과 직접적인 관련이 있다.

(3) DO-333 (Formal Methods Supplement)

DO-333은 공식적 방법이 소프트웨어 생명주기의 일부로 사용되고 추가 지침이 필요할 때, DO-178C와 DO-278A 목표에 추가, 보완, 대체항목을 식별한다. DO-178C를 사용하여 승인받은 시스템에 대하여 공식 방법을 사용하여, 소프트웨어의 생산에 속하는

60) The Impact of RTCA DO-178C on Software Development, cognizant, Oct 2012

61) 모델: 소프트웨어 개발 또는 검증 프로세스를 지원하는 데 사용되는 시스템 소프트웨어 측면을 추상화한 것

감항성(air-worthiness) 인증의 측면을 설명한다. 공식 방법은 소프트웨어 디지털 시스템 측면의 명세, 개발 및 검증에 대한 수학적 기반 기술이다. 이것은 공식로직, 이산수학, 컴퓨터 판독 가능 언어로 구성되어 있다. 공식 방법 사용은 다른 공학 분야와 마찬가지로, 적절한 수학적 분석을 수행하면 설계의 정확성과 견고성을 확립하는데 기여할 수 있다는 기대를 갖고 있다.

4. 의료 부문

의료 소프트웨어는 의학적 맥락에서 사용되는 소프트웨어 항목 또는 시스템으로써, 진단 또는 치료목적으로 사용되는 독립적 소프트웨어, 의료기기 내장 소프트웨어(의료기기 소프트웨어), 의료기기를 구동하거나 사용방법을 결정하는 소프트웨어, 의료기기의 부속품으로 작동하는 소프트웨어, 의료기기의 설계/생산/테스팅에 사용되는 소프트웨어, 또는 의료기기의 품질제어관리용 소프트웨어를 지칭한다. 의료 소프트웨어는 록히드⁶²⁾가 병원부문에서 최초의 컴퓨터정보처리시스템을 고려했던 1960년대 이후로 사용되어왔다. 1970년대 후반과 1980년에 들어서면서 컴퓨팅이 널리 퍼지고 유용해지면서 의료분야에서 데이터와 운영관리툴로써의 의료소프트웨어의 개념은 일반화되었고, Therac-25 방사선 치료 장비 문제로 촉발된 영역에서, 연구 및 입법 공동체에서 안전에 중대한 성격의 추가 조사를 촉진하면서, 의료 소프트웨어는 핵의학, 심장학 및 의료로봇과 같은 분야의 의료기기 부문에서 더욱 눈에 띄게 증가하였다. 1993년 유럽의 의료기기지침(Medical Devices Directive, MDD) 뿐 아니라 ISO 9000-3⁶³⁾표준의 개발은 의료기기와 관련 소프트웨어가 기존의 법률과 조화를 형성하는데 도움이 되었고, 2006년 IEC 62304의 추가로 의료기기 소프트웨어의 개발 및 테스트 방법을 더욱 확고히 하였다. 미국 FDA(Food and Drug Administration) 또한 의료 소프트웨어, 특히 의료기기에 내장된 소프트웨어에 관한 지침과 규제를 제공했다.⁶⁴⁾

IEC 62304는 유럽과 미국에 채택된 의료제품 소프트웨어 설계에 대한 조화된 표준이다. 조화(“harmonised”)되었기 때문에, 이 표준을 채택하는 의료기기 제조사들은 소프트웨어 개발과 관련된 의료기기지침 93/42/EEC (MDD)에 나와 있는 필수 요건을 충

62) 록히드(Lockheed, 원래 Loughhead): 1912년 설립된 미국의 항공기 제조회사이며, 1995년 마틴 마리에타와 합병하여 록히드 마틴을 설립함

63) ISO 9000-3은 품질관리와 품질보증표준으로써, 현재 사용되지 않고 ISO 90003(Guidelines for the application of ISO 9001:2008 to computer software)으로 대체됨

64) Medical software, Wikipedia

족시킬 것이므로 MDD 준수여부를 입증하는데 가장 편리한 방법일 수 있다. 또한 미국 FDA도 ANSI/AAMI/IEC 62304:2006을 의료기기 소프트웨어가 수용 가능한 표준으로 설계되었다는 증거로써 인정하고 있다. 그러므로 IEC 62304로 설계한다는 것은 품질 소프트웨어가 정의되고 제어된 소프트웨어 개발 프로세스를 통해 생성된다는 것을 보증하는 것이다. 다음 섹션에서는 의료기기 소프트웨어 국제표준인 IEC 62304와 미국의 FDA 및 유럽의 의료기기지침인 MDD를 통해 의료 부문 안전활동을 살펴보도록 하겠다.

1) IEC 62304

(1) IEC 62304 표준 및 관련 표준

의료기기 소프트웨어에 대해 중요한 2가지 ISO표준이 있는데, ISO 13485와 ISO 14971이다. 이것은 의료기기에 대한 가장 높은 표준으로써, 가장 일반적이며 가장 단순한 석고부터 가장 복잡한 외과 의사 로봇까지, 모든 의료기기에 적용된다. 그래서 소프트웨어에 대한 정보를 제공하지는 않는다. 의료기기분야에서 소프트웨어에 관한 주요 표준은 IEC 62304이며, 환자의 안전을 보장하기 위해, 의료기기 소프트웨어의 안전 설계 및 유지보수에 필요한 활동과 작업에 대한 소프트웨어 생명주기를 다루고 있다. 그리고 네트워크, 소프트웨어 연계 및 하드웨어에 관한 요구사항으로 IEC 60601-1이 추가되었고, 인체공학에 대하여 IEC 62366이 추가되었다.

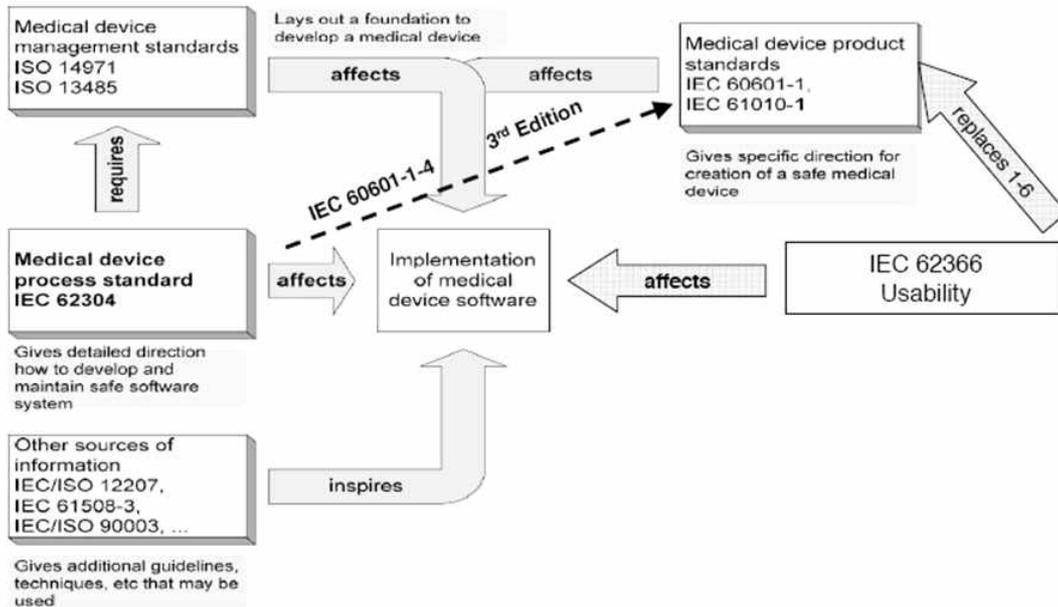
IEC 60601-1은 전기의료기기에 관한 표준으로, 소프트웨어가 내장된 칩은 전기로 공급을 받기 때문에 의료기기소프트웨어에 포함되며 이러한 프로그램 가능한 전기의료기기를 PEMS(Programmable Electrical Medical Devices)라고 지칭한다. IEC 60601-1의 3판에서 PEMS에 대한 요구사항을 적용할 때, IEC 62304의 요구사항을 PESS⁶⁵⁾에 대한 소프트웨어 개발 또는 변경에 적용해야 하며 적합성 또한 IEC 62304로 판단한다고 변경되었다.⁶⁶⁾ IEC 62366은 인체공학과 사용자/기기간의 상호작용에 관한 표준이다. 인체공학은 모든 의료기기에 대해 고려되어야 하며 이 표준을 구현하기 위해서 다른 기기에서와 동일한 방법이 필요한데, 소프트웨어 분야의 우수사례로는 다른 소프트웨어 요구사항과 마찬가지로, 인체공학과 소프트웨어 개념 문서 간 추적매트릭스를 통하여 지속적으로 인체공학 요구사항을 추적하는 것이다.⁶⁷⁾ 아래 그림은 IEC 62304와 다른

65) PESS(Programmable Electrical Sub System): 프로그램 가능한 의료용 전기부시스템으로 소프트웨어 및 인터페이스를 포함하는 하나 이상의 중앙처리장치 기반 시스템

66) 의료기기 소프트웨어 허가/심사 가이드라인, 식품의약품안전평가원, 2015 7월

표준과의 관계도이다.

[그림 2-8] IEC 62304와 다른 표준과의 관계



자료: Legal aspects of medical devices software and software as medical device, GreenbergTraurig, 2011

- IEC 62304: 소프트웨어 생명주기 프로세스에 관한 표준
- ISO 13485: 의료기기 품질관리 요구사항
- ISO 14971: 의료기기 위험관리 요구사항
- IEC 60601-1: 의료기기 제품 표준
- ISO 62366: 의료기기 사용성
- IEC 61508: 전자안전관리시스템의 기능안전 표준

(2) 소프트웨어 안전 분류

IEC 62304는 의료기기 소프트웨어의 안전 등급을 3개로 분류하였으며, 이 분류는 사용자, 환자 또는 다른 사람들에게 상해를 가하는 잠재적인 위험을 초래할 수 있는 가능성에 근거한다.

67) ISO and IEC standards for software in medical devices in a nutshell, MD101 website

〈표 2-13〉 소프트웨어 안전 등급

등급	심각도
Class A	No injury or damage to health is possible
Class B	Non-Serious Injury is possible
Class C	Death or Serious Injury is possible

자료: Developing Medical Device Software to IEC 62304, posted by MDDI staff, June 2010

이 분류를 효과적으로 적용하려면 “심각한 상해“, “비상해“, “상해“ 및 “건강 손상“을 정의하는 것이 중요하지만, 표준에서는 “심각한 상해(Serious Injury)만 정의한다.

심각한 상해(Serious Injury)는 직접 또는 간접적으로 발생하는 상해 또는 질병으로써,

- a) 생명을 위협한다.
- b) 신체 기능에서 영구적인 장애⁶⁸⁾가 생기거나 신체 구조를 영구적으로 손상시킨다.
- c) 신체 기능의 영구적 장애 또는 신체 구조에 대한 영구적인 손상을 방지하기 위해 의학적 또는 외과적 개입이 필요하다.

(3) 분리(Segregation)와 SOUP(Software of unknown provenance)

IEC 62304에서는 분리(Segregation)의 예로, 다른 프로세서에서 소프트웨어 항목⁶⁹⁾을 실행하는 것이고, 분리의 효과는 프로세스 간에 공유된 리소스가 없기 때문에 보장될 수 있다” 라고 언급했다. 이것은 실제로 안전이 중요한 소프트웨어 시스템을 각각 다른 프로세서에서 실행하고 다른 안전 분류를 가지고 각각 다른 프로세서에서 실행하는 항목으로 분리할 수 있음을 의미한다. 시스템이 안전하고 고품질을 유지하고 있으며, 적절한 시간과 비용 가이드라인 내에서 생산된다는 것을 보증하기 위해서 처음부터 올바르게 분리하는 것이 중요하다.

SOUP (Software of unknown provenance)는 출처가 알려지지 않은 소프트웨어로, 정식문서가 없거나 제3자가 개발한 코드이며 개발프로세스를 제어하는 증거가 없다. 그러므로 개발 중인 소프트웨어에 사용되는 SOUP 코드에 대해 소프트웨어 위험분석을 수행하고 이 코드를 사용하는 근거를 제시하는 것이 중요하다. SOUP의 사용은 Class

68) 영구적 장애(Permanant Impairment)란 돌이킬 수 없는 신체구조상의 장애 또는 손상을 의미하며, 사소한 장애 또는 손상은 제외된다.

69) 소프트웨어 항목(Item)은 컴퓨터 프로그램에서 식별 가능한 부분이며, 소프트웨어 단위(Unit)는 다른 항목들로 세분화되지 않는 소프트웨어 항목을 의미한다.

A로 간주되면 더 이상의 타당한 근거 없이 사용될 수 있다. 등급이 올라갈수록, 위험은 증가하고 근거는 정당화하기 어렵게 되므로 실제로 단순한 기능, 널리 알려져 있고 다양하게 적용된 SOUP만이, Class C 응용시스템에 사용될 수 있다는 것을 의미한다. 그러므로 IEC 62304에서는 의료기기 소프트웨어의 SOUP 사용을 식별하고 정당화하는 방법으로 소프트웨어 설계 절차에 통합하여 검증하도록 한다.

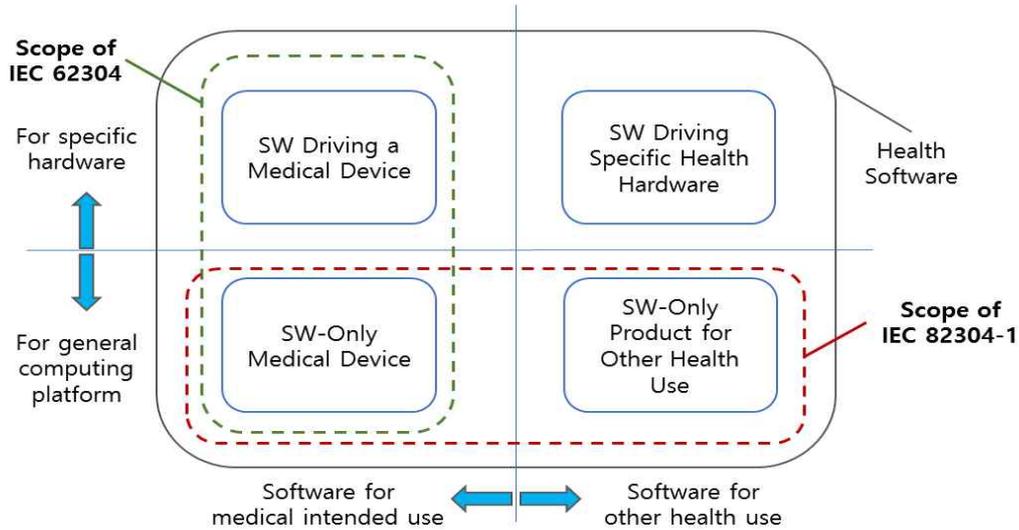
(4) IEC 82304-1 (2016 Health Software에 관한 표준)

의료의 범주가 확대되어 건강 관련 소프트웨어가 증가함에 따라, 건강 소프트웨어의 안전과 보안에 대한 국제표준 IEC 82304-1이 2016년에 발표하였다. IEC 82304-1:2016은 일반적인 컴퓨팅 플랫폼에서 운영되도록 설계된 건강 소프트웨어 제품과 전용 하드웨어 없이 시장에 출하되도록 고안된 건강 소프트웨어 제품에 대한 안전과 보안에 적용된다. 이것의 주요 초점은 제조사에 대한 요구사항에 있으며, 건강 소프트웨어 제품 설계, 개발, 검증, 설치, 유지보수 및 처분을 포함한 전체 생명주기를 다룬다.⁷⁰⁾

좀 더 상세하게 설명하자면, IEC 82304-1은 독립 실행형 소프트웨어만을 다루고, IEC 62304와 달리 의료 기기에 내장되거나 특정 하드웨어가 있는 기기에 내장된 소프트웨어는 다루지 않는다. 범용 운영 체제가 있는 표준 PC, 서버, 태블릿 또는 스마트폰에서 실행되는 소프트웨어는 IEC 82304-1의 범위에 속한다. IEC 82304-1은 IEC 62304와 규제에서 요구하는 소프트웨어 의료 기기 검증 간의 격차를 채워준다. 이를 위해 시스템 레벨에서 필요한 항목을 정의하는 최소한의 조항을 포함하며 소프트웨어 수준에 대한 기존의 ISO 14791이나 IEC 62304와 같은 최신 표준을 참조한다. 아래 그림은 IEC 82304-1 표준의 범위를 나타낸다.

70) 자료: IEC 82304:2016 Health software-Part 1: General requirements for product safety, ISO.org Website

[그림 2-9] IEC 62304와 IEC 82304-1 범위



자료: IEC 82304-1-latest news about the standard on Health Software, MD101 website, 2016

위에서 설명한 바와 같이, IEC 62304는 의료기기에 대한 안전과 고신뢰성 소프트웨어를 개발하기 위한 논리적인 표준이며 국제적으로 채택된 조화된 표준이므로 미국과 유럽의 품질 기대수준을 동등하게 유지하게 할 수 있고 이 표준의 적용으로 더욱 공정한 경쟁시장을 만들기 때문에 환자의 안전뿐 아니라 제조사에도 도움이 될 수 있다.

2) 미국 의료 소프트웨어 안전 활동

(1) FFD&C Act (Federal Food, Drug & Cosmetic Act)

현재는 역사적인 참조로만 남아있고 폐지된 첫 번째 관련법은, 1906년 식품의약품법 (Food and Drugs Act of 1906)으로 세계에서 가장 포괄적이고 효과적인 공공 보건 및 소비자 보호 네트워크 중 하나였다. 이후, 합법적으로 판매된 유독성 엘릭서로 인해 어린이를 포함 107명이 사망한 후, 1938년 “Federal Food, Drug & Cosmetic Act, FD&C Act 또는 FFD&C Act : 연방 식품, 의약품, 화장품법“이 통과되었다. FFD&C 법은 공중보건시스템을 완전히 정비했고, 그 법안을 통해 FDA는 신약의 안전성에 대한 증거를 요구하고 식품 기준을 제정하고 공장검사를 실시하는 권한을 부여받았다. 그 후 결함이 있는 의료기기로 인해 731명의 사망을 포함하여 10,000명의 상해가 발생했다는 미국 상원의 판결에 따라, 1976년 의료기기개정안(Medical Device Amendments

of 1976)에 새로운 기기의 안전 및 유효보호장치를 적용했다. 이는 의료기기 규제를 관장하는 기본 틀로써 1976년 5월 28일에 법제화되었고, FFD&C 법은 1990년 안전한 의료기기법(the Safe Medical Devices Act)과 1992년 의료기기 개정(the Medical Device Amendments)에 의해 재개정되었다. 의료기기를 포함하여 제품을 규제하는 새로운 FDA 수출 통제 조항은 1996년 FDA 수출 개혁 및 강화법 (FDA Export Reform and Enhancement Act)에서 확립되었다. FFD&C Act는 1997년 Food and Drug Administration Modernization Act (the Modernization Act, 현대화법)로 개정되었다. 1997년 11월 21일에 서명되면서, 이 현대화법은 FDA의 관할지역에 있는 모든 제품과 관련한 규제조항을 포함했다.

the Modernization Act의 Section 210(h)에는 ‘Device’ 란, “구성요소, 부품, 부속품을 포함한 다른 비슷한 관련종목에서 기계, 도구, 기구, 장치, 고안품, 이식품” 으로 정의하고 있으며, the Modernization Act의 주요 의료기기 인증과 관련된 법 조항은 아래와 같다.⁷¹⁾

71) Overview of FDA Modernization Act of 1997, Medical Device Provisions, FDA website

<표 2-14> FFD&C Act, Provisions

주요 항목	관련 조항
Investigational Device Exemptions	Section 201 - Changes to Protocols and Devices
	Section 201 - Early Collaboration of Data Requirements for Clinical Studies
	Section 205 - Meeting on Evidence of Effectiveness for PMA's
	Section 203 - Expanded Humanitarian Device Exemption (HDE)
	Section 402 - Expanded Access to Investigational Devices Section 214 - Practice of Medicine
Premarket Approval	Section 201 - Data from Previous Investigations
	Section 202 - Special Review for Certain Devices
	Section 205 - Scope of Review/Collaborative Determinations of Device Data Requirements
	Section 207 - Risk Based Classification of Postamendment Class III Devices
	Section 208 - Classification Panels
	Section 209 - For PMA Collaborative Review Process
	Section 216 - Use of Data
	Section 216 - Product Development Protocol (PDP)
Section 217 - Clarification of the Number of Required Clinical Investigations for Approval	
Section 403 - Approval of Supplemental Applications	
Premarket Notification 510(k)	Section 205 - Collaborative Determinations of Device Data Requirements
	Section 206 - Premarket Notification
	Section 209 - Certainty of Review Timeframes
	Section 210 - Accreditation of Persons for Review of Premarket Notification Reports

자료: Overview of FDA Modernization Act of 1997, Medical Device Provisions, FDA website

(2) 의료기기 규정 (Title 21, Code of Federal Regulations)

미국 FDA의 CDRH(Center for Devices and Radiological Health, 기기 및 방사선 건강 센터)는 미국시장에서 판매되는 의료기기를 제조, 재포장, 재라벨 지정 및 수입하는 회사를 규제하고 레이저, X선 시스템, 초음파 장비, 전자오븐 및 컬러 TV와 같은 방사선 방출 전자 제품(의학 또는 비의학)을 규제하고 있다.

의료기기의 분류에 따라 시장에 출시되는 FDA 허가(Clearance⁷²)에 필요한 시판전제출/신청 유형이 결정된다. 의료기기가 Class I, II이나 면제되지 않는 경우에는, 시판전 신고(Premarket Notification) 510(k)이 필요하고 면제되는 모든 의료기기는 제한 및 면제가 있다. Class III 기기에 대해서, 그 의료기기가 1976년 의료기기 개정안이 통과되기 전 시장에 출시되었거나 그러한 장치와 실질적으로 동등한 사전조치기기가 아닌 경우, 시판전 승인 신청(Premarket Approval Application, PMA)이 필요하고, PMA가 요청되지 않았던 경우 출시를 위해서는 510(k)이 필요하다.

기기 분류 등급은 1)기기의 사용용도와 사용지침에 따라 다르고, 2)위험에 기반하여 분류된다. 첫 번째 예로, 메스 용도는 조직을 절개하는 것이다. 이것의 부분 용도는 “각막 절개용” 과 같이, 특화된 지침 표시가 추가되었을 때 나타나며 사용용도의 의미는 510(k)의 실질적인 동등성 평가에 포함되어 있다. 두 번째로, 기기가 환자나 사용자에게 끼치는 위험이 등급을 결정하는 주요한 요소이다. Class I는 위험성이 낮은 기기들을 포함하고 Class III는 위험성이 높은 기기들을 포함한다. 모든 기기는 일반지침(General Controls)이 있고 일반지침은 FFD&C Act의 기본적인 요구사항으로써 모든 의료기기, Class I, II, III에 모두 적용된다.

〈표 2-15〉 FDA의 의료기기 분류

분류	관련 규제
Class I	General Controls <ul style="list-style-type: none"> • With Exemptions • Without Exemptions
Class II	General Controls and Special Controls <ul style="list-style-type: none"> • With Exemptions • Without Exemptions
Class III	General Controls and Premarket Approval

자료: Classify Your Medical Device, FDA website (fda.gov)

대부분의 의료기기는 Title 21 CFR, Parts 862-892에 있는 장치에 일치하는 설명을 찾아서 분류할 수가 있다. FDA는 1,700여가지의 서로 다른 유형으로 기기를 분류하였고, 그것을 심혈관기기, 귀, 코, 목 기기 등과 같이 16가지의 의학 전문 패널(panel)로

72) Clearance와 Approval 구분: (1)Clearance: FDA로 제출된 premarket notification 510(k) 검토 후, 해당기기를 “clear“하고, (2)Approval: FDA로 제출된 premarket Approval(PMA) 신청을 검토한 후, 해당기기를 “approve“한다.

구성하여, 기기 분류 및 시장 요구사항에 대한 정보를 포함하여 제공하고 있다.

미국 시장에 의료기기를 출시하려고 할 때, 510(k), PMA 등 기본적인 규제사항⁷³⁾을 준수해야 하며 아래는 규제에 대한 간단한 요약 자료이다.

- Establishment registration (21 CFR Part 807)

국내외 모든 의료기기 제조사와 유통업체(수입업체)는 시설을 FDA에 등록해야 하고, FDA가 면제하지 않는 한, 모든 시설 등록은 전자적으로 제출되어야 한다.

- Medical Device Listing (21CFR Part 807)

제조사들은 FDA에 기기들을 등록해야 하고, 기기 등록을 해야 하는 시설은, 제조사, 상업적으로 기기를 유통하는 계약된 제조사 및 계약된 소독기업체, 재포장/재라벨업체, 규격개발자, 일회용 장치 재처리사, 재제조사, 사용자에게 직접 판매하는 부속품 또는 구성품 제조사, 수출전용 장비 미국 제조사 등을 포함한다.

- Premarket Notification 510(k) (21 CFR Part 807 Subpart E)

새로운 기기에 대하여 시판전 신고 510(k) 제출이 필요하다면, FDA로부터 실질적 동등성 레터(Letter of substantial equivalence)를 수령할 때까지 상업적으로 기기를 출시할 수 없으며, 510(k)을 통해 기기가 미국내에 합법적으로 유통되는 기기와 실질적으로 동등하다는 것을 입증해야 한다. 그리고 2002년 의료기기 사용자 및 현대화법(the Medical Device User Fee and Modernization Act)에 의해, FDA가 의료기기 시판전 신고 (510(k)) 검토 비용을 청구할 권한을 가지게 되었다. Class I, II에 대한 510(k)를 Accredited Persons(공인된 사람)에게 검토를 받을 수 있다. 이미 FDA는 670개 유형의 기기에 대한 1차 검토기관으로 12개의 기관을 승인했으며, FDA는 Accredited Person의 추천서를 받은 후, 30일 내에 최종 결정을 내려야 한다. 공인된 사람의 510(k)검토는 수수료가 면제된다.

- Premarket Approval (PMA) (21 CFR Part 814)

PMA를 요구하는 제품은 Class III 기기로서, 질병이나 부상의 위험이 크고, 510(k) 과정을 통해 입증된 Class I, II와 실질적으로 동등하지 않는 것으로 밝혀진 기기이다. PMA과정은 더 복잡하게 얽혀 있고, 의료기기에 대한 클레임을 뒷받침하는 임상자료 제출을 포함하고 있다. 2003년부터 최초 PMA와 특정 유형의 PMA 보완에 의료기기 사용료가 지불되어야 한다.

73) Overview of Device Regulation, FDA website

- Investigational Device Exemption (IDE) for clinical studies (21CFR Part 812)

FDA에 시판전 승인(PMA) 신청서 또는 시판전 신고 510(k) 제출을 지원하는데 필요한 안전성 및 유효성 데이터를 수집하기 위하여 시험용 기기를 임상연구에 사용할 수 있다. 심각한 위험을 가진 시험기기의 임상연구 사용은 연구 시작 전에 FDA와 IRB⁷⁴⁾의 면제승인을 받아야 한다. 심각성이 낮은 시험기기의 임상연구 사용은 IRB의 승인만 받으면 된다.

- Quality System (QS) regulation (21 CFR Part 820)

QS 규제는 의료기기의 설계/구매/제조/포장/라벨링/보관/설치 및 서비스에 사용된 방법, 시설/제어와 관련된 요구사항을 포함하며, 제조와 시설은 QS 요구사항 준수를 확인하기 위해 FDA 검사아래 수행되어야 한다.

- Labeling requirements (21 CFR Part 801)

라벨링은 의료기기에 부착된 설명/정보 인쇄물 뿐 아니라 기기부착 라벨도 포함한다.

- Medical Device Reporting (MDR) (21 CFR Part 803)

의료기기가 사망 또는 심각한 상해를 유발한 사고 및 특정 오작동은 의료기기리포팅(MDR) 프로그램을 통해 FDA에 반드시 보고되어야 한다. MDR 규정은 적시에 문제를 감지하고 해결하는 것을 목적으로 하며, FDA와 제조사가 의료기기를 포함하여 중요한 사고를 식별하고 모니터링하기 위한 방법이다.

위와 같은 규제사항을 참고로 하여 미국시장에 의료기기를 출시할 경우, (1) 시장에 출시하고자 하는 의료기기를 분류하고, (2) 기의 분류(Class I, II, III)에 따라 시판전 제출 유형(510(k), PMA 등)을 선택하며 (3) FDA에 시판전 제출에 대한 적절한 정보를 준비한다. (4) FDA에 이를 제출하고 검토하는 동안 검토 과정의 효율성을 높이기 위하여 FDA 담당자와 정보를 교류한다. (5) FDA로부터 시판전 Clearance 또는 Approval을 받은 후, 시설등록 및 장비목록 등록 과정⁷⁵⁾을 거쳐 완료할 수 있다.

(3) 의료기기에 포함된 소프트웨어

의료기기 소프트웨어에 관한 규정은 Title 21 CFR 820.30과 820.70에 명시⁷⁶⁾되어 있

74) IRB(Investigational Review Board, 시험검토위원회)로, FDA규정에 따라 인간대상과 관련된 생물 의학 연구를 검토하고 모니터링하도록 공식적으로 지정된 그룹이다.

75) How to study and market your device, FDA

76) CDRH Software Regulation, John F Murray Jr.

다. 21 CFR 820.30에서 모든 Class II, III 기기 및 컴퓨터 소프트웨어로 자동화된 Class I 기기의 제조사는 명세되어 있는 설계 요구사항이 충족되는지를 확인하기 위하여 설계통제절차를 수립하고 유지 관리해야 하고, 설계검증은 적절한 경우 소프트웨어검증과 위험분석을 포함해야 한다고 규정하며, 생산 및 프로세스 통제 섹션인 21 CFR 820.70의 자동화된 프로세스 (i)항목에서, ‘컴퓨터 또는 자동화된 데이터 처리 시스템이 생산 또는 품질 시스템의 일부로 사용되는 경우, 제조사는 설정된 프로토콜에 따라 의도된 용도에 대해 컴퓨터 소프트웨어를 검증해야 한다. 모든 소프트웨어 변경은 승인 또는 발행 전에 검증되어야 한다. 이러한 검증활동과 결과는 문서화되어야 한다.’ 라고 규정되어 있다. 소프트웨어 관련 법 규정은 광범위한 용어로 작성되어 있으나, 의료기기 소프트웨어의 목적은 소프트웨어의 안전성과 유효성을 확인하기 위하여 소프트웨어 공학, 위험분석 및 품질시스템을 이용하여 설계되어야 한다는 의미이다.

FDA에서는 ‘의료기기에 포함된 소프트웨어에 관한 시판전 제출 내용지침⁷⁷⁾’ 을 제 공하여 의료기기 소프트웨어의 요구사항에 대한 설명을 부가했다. 이 지침에 따르면 한 개 이상의 소프트웨어 구성요소, 부품 또는 부속품을 포함하는 기기, 또는 “소프트웨어 기기” 로써 단독 소프트웨어로만 구성되어 있는 기기를 대상으로 하며, 의료기기의 펌웨어, 독립적인 소프트웨어 응용시스템, 일반적인 목적의 컴퓨터내에 설치되는 소프트웨어, 의료기기 전용 하드웨어/소프트웨어 및 소프트웨어로 구성된 의료기기 부속품 등이 해당한다. 이 안내지침은 소프트웨어 기기에 대한 모든 유형, 시판전 신고 510(k), 시판전 승인(Premarket Approval, PMA), Investigational Device Exemption(IDE, 임상시험 의료기기 적용면제), Humanitarian Device Exemption(HDE⁷⁸⁾, 인도적 의료기기 적용면제) 등 모든 유형의 시판전 제출 (Premarket Submission)에 적용된다.

시판전 제출에 포함되는 문서는 의료기기의 우려수준(Level of Concern)에 따라 달라 지는데, 우려수준이란 의료기기 고장, 설계 결함 또는 의도된 용도로 의료기기를 사용한 결과로, 환자 또는 작업자에게, 직접 또는 간접적으로 허용하거나 부과할 수 있는 상해의 심각도를 말한다. 의료기기의 우려수준과 소프트웨어 의료기기에 대해 제출할 것으로 권고하는 문서의 범위는 비례한다. 그러나 이러한 우려수준은 의료기기 분류 (Class I, II, III)나 위해/위험 분석과는 무관하다. FDA는 신청자가 당면한 위험에 대한

77)

<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm>
78) HDE(인도적 의료기기 적용면제): HUD(Humanitarian Use Device, 인도적 용도의 의료기기)에 관한 것으로, 미국 내 연간 4000명 이내 환자에게 영향을 끼치는 질병이나 상태의 진단과 치료를 위한 의료기기로써, PMA 신청과 유사한 규정이나 유효성 요구사항은 면제되어 있다.

완화 효과를 반영하기 전에 우려수준을 결정하기를 권고하고 제출서에 우려수준 (Major, Moderate, Minor)을 작성, 어떻게 도출되었는지, 즉, 의료기기 기능과 관련된 소프트웨어 작동이 환자나 작업자에게 끼치는 영향에 기반하여 설명할 것을 권고한다.

• Major Level of Concern

소프트웨어 고장이나 잠재적 결함이 직접적으로 환자나 작업자에게 사망이나 중상 (Serious Injury⁷⁹)을 입힐 수 있는 경우 심각한 수준으로 분류하고, 또한 부정확하거나 지연된 정보 또는 치료 제공자의 행동을 통해 간접적으로 환자 또는 작업자에게 사망 또는 중상을 입힐 수 있는 경우도 해당한다.

• Moderate Level of Concern

소프트웨어 고장이나 잠재적 결함이 직접적으로 환자나 작업자에게 경상을 입혔을 경우 보통 수준으로 분류하고, 또한 부정확하거나 지연된 정보 또는 치료 제공자의 행동을 통해 간접적으로 환자 또는 작업자에게 경상을 입힐 수 있는 경우도 해당한다.

• Minor Level of Concern

소프트웨어 고장이나 잠재결함이 환자나 작업자에게 어떠한 상해도 야기 시키지 않을 경우에는 우려가 거의 없는 수준인 Minor로 분류한다.

<표 2-16> 우려수준 기반의 문서요구사항

SW문서	Minor	Moderate	Major
우려수준	concern 레벨을 지시하는 서술과 각 레벨에 대한 근거 설명		
SW설명	기능 및 소프트웨어 운영 환경에 대한 요약 개요		
기기 위험 분석	심각도 평가 및 완화를 포함하여, 식별된 하드웨어/소프트웨어의 위험에 대한 표 양식의 설명.		
SW 요구사항 명세 (SRS)	SRS에서 기능 요구사항 요약	완전한 SRS 문서	
아키텍처 디자인차트	필수 문서 없음	기능단위, 소프트웨어 모듈단위의 상세 묘사 (차트와 같은 다이어그램 포함)	
SW 디자인 명세 (SDS)	필수 문서 없음	Software design specification(SDS) 문서	
추적성 분석	요구사항, 명세, 식별 위험 및 완화, V&V 테스트 간의 추적성		
SW 개발 환경 설명	필수 문서 없음	소프트웨어 생명주기 개발 계획 요약,	소프트웨어 생명주기 개발 계획 요약,

79) Serious Injury는 21 CFR 803.3(bb)(1)(2)에 정의되어 있으며, 본 보고서의 IEC 62304 (2)소프트웨어 안전 분류의 “심각한 상해” 와 동일하다.

		형상관리 및 유지보수 활동 포함	개발과정동안 생성된 통제문서의 주석목록, 형상관리 및 유지보수 계획 문서 포함
V&V 문서화 (Verification & Validation)	소프트웨어 기능 테스트계획, Pass/Fail 기준 및 결과	단위, 구현 및 시스템 레벨의 V&V 활동설명, 시스템 레벨 테스트 프로토콜, Pass/Fail 기준 및 결과레포트	단위, 구현 및 시스템 레벨의 V&V 활동 설명, 단위, 구현 및 시스템 레벨 테스트 프로토콜, Pass/Fail 기준 및 결과레포트, 요약, 결과
변경이력	변경이력로그, 배포버전 번호 및 날짜 포함		
미해결 이상 (버그/결함)	필수 문서 없음	연산 용법 및 인적 요소 포함한 안전성/효과성 영향에 대해 주석 설명을 첨부한, 잔여 소프트웨어 이상 목록	

자료: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, FDA website

SOUP(Software of Unknown provenance)에 대해서는, 소프트웨어의 출처와 소프트웨어 설명서와 관련된 상황을 설명하고, 위험 분석에는 누락, 불완전한 문서와 이전 테스트에 대한 문서의 부족에 관하여 SOUP과 관련된 위험이 포함되어야 한다. 그러나 의료기기에 대한 충분한 테스트, 소프트웨어 테스트계획 및 결과에 대한 적절한 문서의 제공 책임은 신청자에게 있다.

(4) Consensus Standards (합의표준)

많은 국내 및 국제적인 합의 표준들은 의료기기와 관련된 안전성/유효성 측면을 다루고 있고 이러한 표준들은 CDRH(Center for Devices and Radiological Health) 직원들의 참여로 개발되어 왔으며, 공인된 합의 표준들을 준수함으로써 의료기기의 다양한 적용 가능 측면에 대한 안전성과 유효성을 합리적인 확신을 뒷받침할 수 있기 때문에 CDRH는 의료기기 규제의 모든 영역에서 최소 부담 접근법을 고려하여 합의 표준의 사용과 승인을 지원하고 있다.

그래서 시판전 제출 과정을 간소화하기 위하여, 신청자는 FDA 공인 표준들을 이용할 수 있다. 특정 의료기기에 대한 완전한 수행 표준으로써 FDA 공인 표준들이 있을 때 합의 표준은 유용할 수 있으며, 공인된 합의 표준 준수는 엄격하게 의료기기 제조사가 자발적으로 수행하는 것이다. 제조사는 적용가능한 공인 표준들을 준수하거나 다른 방식으로 관련 문제를 다루기 위해서 선택할 수 있다.⁸⁰⁾

소프트웨어와 관련된 합의 표준의 등장은, 특히 위험 평가와 관리와 같은 중요한 활동과 관련하여, 소프트웨어 개발과 문서의 일관성과 품질을 향상시키는 데 도움을 주었으며, 소프트웨어 관련 안내지침의 용어나 권장사항은 ISO 14971과 같은 소프트웨어 관련 합의 표준과 조화되어 있다. 공인된 합의 표준은 FDA의 “Recognized Consensus Standards”에서 확인이 가능하며 의료기기 부문의 소프트웨어에 대한 표준은 IEC 62304를 포함하여 몇 가지 사용 가능하다.

[그림 2-10] FDA 공인 합의 표준 (소프트웨어)

Recognition Number	Standard Developing Organization	Standard Designation Number And Date	Title Of Standard	FR Publication Date	Specialty Task Group Area
13-87	IEC ISO	15026-2 First Edition 2011-02-15	Systems And Software Engineering - Systems And Software Assurance - Part 2: Assurance Case	12/23/2016	Software/Informatics
13-86	IEC ISO	15026-1 First Edition 2013-11-01	Systems And Software Engineering - Systems And Software Assurance - Part 1: Concepts And Vocabulary	12/23/2016	Software/Informatics
13-85	CLSI	AUTO11-A2	Information Technology Security Of In Vitro Diagnostic Instruments And Software Systems: Approved Standard - Second Edition	12/23/2016	Software/Informatics
13-79	IEC	62304 Edition 1.1 2015-06	Medical Device Software - Software Life Cycle Processes	04/04/2016	Software/Informatics
13-65	ANSI UL	1998 Third Edition 2013	Standards For Safety Software In Programmable Components, Second Edition. [This Standard Contains Revisions Through And Including October 28, 2008]	07/09/2014	Software/Informatics
13-59	IEC ISO	15026-4 First Edition 2012-10-01	Systems And Software Engineering - Systems And Software Assurance - Part 4: Assurance In The Life Cycle	08/05/2013	Software/Informatics
13-36	AAMI	TIR 45:2012	Guidance On The Use Of AGILE Practices In The Development Of Medical Device Software	01/15/2013	Software/Informatics
13-34	IEC	/TR 80002-1 Edition 1.0 2009-09	Medical Device Software - Part 1: Guidance On The Application Of ISO 14971 To Medical Device Software	01/15/2013	Software/Informatics
13-33	AAMI	TIR 36:2007	Validation Of Software For Regulated Processes	01/15/2013	Software/Informatics
13-32	AAMI ANSI IEC	62304:2006	Medical Device Software - Software Life Cycle Processes	08/20/2012	Software/Informatics
13-15	CLSI	AUTO13-A2 (Formerly GP19-A2)	Laboratory Instruments And Data Management Systems: Design Of Software User Interfaces And End-User Software Systems Validation, Operation, And Monitoring: Approved Guideline - Second Edition	07/09/2014	Software/Informatics

자료: Recognized Consensus Standards, FDA website, Sept 2016

특정 기기는 공인된 합의 표준에서 다루지 않는 문제를 야기할 수도 있다. 즉, FDA에서 제정한 표준은 의료기기가 충족시켜야 하는 추가적인 요구사항을 부과할 수도 있으므로, 신청서에 한 개 이상의 합의 표준에 대한 제조사의 적합성 선언이 포함된 경우 검토자는 안전성과 유효성을 평가하기 위해 FDA의 다른 모든 필요정보가 포함되었다는 것을 확인하기 위하여 시판전 제출을 검토해야 한다.

(5) Digital Health

범위한 디지털 건강 범위에는 모바일 건강 (mHealth), 건강 정보 기술 (IT), 웨어러블

80) Guidance for Industry and FDA Staff - Recognition and Use of Consensus Standards, FDA

장치, 텔레 헬스 및 원격 의료, 맞춤형 의학 등의 범주가 포함된다. 스마트폰, 소셜 네트워크, 인터넷 응용시스템과 같은 기술을 사용하는 것은 의사소통방법을 변화시킬 뿐 아니라 건강과 복지를 모니터링하고 정보에 더 많은 접근을 제공하는 혁신적인 방법을 제공한다. 이러한 발전으로 사람, 정보, 기술과 연결이 융합하여 헬스케어와 헬스결과를 개선되고 있다. 이에 CDRH(Center for Devices and Radiological Health)는 이러한 발전과 연결성과 의료기기의 융합, 소비자 기술에 관심을 가지고 무선의료기기, 모바일 의료앱, 헬스IT, 원격의료, 의료기기상호운영 등의 주제에 대해 연구했다.⁸¹⁾

그 중, 본 보고서에는 2013년에 발행되고 2015년에 재발행된 모바일 의료앱에 대한 안내지침을 소개하겠다.⁸²⁾

모바일 의료앱(Mobile Medical Application)은 FFD&C Act의 section 201(h)에 있는 기기의 정의를 충족하는 모바일 앱으로써, 규제되는 의료기기에 부속품으로 사용되거나, 모바일 플랫폼⁸³⁾을 규제된 의료기기로 전환하도록 의도된 모바일 앱이다. 모바일 앱의 의도된 용도가 질병 또는 기타 조건의 진단, 질병의 완치, 완화, 치료 또는 예방을 위한 것이거나 신체의 구조 또는 기능에 영향을 미치기 위한 의도이면, 모바일앱은 장치(기기)이다. FDA의 감독 접근법은 전통적인 기기의 기능성에 초점을 두는 것과 마찬가지로, 모바일앱에 대해서도 앱이 기동하는 모바일 플랫폼에 상관없이 모바일 앱의 기능성에 초점을 두고 있다. 그래서 모바일 앱이 의도한대로 작동하지 않을 경우, 기능이 환자의 안전을 위협할 수 있는 모바일앱에만 감독 권한을 적용한다.

FDA는 장치의 정의를 충족하는 모바일앱 제조사들이 모바일 의료앱의 설계와 개발의 품질시스템 요구사항을 준수하고 환자과 사용자의 상해를 방지하기 위해 모바일앱에 즉각적인 시정조치를 수행하도록 권고한다. 모바일 의료앱에 대해 제조사는 적용가능한 기기 분류와 관련된 요구사항을 충족해야 한다. 모바일 의료앱이, 단독으로, 의료기기 분류에 속하는 경우, 제조사는 그 분류와 관련된 요구 사항을 준수해야한다. 다른 의료기기와 마찬가지로, 모바일 의료앱 또한 Class I (일반지침), Class II (일반지침과 특수지침) 또는 Class III (시판전 승인)으로 분류된다.

모바일 의료앱 중, FDA의 규제감동의 초점이 되는 모바일앱의 부분집합으로는,

첫째, 기기를 제어하는 목적이나 활동적인 환자의 모니터링 또는 의료기기데이터를

81) Digital Health, FDA website, 2017

82) Mobile Medical Applications, Guidance for industry and food and drug administration staff, CDRH, sept 2015

83) 모바일 플랫폼은 핸드헬드형의 유무선, COTS(commercial off-the-shelf) 컴퓨팅 플랫폼으로 정의되며 스마트폰, 태블릿 또는 휴대용 컴퓨터가 포함된다.

분석 용도의 장비에 연결하여 한 개 이상의 의료기기를 확장하는 모바일앱이고,

둘째, 첨부파일, 화면, 센서 사용 또는 현재 규제된 의료기기와 유사한 기능을 포함하여 모바일 플랫폼을 규제된 의료기기로 전환시키는 모바일앱으로써, 이러한 모바일 앱은 변형된 플랫폼과 관련되어 있는 기기 분류를 준수해야 한다.

마지막으로, 환자-특화된 분석을 수행하고 환자-특화된 진단이나 치료권고사항을 제공하여 규제된 의료기기(소프트웨어)가 되는 모바일앱인데, 이것은 앞서 510(k) 또는 승인을 받은 소프트웨어 기기 유형과 유사하거나 같은 기능을 수행하는 형태의 모바일 의료앱이다.

다음은 FDA가 집행재량권을 행사할 의도를 가진 모바일 앱(FDA가 FD&C Act에 따라 요구사항을 시행하려는 의도가 없음)으로 7가지 모바일앱을 안내지침에 정의했다.

1) 일상환경에서 환자가 자신의 건강을 관리하는데 도움이 되도록 코치하거나 촉진하기 위해 보조적인 임상진료를 제공하거나 촉진하는 모바일앱.

2) 환자들의 건강정보를 구성하고 추적하기 위해 간단한 툴을 제공하는 모바일앱

3) 환자의 건강상태와 치료와 관련한 정보에 쉬운 접근성을 제공하는 모바일앱 (의료참조의 전자 복사 제공 제외)

4) 환자가 잠재적인 의료상태를 문서화, 제시하거나 의사소통하는 것을 돕기 위해 특별히 판매되는 모바일앱

5) 임상사례에 사용되는 단순한 계산 수행 모바일앱

6) 개인이 PHR(Personal Health Record)/EHR(Electronic Health Record)시스템과 상호작용하게 하는 모바일앱.

7) 의료기기데이터시스템의 정의를 충족하는 모바일앱.

모바일 의료앱 제조사는 모바일 의료앱의 분류(Class I, II, III)와 관련규제에 따라 규제에 수립된 관련 지침을 준수해야 하며, 이에 대해서는 앞의 (2) 의료기기 규정 (Title 21, Code of Federal Regulations)과 동일하다.

미국의 의료부문 안전 활동을 요약하자면, 미국 FDA는 FFD&C Act(연방 식품/의약품/화장품법)에 따라 의료기기의 안전성과 유효성을 검토하고 시판전 신고에 대한 Clearance와 시판전 승인(Approval)은 선언한다. 이러한 의료기기의 요구사항은 의료기기의 사용용도와 위험정도에 따라 Class I, II, III으로 분류되어 있다. 중요한 인증 과정

으로, 시판전 신고 510(k), 시판전승인(Class III에 해당)과 IDE(임상시험 의료기기의 적용면제) 등이 있다. 의료기기의 검토와 승인은 FDA 산하의 CDRH에서 수행하고 있고 신청자(제조사)의 부담을 최소화하기 위한 접근 방법으로 IEC 62304와 같은 FDA 공인된 합의 표준 (Consensus Standards)를 운영하고 있으며 제조사가 자발적으로 선택하고 표준을 준수할 것을 권고한다. 컴퓨터의 발전과 기기와의 연결성 등으로 의료기기에 많은 변화가 일어나고 있으며, 최근에 지침이 발행된 모바일 의료앱에 대하여 FDA는 모바일 의료앱의 용도와 환자 건강에 대한 위험성에 따라서 규제 감독 대상을 지정하였고, 다른 의료기와 동일한 규제 요구사항을 적용하여 모바일 의료앱 제조사가 이를 준수하도록 규제하고 있다.

3) 유럽 의료 안전 활동

유럽에서 의료기기의 안전성과 성능에 관한 규정은 법규정 원칙에 대한 새로운 방식에 따라 1990년에 조화(harmonised)되었으며 주요한 법률적인 프레임워크는 Council Directive 90/385/EEC on Active Implantable Medical Devices (AIMDD) (1990), Council Directive 93/42/EEC on Medical Devices (MDD) (1993), Council Directive 98/79/EC on In Vitro Diagnostic Medical Devices (IVDMD) (1998)의 3가지의 지침으로 구성된다. 이 지침의 목표는 인간 건강과 안전에 대한 높은 수준의 보호와 단일 시장의 기능을 보장하는 것이다. 본 보고서에서는 MDD를 기준으로 유럽의 의료기기 안전 규정에 대해서 설명하였고 의료기기로서의 소프트웨어에 대한 가이드를 추가하였다.

(1) Medical Device Directive (93/42/EEC) 개요

유럽공동체이사회(The Council of European Communities)는 유럽경제공동체의 조약과 위원회의 제안을 고려하고 유럽 의회와 협력하고 경제/사회 위원회의 의견을 참조하여 Council Directive 93/42/EEC on Medical Devices (MDD) (1993) (의료기기에 관한 지침)를 채택하였다. 재화, 인력, 서비스와 자본의 자유로운 이동을 보장하는 내부 국경이 없는 지역인 내부시장(Internal Market)의 측면에서 안전성, 건강 보호 및 의료기기의 성능 특징에 대해 회원국(Member States)의 법, 규정, 조항의 내용과 범위가 다르고 장비에 대한 인증 및 검사 절차가 서로 다르며, 이러한 불균형이 공동체 내에 거래장벽을 만들기 때문에, 의료기기 사용에 대하여 내부시장내 의료기기의 자유로운 거래를 보증하기 위하여 환자와 사용자, 적절한 경우 다른 사람의 안전과 건강 보호를 위

한 국가 조항이 조화(Harmonized)되어야 할 필요가 있었다. 조화된 조항들(Harmonized Provisions)은 의료기기에 직간접적으로 관련된 공공보건과 질병보험의 자금관리를 위해서 회원국에서 채택한 조치 방법과는 구별되어야 한다.

반면, 필수 요구 사항을 준수하고 적합성을 검증하기 위해서는 의료 기기의 설계, 제조 및 포장과 관련된 위험으로부터 보호하기 위해 유럽 표준을 조화시키는 것이 바람직하였고, 그러한 조화된 유럽 표준은 민영화된 단체에 의해 작성되며, 유럽 표준위원회(CEN)와 유럽전기표준화위원회 (Cenelec)가 위원회와 이 두 기구 간의 협력에 관한 일반 지침에 따라 조화된(harmonized) 표준 채택에 권한 있는 기관으로 인정된다.

이사회는 기술적 조화 지침에서 사용되도록 의도된, 적합성 평가 절차의 다양한 단계 모듈에 관한 1990년 12 월 13일의 90/683/EEC 지침에서 조화된(harmonized) 적합성 평가 절차를 규정했고, 의료 기기도 이러한 모듈 적용에 따라 관련 기기의 유형에 근거한 적합성 평가 절차 동안 제조사와 공인기관의 책임이 결정된다. 모듈에 추가되는 상세사항은 의료기기에 필요한 검증 성격에 의해 결정된다.

적합성 평가 절차를 위해서 의료기기를 4가지 제품 Class로 구분하는 것이 필요하다. 분류 규칙은 의료기기의 기술적인 설계 및 제조와 관련된 잠재적인 위험을 감안한 인체의 취약성에 근거한 것이다. Class I 의료기기의 적합성 평가 절차는 일반적인 규칙으로써 취약성이 가장 낮은 수준으로 제조사 자체의 책임하에 수행된다. Class IIa 의료기기에 대해 생산단계에서 인증기관(Notified body)이 강제적으로 개입되어야 하고, 잠재적인 위험이 높은 Class IIb, III 의료기기에 대하여 의료기기의 설계와 제조단계에서 인증기관(Notified body)의 검사가 필요하다. Class III는 시장에 출시하기 위하여 적합성에 관한 명백한 사전 승인을 요구하는 가장 중요한 의료기기에 배정된다.

의료기기에는 법적인 요구사항을 충족한다는 것을 지시하고 EEA(Europe Economic Area, 유럽 경제 지역)에서 자유롭게 유통하고 의도된 목적대로 사용될 수 있도록 CE 마크를 부착해야 한다. 제조사, 다른 경제운영자, 적합성평가기관들은 제품, 서비스, 절차가 관련된 EU 법규에 부합한다는 것을 입증하기 위해 조화된 표준을 사용할 수 있다. 의료기기부문(MDD)에서 소프트웨어 관련 조화된 표준 목록⁸⁴⁾은 EU의 홈페이지에서 확인이 가능하다.

84)

https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en

(2) 용어 정의

의료기기(Medical Device)는 “진단 그리고/또는 치료 목적으로 특별히 사용되며 적절한 적용을 위해 제조사가 의도한 소프트웨어를 포함하여, 단독으로 또는 조합하여 사용되는 모든 기기, 장치, 도구, 소프트웨어, 재료 또는 기타 제품을 의미한다.

부속품(Accessory)은 기기 제조사가 의도한 기기의 사용에 따라 사용될 수 있도록 함께 사용되도록 고안된, 그러나 기기가 아닌, 물품을 의미한다.

맞춤형 기기(Custom-made device)는 특별 환자 단독 사용을 목적으로 특정 설계 특성을 부여하고 정당한 자격을 갖춘 의료 행위자의 서면 처방에 따라, 그의 책임하에 특별히 제작된 기기를 의미한다.

제조자(Manufacturer)는 기기가 자신의 이름으로 시장에 출시되기 전에 기기의 설계, 제조, 포장 및 라벨링에 대한 책임이 있는 자연인이나 법인을 의미하며, 이러한 작업을 자신이 직접하는지 본인을 대신하여 제3자가 수행하는지는 관계없다.

(3) 규칙에 따른 분류

의료기기는 MDD의 부속서 IX에 나와 있듯이, 18가지 규칙(Rule)에 따라 Class I, IIa, IIb, III의 4가지로 분류된다. 규칙(Rule)은 지속시간(Duration⁸⁵)과 침습성기기(Invasive Device), 재사용외과도구(Reusable surgical instrument) 등을 포함하여 8가지 분류기준과, 아래의 6가지 구현 규칙에 따라 정의된다.

- 1) 분류 규칙 적용은 기기의 의도된 용도에 의해 규율된다.
- 2) 기기가 다른 기기와 함께 사용되도록 의도된 경우, 분류 규칙은 각각 기기에 분리되어 적용되며, 부속품 또한 사용되는 기기와 분리하여 자체적으로 분류된다.
- 3) 기기를 구동, 기기사용에 영향을 주는 소프트웨어는 기기와 같은 등급에 속한다.
- 4) 기기가 신체의 특정 부분에서 단독으로, 주로 사용되는 의도가 아닌 경우, 가장 중요한 특정 용도를 기반으로 분류되어야 한다.
- 5) 제조자가 기기에 대해 지정한 성능을 기준으로 동일한 기기에 여러 규칙이 적용되는 경우, 더 높은 등급이 되게 하는 가장 엄격한 규칙이 적용된다.
- 6) 지속시간 계산시, 지속적인 사용이란 의도된 목적을 위해 기기를 중단없이 사용하

85) Duration은 Transient(60초이내), Short term(30일이내), Long Term(30일초과)로 구분한다.

는 것을 의미한다. 기기를 같거나 동일한 기기로 즉시 교체하기 위해 기기를 중단한 경우는 기기의 연속 사용의 연장으로 간주한다.

〈표 2-17〉 규칙에 따른 의료기기 분류

구분	규칙	분류
비침습성 기기	Rule 1	Class I: 다른 규칙에 적용 안 될 경우.
	Rule 2	Class IIa: 최종 주입, 투여 또는 신체 내 주입용으로 혈액, 체액 또는 조직, 액체 또는 가스를 흘려보내거나 저장하도록 의도된 모든 비 침습성 장치
		Class I: Class IIa와 그 이상의 Class의 Active 기기 연결용 혈액/체액의 채널링/보관용, 장기/장기일부/신체조직 보관용
	Rule 3	Class IIb: 인체에 주입하기 위하여 혈액/체액을 생물학적/화학적으로 변경하기 위한 용도. - Class IIa: 위의 경우에 처리가 여과, 원심분리, 기체/열 교환으로 구성되지 않을 경우.
Rule 4	상처 난 피부와 접촉하는 모든 비침습성 기기에 대해, - Class I: 삼출물 압착/흡수를 위해 기계적 장벽으로 사용 - Class IIb: 진피를 침범한 상처에 주로 사용되고 2차 의도로만 치유될 수 있는 경우. - Class IIa: 주로 상처의 미세환경 관리 용도를 포함하여 그 외 모든 경우.	
침습성 기기	Rule 5	외과 침투성 장치를 제외한 신체 구강과 관련하여 Active 의료기기와 연결용도가 아니거나 Class I의 Active 의료기기와의 연결용도인 모든 침습성기기에 대해, - Class I: 일시적인 사용 목적인 경우 - Class IIa: 단기간 사용 목적인 경우 - Class I: 단기간이나 구강에서 인두까지, 외이도부터 고막까지, 비강에 사용되는 경우. - Class IIb: 장시간 사용 목적인 경우. - Class IIa: 장시간 사용하나, 구강에서 인두까지, 외이도부터 고막까지, 비강에 사용되고 점막에 흡수될 것 같지 않는 경우.
	Rule 6	Class IIa: 아래의 용도를 제외하고, 일시적 사용 목적의 모든 외과적 침습성 기기 - Class III: 신체 부분과 직접 접촉하여 심장 또는 중앙순환계의 결함을 제어, 진단, 감시, 교정하기 위해 특별히 고안된 기기. - Class III: 특히, 중추신경계와 직접 접촉에 사용되는 기기 - Class IIb: 이온화방사선형태의 에너지 공급용 기기 - Class IIb: 생물학적 효과를 가지거나 전적/주로 흡수되기

		<p>위한 목적</p> <ul style="list-style-type: none"> - Class IIb: 적용방식을 고려하여 잠재적으로 위험한 방식으로 수행되는 경우, 전달체계의 수단으로 약물을 투여하기 위해 고안된 기기 - Class I: 재사용이 가능한 수술도구
	Rule 7	<p>Class IIa: 아래의 용도를 제외하고, 단기간 사용 목적의 모든 외과적 침습성 기기</p> <ul style="list-style-type: none"> - Class III: 신체 부분과 직접 접촉하여 심장 또는 중앙순환계의 결함을 제어, 진단, 감시, 교정하기 위해 특별히 고안된 기기. - Class III: 특히, 중추신경계와 직접 접촉에 사용되는 기기 - Class III: 생물학적 효과를 가지거나 전적/주로 흡수되도록 고안된 기기 - Class IIb: 이온화방사선형태의 에너지 공급용 기기 - Class IIb: 기기를 치아에 배치하는 것을 제외하고, 신체에 화학적 변화를 일으키거나 또는 약물을 투여할 목적
	Rule 8	<p>Class IIb: 아래의 용도를 제외하고, 모든 이식 가능한 기기와 장시간 사용되는 외과적 침습성 기기.</p> <ul style="list-style-type: none"> - Class IIa: 치아 이식 목적 - Class III: 심장, 중앙순환계, 중추신경계에 직접 접촉하여 사용 - Class III: 생물학적 효과를 가지거나 전적으로/주로 흡수되도록 고안된 기기 - Class III: 기기를 치아에 배치하는 것을 제외하고, 신체에 화학적 변화를 일으키거나 또는 약물을 투여할 목적
작동 기기에 적용 가능한 추가 규칙	Rule 9	<p>Class IIa: 에너지를 주입하거나 교환하도록 의도된 모든 능동형 치료기기.</p> <p>Class IIb: 위의 특성이 에너지의 성질, 밀도, 적용 부위를 고려했을 때 잠재적으로 위험이 있는 방식으로 인체에 또는 인체로부터 에너지를 주입하거나 교환하는 경우.</p> <p>Class IIb: 능동형 치료기기의 성능을 제어 또는 감시하는 목적의 모든 능동형 기기. 직접적으로 이러한 기기의 성능에 영향을 미치는 능동형 기기.</p>
	Rule 10	<p>Class IIa: 진단용 능동형 기기</p> <ul style="list-style-type: none"> - 가시광선 스펙트럼에서 인체에 흡수될 에너지를 공급할 의도인 경우, 환자의 신체를 비추는데 사용되는 기기는 제외. - 방사선의약품의 생체내 분포를 이미지화하는 기기 - 생리학적 과정을 직접 진단하고 모니터링할 목적인 경우, <p>Class IIb: 특히, 생체생리학적 매개변수를 모니터링하기 위한 목적인 경우, 변화의 성격이 심장기능, 호흡과</p>

		중추신경계 활동 등 환자에게 직접적인 위험을 일으킬 수 있는 경우. Class IIb: 이온화방사선을 방출하고 진단/치료의 중재적 영상의학 목적으로 하는 기기. 그러한 기기를 제어하고 모니터링하며 직접 성능에 영향을 끼치는 기기 포함.
	Rule 11	Class IIa: 의약품, 체액 또는 기타 물질을 인체에 투여 또는 제거하는 모든 능동형 기기 (아래방식 제외) - Class IIb: 관련된 물질의 성질, 해당 신체 부분과 적용 모드를 고려했을 때 잠재적으로 위험이 있는 경우.
	Rule 12	Class I: 그 외 모든 능동형 기기
특별 규칙	Rule 13	Class III: 별개로 사용된다면 의료제품으로 간주될 수 있고 기기에 보조적인 역할로 인체에 작용할 것 같은 구성요소/물질로 혼합시키는 모든 기기. 구성요소로서 혈액제제를 혼합시키는 모든 기기
	Rule 14	Class IIb: 피임 또는 성병전염예방을 위한 모든 기기 Class III: 위의 기기가 이식가능하거나 장시간 침습성기기인 경우.
	Rule 15	Class IIb: 콘택트렌즈를 소독, 세척, 행굼, 적절한 경우 하이드레이팅하기 위해 사용되는 모든 기기 Class IIa: 의료기기 소독에 사용되는 모든 기기 Class IIb: 침습성 기기 소독에 사용되는 기기 물리적 조치를 통해 콘택트렌즈 외에 의료기기를 세척할 의도인 제품에는 적용되지 않는다.
	Rule 16	Class IIa: X-ray 진단 이미지를 기록하는 기기
	Rule 17	Class III: 동물조직이나 derivatives rendered non-viable를 활용하여 제조된 모든 기기, 해당기기가 손대지 않은 피부에만 접촉하는 경우 제외.
	Rule 18	Class IIb: 혈액 백(Blood Bags)

(4) 적합성 평가 절차 (conformity Assessment Procedure)

측정기능이 없고 멸균하지 않는 Class I 의료기기만 인증기관(Notified body)의 참여가 필요하지 않다. 해당기기의 제조자는 자신의 책임아래 번호가 부여되지 않는 CE 마크를 부착하고 다른 모든 기기는 제조자가 인증기관(Notified body)의 번호가 있는 CE 마크를 부착하기 전에 인증기관의 인증이 필요하다. 기기의 분류에 따라 제조자는 여러 가지 인증 경로를 선택하고 보통 인증절차는 아래와 같다.

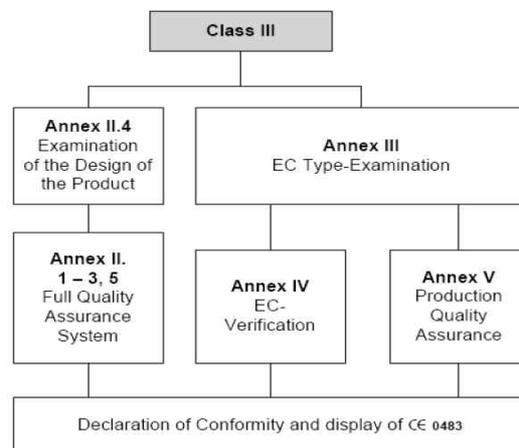
- 제품이 의료기기인지, 유럽의 MDD 범위 내에 있는 것인지 결정하고,

- 제조자가 기기를 분류한다.
- 인증기관(Notified body)과 접촉하여 사전 토론, 정보 교환 및 인증기관(Notified body)을 선택한다.
- 선택한 인증기관(Notified body)은 특정 질의응답을 수행하고 기기분류를 확정하여 다양한 인증경로를 평가하며 제조자는 인증 경로를 선택한다.
- 공식적인 신청 및 인증 계약을 수행한다.
- 인증기관(Notified body)에 문서를 제출한다.
- 제출된 문서와 보고서를 평가하며,
- 제조자의 운영, 필요시 공급업체/부계약자의 시설을 평가한다.
- 인증을 결정하고 관련된 인증서(보통 5년 유효)를 발행한다.
- 주기적인 감시 평가를 수행하고,
- 보통 5년 이후 전체적인 재평가를 실시하고 신규 인증서를 발행한다.

가. Class III에 속하는 의료기기

맞춤형 기기 또는 임상 시험 목적의 기기를 제외하고, 제조자는 CE 마크를 부착하기 위하여, MDD의 부속서 II (full quality assurance)의 EC 적합성 선언을 따르거나, 부속서 IV의 EC 검증(verification)이나 부속서 V (production quality assurance)의 EC 적합성 선언과 함께 부속서 III의 EC 형식검사(type-examination)와 관련된 절차를 따라야 한다.

[그림 2-11] Class III의 적합성 평가 절차

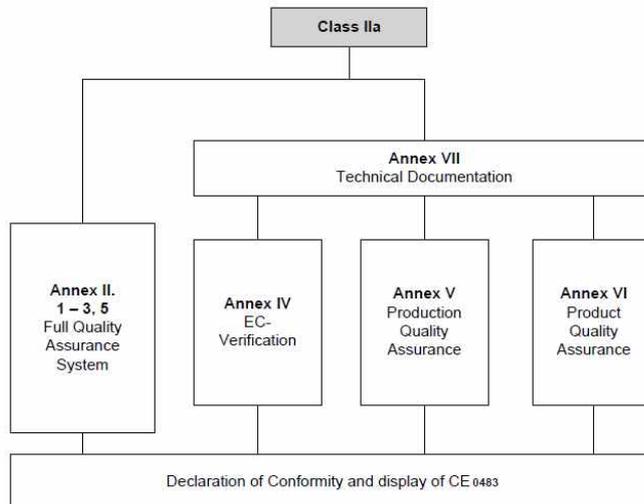


자료: Basic Information about the European Directive 93/42/EEC on Medical Devices, mdc, 2009

나. Class IIa에 속하는 의료기기

맞춤형 기기 또는 임상 시험 목적의 기기를 제외하고, 제조자는 CE 마크를 부착하기 위하여 MDD의 부속서 IV의 EC 검증(verification)이나 부속서 V (production quality assurance)의 EC 적합성 선언, 부속서 VI (product quality assurance)의 EC 적합성 선언과 관련된 절차와 함께, 부속서 VII의 EC 적합성 선언 절차와 관련된 절차를 따라야 한다. 또는 이러한 절차를 적용하는 대신에, 제조자는 부속서 II (full quality assurance)의 EC 적합성 선언과 관련된 절차를 따를 수도 있다. 이 경우에 부록 II.4는 적용가능하지 않다.

[그림 2-12] Class IIa의 적합성 평가 절차

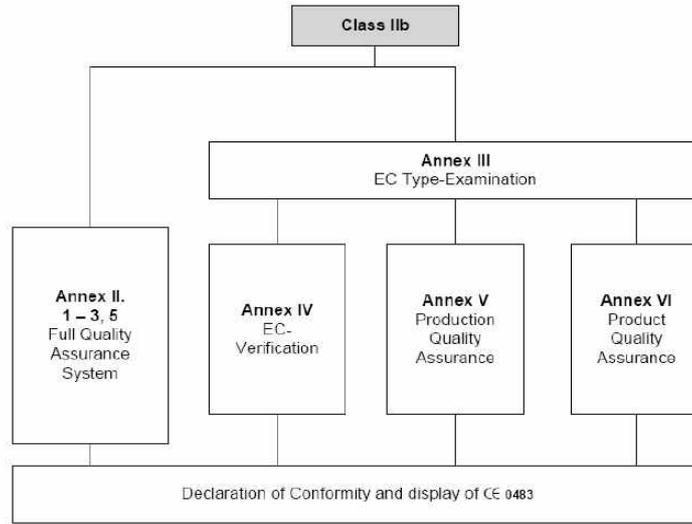


자료: Basic Information about the European Directive 93/42/EEC on Medical Devices, mdc, 2009

다. Class IIb에 속하는 의료기기

맞춤형 기기 또는 임상 시험 목적의 기기를 제외하고, 제조자는 CE 마크를 부착하기 위하여 MDD의 부속서 II (full quality assurance)의 EC 적합성 선언과 관련된 절차를 따를 수도 있다. 이 경우에 부록 II.4는 적용가능하지 않다. 또는, 부속서 IV의 EC 검증(verification)이나 부속서 V(production quality assurance)의 EC 적합성 선언, 부속서 VI(product quality assurance)의 EC 적합성 선언과 관련된 절차와 함께, 부속서 III의 EC 형식검사(type-examination)와 관련된 절차를 따라야 한다.

[그림 2-13] Class IIb의 적합성 평가 절차

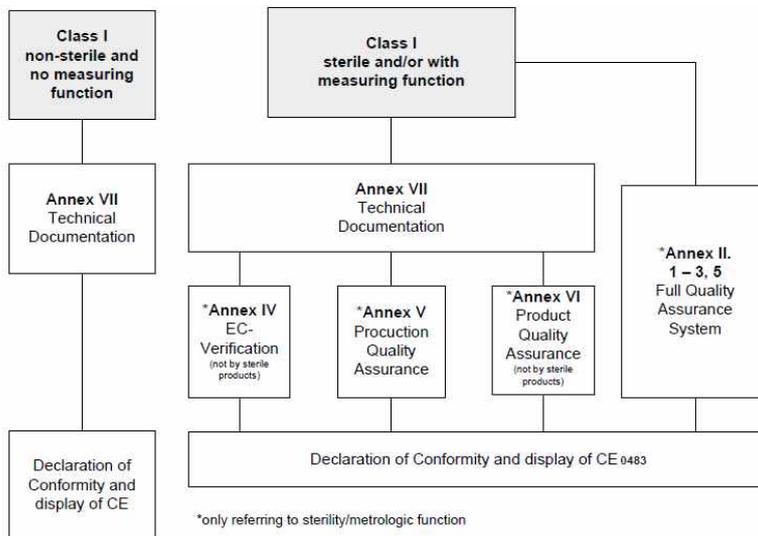


자료: Basic Information about the European Directive 93/42/EEC on Medical Devices, mdc, 2009

라. Class I에 속하는 기기의 경우, 맞춤형 기기 또는 임상 시험 목적의 기기를 제외하고, 제조자는 CE 마크를 부착하기 위해 부속서 VII에 언급된 절차를 따르고 기기를 시장에 출시하기 전에 필요한 EC 적합성 선언서를 작성해야 한다. 멸균 상태로 출시되고 측정기능을 가진 Class I 의료기기에 대해서, 제조자는 부속서 VII에 언급된 절차 뿐 아니라, 부속서 II, IV, V, VI에 관련된 절차 중 하나를 따라야 한다.

맞춤형 기기의 경우, 제조자는 부속서 VIII의 절차를 따르고 시장에 출시하기 전에 부속서 VIII에 명시된 진술서를 작성해야 한다. 제조자는 회원국의 영역내에 서비스를 제공하는 기기 목록을 관할당국에 제출해야 한다.

[그림 2-14] Class I의 적합성 평가 절차



적합성 선언에 대한 절차는 MDD의 부속서 II~VII에 제시되고 있다.

<표 2-18> MDD의 부속서

부속서	내용
부속서 II	<p><u>EC 적합성 선언(전체 품질보증 시스템)</u></p> <ul style="list-style-type: none"> - 새로운 장치의 설계단계 또는 기존 장치의 변경을 포함한 전체 품질 시스템을 언급하는 가장 포괄적인 적합성 평가 절차. - 부속서의 Section 4. 제품설계검사는 Class III 기기에만 적용되며, - - 부속서 III의 EC 형식검사와 유사하나, 부속서 II는 제조자 자신의 전체 품질경영체계에서 얻은 사내 테스트결과가 인증의 근거로 사용될 수 있다는 차이가 존재함.
부속서 III	<p><u>EC 형식검사(Type-examination)</u></p> <ul style="list-style-type: none"> - 의료기기의 대표 샘플 검사와 제3자 테스트 및 지침의 필수요건을 충족한다는 인증을 포함하는 제품 설계에 대한 적합성 평가 절차 - 인증기관은 EC 형식검사 인증서 발행함. - Class IIb , III 의료기기에만 적용가능.
부속서 IV	<p><u>EC 검증(Verification)</u></p> <ul style="list-style-type: none"> - 제조공정이 EC 형식검사 인증에 설명된 형식과 지침의 요구사항을 준수하는 제품을 생산한다는 것을 입증 - 인증기관(Notified body)은 모든 기기의 검사/테스트를 수행하는 적합성 평가 절차. (제조자가 같은 종류의 배치를 제조하는 경우 통계적 기준을 근거로 기기를 검사/테스트함) - 인증기관(Notified body)은 각 승인받은 제품에 식별번호를 부착하고 수행테스트에 대한 적합성 인증을 서면으로 작성함. - Class IIa , IIb and III 적용가능.
부속서 V	<p><u>EC 적합성 선언(생산 품질보증)</u></p> <ul style="list-style-type: none"> - 관련 제품의 제조(생산)를 위해 승인된 품질 시스템을 적용하고 최종검사를 수행한다는 것을 보증하는 절차. - Class IIa 멸균기기에 가장 적합하고, 부속서 III와 결합하여 Class IIb, III 기기에도 적용가능.
부속서 VI	<p><u>EC 적합성 선언 (제품 품질보증)</u></p> <ul style="list-style-type: none"> - 제품의 최종검사와 테스트에 대해 승인된 품질 시스템을 적용한다는 것을 보증하는 절차. - 멸균과 같이 유효성 확인이 필요한 특수 제조공정을 포함하는 기기에는 적합하지 않으며, Class III 제품에 사용되지 않음.
부속서 VII	<p><u>EC 적합성 선언</u></p> <ul style="list-style-type: none"> - 제조자가 직접 기기의 적합성 선언. - Class I 기기에 적합, 부속서 IV, V, VI과 결합된 Class IIa에 필요.

(5) 인증기관(Notified Body)

인증기관(Notified Body)에 관한 규정은 MDD(Medical Device Directive)의 Article 16. 인증기관(Notified Body)에 상세하게 규정되어 있다. 이에 따르면, 회원국(Member State)은 Article 11(Conformity assessment procedures)에 규정된 절차와 그 기관에 지정된 특정 임무를 수행하기 위해, 회원국이 지정한 기관을 위원회와 다른 회원국들에게 통보해야 하고 위원회는 이러한 기관들에게 고유번호를 부여해야 한다. 이러한 기관을 Notified Body라고 명명한다. 그리고 위원회는 the Official Journal of the European Communities에 인증기관(Notified Body)에 부여된 고유번호와 업무와 함께 Notified Body 목록을 발행⁸⁶⁾하고 최신으로 유지해야 한다.⁸⁷⁾ 인증기관(Notified Body)은 EU 또는 다른 제3국에서 설립된 제조사에도 통보되므로 적합성 평가 서비스를 제공하는데 자유로우며, 다른 국가 지역에서도 자신의 직원이나 부계약자와 이러한 활동을 수행할 수 있다.

인증기관(Notified Body)은 관할당국(Competent Authorities)에게 모든 발행, 변경, 보완, 중단, 철회, 거부된 인증서를 통보해야 하고, 요청이 있을 경우 다른 인증기관(Notified Body)들에게도 통보해야 한다. 따라서 요청에 따라 인증기관(Notified Body)은 모든 추가적인 관련 정보를 사용할 수 있도록 해야 한다. 인증기관(Notified Body)은 기관의 직원, 시설 또는 부계약자의 추가나 변경이 발생할 경우에 관할당국에 즉시 보고해야 한다. 또한 인증기관(Notified Body)은 고객과 다른 이해관계자들에게 제 3자로서 독립성을 유지해야 한다.⁸⁸⁾

관할당국은 인증기관(Notified Body)을 지정하는 책임을 가지고 있는데, 지정 전에 먼저 후보에 대해, 인증기관(Notified Body)이 갖추어야 하는 기준, 일반적인 요구사항으로 MDD에서 요구하는 적합성 평가의 자원 제공, 독립성 요건, 공정성, 실력, 내부 절차와 시설, 비밀유지, 책임 보험 등 요구사항을 충족하는지를 확인하기 위해 사전 평가를 수행해야 한다. 요구사항을 충족하여 인증기관(Notified Body)으로 지정을 하면 위원회와 다른 회원국에 통보해야 한다. 그리고 관할당국은 인증기관(Notified Body)에 대해 초기 평가와 감시 평가를 수행한다. 초기 평가는 모든 운영활동을 포함하고 감시 평가는 특정운영활동에 대해서 수행되며 감시 평가는 최소 18개월마다 수행한다. 관찰

86) NAMDO(New Approach Notified and Designated Organizations)에서 제공하고 있다.
<http://ec.europa.eu/growth/tools-databases/nando/index.cfm>

87) Medical device directive의 article 16

88) Basic Information about the European Directive 93/42/EEC on Medical Devices, mdc, 2009

평가(Observed Audit)는 최소 18개월마다 인증기관(Notified Body)이 제조사의 사이트에서 디자인 검토, 테스트, 수행하는 EC 적합성 선언, 승인 등의 과정동안 수행하여 지침의 표준과 인증기관(Notified Body) 자체의 절차를 준수하는지를 확인한다. 또한 관할당국에 보고된 경계 보고서, 규제 준수 사례, 다른 관할당국에서 수신된 정보와 같은 특별 사례에 대해 인증기관(Notified Body)과 함께 대응해야 한다.⁸⁹⁾ 유럽의 지침과 관할당국에 대한 정보는 EU위원회 웹사이트의 Notifying Authorities⁹⁰⁾에서 확인 가능하다.

(6) 독립실행형(Stand alone) 소프트웨어

독립실행형(Stand alone) 소프트웨어에 관한 가이드라인은 MEDDEV 2.1/6 (Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices)에, 소프트웨어 정의를 비롯하여 의료기기로서의 소프트웨어와 분류 기준 등에 대하여 가이드를 마련해 두었다. 이 가이드에 따르면, 독립실행형 소프트웨어란, 시장에 출시되거나 이용할 수 있는 시점에 의료기기에 통합되지 않는 소프트웨어를 의미하며, 소프트웨어란 입력데이터를 처리하여 출력데이터를 생성하는 일련의 명령어로 정의한다. SaMD(Software as a Medical Device)란, 한 개 이상의 의료목적에 위해 사용되는 소프트웨어로 하드웨어 의료기기의 일부가 되지 않고 이러한 목적을 수행하는 소프트웨어를 지칭한다.

지침 2007/47/EEC의 항목 6에서, “소프트웨어는, 본질적으로 의료기기의 정의에서 규정된 한 개 이상의 의료 목적을 위해 사용되도록 특별히 제조자에 의해 의도된 의료기기라고 분류하는 것이 필요하다. 의료 환경에서 사용될 때 일반적인 목적에 대한 독립실행형 소프트웨어는 의료기기가 아니다” 라고 작성되어 있다. 독립실행형 소프트웨어는 만약 지침 98/79/EC에 규정된 IVD의 정의 또는 IVD 부속품의 정의를 충족할 경우, 체외 진단(In vitro diagnostic, IVD) 의료기기나 IVD의 부속품으로 자격이 주어져야 한다. 또한 작동의료기기(Active medical device)는 인체나 중력으로 직접 생성되는 것 외에 전기에너지나 전력원에 의존하여 이 에너지를 변환하여 작동하는 의료기기를 말하는데, 독립실행형 소프트웨어는 작동의료기기로 간주⁹¹⁾된다.

독립실행형 소프트웨어에 대한 인증을 위해서는 소프트웨어의 분류(Classification)가

89) DESIGNATION AND MONITORING OF NOTIFIED BODIES WITHIN THE FRAMEWORK OF EC DIRECTIVES ON MEDICAL DEVICES, MEDDEV 2.10-2 Rev.1, April 2001

90) <http://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=na.main>

91) Classification of medical devices, MEDDEV 2.4/1 Rev.9 June 2010

필요하며 2가지 기준에 따라 MDD의 규칙을 따를 필요가 있다. 1) 의료기기 정의를 충족하는 독립실행형 소프트웨어는 작동의료기기(Active medical device)로 간주되어야 하며 이것은 MDD의 규칙 9, 10, 11, 12에 적용된다. 2) 지침 93/42/EEC의 부속서 IV Classification Criteria의 2.3에는 “기기를 구동하거나 기기의 사용에 영향을 끼치는 소프트웨어는 자동적으로 같은 Class로 분류된다” 는 구현 규칙이 마련되어 있다. 작동 치료 의료기기로서의 소프트웨어 중, 환자에게 투여할 이온화방사선의 선량을 계산하는데 사용되는 방사선 치료계획 시스템 또는 인슐린 투여계획 독립실행형 소프트웨어 등은 규칙 9⁹²⁾에 해당하고, 정기검진 또는 집중치료 모니터링 중 심박수 또는 다른 생리적 매개변수를 나타내는 소프트웨어의 경우는 규칙 10에 해당하며, 규칙 적용에 따라 Class IIa 또는 IIb에 적용될 것이다. 체외진단 의료기기로서의 요건을 갖춘 독립실행형 소프트웨어는 지침 98/79/EC에 따라 규제된다.

일부 독립실행형 소프트웨어는 중요한 많은 응용시스템으로 나눌 수 있고 이것은 모듈과 관련되어 있다. 그 모듈 중 일부는 의료목적에 가질 수 있으나 나머지는 아닐 수도 있다. 이러한 경우, MDD에 적용되는 모듈은 MDD의 요구사항을 충족해야 하고 CE 마크가 있어야 하고, 의료기기가 아닌 모듈은 MDD의 요구사항이 적용되지 않는다. 제조자는 서로 다른 모듈간의 경계와 연계를 식별해야 한다.

경계(Borderline)와 관련하여 매뉴얼(Manual on borderline and classification in the community regulatory framework for medical devices)⁹³⁾이 배포되었고 소프트웨어 및 모바일앱에 대한 분류는 9번 항목에 언급되어 있다. 특히 모바일앱에 대하여 살펴보면, ECG 절차에 대한 모바일앱은 MDD의 규칙 9가 적용되어 Class IIa로 분류될 수 있는데, 이 앱은 의료기기와 통합되어 있지 않지만 외부소스에서 나온 시그널 데이터를 사용하여 이를 ECG 파형으로 처리하여 개별 환자의 의학적 이익을 위해 저장 이외의 데이터에 대한 작업을 수행하기 때문이다. 그러나 출산동안 환자와 간병인간의 의사소통 모바일앱의 경우, 저장과 단순한 검색에 한계를 두고 데이터에 작업을 수행하므로 의료기기로서의 자격요건이 되지 않으며, 해부학 용어/위치/의학적 이미지를 소개하는 인체해부를 보는 앱의 경우도 단순데이터검색을 수행하고 직접적으로 개별 환자의 의학적 혜택을 위해 사용되지 않으므로 의료기기로서의 자격요건이 되지 않는다.

(7) 유럽 의료 규제의 변화

92) 규칙(Rules)은 (3) 규칙에 따른 분류 항목에 설명되어 있다.

93) Manual on borderline and classification in the community regulatory framework for medical devices, Version 1.17 (09-2015)

일반적으로 고위험 기기의 적합성 평가에는 인증기관(Notified Body)의 관련성이 높고 엄격한 요건이 적용된다. 가장 위험도가 낮은 기기는 인증기관(Notified Body)의 참여가 없는 제조업체의 자체 적합성 선언만 필요하며, 위험도가 높은 기기는 형식검사(Type Examination) (인증기관(Notified Body)이 디바이스의 대표 샘플을 정밀 조사)을 요구할 수 있으며 위험도가 가장 높은 기기는 인증기관(Notified Body)의 감사 및 예고 없는 방문을 포함한 전체 품질 평가가 필요하며 모든 장치는 임상 데이터로 지원되어야 한다. (위험 요소가 낮은 기기의 제조업체는 해당 장치와 “동등“하다고 표시된 장치에서 현재 사용 가능한 문헌을 편집하여 이 요구 사항을 충족시킬 수 있음). 또한 제조업체는 유해 사례와 관련된 정보를 수집하고 보고하기 위해 장비를 등록하고 시판 후 감시시스템(Post-market vigilance system)을 구현해야 한다. 적합성 평가가 완료되면 제조업체는 기기가 지침의 필수 요구사항을 준수한다는 의미의 CE마크를 기기에 부착할 수 있으며, CE마크가 있는 기기는 EEA 어디에서나 판매될 수 있다.

최근 몇 년 동안, 이 규제 체계는 여러 가지 발전을 거듭해 왔다. 2007년에 통과되고 2010년 시행된 수정 지시문은 의료기기에 대한 시판후 감시 요구사항을 확대하고 특정 임상 데이터 요구사항에 대한 표준을 강화했으며 의료기기를 구성하는 품목 목록에 소프트웨어를 추가했다. 또한 2011년 5월 1일부터 관할당국은 의료기기 관련 유럽 데이터뱅크(EUDAMED⁹⁴)에 기기 인증, 임상 조사 및 경계 관련 데이터에 대한 정보를 제출해야 한다. 데이터뱅크는 관할당국과 유럽집행위원회에서만 이용할 수 있다. 이것은 특정 장치가 판매된 각 회원국에 별도로 통보해야 한다는 이전 요구사항을 제거하여 의료 기기를 시장에 출시하는 프로세스를 간소화하기 위한 것이다.

이러한 발전노력에도 불구하고 관할당국과 인증기관(Notified Body)에 규제책임을 위임함으로써 지침이 회원국간의 조율이 거의 이루어지지 않으므로 국가들간 정책 통일성이 결여되고 인증기관(Notified Body)의 적합성 평가 실행의 일관성이 부족하다는 비판을 받기도 하며, 신규 기술에 대한 인증기관(Notified Body) 자체의 전문성 기술 부족에 대한 문제가 대두하기도 하였다. 이에 대해 2012년 인증기관(Notified Body)은 자발적인 행동 규범(Code of Conduct)을 발표하는 등 유럽집행위원회를 포함한 이해관계자들은 꾸준한 노력을 기울이고 있다.⁹⁵⁾

94) the European Databank on Medical Devices, 의료기기에 관한 유럽 데이터뱅크

95) Future Medical Device Regulation in the European Union: Prospects for Reform,

http://www.mddionline.com/article/future-regulation-medical-devices-european-union-prospects-reform#_ftn24

4) 미국과 유럽의 의료 규정 비교

미국은 의료 안전에 대하여 FFD&C Act를 기초로 CDRH의 단일규제기관과 단일규정을 통해 엄격하게 규제하고 있는 반면, 유럽은 MDD와 같은 회원국에 조화된 법규정을 제정하고 회원국에서 지정한 여러 인증기관(Notified Body)을 통하여 인증활동을 수행한다. 그러나 미국과 유럽 모두 의료기기에 대한 필수인증을 받아야 시장판매가 가능하고, 의료기기와 관련된 소프트웨어 요구사항에 관한 일관된 지침을 제공하고 있으나, 안전성과 효율성을 보증하기 위한 절차나 방법의 적용에 있어서는, 제조사들이 자신들의 제품에 적절한 조화된 국가내/국제 표준을 이용할 수 있도록 허용한다.

<표 2-19> 미국과 유럽의 의료 규정 비교

구분	미국	유럽연합
법규정	FFD&C Act(Federal Food, Drug & Cosmetic Act), Title 21 of CFR(Code of Federal Regulations)	유럽연합에 조화된 법규정 Council Directive 90/385/EEC on Active Implantable Medical Devices (AIMDD), Council Directive 93/42/EEC on Medical Devices (MDD), Council Directive 98/79/EC on In Vitro Diagnostic Medical Devices (IVDMD)
규제기관	FDA의 CDRH(Center for Devices and Radiological Health, 기기 및 방사선 건강 센터)	유럽집행위원회(EU Commission), 각 회원국의 관할당국 및 Notified Body
필수인증	FDA인증	CE마크
적용제품	미국시장 내 제조/유통/판매되는 의료기기제품	유럽경제구역(EEA)에서 제조/유통/판매되는 의료기기제품
분류	Class I, II, III FDA에서 기기분류 및 시장 요구사항 정보 제공.	Class I, IIa, IIb, III 18개의 규칙(rules)에 따라 분류
인증유형	Premarket notification 510(k), Premarket Approval(PMA)	Conformity Assessment
의료기기 소프트웨어	의료기기 소프트웨어의 시판전제출 내용에 대한 안내지침 제공. 소프트웨어의 우려수준(Level of concern)에 따라 소프트웨어문서 요구사항은 달라짐.	의료기기 구동 및 기기 사용에 영향을 끼치는 소프트웨어는 기기와 같이 분류됨. 독립실행형(stand alone) 소프트웨어에 대한 가이드라인 제공.
적용가능 표준	FDA공인된 합의표준 정보를 제공하며 미국표준 및 국제표준 해당.	유럽집행위원회에서 조화표준 목록 제공.

5. 조사 결과 요약 및 시사점

주요 산업도메인으로 자동차, 국방, 항공 및 의료부문에 대한 소프트웨어 안전 표준 및 주요 선진국의 안전 활동을 조사하였다. 자동차, 국방, 항공 부문의 안전 활동은 전년도인 2015년에 이은 조사로써 주로 소프트웨어 안전 표준 및 활동의 변화 추이에 주안점을 두었는데, 1) 전자시스템/소프트웨어의 안전 중요성이 증가함에 따라 타 산업에 적용되고 있는 안전 표준을 분석/활용함으로써 안전 표준의 융복합화가 일어나고 있었으며 2) 산업 도메인별 안전 표준은 기술 발달에 따라 점차 상세화 되는 방향으로 발전하고 있었다. 2016년 보고서에 새롭게 조사된 의료부문은 의료기기의 소프트웨어 안전성과 유효성 적합성에 사용되고 있는 조화된 국제 표준인 IEC 62304와 전 세계 의료시장의 대부분을 차지하고 있는 미국과 유럽의 의료 부문 안전 활동에 대하여, 자동차, 국방, 항공 부문의 결과와 따로 분리하여 3)번 항목으로 요약하였다.

1) 전자시스템/소프트웨어 안전 중요성 급증 및 안전 표준의 융복합화

모든 산업 도메인 안전 핵심 분야에 자율비행 또는 자율주행차 등과 같은 인공 지능 및 이를 활용한 자율화 기능 도입이 증가함에 따라 전자시스템 기능 안전 및 소프트웨어 안전에 대한 중요성도 더불어 증가하고 있다. 또한, 높은 수준의 안전 요구사항을 충족하기 위해 필요에 따라 타 산업 도메인의 안전 표준 및 가이드를 연구하고 적용하는 융복합화가 진행되고 있다.

미 도로교통안전국(NHTSA)은 자율주행차 정책 가이드라인에서 자동차 운전을 위해 ISO 26262 뿐만 아니라 필요에 따라 MIL-STD-882E, DO-178C 등의 안전 표준 활용을 권고하고 차세대 자동차 안전 규제를 위해 미 연방항공청 규제 제도를 분석하고 있으며 NHTSA는 자동차 안전 신뢰성 향상을 위해 2016년 6월 전자 장비 안전 표준에 관련된 6개 주요 안전 표준을 분석하였다. 연방자동차안전표준인 FMVSS(Federal Motor Vehicle Safety Standards) 및 소프트웨어 안전 프로세스 준용을 위해 ISO 26262, MIL-STD-882E, DO-178C의 3가지를, 구체화된 방법에 대하여 아키텍처에 대한 표준에 대해 AUTOSAR를, 코딩표준과 관련하여 MISRA C를 중심으로 다양한 표준을 비교 검토하고 있다.

2) 소프트웨어 안전 표준의 부상과 상세화

소프트웨어 안전과 관련된 표준은 추상적인 시스템 기능 안전표준에서 상세 화되고

있으며, 소프트웨어 안전이 부각되는 방향으로 진화하고 있다.

먼저, 자동차부문의 MISRA C는 2004년 버전의 모호한 용어를 명확하게 정의하고 코딩 규칙을 142개에서 159개로 증가시켜 2012년 버전을 발표하였다. 그리고 2016년 4월 MISRA Compliance를 발표하여 MISRA C와 MISRA C++에 대하여 적용 가이드라인의 종류, 시행 방법의 효과, 사용된 편차의 범위, 규율화된 소프트웨어 개발 프로세스의 사용, 프로젝트 외부에서 개발된 컴퍼넌트 현황 등을 밝히도록 준수 지침을 강화하였다.

국방부문의 MIL-STD-882E는 시스템 엔지니어링 안전 표준으로 위험에 대한 식별, 분류, 회피에 대한 표준 및 일반적 방안으로써 기존의 MIL-STD-882D에 이어 소프트웨어 시스템 안전 기법 및 실무 등이 추가되었다. 또한 시스템 환경에서 소프트웨어를 감내할만한 위험수준에서 실행하기 위한 소프트웨어 제작 관리 및 엔지니어링 가이드라인으로 Joint Software Safety System Engineering Handbook을 작성하였다. 이 가이드라인은 미국방성, 미 육/해/공군, 항공우주국, 연방항공청 외에 주요 민간, 학계에서 참여하였으며 시스템 안전 관리자 및 소프트웨어 개발 관리자가 업무를 수행할 수 있도록 충분한 정보를 제공하는 목적이다.

항공부문은 새로운 소프트웨어 동향과 신규 기술을 수용하고 안전 프로세스 간 명확하고 일관된 연결관계를 제공하기 위해 DO-178B에 이은 새로운 표준으로 DO-178C가 2011년에 작성되었다. DO-178C는 기존 표준을 활용되고 있는 DO-178B의 수립된 원칙을 따르고 변경을 최소화하기 위하여 신규 표준과 함께 상세한 보충서가 제작되었다. DO-178C와 한 세트의 작성된 지침은, 지상 기반의 CNS/ATM 소프트웨어 인증을 위한 신규 지침인 DO-278A, DO-178C와 DO-278A의 설명서인 DO-248C가 있고, 툴 자격에 관련하여 항공기 뿐 아니라 다른 도메인에도 적용가능하도록 구성된 DO-330, DO-331 (Model-Based Development and Verification Supplement), DO-332 (Object-Oriented Technology and Related Techniques Supplement), DO-333 (Formal Methods Supplement)의 기술 보충서가 있다. 이러한 기술 보충서는 기술 수용에 따라 향후 추가될 수도 있다.

3) 미국/유럽의 의료부문 안전활동

의료부문의 소프트웨어 표준 중, IEC 62304는 유럽과 미국에 채택된 의료제품 소프트웨어 설계에 대한 조화된(harmonized) 표준으로써 의료제품의 소프트웨어에 대한 FDA, CE인증을 받을 경우 IEC 62304의 적용이 가능하다. 또한 전기의료기기에 관한 표준인 ISO 60601-1에서는, PEMS(Programmable Electrical Medical Devices)에 대한 요

구사항을 적용할 때 IEC 62304 요구사항을 소프트웨어 개발 또는 변경에 적용하고 적합성 또한 IEC 62304로 판단하도록 요구하고 있다. IEC 62304는 소프트웨어 안전 등급을 Class A, B, C로 구분하고 있고 응용시스템을 분리(segregation)하여 소프트웨어 항목(item)에서 안전 등급을 적용하도록 하며, 의료기기 소프트웨어의 SOUP⁹⁶⁾ 사용을 식별하고 정당화하는 방법으로써 SOUP을 소프트웨어 설계 절차에 통합하여 검증하도록 한다. 그리고 건강에 관련된 소프트웨어가 증가함에 따라 건강 소프트웨어의 안전과 보안에 대한 국제표준인 IEC 82304-1이 2016년에 발표되었다. 이 표준은 현재 독립실행형(stand alone) 소프트웨어만 다루고 있고, IEC 62304 표준에서 요구하는 소프트웨어 의료기기 검증 간의 간격을 채워주고 있다.

전세계 의료시장의 대부분을 차지하고 있는 미국과 유럽은 각각 FDA인증과 CE마크를 통하여 미국시장 내, 유럽시장 내 의료기기의 판매를 허용하고 있다. 미국은 FDA(미국식품의약국)의 CDRH⁹⁷⁾에서 의료기기제품의 510(k)(premarket notification 510(k), 시판전통보), PMA(pre-market approval, 시판전승인)을 관할하고 있고, 유럽은 유럽연합의 조화된 의료관련지침(AIMDD, MDD, IVD)을 기초로 각 EU 회원국의 관할당국에서 인증기관인 Notified Body와 CE인증을 관할한다. 미국은 의료기기분류를 Class I, II, III 3가지로 구분하는 반면, 유럽은 Class I, IIa, IIb, III 4가지로 구분한다. 두 지역 모두 의료제품의 분류에 따라 인증 요구사항은 달라지며 Class III로 갈수록 엄격한 절차가 요구된다. 의료기기 소프트웨어는 기본적으로 의료제품의 분류를 따르고 이에 대한 요구사항은 조화된 표준으로 공인된 국내 또는 국제표준을 사용하도록 권고하고 있다.

제2절 해외 TIC 시장 현황 조사

1. 해외 TIC 선진사 현황

1) 일반 현황 (Company Profile)

주로 유럽을 중심으로 활동하고 있는 TIC 매출 상위 5개 기업(SGS, Bureau Veritas, Intertek, Dekra, DNV GL)은 TIC 전체 시장의 매출 25%이상을 점유⁹⁸⁾하고 있으며, 대

96) Software of unknown provenance, 출처가 알려지지 않은 소프트웨어

97) Center for Devices and Radiological Health

98) Catalyst Corporate Finance LLP, "Global Testing, Inspection and Certification Summer 2016"

략 100년 이상의 역사를 가지고 있는 회사로 구성되어 있다. 이들 기업의 최근 5년간 연간실적보고서를 살펴보면 연평균 최소 5%에서 최대 23%의 꾸준한 매출 성장을 확인할 수 있다. 그 중에서 DNV GL의 경우 성장세가 상대적으로 큰 이유는 2013년 DNV와 GL의 합병 때문이며, 2015년 SGS의 매출실적 하락은 통화 가치의 변화에 의한 것으로, 기존 통화기준을 적용 시 전년대비 3.6%의 매출이 증가했다.

<표 2-20> TIC 매출 상위 기업의 일반 현황 (단위: \$ millions)

TIC 상위 기업	본사	설립연도	2015 매출
SGS	스위스	1878년	5,763
Bureau Veritas	프랑스	1828년	5,063
Intertek	영국	1880년	3,212
DEKRA	독일	1925년	2,971
DNV GL	노르웨이	1864년	2,657

<표 2-21> TIC 매출 상위 기업의 매출 현황 (단위: millions)

TIC 상위 기업 (화폐단위)	2011년	2012년	2013년	2014년	2015년	CAGR (2011~2015)
SGS (CHF)	4,797	5,569	5,830	5,883	5,712	4.5%
Bureau Veritas (EUR)	3,359	3,902	3,933	4,172	4,635	8.4%
Intertek (GBP)	1,749	2,054	2,184	2,093	2,166	5.5%
DEKRA (EUR)	2,007	2,164	2,311	2,510	2,720	7.9%
DNV GL (NOK)	10,156	12,532	15,234	21,623	23,390	23.2%

인력 현황은 full time employee를 기준으로 산정된 것으로 보통 6% ~ 15% 정도의 안정적인 인력 증가 추세를 보이고 있다. 이러한 매출의 신장과 인력의 유입 증가세는 대체적으로 TIC 시장이 계속 확장될 전망이라고 예측해 볼 수 있다. 매출 부분에서 주목할 점은 스위스의 SGS와 프랑스의 Bureau Veritas가 전체 TIC 시장의 14%를 점유하며 시장을 주도하고 있다는 것이다.

〈표 2-22〉 TIC 매출 상위 기업의 직원 수 현황 (단위: 명)

TIC 상위 기업	2011년	2012년	2013년	2014년	2015년	CAGR (2011~2015)
SGS	67,633	76,790	80,510	83,515	85,903	6.2%
Bureau Veritas	52,148	58,924	61,581	66,494	65,995	6.1%
Intertek	31,712	34,882	36,864	38,407	41,434	6.9%
DEKRA	27,321	28,340	32,591	35,021	36,673	7.6%
DNV GL	8,453	10,294	16,107	15,712	14,954	15.3%

2) 소프트웨어 안전 관련 주요 제공 서비스

(1) SGS

SGS는 기능안전영역(Functional Safety)에서 소프트웨어 안전과 관련된 국제표준 IEC 61508, ISO 26262, IEC 62061, ISO 13849, IEC 61511, IEC 60601을 적용하여 Automotive, Industrial Manufacturing, Consumer Goods and Retail 등의 산업영역에서 검사, 컨설팅, 인증 및 교육 서비스 등을 제공하고 있다. 특히 의료기기 부문은 IEC/EN 60601 및 IEC/EN 61010 시리즈의 전체 범위에 대한 제품 안전 및 EMC 테스트 서비스를 제공한다.

SGS의 기능 안전 전문가들은 적절한 국제 표준을 준수하는 제품 및 프로세스를 개발하는데 도움을 주고 있다. 주로 기능 안전에 관련해서 교육 및 개인자격 검정, 컨설팅, 안정성 분석, 평가, 감사, 인증 등 서비스를 제공하고 있다. 주로 모빌리티 농업 및 임업, 자동화, 기계, 의료기술, 공정 산업, 반도체, 소프트웨어의 산업분야에서 서비스를 제공한다. 그 중 의료 부문에서는 의료기기 시험, 인증, 심사 및 교육 서비스를 제공하고 있으며, 제품 출시에 필요한 필수 요구사항 및 규정 준수에 도움을 주고 있다. 또한 35개국 이상에서 사업을 운영함으로써 글로벌 솔루션 및 지역 특성에 맞춘 솔루션을 제공하고 있다.

- 인증: ISO 9001, ISO 13485, EC Directive 93/42/EEC (MDD), EC Directive 98/79/EEC(IVDD), CMDCAS (캐나다), PMD Act (일본), INMETRO (브라질), FDA Accredited Persons Program, 한국, 대만, 홍콩, 호주, 사우디아라비아 또는 각국의

추가적인 요구사항을 포함한 Good Distribution Practice(GDP).

- 전기 의료기기 테스트: CB, NRTL 승인 및 ISO 17025 인가를 포함해 IEC/EN 60601 및 IEC/EN 61010 시리즈의 전체 범위에 대한 제품 안전 및 EMC 테스트.
- 미생물학 및 의약품 테스트: 멸균, 생체적합성, 바이오분석.
- 그 밖의 테스트: 무선/원격의료 배터리, RoHS 2, 포장.
- 교육: 공개 및 내부 과정을 통한 QMS/심사, 내부 심사, 전 세계 규정, 멸균 공정, 위험 관리, 제품 안전/EMC.
- 심사: 공급업체 심사, 캡 분석 심사, 의약 GMP 심사.

SGS는 자동차 부문에서 선두적인 역할을 담당하고 있는데, 자동차 전기 시스템 안전에 관한 국제규정의 새로운 표준 제정 참여 및 ISO 26262와 관련된 ISO그룹 TC22/SC3/WG16나 IEC61508과 GK914 같은 표준화 위원회에서 활동하고 있다. 자동차의 기능안전과 관련하여 AFSP (Automotive Functional Safety Professional) 및 AFSE (Automotive Functional Safety Expert)의 개인 자격을 제공하고 있다.

그 밖에 기능 안전에 관련하여 제공하는 자격 서비스는 IFSP(Industrial Functional Safety Professional), IFSE(Industrial Functional Safety Expert), MFSP(Machinery Functional Safety Professional), MFSE(Machinery Functional Safety Expert), AGFSP(Agriculture Functional Safety Professional), PIFSP(Process Industry Functional Safety Professional)가 있다.

또한 SGS와 TUV가 운영하는 단일 단위의 기능 안전팀(SGS-TÜV)은 공인 기관으로 주로 기계부문의 안정성 및 시장 적합성을 확인하는 역할을 하며, 고객에게 공인 표준의 요구사항에 대한 컨설팅과 인증서를 제공하고 있다.

(2) Bureau Veritas

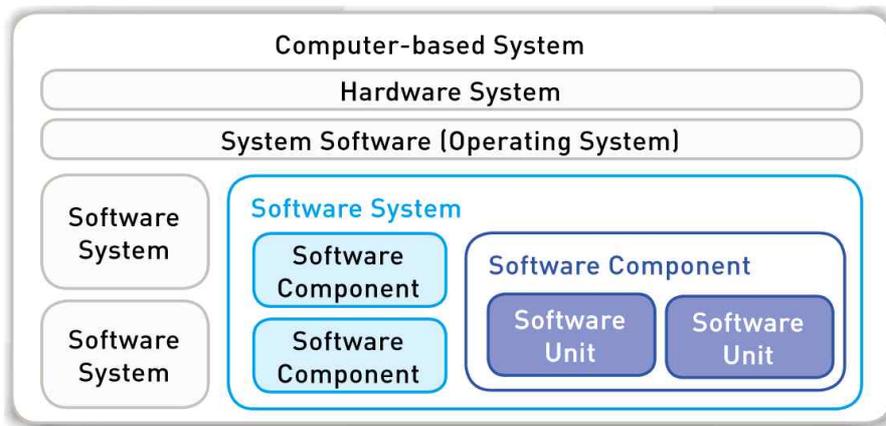
Bureau Veritas는 SGS와 TIC 시장을 선도하는 업체로 기능안전영역에서 소프트웨어 안전과 관련된 국제표준 IEC 61508, DO 178, IEC 62433, IEC 62304, IEC 60880/62138, ISO 26262, CENELEC 50128, ISO 26262, IEC/EN 60601을 적용하여 항공, 철도, 자동차, 건설, 소비재, 오일&가스 등의 산업영역에서 검사, 컨설팅, 인증 및 교육 서비스 등을 제공하고 있다.

Bureau Veritas는 기능 안전 관련 검사, 테스트, 인증과 더불어 업무와 관련된 임베

디드 소프트웨어의 테스트와 위험평가에 관한 가이드 작성하여 제공하고 있다. 임베디드 소프트웨어는 소프트웨어의 안정성, 가용성, 안전성, 무결성 및 성능을 제공하기 위한 파괴적인 접근 방식을 제공한다. 소프트웨어의 실패는 심각한 인적, 전략적, 경제적, 환경적 또는 브랜드 이미지의 결과를 초래할 수 있기 때문에 중요성이 점차 대두되고 있다. 또한 임베디드 소프트웨어는 기계 인터페이스를 통해 제어되는 부분이기 때문에 성능평가 및 고장 발생 시 위험 평가의 어려움, 설계부터 검증까지의 시스템 보호의 문제를 해결하기 위해 아래와 같은 접근방식과 솔루션을 제공한다.

- 소프트웨어 구조 및 코드 분석을 위한 '화이트 박스' 접근법
- 보안 기대치를 충족시키는 위험 우선순위 접근 방식
- 시스템 설계로 인한 실패 가능성에 대한 포괄적인 테스트
- 국제 표준 준수를 위한 적합성 평가 및 교육
- 전문지식: 소프트웨어 설계, 코드 분석, Frama-C 검증, 테스트, 맞춤형 사양 개발

[그림 2-15] 소프트웨어 시스템의 경계 및 구조



자료: Software Guidelines Development & Assessment, 2016, Bureau Veritas

이 그림은 임베디드 소프트웨어의 가장 큰 특징인 화이트 박스 접근법을 설명하기 위한 소프트웨어 시스템의 경계 및 구조를 나타낸 것으로, 소프트웨어 시스템에 의해 달성되는 성능 수준을 평가하기 위한 소프트웨어 범주 및 관련 기준을 보여주는 것이다. 블랙박스 접근법은 소프트웨어 시스템, 소프트웨어 구성 요소 및 소프트웨어 유닛의 내부 구조를 참조하지 않는 기능 또는 비 기능 테스트를 말하며, 화이트박스 접근법은 소프트웨어 시스템, 소프트웨어 구성 요소 또는 소프트웨어 단위의 내부 구조를 분석하여 테스트하는 것을 말한다. 또한 소프트웨어 기능 구현은 소프트웨어 컴포넌트

구현이 일련의 기능적 요구 사항을 만족시키는지 평가하기 위해 구성된 활동을 말하며, 소프트웨어 검사는 정적 분석 및 테스트를 포함한다.

Bureau Veritas는 전자기기 호환성, 전기안전, 방사선 촬영, 유해 물질 분석, 수명주기 분석, 전자기장(EMF)등의 의료기기 분야에서 IEC/EN 60601 관련하여 전기안전 및 전자파 적합성 테스트 서비스를 제공한다. 또한 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.

(3) Intertek

기능안전영역에서 소프트웨어 안전과 관련된 국제표준 IEC/EN 62061, ISO 13849, IEC 61508, IEC 61511, IEC 60601을 적용하여 소비재, 전기전자, 석유화학 등의 산업영역에서 검사, 컨설팅, 인증 및 교육 서비스 등을 제공하고 있다. 또한 100여개 국가, 1,000여개 지역에 시험소 및 사무소를 운영, 41,000여명의 직원이 서비스를 제공하고 있으며, 특히 2010년 국내 최대 규모의 섬유 및 화학시험소를 설립하여 TIC 서비스를 국내 고객에게 제공하고 있다. 기능 안전성은 일반적으로 감각, 논리 및 작동 요소가 있는 장비를 통해 수행되는 프로세스의 위험을 완화하기 위해 전자 및 기타 유형의 시스템을 사용하는 데까지 확장되는데, 이러한 시스템은 성능 레벨(PL), 안전 무결성 레벨(SIL), 고장 모드 및 영향 분석 등을 포함하여 기능 안전성을 평가하고 수행한다.

특히 Intertek은 차세대 지능형 전력망인 스마트그리드 서비스에 대한 글로벌 네트워크 시험 기관으로서 시험, 인증, 상호 운용성 및 전문가 컨설팅 서비스를 제공하고 있다. 유일하게 공식 OpenADR 시험 파트너이면서 ZigBee Alliance에 멤버인 Intertek은 유럽(CE), 북미(ETL/Ceti) 인증에 대한 서비스를 제공하고 있다.

의료기기 관련해서 Intertek은 국제표준 IEC 60601 관련한 위험관리, 테스트, 인증, 감사를 하고 있으며, 아래와 같은 솔루션을 제공한다.

- 리스크 관리 컨설팅
- 맞춤형 현장 및 교육 세미나
- 리스크 관리 시스템 인증 및 감사 : ISO 14971
- 개정사항을 포함한 국제표준 IEC 60601-1 시험 및 인증

또한 의료기기의 EMC 지침 요구사항을 충족하기 위해 정전기 방전 (ESD) 테스트, EMC 사전 컴플라이언스 검사, 방사성 방출 테스트, 방사 면역 테스트를 고객에게 제

공한다.

(4) DEKRA

안전에 필수적인 임베디드 장치의 기능적 안전에 대해 입력에 대한 대응, 하드웨어 및 소프트웨어 오류 가능성, 환경 변화, 운영자 오류, 손상된 정보의 이해, 전자기 환경의 변화, 특성의 변화, 제품 수명주기 전반에 걸친 부품의 무작위 고장 및 고의적인 조작의 기능을 평가한다. 이러한 위험 평가를 통해 기능 안전 및 안전 무결성 레벨(SIL)을 정의하고 그 후에 하드웨어 및 소프트웨어 요구 사항, 설계 프로세스, 검증 테스트 등을 포함한 제품 수명주기에 대한 평가를 한다. 또한 기능안전에 대한 국제표준인 IEC 61508을 기본으로 하며 이 외에도 IEC 61508, IEC 62304, IEC 61511, ISO 26262, IEC 62061, ISO/IEC 14762 등 특정 제품 표준에 맞추어 기능 안전성을 평가하고 수행한다.

의료기기 부문에서 DEKRA는 국제표준 IEC 60601과 관련한 소프트웨어 라이프 사이클 프로세스 평가 및 EU 시장 진입을 위한 적합성 평가를 제공하고 있으며, 이 외에 510(k) 및 ISO 13485 인증도 제공하고 있다.

특히 DEKRA는 국내에 방폭 전기기기와 관련된 폭발 안전 (Explosion Safety) 사무소를 설립하여 국제표준 IEC 60079와 관련된 아래와 같은 서비스를 제공한다.

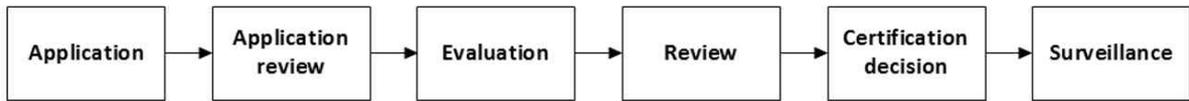
(IEC 60079-29-3: 가스 탐지기 - 고정 가스 탐지 시스템의 기능 안전에 관한 지침)

- ATEX 및 IECEx scheme에 따른 지도, 시험 및 인증 서비스
- 서면 합의에 따른 세계 각국 인증을 위한 Test protocol 구축 서비스
- 정전기 발생과 관련된 문제에 대한 시험 및 인증 서비스
- EN/IEC 60079의 방폭기기와 관련된 교육 및 세미나

(5) DNV GL

기능안전영역에서 소프트웨어 안전과 관련된 국제표준 ISO 26262, EN 50128, IEC 60601I, IEC 61508, IEC 62304, IEC 61513, IEC 62061을 적용하여 인증, 평가, 검토 등의 서비스를 제공하고 있다. 아래의 그림은 기능안전의 인증 프로세스와 일반적인 요구사항을 보여준다.

[그림 2-16] 기능안전 인증 프로세스



[그림 2-17] 기능안전 요구사항

Required activity	IEC 61508	IEC 61511	OLF-070	Typical documentation	System	System integration	Equipment	Safety management	Tool	Subsystem
Management of functional safety	6	5	5	Safety life-cycle plan. Evidence of competence management. Configuration management plan and documentation	x	x	x	x	x	x
Functional safety assessment and auditing	8	5.6.2	6	Functional safety assessment report. Audit reports	x	x	x	x	x	x
Verification	7.18	7	6	Verification plan. Verification documentation	x	x	x	x	x	x
Setting safety requirements for the safety instrumented functions	7.6	8, 9	7	High-level safety requirements specification	x					
				Safety integrity level allocation report	x					
Safety instrumented system design and engineering	7.11, Part 2, Part 3	11	8	Functional design specification			x			
				Safety integrity level verification report	x	x	x	x	x	x
Development of application software	Part 3	12	8	Software			x			x
				Evidence of module testing			x			x
				Programming standard and evidence of compliance			x			x
Factory acceptance test	7.14	13	8.9	Signed factory acceptance test documentation			x		x	
Installation and commissioning	7.13	14	9	Installation and commissioning records	x	x				
Operation and maintenance	7.15	16	10	Operation manual. Maintenance manual	x					
Modification	7.16	17	11	Change management procedure. Impact analyses for modifications. Test documentation	x	x	x	x	x	x
Decommissioning	7.17	18	12	Decommissioning plan	x					

자료: Service specification DNVGL-SE-0141, 2015, DNV GL

2013년 노르웨이의 DNV(Det Norske Veritas)와 독일의 GL(Germanischer Lloyd)이 합병하여 설립된, DNV GL은 해상, 석유 및 가스, 에너지 산업, 헬스 케어 및 식음료 관련 사업을 하고 있으며, 세계 최대 선급회사로서 독립적 인증 및 기술 자문 서비스를 제공하고 있다. 주로 해운산업의 선박에서 해상 구조물까지 안전과 품질, 에너지 효율 추구하는 선두적인 자문기관이다.

의료기기 관련해서 DNV GL은 Medical Device Directive 93/42/EEC의 부속서 II, IV, V에 대한 적합성 평가를 수행할 수 있는 인증기관으로 등록되어 있다.

2. M&A 현황

1) 주요 M&A 활동

TIC 시장의 매출 상위기업들은 지속적인 M&A 활동을 통해 유럽 중심의 지역에서 북미, 캐나다, 호주 등으로 확장하고 있으며, 서비스 영역도 식품, 제약, 환경 분야 등 여러 분야로 확장하고 있다. M&A 시장은 주로 상위 업체에 의해 주도되고 있으며, 2010년부터 2015년까지 350건 이상의 거래가 진행⁹⁹⁾되고 있으며, 그 중 SGS와 Bureau Veritas가 활발한 활동을 하고 있다.

[그림 2-18] 최근 5년 M&A 현황

Company	Revenues CAGR 2010-2014 (organic growth) ¹⁾	Number of acquisitions (2010-2015)	Main acquisitions since 2010 (companies over €30m in sales)		
			Year	Company	Target sales (€m) ²⁾
	20.0% (6.0%)	52	2015 2015 2015 2015 2014 2011 2011	Bionnis Bioaccess Diatherix Laboratory Boston Heart Diagnostics ViraCor-IBT Lancaster Laboratories IPL	220 140 37 78 60 81 45
	15.9% (11.3%)	20	2012	Velosi	1,433
	13.9% (6.6%)	26	2011	Moody	359
	9.2% (2.2%)	56	2015 2014 2014 2014 2012 2012 2010	Shandong Chengxin Maxam Analytics Matthews Daniel Sistema FRI Tecnicontrol TH Hill AcmeLabs Inspectorate	40 187 34 40 74 36 55 338
	7.7% (4.3%)	32	2013 2012 2011 2010	Vehicle Testing BST Group AutoContact AF-Kontroll AB	57 34 52 43
	7.6% (5.4%)	15	2014 2010	Risktec Solutions Gens	39 32
	7.3% (6.0%)	32	2010	Global Risk	40
	7.3% (6.0%)	2	2013	Senergy	139
	6.6% ²⁾ (2.1%)	14	2012	KEMA	245
	6.5% (4.3%)	78	2012 2012 2010	ETSA CIMM General de Servicios ITV	36 44 64
	5.7% (-2.8%)	16	2013 2011 2010 2010	Reservoir Group Stewart Holdings Group Ammtec PearlStreet	174 59 39 59
	4.2% (2.8%)	12	2011	Alter Technology	60

자료: Catalyst Corporate Finance LLP, 2016

99) Catalyst Corporate Finance LLP(2016), “Global Testing, Inspection and Certification Summer 2016”

2) 지역별 M&A 현황

현재까지 M&A는 유럽지역에서 활발하게 이루어졌는데, 그 이유는 TIC의 주요 선두 업체가 유럽을 중심으로 발전했고, 시장규모가 크고 성숙하기 때문이다. 미국은 두 번째로 M&A가 활발한 지역으로 선두업체의 부재와 분화된 시장으로 시장의 통합이 가속화되고 있는 매력적인 곳이다. 또한 APAC 시장은 2022년까지 유럽을 앞지를 것으로 예상¹⁰⁰⁾되며, 현재 TIC 시장 규모는 작으나 성장 잠재력이 높은 곳으로 향후 M&A가 가장 활발하게 진행될 것으로 예상된다.

시장을 선도하는 업체 중 Bureau Veritas의 시장전략을 통해 이러한 지역적 M&A의 특징을 미리 예측해 볼 수 있다. 이 업체는 앞으로 가장 매력적인 지역으로 미국과 중국을 선정했다.([그림 2-17], [그림 2-18]) 미국 시장은 미국의 경제 성장, 소비의 증가, 새로운 규제 증가를 동인으로 시장 성장을 전망했다. 그러나 현재 미국은 상위 3개 업체가 5%이하의 시장을 점유하고 상위 12개 업체가 10%이하를 점유하는 등 분열된 시장이므로 활발한 M&A를 통해 미국의 시장 점유율을 확대할 계획이다. 특히 Oil & Gas와 Consumer & Retail 분야를 목표로 선정했다.

[그림 2-19] Bureau Veritas의 TIC 미국 시장 전략

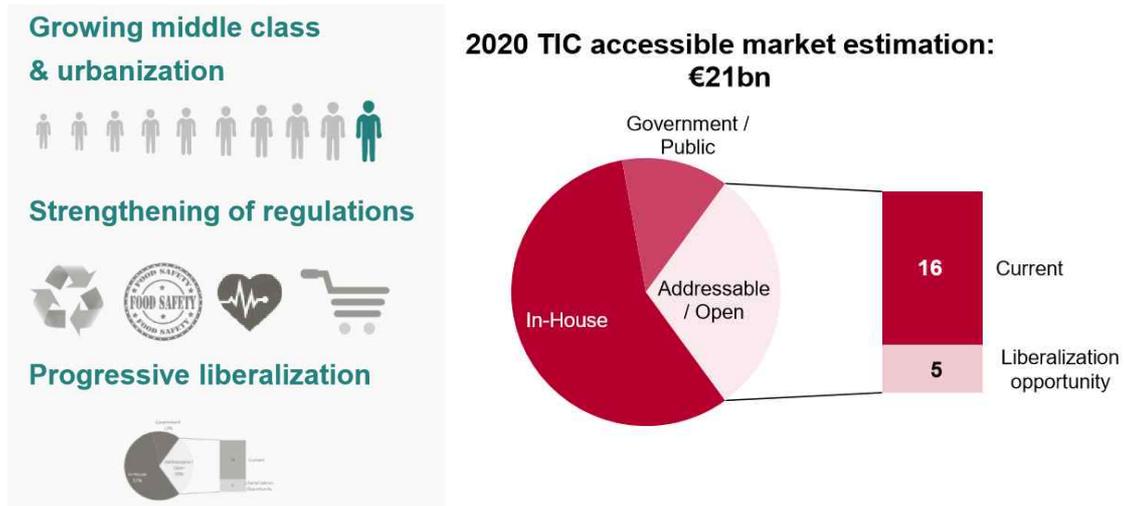


자료: Bureau Veritas Investor days 2015

중국은 지속적인 성장은 경제 성장, 중산층(Middle class)의 확대, 규제의 강화, 점진적인 자율화로 인해서 TIC의 가장 큰 시장이 될 것으로 전망한다.

100) Martet and market(2016), "Testing, Inspection and Certification (T.I.C.) Market"

[그림 2-20] Bureau Veritas의 TIC 중국 시장 전략



자료: Bureau Veritas Investor days 2015

3) 최근 M&A 현황

SGS 그룹은 최근 1년간 Laboratoire LCA, Accutest, Quality Compliance Laboratories Inc를 인수하여 모로코, 북미, 캐나다의 식품, 환경, Health & Safety, 제약 분야의 역량을 강화하였고 Bureau Veritas는 호주의 식품 실험실 테스트 및 분석회사인 DTS 인수하여 아시아·태평양 지역의 주요 농·식품 시장에 진입하였으며 Intertek는 이탈리아의 식품안전에 대한 감사 및 실험실 테스트 업체인 FIT-Italia S.r.l를 인수하여 식품 안전 검증 서비스를 제공하게 되었다. 이러한 선두업체들은 활발한 M&A 활동을 통해 지역 및 서비스의 포트폴리오를 확장하고 있다.

3. TIC 시장 전망

최근 보고서를 살펴보면 TIC 시장은 2015년 약 80억 달러로 평가되었으며 2016년부터 2022년까지 CAGR¹⁰¹⁾ 5.15%의 지속적인 성장과 2022년 1,132억 달러 정도의 시장 규모¹⁰²⁾를 예측하고 있다. 이러한 지속적인 성장은 주로 4가지의 요인을 배경으로 작용하고 있다. 1. 산업안전표준 기반의 규제강화, 2. 글로벌화로 인한 시장의 확대, 3. 아웃소싱의 증가, 4. 안전 및 품질관리의 증가가 TIC 시장의 성장을 이끌고 있다.

101) Compound Annual Growth Rate(연평균 성장률)

102) Martet and market(2016), "Testing, Inspection and Certification (T.I.C.) Market"

1) 산업안전표준 기반의 규제강화

글로벌화로 인해 다양한 지역의 여러 규제 및 표준으로 인해 규제기관은 국제 품질 기준을 충족하고, 제품 품질에 대한 최종 사용자(End user)의 요구를 충족시키기 위해 새로운 표준을 개발하고 규제를 강화하고 있다. 식품 및 건강관리는 제품의 품질 및 위생에 관한 관심이 높아 규제가 엄격하며, 의료 기기업계의 제조업체는 엄격한 기준을 따르도록 요구 받는다. 또한 신흥시장이 성장하며, 급속하게 확대된 중국 중산층의 소비증가는 동남아시아에서 규제감독 강화를 요구한다.

2) 글로벌화로 인한 시장의 확대

글로벌화로 인해 국가 간 무역이 증가하면서 제품의 수입 및 수출 중 품질에 영향을 줄 수 있는 모든 단계에서 제품 품질을 유지하기 위해 엄격한 규제와 품질검사가 적용되고 있으며, TIC(Testing, Inspection & Certification) 서비스는 필수 요건으로 시장 성장의 동력이 되고 있다. 특히 아시아 태평양 및 라틴 아메리카와 같은 신흥시장은 국제적인 수입과 수출의 허브의 역할을 하며, TIC 시장에서 커다란 성장 잠재력을 보유하고 있다. 그 중 많은 제조 단위를 보유하고 있는 중국시장은 비약적인 성장의 기회를 갖고 있다.

TIC 시장을 주도하는 매출 상위 업체들은 주로 유럽을 중심으로 성장해 왔으며, 글로벌화로 인해 유럽 및 미국 시장에서 아시아 시장으로 확대되고 있다. APAC 시장은 2022년까지 유럽을 앞지를 것으로 예상되며, 향후 TIC 시장에서 중요한 역할을 할 것으로 보인다.

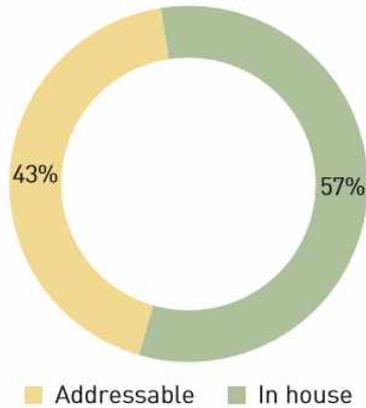
3) 아웃소싱의 증가

TIC (Testing, Inspection and Certification) 시장은 기업의 내부에서 TIC를 수행하는 내부(In house)시장과 외부 전문 업체에 의한 아웃소싱(addressable outsource)시장으로 구분할 수 있다. 아웃소싱 시장은 최종사용자, 구매자, 이해당사자 또는 공공기관이나 민간기관을 대신해서 테스트를 수행하는데, 재정적 이유 및 행정당국에 요구에 의해 독립적인 제3자 업체인 아웃소싱하고 있다.

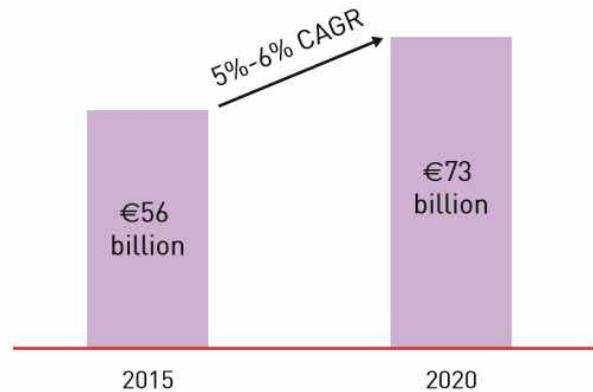
매년 증가하는 규제로 인해 내부시장에서 모든 테스트를 수행하는 것은 많은 비용과 책임을 수반한다. 공공기관과 대기업은 내부 비용을 줄이고, 복잡한 준수 문제에 대한 책임을 분산시키기 위해 TIC 서비스를 전문으로 하는 업체에 아웃소싱을 맡기는 추세

가 증가하고 있다. 이러한 이유로 전체시장의 43%를 차지하는 아웃소싱 시장은 매년 5~6%의 높은 성장이 예상된다.

[그림 2-21] TIC 시장의 구분



[그림 2-22] 아웃소싱 시장의 성장률



자료: Catalyst Corporate Finance LLP, 2016

4) 안전 및 품질관리의 증가

자동차, 석유화학, 항공 우주, 식음료 분야와 같은 다양한 산업분야에서 테스트, 검사, 인증 등 TIC 서비스의 수요가 높아지고 있다. 또한 제품의 글로벌 거래 및 제조의 분산화로 인해 제품의 안전 및 품질관리의 증가를 요구한다. 특히 중국 및 인도와 같은 신흥시장의 제조가 증가되고 있으며, 이러한 신흥시장은 선진국보다 엄격한 표준 준수를 요구 받는다. 이에 따라 안전 및 품질관리는 산업안전 표준기관의 규제 강화와 연관하여 지속적으로 증가하고 있다.

4. 조사 결과 요약 및 시사점

글로벌 TIC 업체 및 TIC 시장 동향은, 2015년과 동일하게 매출 상위 업체인 SGS, Bureau Veritas, Intertek, DEKRA, DNV GL이 전체 TIC 시장을 주도하고 있다. TIC 시장은 매년 5.15%의 지속적인 성장이 예상되며, 2022년 약 1,132억 달러의 시장규모가 될 것으로 예측된다. 이러한 시장의 성장은 산업안전표준 기반의 규제 강화와 글로벌화로 인한 시장의 확대, 아웃소싱의 증가, 안전 및 품질관리의 증가가 주요 요인으로 작용한다. 특히 아웃소싱 시장은 새로운 규제의 증가와 강화로 인한 기업 내부의 비용 절감과 책임분산의 방편으로 증가하고 있으며, 매년 5~6%의 높은 성장이 예상된다. 해

외 TIC 시장은 M&A를 통한 규모의 경제를 이루어 이를 토대로 지역 및 서비스 영역을 확장하고 있다. TIC 시장은 유럽 중심에서 미국으로 이동하고 있으며 향후 아시아(중국)지역이 가장 큰 시장이 될 것으로 전망된다. 특히 중국은 현재 TIC 시장 규모는 작으나 경제성장, 중산층 확대, 규제 강화 등 성장 잠재력이 높은 곳으로 향후 TIC 시장에서 중요한 지역이 될 것으로 예측된다.

제3장 국내 소프트웨어 안전 산업동향 분석

제1절 학계 및 공공기관

1. 개요

학계 및 공공기관(Governing Sector)의 관점에서 소프트웨어 안전의 개념 및 동향은 2015년도에 총 5개(3개 대학, 2개 기관)를 대상으로 수행한 결과를 바탕으로 개념 재확인, 학계 및 정책 트렌드 변화 방향 등을 중심으로 인터뷰를 수행하였다.

인터뷰 결과는 2015년도 수행 절차인 1. 개념정의, 2. 문제점 도출, 3. 해결방안 제시의 3단계 구조를 준용하였으며, 새로운 의견이나 2015년도 대비 변경된 내용에 초점을 맞추어 분석하였다.

[그림 3-1] 학계 및 공공기관 대상 조사결과 분석 틀

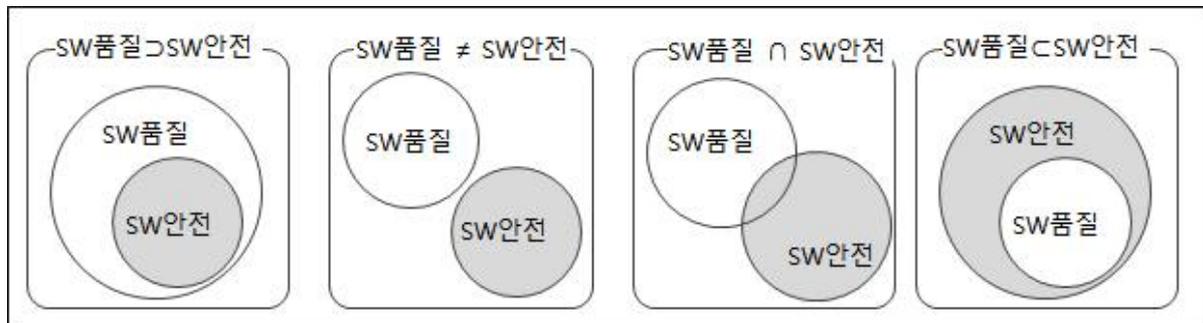


2. 인터뷰 상세내역

1) 소프트웨어 안전 개념

‘소프트웨어 안전’의 개념에 대해서 2015년도 조사에서는 1. 소프트웨어 품질과 동일, 2. 소프트웨어로 인하여 발생하는 인명이나 재산의 사고를 회피하는 방안(Safety Mechanism)으로써 소프트웨어 품질과는 확연히 구별된다는 의견이 주를 이루었으나, 본 조사에서는 3. 사람의 생명 및 건강에 직·간접적으로 연관되어야만 소프트웨어 안전이라고 정의하여, 특히 경제적·재산상의 손해 등은 소프트웨어 신뢰성의 문제라는 의견이 제시 되었다.

[그림 3-2] 소프트웨어 안전 개념 유형



소프트웨어 품질과 안전의 관점에서 소프트웨어 안전을 정의하기 위해서는 [그림 1]에서처럼 4가지 경우의 수로 좁혀지는데, 현재 신규(emerging) 분야인 점을 감안하면 좀 더 포괄적인 정의가 합리적일 것으로 보이며, ‘소프트웨어 안전이란, 인명이나 재산상 피해를 주는 사고 발생을 회피하기 위한 능동적인 방안(Safety Mechanism / Functional Safety)을 포함한 개념’으로 정의할 수 있다.

<표 3-1> 소프트웨어 안전의 개념에 대한 주요 결과

주요 도출 결과	주요 답변
소프트웨어 안전은 품질과 차별화 되는 개념	<ul style="list-style-type: none"> 소프트웨어의 안정성에서 발전된 개념으로써 소프트웨어 품질과는 별도의 개념임 향후 소프트웨어 안전 분야가 정립되면 소프트웨어 안전이 소프트웨어 품질을 포함하는 개념으로 발전할 개연성이 있음
소프트웨어 안전의 범위	<ul style="list-style-type: none"> 기존 소프트웨어 안전의 범위는 재산상의 손해까지 포함한 개념이었으나, 사람의 생명, 건강에 직·간접 관련이 있어야 소프트웨어 안전임 경제·재산 등과 관련된 소프트웨어의 범위는 신뢰성 영역임 (예를 들어, 공장 자동화 시스템의 경우는 멈추면 손실 측면임)

2) 현황 및 문제점

(1) 국내 소프트웨어 산업

국내 소프트웨어 산업의 문제점으로 2015년도에는 ‘소프트웨어 개발자들이 체계적인 절차와 방식에 따라 소프트웨어를 개발하고, 이를 문서화하는 문화가 부족’에서 기인한다는 답변이 주를 이루었다. 그러나 본 조사에서는 1. 설계 및 개발 보다는 코딩 자체에만 주력하는 소프트웨어 개발 문화가 문제라는 의견과 2. 소프트웨어 산업에서의 개발자에 대한 선순환 구조가 미흡하여 열악한 환경으로 인한 품질저하가 문제라는 의견이 많았다.

〈표 3-2〉 국내 소프트웨어 산업 현황 관련 주요 답변

주요 도출 결과	주요 답변
건전한 소프트웨어 개발 문화 결여 및 전문 인력 양성의 문제	<ul style="list-style-type: none"> • 국내에서는 소프트웨어에 대한 인식의 변화가 필요 • 소프트웨어 중요도에 대한 인식이 낮으므로 단가 및 인력에 대한 문제가 발생 • 미국 등 선진국은 천천히 개발하고, 제품이 좋으면 시장에서 Buying 한다는 기본 전제가 있으나, 우리나라는 무조건 빨리빨리 개발하려는 문화가 정착됨 • 안정적인 환경에서 개발할 수만 있게 해주면, 소프트웨어 개발 선진국 진입이 가능하나, 소프트웨어 엔지니어들에게 안정적인 성장경로를 제공하지 못하고 있음

(2) 국내 소프트웨어 안전 산업

소프트웨어 안전에 대한 인식과 개념 부족, 관련 법·제도 확립, 전문 인력 부족 등에 대해서는 2015년도 현황조사 결과와 비슷한 의견들이 주를 이루었으나, 그 요구 정도가 더욱 강력해지고 있으며, 특히 건전한 소프트웨어 안전 관련 산업구조 확립을 위한 본질적인 산업구조 개편이 필요하다는 의견이 많았다. 정리하면 소프트웨어 안전에 대한 사회적인 요구사항은 지속적으로 많아지는 데 반하여, 개념 정립 부족, 법·제도적 기반 미흡, 전문 인력 양성을 위한 학계의 프로그램 미흡, 절대적인 전문 인력의 수 부족, 외산 소프트웨어의 도입과 국산 소프트웨어 개발 분야에 대한 명확한 추진 전략 부재 등의 문제점이 발견되었다.

또한 소프트웨어 안전 분야의 발전을 위해서는 소프트웨어 산업 자체의 구조적인 개선이 반드시 선행되어야 한다는 점도 강조 되었다.

〈표 3-3〉 국내 소프트웨어 안전 산업 현황 관련 주요 답변

주요 도출 결과	주요 답변
소프트웨어 안전에 대한 인식 부족	<ul style="list-style-type: none"> • 학계에서는 소프트웨어 안전 관련 교육이 아직은 없으나, 임베디드 시스템 교육이 많아지면서 늘어날 것으로 예상됨 • 소프트웨어 안전에 대한 세미나 등이 연구실 자체적으로 수행되고 있음
소프트웨어 안전 관련 법·제도 정립 필요	<ul style="list-style-type: none"> • 소프트웨어 안전에 대해 관련법에 명확히 명시 하는 등 법·제도적인 기반 필요 • 법·제도가 마련되면 이를 토대로 적극적인 관련 중소기업 지원 정책 등 필요
소프트웨어 안전 관련 산업 구조 문제	<ul style="list-style-type: none"> • 국내 소프트웨어 시장은 그 규모가 작아 대부분 외산 소프트웨어를 구매하여 사용함 • 아직까지 소프트웨어 안전은 필수요소 보다는 소프트웨어 개발원가에 추가비용 부담으로 인식되어지고 있는 경향이 많음 • 소프트웨어 안전과 관련된 embedded system 개발 업체 등이 대부분 영세하여 소프트웨어 안전까지 고려하여 개발할 여건이 미흡함
소프트웨어 안전 전문 인력 부족	<ul style="list-style-type: none"> • 소프트웨어 안전 산업 활성화를 위해서는 전문 인력 양성이 반드시 선행 되어야 함 • 소프트웨어 안전 관련 전문 인력이 턱없이 부족하여 국가적인 차원에서의 지원이 반드시 필요함

3) 해결방안

(1) 법/제도/인증

소프트웨어 안전이 특히 중요시 되는 자동차, 원자력, 우주항공, 철도, 의료 등을 중심으로 관련 법·제도를 체계적으로 정비 할 필요가 있으며, 소프트웨어 안전 전반에 대한 부문과 관련 분야별로 필요한 부문으로 구분하여 법·제도를 정립 할 필요가 있다는 의견이 주를 이루었다. 최근 관심이 고조되는 인공지능, 자율주행차 등 기술발전

에 발맞추어 소프트웨어 안전 관련 법제정이 시급하며, 법제정 시에는 윤리적인 측면이 반드시 고려되어 이를 활용하는 인간에 대한 존엄을 무시해서는 안된다는 의견이 있었다. 또한, 관련 산업 발전을 위하여 대기업 보다는 현재 국내외적으로 인정받고 있는 전문 중소기업을 중심으로 지원이 이루어지도록 정책을 수립해야한다는 의견이 많았다.

인증의 경우에는 소프트웨어 안전 관련하여 별도의 국내 인증을 진행하기 보다는 원활한 완성품 수출 등을 위한 국제 표준 및 인증을 준용할 수 있도록 유도하는 것이 바람직하다는 의견이 있었다.

〈표 3-4〉 해결방안 - 법/제도/인증 관련 주요 답변

주요 도출 결과	주요 답변
정부의 역할에 대한 법·제도적 기반 정립 필요	<ul style="list-style-type: none"> • 전 세계적으로 자율주행차에 대한 관심 급등 등 최신 기술에 대한 수요가 급증하는 상황에서 정부 주도의 정책 수립이 미흡 • 소프트웨어 안전 관련기술은 빠르게 발전하나 제도적 뒷받침이 느린편임 • 소프트웨어 안전 및 자동차, 원자력, 우주항공, 국방 등 관련된 법·제도의 면밀한 검토를 통하여 관련 분야와 유기적으로 연결되는 실효성 있는 법제정 필요 • 법·제도 수립 시에는 윤리적인 측면까지 고려되어야 함
국내인증에 대해서는 본질적인 고찰 및 충분한 의견수렴 등이 필요	<ul style="list-style-type: none"> • 소프트웨어 안전 관련하여 별도의 국내 인증을 진행하기 보다는 원활한 완성품 수출 등을 위한 국제 표준 및 인증을 준용할 수 있도록 유도하는 것이 바람직함
국내 소프트웨어 안전 산업 활성화를 위한 전략적 정책 수립 필요	<ul style="list-style-type: none"> • 소프트웨어 안전 분야는 주로 북미, 유럽 등 선진국에서 우선 적용하는 분야로 국제적인 위상이 높은 국내 대기업 위주의 정책보다는 소프트웨어 안전 전문업체인 중소기업을 위한 정책이 필요함

(2) 표준/절차/가이드

현재 소프트웨어 안전 관련 국제표준을 기반으로 하여 소프트웨어 안전 분야 사업

기업 및 각 산업도메인별 기업 등에서 이를 적용할 수 있는 매뉴얼/가이드 그리고 관련 도구 등을 개발하여 사용하고 있으므로, 학계 주도로 이러한 정보 등을 서로 공유하고 교류하는 장을 마련하여 개별적으로 축적된 지식을 통합하고 공유하여 시너지 효과를 발휘할 수 있도록 해야 한다. 또한, 국제 표준 활동에 국내 관련 기업 및 연구자가 적극적으로 참여할 필요가 있으나 각 산업도메인별로 국제적인 위상 등에 의해 참여 가능 여부가 결정되므로 국제표준 활동에 실질적인 역할을 하는 데에는 한계가 있는 것으로 조사되었다.

〈표 3-5〉 해결방안 - 표준/절차/가이드

주요 도출 결과	주요 답변
글로벌 표준만으로 충분함	<ul style="list-style-type: none"> • 반드시 국내 자체적인 표준이 필요한 것은 아니라고 생각함 • 현재 존재하는 글로벌 표준만으로도 충분함 • 국내 자체 표준을 만들어야 실효성이 있는 것은 아닐 뿐 아니라, 현장에서는 표준이 하나 더 늘면 업무 과부하만 초래될 우려가 있음 • 현재 국제적으로 시장점유율이 높은 자동차 분야, 원자력 분야 등에 대해서만 글로벌 표준 참여 가능성이 높으나, 지속적으로 철도, 우주항공 등 분야에서도 적극적인 글로벌 표준 참여가 필요(각 분야의 산업발전이 선행되어야 하는 어려움은 있음)
관련 지식에 대한 통합과 공유 필요	<ul style="list-style-type: none"> • 학계 주도로 이러한 정보 등을 서로 공유하고 교류하는 장을 마련하여 개별적으로 축적된 지식을 통합하고 공유하여 시너지 효과를 발휘
민간 업체 자율적인 표준 진행	<ul style="list-style-type: none"> • 정부 등 공공기관에서 각자 표준을 만들어 민간 업체들에게 이 표준을 따르라고 하면 안됨 • 즉, 중앙집중식으로 표준을 만들어 강제화 하는 것은 비효율적임 • 다만, 신규 분야에 대해서는 우리나라(국내)에서 주도적으로 표준화 추진 검토 가능함

(3) 조직/기관

조직/기관을 통한 해결 방안으로는 범국가적인 소프트웨어 안전 컨트롤 타워를 수립하여, 사고 발생 시 관련 부처가 유기적으로 대응할 수 있는 비상 대응 체계를 마련

해야 한다는 의견이 조사되었다.

〈표 3-6〉 해결방안 - 조직/기관

주요 도출 결과	주요 답변
소프트웨어 안전을 위한 범국가적인 컨트롤 타워의 필요	<ul style="list-style-type: none"> • 소프트웨어 안전에 대한 컨트롤 타워 필요 : 미래부, 안전처, 산자부 등에서 별도로 연구 중이며, 범부처 기간(국무총리산하)의 컨트롤 타워가 필요함 • 향후 자율주행차, 드론, 원자력 등 소프트웨어 안전과 관련한 분야에서 사고 발생 시 대처할 수 있는 컨트롤타워가 지금부터 고려되어야 함 • 소프트웨어 안전은 자칫 범국가적 대형사고로 발전할 수 있는 원인이 될 수 있으므로 범국가적 컨트롤타워 마련이 시급함

(4) 인력/교육

교육부분에서는 Mass Production 관점에서의 인력양성이 아닌, 소프트웨어 안전 관련 인력양성을 위한 타게팅(targeting)된 교육 프로그램이 필요하며, 이러한 프로그램은 정부 및 공공기관이 주도하여 민간에 지월 할 수 있도록 정책 수립이 필요하다고 조사되었다.

〈표 3-7〉 해결방안 - 교육

주요 도출 결과	주요 답변
정부 및 공공기관 주도의 소프트웨어 안전 교육/연구에 대한 지원이 필요	<ul style="list-style-type: none"> • 소프트웨어 안전과 같은 관련 산업 발전을 통한 일자리 창출 필요 • 소프트웨어 인력에 대한 노임단가 현실화 등으로 인한 근본적인 소프트웨어 산업의 구조 개편이 선행되어야 함 • 각 도메인별로 특정 학과, 특정 기업 출신만 받아들이는 Closed Group인 경우가 많아 소프트웨어 전문 인력 각 도메인으로 진출할 수 있는 기회가 극히 제한되어 있는 산업구조를 타파해야 함 • 소프트웨어 인력 양성을 논할 때, 1만 명, 2만 명과 같이 Mass Production 관점으로만 접근하는 오류 존재하며, '소프트웨어 안전 전문가' 등 전문가

	<p>중심의 양성이 더 시급함</p> <ul style="list-style-type: none"> • 현재 국내 상황에서는 소프트웨어 안전 산업 활성화를 위해 초기에는 공공기관 등에서 전문 인력 양성 프로그램을 진행해야 함
--	--

(5) 業 환경개선

業 환경개선을 통한 소프트웨어 안전 제고 방안으로는 국가적 차원의 소프트웨어 안전을 위한 공통기반 사업을 먼저 추진하고, 학계 및 각 산업도메인별로 소프트웨어 안전이 필수사항으로 고려되어 분석/설계 될 수 있도록 개별적으로 지원 하는 것이 바람직하다는 의견이 주를 이루어 2015년도 조사 결과와 큰 차이가 없었다.

<표 3-8> 해결방안 - 業 환경개선

주요 도출 결과	주요 답변
<p>국가적 차원의 소프트웨어 안전을 위한 공통기반 사업을 먼저 추진하고, 학계 및 각 산업도메인별로 소프트웨어 안전이 필수사항으로 고려되어 분석/설계 될 수 있도록 개별적으로 지원</p>	<ul style="list-style-type: none"> • 국가 주도로 공공기관 등에서 먼저 설계 및 개발 시 소프트웨어 안전을 고려하여 개발 할 수 있는 환경을 조성할 필요가 있음 • 국가적 차원에서는 소프트웨어 안전의 공통기반 등에 대한 사업을 추진 할 필요가 있음 • 학계에서는 학문적인 관점에서 소프트웨어 안전에 대한 지속적인 연구를 수행하고, 업계에서는 안전이 필요한 분야 중심으로 각 도메인별 전문가에게 소프트웨어 안전을 재교육하는 방식으로 소프트웨어 안전 전문가를 양성할 수 있도록 해야 함 • 세계적인 트렌드는 소프트웨어 개발 시 보안(security)과 안전(safety)을 별도로 구분하지 않고 개발하는 추세임 • 예를 들어 Misra C에도 보안 코딩 가이드(부록)가 포함될 예정이고, CMU SER(보안 연구소)에서도 소프트웨어 안전을 고려하여 개발 할 수 있도록 함

(6) 프로세스

프로세스 측면에서는 2015년도 조사결과와 같이 소프트웨어 디자인, 설계, 개발, 사용, 관리의 전체 단계에서 소프트웨어 안전 활동을 수행해야 하지만, 기존 소프트웨어

개발 프로세스 진행에 과부하가 걸리지 않도록 구체적인 적용 방안에 대한 논의가 필요하다는 의견과, 각 부품에 대한 안전 테스트뿐만 아니라 완제품에 대한 안전 테스트 절차도 충실이 이행할 수 있도록 프로세스 개선이 필요하다는 의견이 조사되었다.

〈표 3-9〉 해결방안 - 프로세스

주요 도출 결과	주요 답변
소프트웨어 개발 전체 단계에서 소프트웨어 안전 활동을 수행하고, 완제품에 대한 충분한 안전 테스트 절차 수립 필요	<ul style="list-style-type: none"> • 소프트웨어 디자인, 설계, 개발, 사용, 관리 차원에서 안전(Safety)에 대한 고려가 필요 • 소프트웨어 개발 전 단계에서 소프트웨어 안전 활동을 수행해야 하지만, 기존 소프트웨어 개발 프로세스 진행에 걸림돌이 되지 않도록 구체적이고 단순한 적용 방안에 대한 논의가 필요 • 현재 국내 산업계에서는 충실히 수행중인 각 부품별 소프트웨어 안전 절차를 조립된 완제품의 경우에도 충분히 테스트 할 수 있는 절차를 확립해야 함

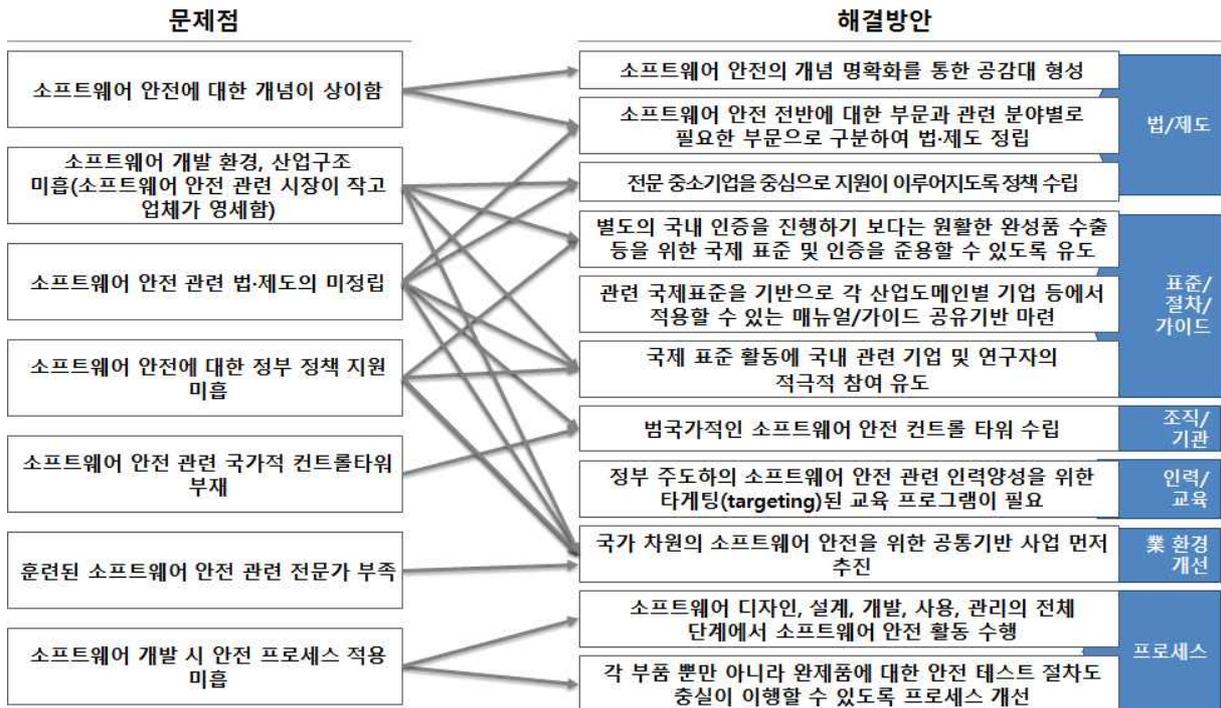
3. 조사 결과 종합 및 시사점

학계 및 공공기관 인터뷰 결과는 2015년도 조사 결과와 같은 목적으로 거시적인 측면에서 법·제도, 정책, 조직, 인력, 業 환경 그리고 프로세스의 개선 방안을 제시하였다. 특히 소프트웨어 안전의 개념은 공통의 공감대는 형성되어 있으나, 세밀한 정의 부분에 있어서는 소프트웨어 품질과 중복 되는 등 다양한 의견이 존재하여, 보다 단순화 시켜 다수가 공감하는 내용으로 정의 할 필요가 있다. (‘소프트웨어 안전이란, 인명이나 재산상 피해를 주는 사고 발생을 회피하기 위한 능동적인 방안(Safety Mechanism / Functional Safety)을 포함한 개념’)

현황 및 문제점으로는 주로 국내 소프트웨어 및 소프트웨어 안전 산업의 구조적인 문제인 소프트웨어 자체에 대한 인식 및 문화의 후진성 문제, 법·제도의 미정립, 정책 지원 미흡, 소프트웨어 안전 관련 국가적 컨트롤타워 부재, 전문 인력 부족, 관련 산업 구조적 문제 등이 주요 문제로 제기 되었다. 이의 해결을 위해서는 소프트웨어 안전 문화 정착, 소프트웨어 안전 관련 법·제도 수립을 통한 필요성 인식, 소프트웨어 안전 전문 중소기업 지원 정책 수립, 소프트웨어 안전 범정부 컨트롤 타워 확립, 현장에 즉시 투입 가능한 전문 인력 양성 방안 수립, 선순환 구조의 소프트웨어 안전

산업 구조 마련 그리고 소프트웨어 개발 전체 단계에서의 안전을 고려한 개발 등이 필요하다.

[그림 3-3] Governing 문제점 및 해결 방안



제2절 소프트웨어 안전 분야 사업 기업

1. 개요

소프트웨어 안전 분야 사업 기업의 산업동향 조사를 위해서 2015년도와 같이 TIC (Testing, Inspection and Certification, 안전사업포함) 시장에서 활동하는 기관 및 기업을 그 대상으로 하였다.

본 조사를 위한 설문은 2015년도에 개발한 설문지를 기준으로 크게 회사 일반 현황, 소프트웨어 안전 프로세스 현황, 소프트웨어 안전 인프라 현황 및 니즈(needs)에 대한 3개 분야로 이루어졌으며, 보다 정확한 결과 도출을 위해 대상 기업 및 기관에 대해 모두 대면 인터뷰를 수행하였다.

대상 기관 및 기업들의 주요 사업 영역으로는 소프트웨어 엔지니어링 컨설팅, 소프트웨어 품질 향상을 위한 프로세스(Process), 제품(Product), 전문인력(People) 측면의 솔루션 제공, 소프트웨어 테스트 자동화 도구 및 서비스 개발 및 공급, 임베디드 소프트웨어 테스트 솔루션 제공, 엔지니어링 시뮬레이션, 각종 인증 지원 등이 있다. 또한 대상 기업들의 경우 자동차, 철도, 원자력, 우주항공, 의료, 국방 등 특정 도메인에 특화되어 소프트웨어 메카니즘 설계, 시스템 소프트웨어 구현, Safety 검증/인증, 신뢰성 테스트 등을 복합적으로 수행하는 경우가 많아 명확히 그 경계를 구분하기 어려운 경우도 많다.

제1절 학계 및 공공분야와 같은 방법으로 이슈 및 문제점을 제기 하였고, 해결방안을 제시하였다.

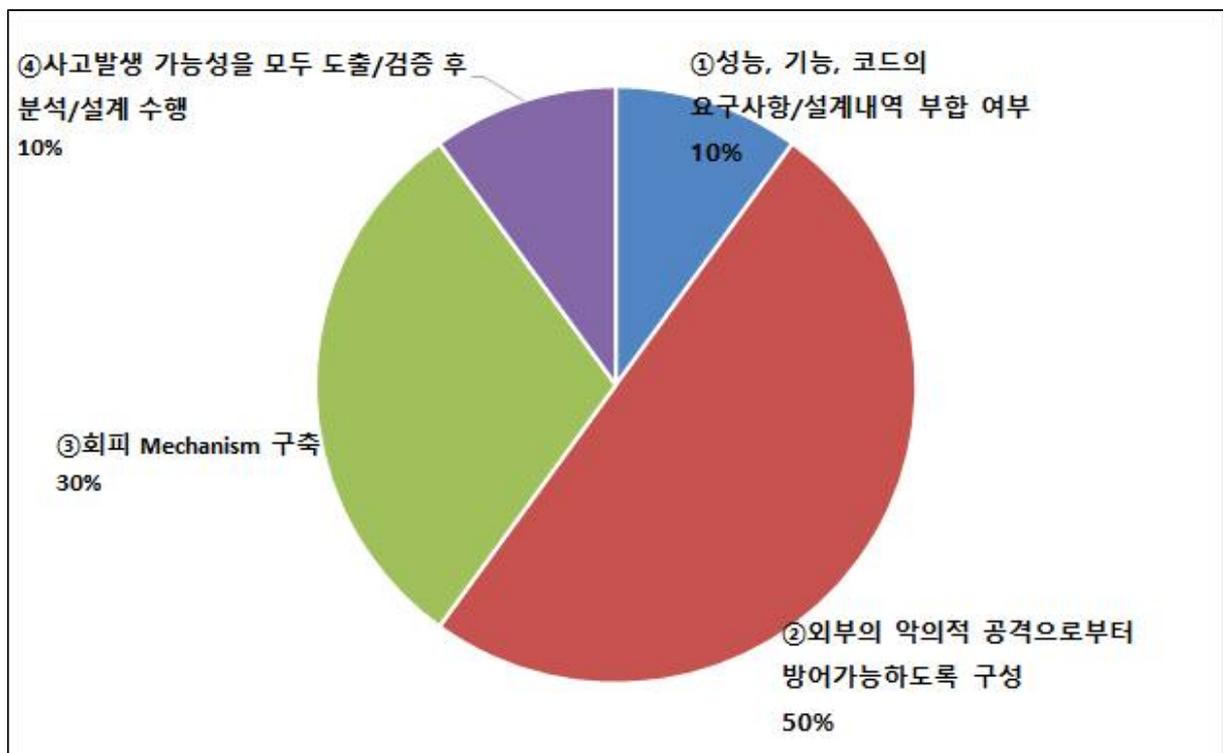
2. 회사 일반 현황

1) 소프트웨어 안전 개념 인식

소프트웨어 안전의 개념에 대해서는 50%가 ‘② 소프트웨어가 외부의 악의적 공격으로부터 방어할 수 있게 구성’ 하는 것을 소프트웨어 안전의 개념으로 선택하였으며, 30%가 ‘③ 예기치 못한 외부 환경 변화에 의하여 소프트웨어가 원인이 된 사고가 발생하는 것에 대한 회피 Mechanism을 구축’ 을, 10%가 각각 ① 소프트웨어의 성능, 기

능, 코드가 요구사항 및 설계내역에 부합 여부 ‘④ 사고발생 가능성을 모두 도출/검증 후 분석/설계 수행’ 하는 것을 소프트웨어 안전의 개념으로 인식하고 있었다. 이를 통해 관련 기관 및 업계는 소프트웨어 안전에 대해서 일반적인 안전의 개념과 비슷하거나 동일하게 인식하는 경향이 강함을 나타낸다. 하지만, 분석, 설계, 회피 메커니즘 등 전문 엔지니어링 측면에서 인식하는 경향도 40%로 결코 낮지 않아 소프트웨어 안전을 보편화하고, 문화를 확산하는데 오히려 걸림돌로 작용할 여지가 많다.

[그림 3-4] 소프트웨어 안전에 대한 인식 조사

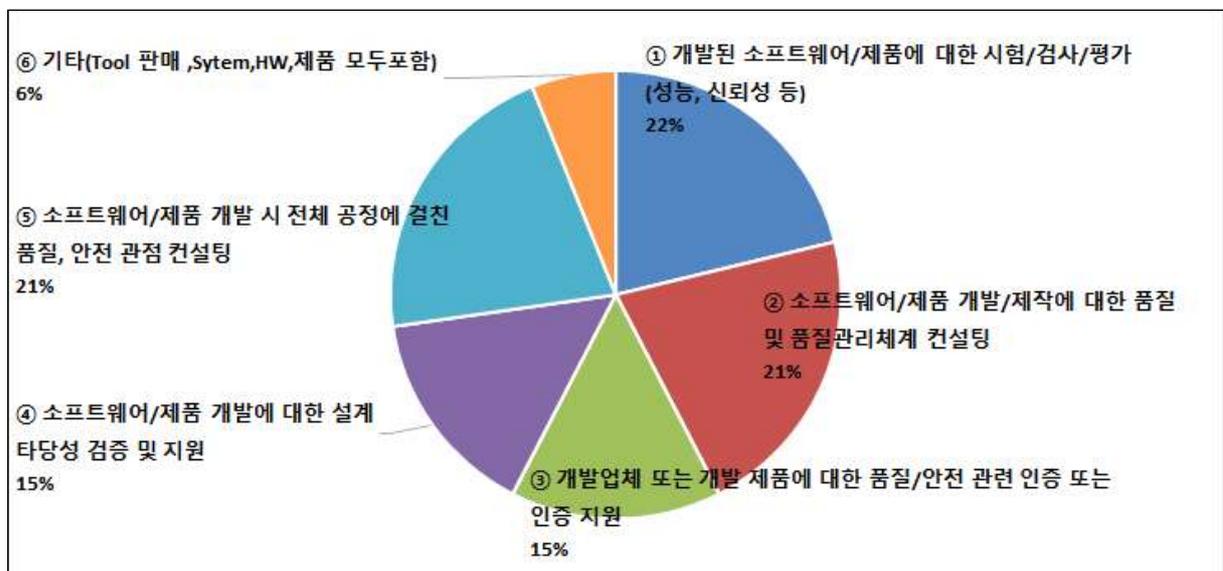


2) 소프트웨어 안전(Safety) 관련 주요 제공 서비스

대상 기관 및 기업에서 제공하는 주요 서비스는 성능/신뢰성, 컨설팅, 인증관련 서비스, 설계 타당성 검증/지원 등의 관점에 대해서 인터뷰를 진행하였는데, 다양한 분야에 고루 분포하는 것으로 나타났다. 그 중에서 ‘① 개발된 소프트웨어/제품에 대한 시험/검사/평가 (성능, 신뢰성 등)’ 서비스가 22%로 가장 높게 나타났고, ‘② 소프트웨어/제품 개발/제작에 대한 품질 및 품질관리체계 컨설팅’, ‘⑤ 소프트웨어/제품 개발 시 전체 공정에 걸친 품질, 안전 관점 컨설팅’ 등 소프트웨어 안전 관련 컨설팅 서비

스가 각각 21%로 그 뒤를 이었다. ‘③ 개발업체 또는 개발 제품에 대한 품질/안전 관련 인증 또는 인증 지원’, ‘④ 소프트웨어/제품 개발에 대한 설계 타당성 검증 및 지원’ 등의 서비스는 15%의 기관 및 기업에서 서비스를 제공하고 있었으며, 자동화 툴(Tool) 등 관련 제품을 직접 판매하는 경우도 있었다. 하지만, 자동화된 툴의 경우 소프트웨어 테스트 시 사용되는 Code Inspector, 소프트웨어 설계, 코딩, 테스트, 커버리지 분석, 요구사항 관리도구, 성능검증 시 부하발생 부문에 대해 사용하는 툴, 위험 분석 툴 등 자체 개발한 툴의 형태이며, 국제적으로 사용되는 외산 툴처럼 규격화, 제품화되기에는 부족한 형편이다. 향후 정부지원, 산학협력 등을 통해 전략적인 제품으로 개발하여 국제적인 경쟁력을 제고 할 필요가 있다.

[그림 3-5] 소프트웨어 안전(Safety) 관련 주요 제공 서비스



3) 관련자격 및 특허 보유 현황

관련자격 보유 현황에 대해서는 2015년 조사결과와 많이 다르지 않으며, 업계에서는 자격증의 필요성은 있으나 업무에 적합한 자격이 존재하지 않거나, 자격 보유여부가 업무 생산성과 연관도가 낮다고 판단하고 있어 그리 큰 비중을 두고 있지 않고 있다.

특히 소프트웨어 안전에 적합한 자격이 없어, ITQA (국제기술품질인증원) 등 테스트링 부문의 자격으로 대신하거나, ISTQB(국제 소프트웨어 테스트링 자격증) 등 기능안전(FUNCTIONAL SAFETY) 관련 해외 민간 자격증을 인정해 주는 경향이 있다. 정보처리

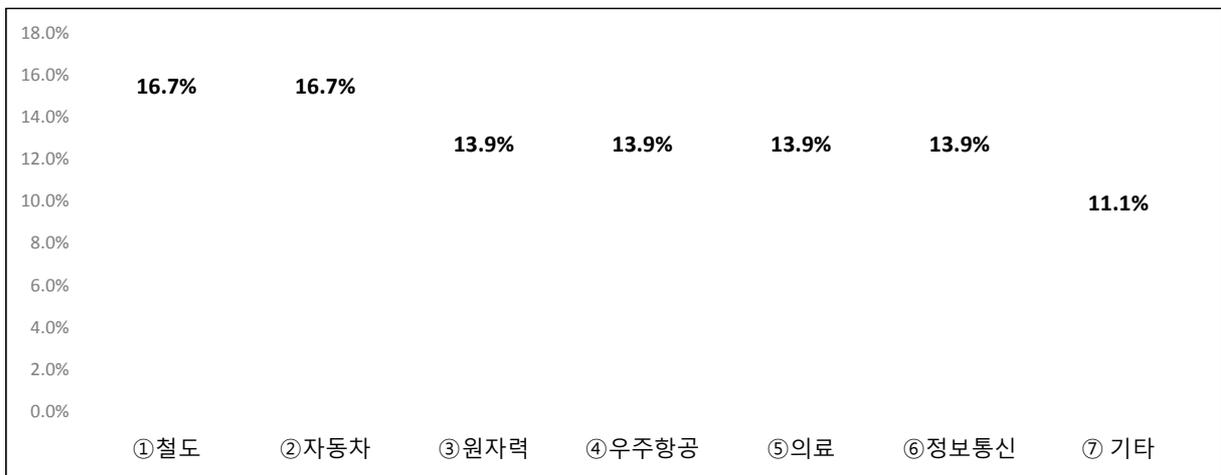
기사/기술사 등 일반적으로 통용되는 국내 자격증 정도만 필요하다는 의견도 있었다.

특허는 기관보다는 기업에서 정형언어 기반의 모델로부터 C/Ada 코드 자동 생성, 소프트웨어 안전 관련 도구(Tool) 관련 알고리즘 등 소프트웨어 개발 관련 부문과 자동차 전방인지관련 특허, 각종 제품 관련 특허 등 적용 도메인별 관련 특허를 보유하고 있다.

4) 고객 현황 및 요구사항

소프트웨어 안전 분야의 사업을 수행하는 기업의 해당 산업은 철도, 자동차, 원자력, 우주항공, 의료, 정보통신 산업 등에 고루 분포되어 있어, 2015년도 조사시 자동차 중심으로 편중되어있던 결과와는 다른 결과를 보여준다.

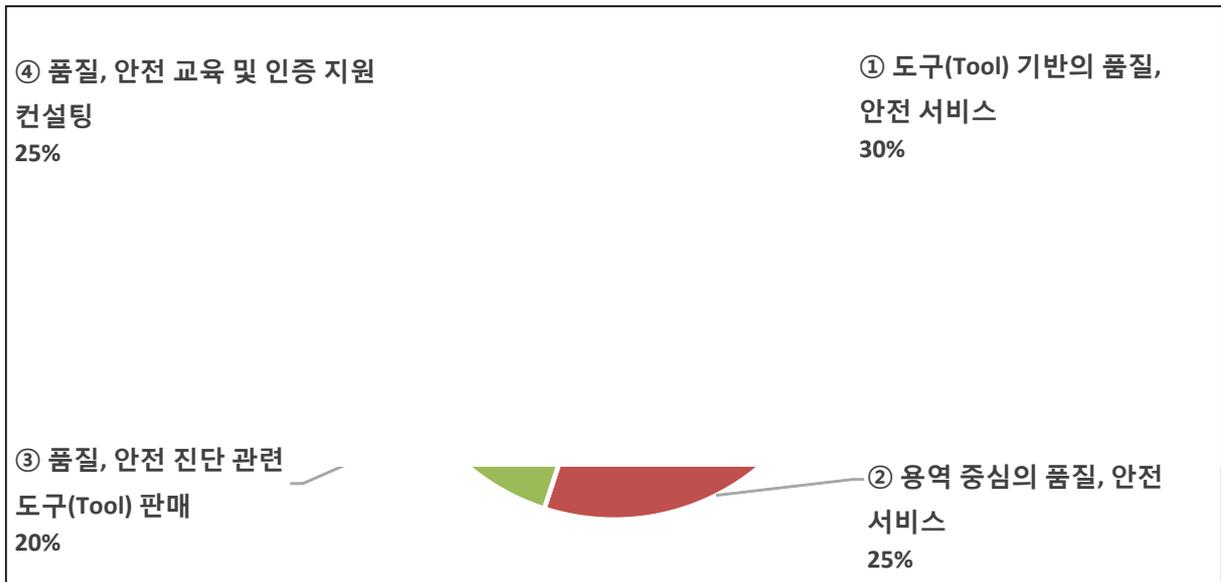
[그림 3-6] 주요 고객 산업군 분포 비중



대상 기업의 고객사에서 소프트웨어 인증/테스트/검사/안전 관련한 요구사항은 코드 테스트, 코딩 룰(rule) 검사, 소프트웨어 신뢰도 검증, 프로세스 컨설팅, 설계 규칙 컨설팅, 아키텍처/설계 컨설팅/리뷰, 테스트 컨설팅, 퍼포먼스 튜닝, 개발관련 문서 검증 등이다. 특히 자동차 분야의 경우에는 하드웨어를 포함한 기능안전 관련 엔지니어링 컨설팅을 요구하고 있는 경우도 있었다. 구체적으로 고객사에서 SW인증/테스트/검사/안전에 대하여 요청하는 대상은 [그림7]과 같다. ‘① 도구(Tool) 기반의 품질, 안전 서비스’에 대한 요구가 30%로 가장 많았고, ‘③ 품질, 안전 진단 관련 도구(Tool) 판매’와 ‘④ 품질, 안전 교육 및 인증 지원 컨설팅’이 각각 25%, ‘② 용역 중심의 품질, 안전 서비스’가 20%로 가장 낮게 나타났다. 아직까지 소프트웨어 안전 분야는 도구(Tool) 자체를 판매하기 보다는 도구(Tool) 기반의 컨설팅 서비스를 제공받기를 원

한다는 것이다. 이는 아직 도구(Tool)자체의 제품으로서의 완성도가 기대만큼 높지 않다는 반증이기도 하다.

[그림 3-7] 고객사 주요 요구사항



5) 국내 경쟁사 및 해외 선진사

소프트웨어 품질 및 안전관련 국내 기업은 대부분 그 규모가 작은 편이지만, 오랜 기간 소프트웨어 안전이라는 불모지를 지속적으로 개척해온 선구자들로서 투자, 전체 프로세스 관리, 관련 도구 활용 등에 강점을 가지고 있다. 이러한 결과는 2015년도 조사 결과와 많이 다르지 않다.

<표 3-10> 국내 선도 소프트웨어 사업자 강점

구분	강점	비고
도탈 서비스 제공	소프트웨어 안전 관련 고객 요구사항으로부터, 테스트에 이르기까지 소프트웨어 라이프사이클 전과정을 점검할 수 있는 품질관련 도탈 솔루션 제공	프로세스 전과정에 대한 관리 경험
과감한 투자	과감하고 지속적인 투자로 전문인력 확보를 통한 핵심 도구(Tool)를 개발 기반 마련	Tool의 보유 유무

대상 기업은 경쟁력 강화를 통하여 57%가 해외 진출을 원하고 있으며, 기존에 소프트웨어 안전 분야에서 선진국으로 통하는 유럽, 북미 보다는 시장을 선점할 기회가 많

은 아시아퍼시픽에 우선 진출하기를 원하고 있다. 이를 기반으로 향후 미국, 유럽(프랑스, 독일, 영국, 이탈리아), 러시아, 인도, 브라질, 캐나다 등에 도구개발/판매/지원/컨설팅 등 토탈 서비스를 제공할 계획을 세우고 있는 기업도 있었다.

〈표 3-11〉 해외 소프트웨어 선진사 강점

대 상	강 점
WindRiver	Safety Software 및 국제 안전 표준 기반의 심사 경험, 이론적 기반
엑시다	소프트웨어 안전 도메인에서 유명하며, 시스템 중심의 안전에 특화되어있고, 인력, 업무 노하우(반도체, 자동차 등) 등에 강점

6) 국제 표준

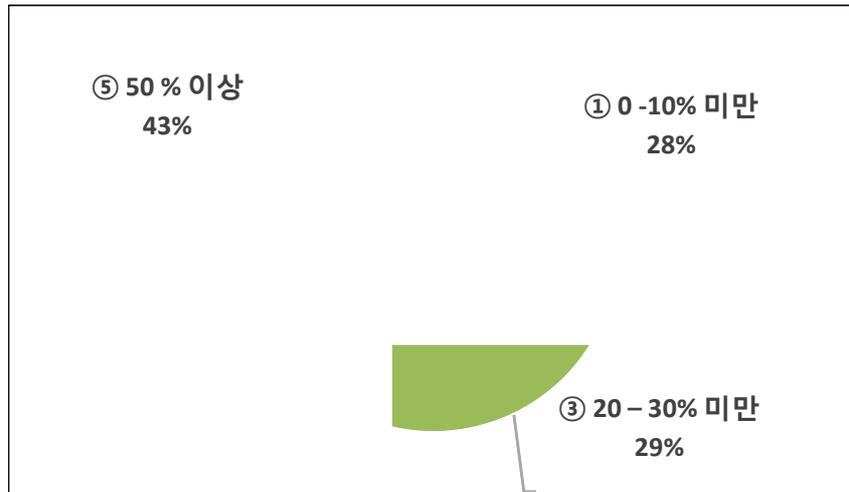
2015년도 조사와 같이 모든 국내 소프트웨어 안전 사업 수행자는 국제표준은 해당 ISO 및 IEC 가이드를 근간으로 각 산업 도메인마다 특화된 국제표준의 존재를 알고 있으며 이를 준용하고 있으며, 자동차 ISO26262, 철도 EN 50128/IEC 62279, 우주항공 DO178 등 현재 Global 표준을 준용하고 있다.

3. 프로세스 분석

1) 소프트웨어 안전이 차지하는 비중

제품개발 혹은 컨설팅 시 비용과 기간측면에서 ‘안전’ 이 차지하는 비중은 ‘⑤ 50% 이상’ 인 경우가 43%로 가장 많았다. 만일 ‘안전’ 에 대한 구분이 어려운 경우는 안전에 대한 정의 불분명 등으로 모집단에 대한 정의 어렵거나 불분명하거나 소프트웨어 안전이 품질, 신뢰성, 기능성 등과 혼재되어 사용되기 때문인 것으로 나타났다.

[그림 3-8] 소프트웨어 안전 사업 비중



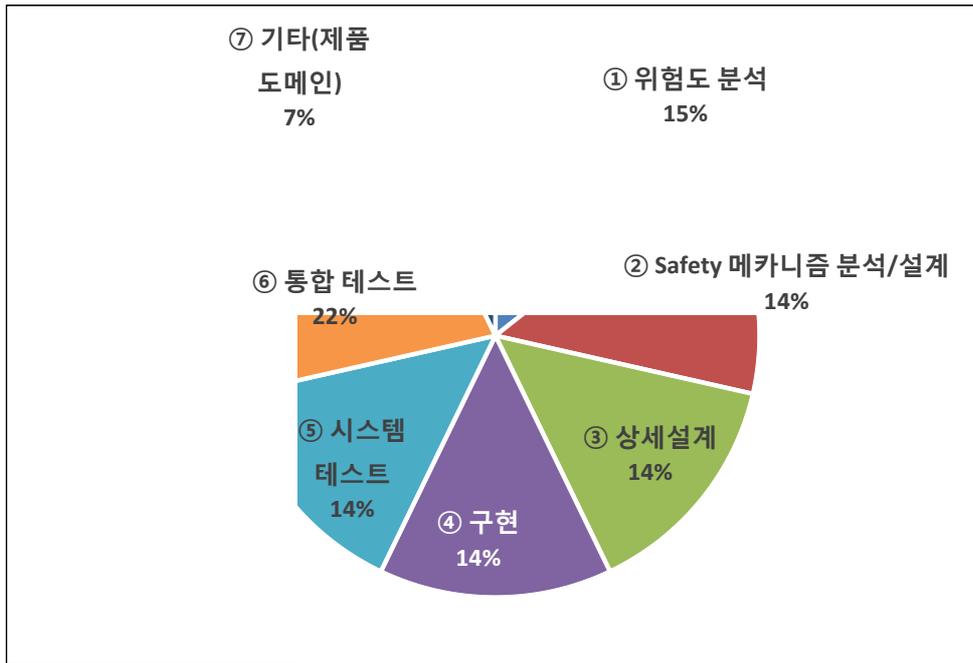
2) 소프트웨어 안전을 위해 가장 중요한 활동

관련 기관 및 기업에서 소프트웨어 품질, 테스트, 인증 등을 포함한 소프트웨어 안전의 관점에서 가장 중요하다고 생각되는 활동은 ‘⑥ 통합 테스트’ (22%)로 조사되었는데, 이는 제품을 만들기 위한 각 모듈 및 반제품에 탑재된 소프트웨어들이 통합되었을 때, 충분한 통합 테스트를 통한 안전에 대한 담보가 필요하기 때문으로 보인다.

통합 테스트 외에도 대부분의 활동이 비슷하게 중요하게 조사(위험도 분석 15%, Safety 메카니즘 분석/설계 14%, 상세설계 14%, 구현 14%, 시스템 테스트 14%) 되었는데, 그 이유는 답변자들 상당수가 아직 소프트웨어 안전을 소프트웨어 품질에 속한다고 인식하기 때문으로 판단된다.

안전은 근본적으로 결함을 가정하고 접근하는 것이 원칙으로 ‘① 위험도 분석’, ‘② Safety 메카니즘 분석/설계’가 안전의 기본요소인데, 이 중 Safety 메카니즘 분석/설계가 위험도 분석 보다 조금 더 중요하다고 조사되었는데, 그 이유로는 안전 관점에서는 ‘위험도 분석’이 가장 근간이 되는 작업으로 소프트웨어 안전은 시스템 엔지니어링 단계에서부터 넘어온 Hazard/Risk Data로부터 어떠한 Safety Requirements를 개발 하는지가 핵심 요소이기 때문이다.

[그림 3-9] 소프트웨어 안전에 필요한 활동 중요도



3) 소프트웨어 관련 인증 제도(GS인증, SP인증 등)의 효과성

현재 국내에서 적용되고 있는 소프트웨어 관련 인증 제도(GS인증, SP인증 등)은 소프트웨어 안전성 확보에 효과적이냐는 질문에는 57%가 ‘② 그렇지 않다’ 라고 대답하여 소프트웨어 안전 관점에서는 국내 소프트웨어 관련 인증이 그리 중요하지 않다는 의견이 주를 이뤘다. 그러나 최소한의 품질기반 하에 최소한의 안전이 보장 된다면, 소프트웨어 공학에 대한 기본적인 이해가 없는 조직에 소프트웨어 공학과 문서화 등에 대한 기본적인 이해를 제공해 주는 역할을 통하여 효과성이 입증되었다는 의견도 43%에 달한다.

이러한 불합리성을 극복하기 위해서는 기존체계와는 대상 및 범위가 다른 새로운 인증체계/활동 등이 필요하고, 소프트웨어 안전을 위한 인증 문화/마인드 혁신 등이 필요하다. 또한 보다 실질적이고 손쉬운 접근방법을 소개하고, 각 활동의 근본적인 취지와 목적을 이해시키는 것이 중요하다. SP인증 등 기존 인증제도를 보완하는 것보다는 소프트웨어 안전 관련 신규 인증을 도입하는 것이 필요하다는 의견도 개진되었다. 그러나 충분한 논의가 부족한 상태에서 의욕만 앞서워서는 실제 활용도가 낮은 무용지물이 될 우려도 적지 않다.

4) 소프트웨어 안전에 대한 등급/수준 구분

제공 서비스가 해당하는 산업 분야별로 소프트웨어 안전에 대한 등급 및 수준을 구분하여 서비스하고 있다는 대답이 86%로 압도적으로 높으며, 산업 도메인별로 별도의 국제표준이 존재하므로 각각 상이한 수준을 요구하고 있다. 특히 수출기업은 국제표준에 부합하는 등급채택이 필수인 경우가 많다. 또한 등급체계가 A~D, 1~5등급 등 표시방법이 다양하나 동일 산업 도메인 내에서는 표시방법 일원화를 통해 혼란을 최소화해야 한다는 의견도 있었다.

〈표 3-12〉 업계에서 적용 중인 등급/수준 예

구분	내용	비고
자동차의 위험 등급(Automotive Safety Integrity Level, ASIL)	<ul style="list-style-type: none"> ASIL은 ISO 26262 준수를 위한 핵심 사항으로 개발 프로세스가 시작될 때 결정됨 시스템의 각 기능들은 일어날 수 있는 위험에 따라 분석됨 ASIL은 “실패할 경우, 운전자와 다른 운전자에게 어떤 일이 발생할까요?” 라는 질문을 하게 됨 <p>A (안전이 별로 중요하지 않은 레벨) B, C (안전이 중요한 레벨) D (안전이 가장 중요할 레벨)</p>	D등급이 안전이 중요한 프로세스와 엄격한 테스트 규제를 가지는 등급

4. 소프트웨어 안전 인프라 현황 및 니즈(Needs)

1) 법·제도 방향성

현재 영위하고 있는 비즈니스가 강화되기 위해 현재의 법/제도 차원에서 추가적인 제정이나 변경이 필요하다는 의견은 86%가 ‘① 그렇다’ 라고 대답했다. 하지만, 구체적인 적용 방법에 대해서는 법과 표준에 대한 명확한 운영 방안이 먼저 확립되어야 하고, 여타 관련 법령과의 관계설정도 쉽지 않을 것이고, 법령이 제정 되더라도 즉시 적용 혹은 점진적 적용 등 적용시점도 고려되어야 한다는 의견이 많았다. 대기업에 비해서 중소기업은 사업 진행이 어렵기 때문에 중소기업 활성화를 위한 법 개정이 필요하며, 국제표준을 국내 실정에 맞게 가볍게 적용할 필요가 있다.

소프트웨어 안전은 컨설팅, 검증 등 제3의 독립적인 기관이 수행하는 것이 적절하고, 소프트웨어산업진흥법 내에도 소프트웨어 검증 및 인증 비용을 예산에 포함시키는 규정 등이 필요하다.

2) 관련 매뉴얼/Tool

대상 기관 및 기업 모두 소프트웨어 안전 관련 매뉴얼과 도구(Tool)를 보유하고 있으며, 시험절차, 시험환경 구성, Test Case 도출 방법 등에 대한 매뉴얼이 존재하고, 선진 외국의 도구(Tool)를 사용하고 있다는 의견이 많았다. 그러나 국제표준 및 기존의 도구(Tool)만으로 실제 국내 산업에서 적용하기에는 한계가 존재하고, 외산 도구(Tool)는 그 가격이 너무 높아 비용부담이 커서, 각 기관 및 기업의 상황에 맞게 적절히 Tailoring하거나 자체 개발하여 활용하고 있다. 이런 도구(Tool)에는 코드 검증, 모델 검증, 상위 개념으로써의 품질 검증 등을 위한 도구(Tool) 등을 자체 개발 하여 사용하는 경우도 많았다. 특히 국방 등 특정 도메인에서는 자체 개발하여 사용하는 경우가 더욱 많았다.

3) 인력 현황

대상 기관 및 기업 등은 해외인력 소싱에 대해서 57%가 ‘② 그렇지 않다’ 라고 대답하여 해외에서 인력을 데려오기 보다는 국내에서 인력을 원활히 채용하기를 더욱 원하고 있다고 볼 수 있다. 그러나 앞서도 언급했듯이 국내 소프트웨어 산업의 구조적인 문제 등으로 인한 소프트웨어 인력 처우의 개선이 시급하다.

해외인력을 소싱하고자 하는 43%는 전문성 제고, 경험확보, 신규정보 취득 등의 목적으로 전체 보유 인력의 10%~20% 정도의 비중으로 채용하기를 원했다. 또한 해외인력 소싱을 위해서 고객 니즈 파악, 전문인력 수배, 예산확보, 고객협의, 통역준비 등의 절차를 수행하고 있었다.

전문인력 확보 및 육성을 위해서는 소프트웨어 안전 분야에 대한 Best Practice를 많이 확보하여야 하며, 초기 전문가 그룹 확보를 위해 초기 전문가 그룹에 집중투자, 전문가별 전문영역 확보, 해외 세미나 참석/사례 및 기술 등 벤치마킹이 필요하다는 의견이 있었다. 각 영역별 교육 과정 개발 및 강사 양성을 위해서는 현 소프트웨어 안전 교육 문제점을 분석하고, 이론과 실무가 조화된 교육을 시행하고, 강사 커뮤니티 참여 및 지속적 자격 관리, 표준 교육 교재 개발 등이 필요하다.

4) 시장 측면

철도, 원자력, 우주항공, 국방 등은 공공성이 강하나 실제 정부 주도로 소프트웨어 안전을 강조하는 발주는 이뤄지지 않고 있으며, 공공성이 강한 분야에 대한 소프트웨어 안전을 담보할 수 있는 공통기반 마련 미흡하다. 해결방안으로는 안전이 강조된 공공성이 강한 분야가 많으므로 소프트웨어 안전 자체를 공공성이 강한 것으로 부각하여 관련 사업 예산 수립 및 발주가 필요하며 소프트웨어 안전에 대한 공공성을 부각할 필요가 있다.

5. 조사 결과 종합 및 시사점

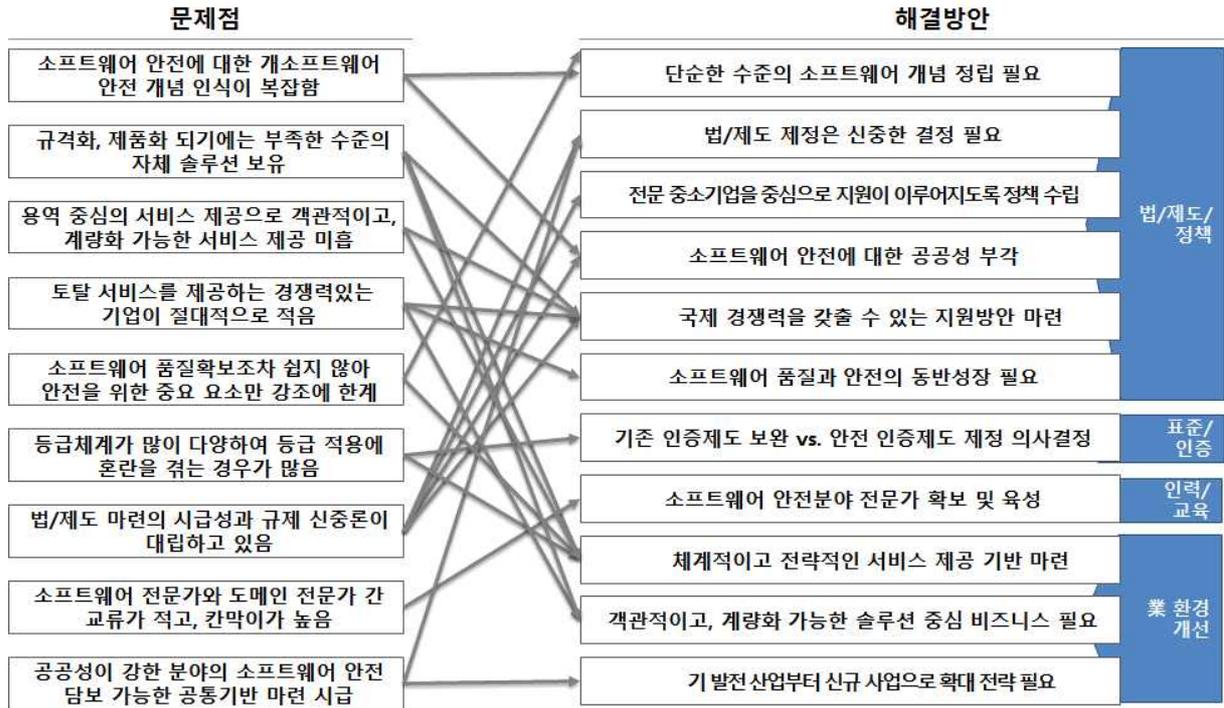
소프트웨어 안전 전문기업 간에도 그 개념의 차이가 존재하며, 그 이유는 명확한 개념 정립 후 사업을 영위하기 보다는 관련 산업에 종사하면서 나름대로의 개념정립을 하여 개념이 복잡하게 얽혀 있는 경우가 많다. 좀 더 단순한 개념 정립을 통하여 관련 업계뿐만 아니라 법/제도, 정책 수립 시에도 명확한 공감대 형성을 통해 커뮤니케이션 오류를 최소화 할 필요가 있다.

국내 안전분야 사업 기업의 경우 규격화, 제품화되기에는 부족한 수준의 자체 개발 결과물을 솔루션화 하여 컨설팅 등과 함께 서비스 하는 수준이며, 객관적이고 계량화가 가능한 수준의 글로벌 경쟁력을 갖춘 솔루션 중심의 비즈니스로의 전환이 반드시 필요한 상황이다. 이를 위해서는 법/제도, 정부의 정책적인 지원이 뒷받침 되어야 하며, 이를 통하여 소프트웨어 안전에 대한 공공성을 부각 시키고, 기존에 소프트웨어 품질에 국한되었던 것을 ‘안전’ 이라는 개념으로 확장 시킬 필요가 있다. 특히 법/제도 마련은 시급하다는 주장과 관련 법/제도 제정이 새로운 규제로 산업 발전을 전할 수 있다는 신중론이 양립하고 있어 관련 분야 전문가, 법률 전문가, 정책 수립자 등 이해관계자 간의 면밀한 검토가 반드시 필요하다.

관련 전문인력 부족의 문제는 안전분야 사업을 수행하고 있는 기업들도 예외는 아니어서 자동차, 철도, 우주항공, 원자력, 의료 등 도메인 전문가를 중심으로 소프트웨어 안전에 대하여 논하는 그룹이 있는가 하면, 소프트웨어 공학적인 측면에서부터 시작하여 각 도메인쪽으로 접근하는 방식으로 소프트웨어 안전을 논하는 그룹이 있다. 이 두 그룹간의 원활한 정보 공유의 장이 주기적으로 마련될 필요가 있으며, 특히 향후 폭발적으로 증가할 것으로 예상되는 소프트웨어 안전 관련 인력 양성을 위한 고등교육기

관, 정부 주도의 교육 기관 등에서의 체계적인 교육이 필요하다.

[그림 3-10] Supervising 문제점 및 해결 방안



제3절 End User 기업

1. 개요

조사대상은 정보통신, 자동차, 금융, 우주항공 및 기타(댐/상하수도 등) 부문의 소프트웨어 개발/판매 기업을 대상으로 하여 1:1 대면 인터뷰 방식으로 진행되었다. 인터뷰는 기업 내의 사업담당 임원, 현장 실무 책임자(기술진) 또는 품질 담당자를 대상으로 진행되었다.

조사영역은 소프트웨어 안전/품질 관련 일반 현황, 예방점검 활동, 대응관리 활동, 소프트웨어 안전에 관한 정책요구사항으로 구분하였고, 이러한 영역에 대한 설문을 기반으로 인터뷰를 수행하였다. 인터뷰 대상 기업은 일반적인 업무용 소프트웨어 개발 및 특정 솔루션 개발, 하드웨어 제작과 더불어 펌웨어 개발 등을 수행하는 기업이기 때문에, 소프트웨어 안전 뿐 아니라 소프트웨어 품질 및 테스트의 범주도 포함하여 인터뷰가 수행되었다. 그리고 대기업, 중견기업, 중소기업 및 신생 벤처기업 등 기업 규모의 다양성을 포함했으며, 종합 IT서비스(업무용 소프트웨어 개발 포함), 소프트웨어 솔루션 개발, 장치제조와 융합된 소프트웨어 개발 등 사업유형의 다양성 또한 포함하였다. 2015년 조사 대비 4배가 넘는 20여 개 이상의 기업을 대상으로 하였으며, 설문/인터뷰 시 그 답변에 실효성이 극히 낮은 경우를 제외하고 19개 기업의 답변을 기반으로 현황분석을 실시했다.

〈표 3-13〉 End User 부문 조사 대상

업종	기업 사업유형	기업 규모	조사방식	완료여부
정보통신	종합IT 서비스	대기업/중견 및 중소기업	대면 인터뷰	완료
정보통신	전문 솔루션 개발	중소기업	대면 인터뷰	완료
정보통신	장치 제조 + 펌웨어 개발	중견기업, 중소기업	대면 인터뷰	완료
금융	제1금융권 IT서비스	중소기업	대면 인터뷰	완료
자동차	장치 제조 + 펌웨어 개발	대기업	대면 인터뷰	완료
우주항공	장치 제조 + 펌웨어 개발	대기업, 신생 벤처기업	대면 인터뷰	완료
기타(댐, 상하수도 등)	종합IT 서비스	중소기업	대면 인터뷰	완료

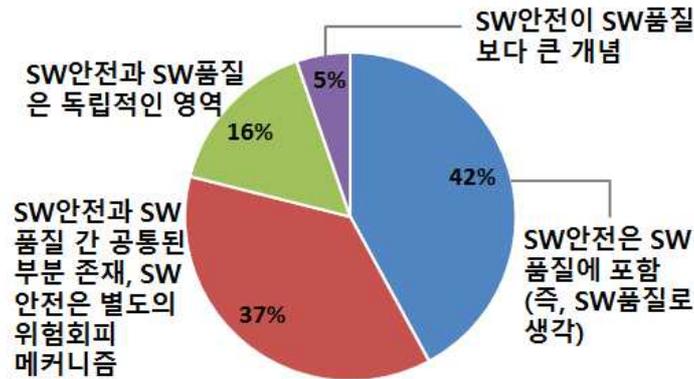
2. 소프트웨어 안전 일반 현황

1) 소프트웨어 안전에 대한 인식과 정의

전체 인터뷰 대상 중 32%의 기업만 소프트웨어 안전에 대한 개념을 인지하고 있는 상황이며, 인지하고 있더라도 기업 차원(또는 조직 차원)의 인지가 아니라 대부분 인터뷰 대상자인 개인 차원의 인지였다.

소프트웨어 안전에 대한 정의에 대해서 상이한 의견들이 존재했으며, ‘소프트웨어 안전은 소프트웨어 품질 영역에 포함’ 된다는 의견이 가장 많았으며(42%), ‘SW안전과 SW품질 간 공통된 부분은 존재하나 SW안전은 별도의 위험회피 메커니즘’ 이라는 의견 또한 다수(37%) 존재했다. 이에 대한 상세한 답변 내역은 아래와 같다.

[그림 3-11] 소프트웨어 안전에 대한 정의



대부분의 기업들은 소프트웨어 안전을 독립적인 영역이 아니라 품질과 연계하여 생각하고 있으며, 소프트웨어 안전을 독립적 영역으로 정의한다면 향후 설문/인터뷰에서 답변 할 내용이 거의 없다는 의견을 제시했다.

2) 소프트웨어 운영관리체계 및 인증

End User 기업 중 89%가 전사 차원의 소프트웨어 운영 관리 규정과 절차를 보유하고 있었으며, CMMI 혹은 ISO20000 등과 같은 국제표준인증을 취득했거나 준비 중인 기업은 그 보다는 약간 적은 78.9%였다. 그러나 Safety-Critical SW에 대하여 요건설계, 테스트, 인증 등 적절한 SW안전을 위한 검증활동을 수행하는 기업은 57.9%만 존재했다.

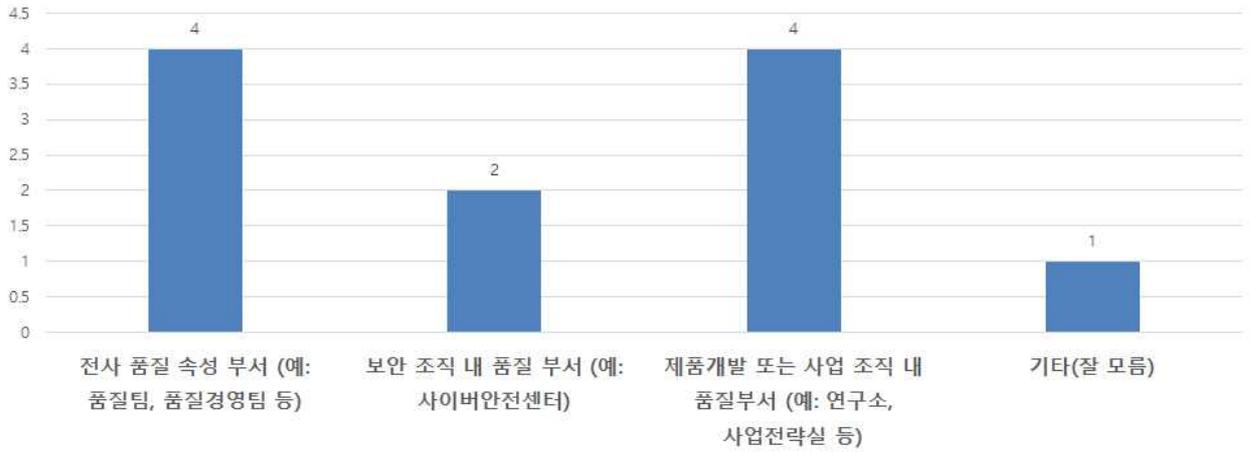
즉, 대부분의 기업에서 소프트웨어에 대한 전사적이고 체계적인 관리 규정 등은 존재하나, 안전이나 품질 관점에서 구체적인 검증활동을 수행하는 경우는 상대적으로 적었다.

소프트웨어의 품질 및 안전에 대한 관리 관점에서 형식적인 체계, 절차는 존재하나 소프트웨어에 대한 구체적인 검증활동은 상당히 미흡하여 현행 체계와 지침에 따른 활동만 충실히 수행하더라도 기본적인 품질과 안전 수준이 향상 될 것으로 추정된다.

3) 소프트웨어 안전 및 품질 관련 조직

소프트웨어 안전을 담당하는 부서 및 담당자가 지정된 경우는 전체의 57.9%이며, 이러한 부서들은 대부분 소프트웨어 품질관리 집중하고 있다.

[그림 3-12] 소프트웨어 안전 관련 업무 담당하는 부서의 속성



대부분의 관리부서는 품질경영팀, 연구소 등 소프트웨어 및 제품 품질관리 위주의 부서였으며, 소프트웨어 안전만을 관리하는 부서는 존재하지 않았다.

3. 소프트웨어 안전 예방점검 활동

1) 안전 또는 품질을 위한 활동 내역

소프트웨어 기능오류로 인한 안전사고 예방활동은 ‘Safety-Critical SW 구축 시, 별도의 소프트웨어 안전 전문가 투입’ (35.7%), ‘소프트웨어 안전에 관련된 요건 정의 및 준수’ (32.1%), ‘제3자 전문 테스트 업체 활용’ (25.0%) 등을 수행하고 있다,

[그림 3-13] 소프트웨어 기능오류로 인한 안전사고 예방 활동



안전사고 예방활동은 대부분 ‘안전’ 보다는 ‘품질’ 관점이며, 활동의 대부분을 차지하는 ‘Safety-Critical SW 구축 시, 별도의 소프트웨어 안전 전문가 투입’, ‘소프트웨어 안전에 관련된 요건 정의 및 준수’는 내부 기술인력 및 전문가를 활용하여 수행하고 있다. 이에 반하여, 객관성이 확보 될 수 있는 제3자를 활용한 검증은 전체의 25.0%만 차지하고 있다.

Safety-Critical SW 검증활동 수행 시 활용하는 외부업체는 국내업체(88.9%)가 해외업체(11.1%)에 비하여 절대 다수를 차지하며, 이러한 외부업체를 활용하는 이유는 제3자를 활용한 객관적인 신뢰성 확보가 50%를 차지하고 나머지 50%는 고객의 요구 때문이었다.

소프트웨어 품질 및 안전을 강화하기 위하여 사용되는 비용은 IT서비스 업체의 경우에는 프로젝트 기반으로 진행되기 때문에 정확한 산출이 어려웠으며 솔루션 개발/판매, 장치 제조 기반으로 펌웨어 개발 업체에서는 구체화된 제품을 출하하기 때문에 제품 인증비용, QC 인력 등에 대한 비용 산출이 가능했다. 이러한 경우에도 각 기업마다 비용 산정 단위(M/M, 원화 등등)와 관리 관점이 상이하여 평균치 등의 산출은 불가능했으며, 각 기업별 1천만원 소요/년, 제품별 인증 비용 1.5억 원/년, 솔루션 품질관리 인력 24M/M 등의 개별 정보만 도출되었다.

2) Safety-Critical 소프트웨어 검수 표준 및 지침

Safety-Critical SW 검수에 대한 회사 내부의 표준을 보유하고 있는 기업은 84.2% 이나, 해당 표준이나 지침을 부품업체 또는 하도급 업체에도 전달되어 적용되는 경우는

이보다 적은 68%였다.

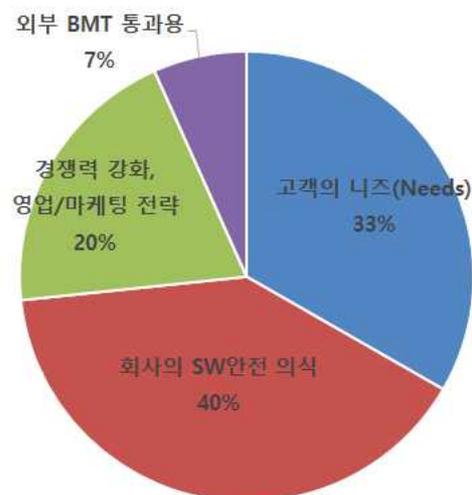
Safety-Critical SW 검수에 대한 표진 및 지침이 부품업체 또는 하도급 업체에 적용이 안 될 경우 제품 전체의 품질과 안전에 악영향을 미칠 수 있다고 판단된다.

3) 안전성을 강화한 소프트웨어 제품 제조 및 판매 계획

안전성(Safety)을 강화한 제품을 제조/판매하고 있거나 양산할 계획이 있는 기업은 전체의 47.4%이며, 이러한 기업들은 자동차 제조, IT인프라(서버 등) 제조, 우주항공(드론 등) 등 장치제조 기반의 IT 기업들이 다수를 차지하고(55.6%) 있다. 그 외 기업들은 대기업군 이거나 솔루션 개발 기업들이었다.

양산 계획이 있는 이유는 고객의 니즈(Needs), 제품 경쟁력 강화/영업 전략, 외부 BMT 통과용 등 외적 요인이 다수를 차지하고 있다.

[그림 3-14] 안전성 강화 제품의 제조/판매할 계획이 있는 경우 그 이유



고객의 니즈(Needs), 외부 BMT 통과용은 직접적인 외부 환경에 기인한 것이며, 제품 경쟁력 강화/영업 전략은 외부 환경에 선제적 대응을 하여 매출 증대를 위한 것으로 이러한 외적 요인에 기인한 이유가 총 60%를 차지하며, 회사의 SW안전 의식에 기인한 경우 즉, 내적 요인에 기인한 경우는 40%를 차지한다.

4. 소프트웨어 안전 대응관리 활동

1) 소프트웨어 사고에 대한 대응 시나리오

제품과 관련된 사고에 대한 대응 시나리오를 보유하고 있는 기업은 58%이며, 58% 기업의 대부분은 대기업이거나 자동차 및 서버 제작 등 제조 기반 ICT 기업들이 다수였다.

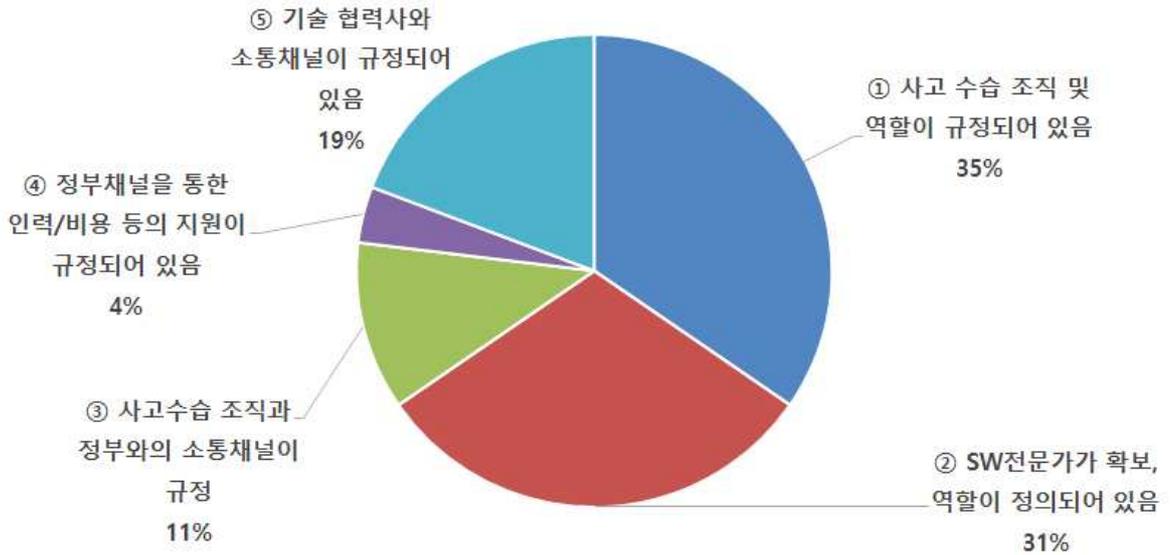
[그림 3-15] 제품(솔루션) 관련사고 대응 시나리오 보유 현황 및 보유 기업 속성



즉, 비교적 자금 여유가 있는 기업이나 제품의 사고가 기업의 존속과 직접 연결되는 기업중심으로 사고에 대한 대응 시나리오를 보유하고 있다. 이와 더불어, 사고 대응 시나리오를 보유하고 있더라도 시나리오에 따라 정기적인 대응훈련을 실시하고 있는 기업은 18.2%에 그치는 소수였다.

제품(솔루션)에 대한 사고 대응 시나리오 내 소프트웨어 영역이 정의되어 있는지에 대한 질의에서 대부분 기업(90.9%)이 정의 되어 있다고 답변했다. 이러한 소프트웨어 영역에서 적용되는 항목 중 많은 부분을 차지하고 있는 것은 사고 수습 조직 및 전문가 확보와 역할 정의 부분이었으며, 그 상세한 내용은 아래와 같다.

[그림 3-16] 사고 대응 시나리오 중 소프트웨어 관련 영역 적용 항목



사고 대응 시나리오 내 소프트웨어 영역 항목 중 사고 수습조직 및 역할 규정, 소프트웨어 전문가 확보 및 역할 정의 등 기업 내부 관점에서의 기본적인 대응 체계는 존재하고 있으나, 정부와의 소통채널 및 협력사와 소통채널과 같이 기업 외부와의 관계, 의사소통 등에 대한 대응 체계는 극히 취약한 수준이다.

2) 사고 발생 시 문제해결 요소 및 자동화 틀

소프트웨어 관련 사고 발생 시 문제해결을 위하여 필요한 요소의 순위에 대한 질의 시 필요 요소는 ‘Best Practice : 유사 해결사례’, ‘인력’, ‘예산(비용)’, ‘의사결정/소통’, ‘정부지원’, ‘기타’ 를 제시하였다. 대부분 ‘기타’ 를 제외하고 제시된 5개가 필요 요소라고 인정하였으며, 이 중 ‘인력’ 이 가장 우선순위 높은 문제해결 필요 요소라 답변하였다.

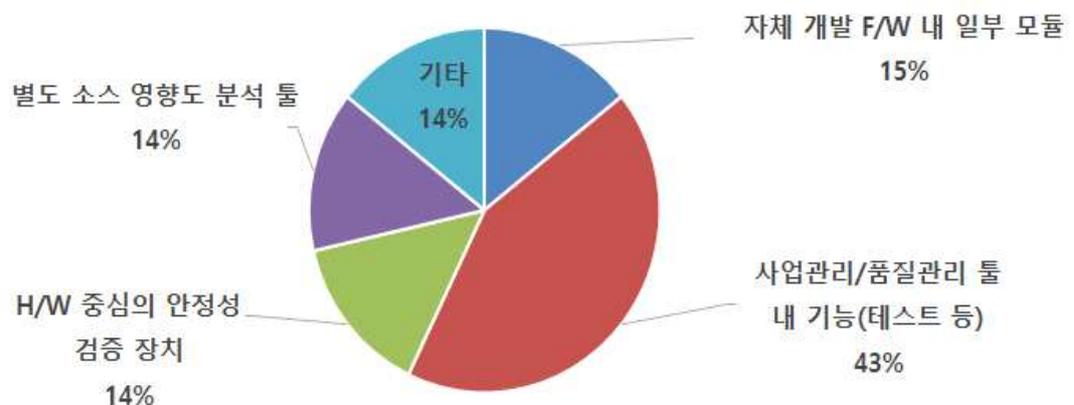
[그림 3-17] S/W 관련 사고 발생 시 문제해결을 위하여 필요한 순위



사고 발생 시 문제해결을 위하여 필요한 요소 중 1위인 인력, 2위인 유사해결사례는 모두 기술력 관점의 필요 요소이다. 또한, 1위부터 3위까지 순위는 존재하나 그 격차에는 큰 차이가 없는 바, 문제해결을 위하여 가장 필요한 요소는 ‘기술과 비용’으로 정의 할 수 있다. 이와 더불어, 유사해결사례의 경우에는 각 기업들에서 ‘자체 보유 해결사례는 외부 공유가 어렵다(사내 보안 및 해결사례 자체가 하나의 자산이다 등)’ 및 ‘그럼에도 타 사의 해결사례 등은 알고 싶다’ 라는 비공식적 의견이 많았다.

소프트웨어 안전에 관한 전반적인 검증활동을 관리하는 툴 또는 시스템을 보유하고 있는 기업은 전체 인터뷰 대상 중 36.8% 이었다. 이들 기업이 보유하고 있는 툴(또는 시스템) 중 대다수를 차지하는 것은 ‘사업관리/품질관리 툴 내 기능(테스트 등)’로 42.9%를 차지하고 있으며, 보유 툴에 대한 상세 현황은 아래와 같다.

[그림 3-18] SW안전에 관한 전반적인 검증활동을 관리하는 툴 보유 현황



전문 검증 툴이 아니고 관리시스템 내 일부 기능이며, 소프트웨어 안전 검증 관련 툴(시스템)이 아니라 품질 관리 및 사업 관리를 위한 툴(시스템)만 보유하고 있다.

3) 소프트웨어 안전 사고사례 정보 관리

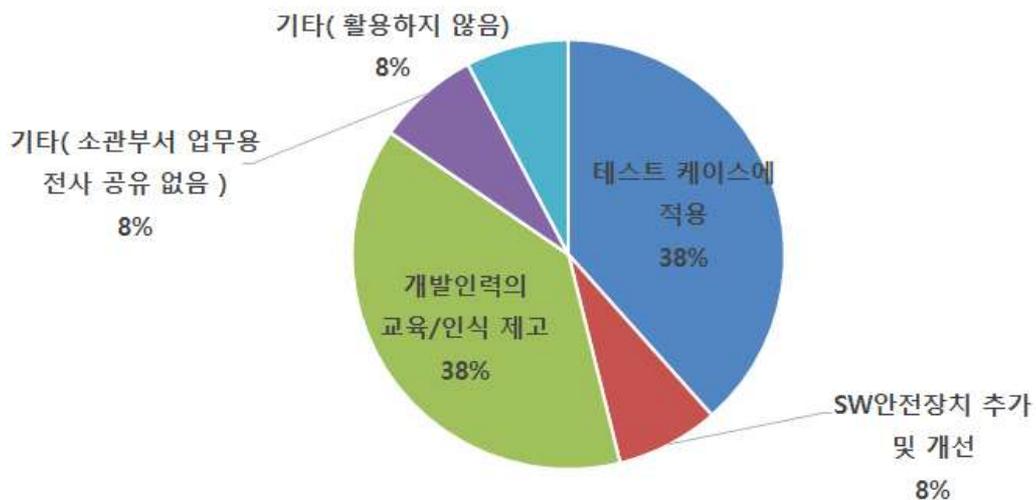
전체 인터뷰 대상 기업의 31.6%가 소프트웨어 안전 테스트 및 사고사례정보를 수집/축적하고 있다. 이러한 기업들의 속성은 자동차, IT장비제조, 솔루션 개발, 대기업, 공공기관으로 대기업과 공공기관은 경영/품질관리 규정 때문에, 그 외 기업은 제품개발 등 사업추진 시 필요하여 정보를 수집/축적하고 있다. 정보를 수집/축적하는 기간은 3년 미만과 5년 미만이 가장 많았으며, 10년 이상 축적하는 기업은 자동차 제조 기업 하나만 존재 했다.

[그림 3-19] SW안전 테스트 및 사고사례정보를 수집/축적 기간



수집/축적 된 안전 테스트 및 사고사례정보는 주로 ‘테스트 케이스에 적용’, ‘개발인력의 교육/인식 제고’에 활용되며 소프트웨어 안전기능 개선에 활용되는 경우는 극히 드물었으며, 정보를 단순히 수집/축적만 하고 활용이 없는 경우도 존재했다.

[그림 3-20] 소프트웨어 안전 테스트 및 사고사례정보 활용 내역



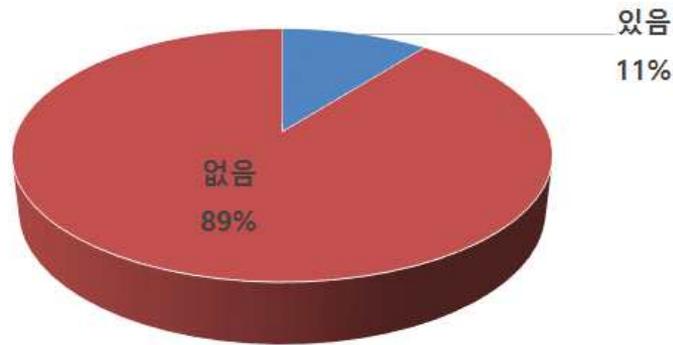
5. 소프트웨어 안전에 관한 정책 요구사항

1) 정부의 정책적 지원을 받은 경험

소프트웨어 품질을 포함한 소프트웨어 안전관련 인증(예: SP인증)을 위한 정부의 정책적인 지원을 받은 경험이 있다는 답변은 11%이며, 있다고 답변한 End User의 속성

은 정부의 시스템 운영하는 공공기관, 제1금융권 IT서비스 기업이었다. 위 기업의 속성을 고려 할 때 정부의 정책적인 지원은 거의 전무 했다고 추정된다.

[그림 3-21] 소프트웨어 안전 인증 관련 정부의 정책 지원을 받은 경험



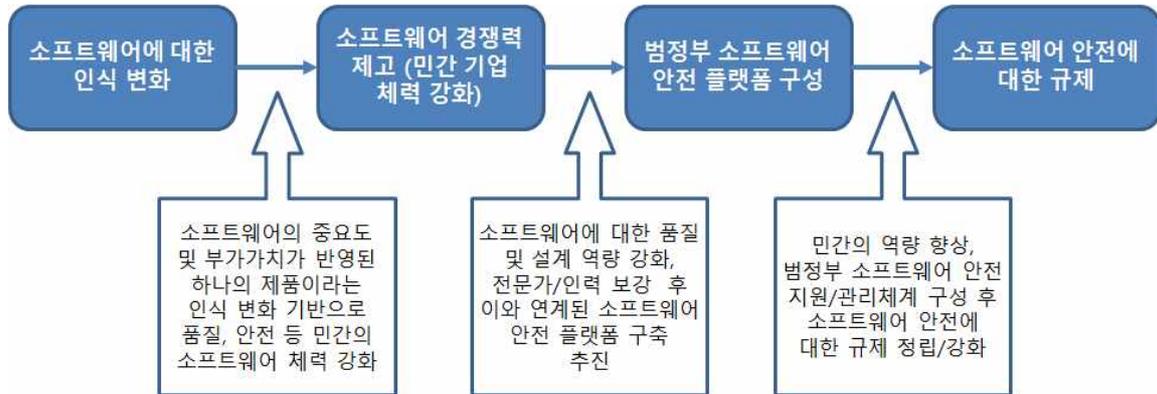
소프트웨어 품질을 포함한 소프트웨어 안전관련 정부의 정책적인 지원을 받는다면 필요한 주요 요소에 대한 답변은 ‘예산(비용)’, ‘Best Practice : 유사 해결사례’, ‘인력’ 이었다. 그 외, 기타 필요 요소로 해외 판로 개척에 대한 지원, 교육 등이 존재했다.

2) 정부의 지원 요구 및 개선사항

소프트웨어 안전 및 품질 관련 정부를 대상으로 민간 기업이 지원을 요구하는 내용은 상당히 다양하다. 각 기업들이 당면한 상황과 사업 환경의 차이로 정부 지원에 대한 요구는 존재하는 기업 수 만큼 다양하게 도출된다. 그럼에도 가장 공통된 부분은 ‘규제’ 와 ‘지원’ 이 균형을 이루어야 한다는 것과 보다 구체적이고 현실적인 지원이 이루어져야 한다는 것이다.

소프트웨어 안전에 대한 정부를 대상으로 한 민간의 요구사항을 도출한 결과 시계열 흐름에 따른 단계적 요구사항 추진절차가 구성되었다. 이는 ‘소프트웨어에 대한 인식의 변화’ 로부터 시작되어 ‘소프트웨어 안전에 대한 규제’ 로 이어지는 총 네 개 단계로 구성된다.

[그림 3-22] 정부에 대한 지원 요구사항 : 단계별 요구내역 추진절차



소프트웨어에 대한 인식이 사회전반에 걸쳐 그 중요도가 높으며, 부가가치 높은 제품이라고 변화된 후 민간 기업 중심으로 소프트웨어 설계/개발/관리에 대한 기초체력 강화 실시, 이를 기반으로 정부 주도로 소프트웨어 안전 플랫폼을 구성한 이후 안전에 대한 규제를 강화해야 한다. 이러한 일련의 흐름 중 순서가 바뀌게 되면 기반이 매우 취약한 추진이 이루어지게 되어 어떠한 훌륭한 정책, 제도라 하더라도 현실적인 도입이 불가능해진다.

(1) 소프트웨어에 대한 인식 변화

가장 먼저 우선되어야 할 것은 소프트웨어를 바라보는 인식/문화에 대한 변혁이다. 소프트웨어는 현재 대부분의 제품/장치에 포함되어 있거나 일반적인 업무 수행, 사회 생활에 필수적인 영역으로 그 중요도는 매우 높다. 그러나 아직까지도 우리나라 사회에서는 소프트웨어를 개발과 변경을 손쉽게 할 수 있는 것, 그다지 많은 원가가 투입되지 않더라도 생산이 가능한 것 등 제대로 생산/관리하겠다는 인식이 극히 낮다.

소프트웨어를 기술집약적 고부가가치 제품으로 인식해야하며, 이런 인식이 선행되어야 올바른 설계, 구축이 이루어지고 사고 발생 가능성이 낮아지게 된다.

이와 더불어 품질, 안전에 대한 인식 또한 변화해야 한다. 소프트웨어의 품질 확보 및 강화, 안정성 제고 등이 보장 받으려면 품질/안전은 당연히 고려해야 한다는 인식이 확산되어야 한다. 품질/안전은 누군가가 별도로 보는 것 또는 이에 소요되는 비용은 절감 가능한 것 등의 인식이 사라지지 않으면 품질, 안전에 대한 보장은 영원히 이루어지지 못한다. 즉, 사회 전반에 걸쳐 소프트웨어에 대한 인식과 문화의 변혁이 절실하게 필요하다.

(2) 소프트웨어 경쟁력 제고(민간 기업 체력 강화)

소프트웨어에 대한 인식/문화의 변혁 이후, 소프트웨어를 개발, 판매, 유지관리하는 기업들의 역량강화가 필요하다. 특히, 중소기업들은 소프트웨어 공학의 도입/품질 관리/안전성 제고 등을 위하여 별도의 예산과 전담인력을 투입 할 여력이 없다. 이러한 부분의 보강을 위하여 정부 차원의 예산 지원 및 관련 분야 사업화가 필요하다.

이와 더불어 정부 발주 정보화 사업 추진 시 설계의 품질, 개발/구현의 품질 모두 고려 할 수 있도록 예산을 추가 확보해야 한다. 사업 발주 시 해당 부분에 대한 명확한 고려를 명시하고 이에 수반되는 사업비를 책정하게 되면 민간 기업들은 품질과 안전 모두 포함하는 역량을 보유하게 된다. 즉, 외부 사업 환경 변화에 맞추어 기업의 체질과 체력 또한 강화되는 것이다.

CMMI 또는 해외 수출관련 필요 인증 취득 시 인증 요구사항의 의미, 절차 및 프로세스 등을 몰라 장기간이 소요되거나 인증 취득에 실패하는 중소기업들이 다수 존재한다. 대기업의 경우에는 별도 전담 조직이 있으나 중소기업의 경우는 그렇지 못하며, 민간의 인증컨설팅 기업이 존재하더라도 신뢰도, 비용 측면에서 무리가 있는 경우도 존재한다. 인증 취득에 대한 정부 차원에서 관련 지원이 필요하며, 현재 인증 지원을 하는 공공기관의 서비스도 그다지 구체적이지 못하며 현실적 지원이 미흡하다.

(3) 소프트웨어에 안전에 대한 규제

국내 소프트웨어 안전 관련 정책 기반 및 시장 환경이 구성 된 후 안전에 대한 규제가 강화되어야 한다. 개별 기업의 준비, 관련 역량 강화, 국가적인 지원체계 등이 선행되지 않은 상태에서 규제는 현실적이지 못하며, 효과성 또한 극히 낮다.

대부분의 기업들은 소프트웨어 안전 영역에 대하여 설문/인터뷰 시 또 하나의 규제가 만들어져서 업무 부담 과중 및 소요 비용 증가로 이어지는 것이 아닌지에 대한 우려가 높았다. 이와 더불어 초반에는 정부가 규제 말고 지원을 중심으로 정책을 수립하고 활동해야 한다는 의견이 다수 존재했다.

결론적으로 소프트웨어 안전에 대한 규제는 필요하나, 앞서서 논의된 지원체계가 구성 된 후 실시하는 것이 실효성이 높다고 조사 되었다.

6. 조사 결과 종합 및 시사점

End User 기업을 대상으로 주로 사용자 관점에서의 안전 활동, 문제점 및 요구사항 등이 조사되었으며, 보다 세부적으로는 소프트웨어 안전 일반 현황, 소프트웨어 안전 예방점검활동, 소프트웨어 안전 대응관리활동, 소프트웨어 안전에 관한 정책 요구사항 분야에 대하여 설문/인터뷰를 진행하였고, 이에 따라 시사점과 개선방향이 도출되었다.

소프트웨어 안전 일반 현황에서는 32%의 End User 기업 만 소프트웨어 안전에 대한 개념을 사전에 인지하고 있었으며, 소프트웨어 안전의 정의에 대해 상이한 의견이 혼재하고 79%는 안전은 품질과 연계 되거나 품질기반이라 생각하고 있다. 또한, 대부분 기업에서 소프트웨어 품질/안전에 대한 관리체계는 보유하나 구체적인 검증활동 수행은 미흡하였고 절반 이상 기업(57.9%)에서 소프트웨어 품질/안전 전담 조직이 존재하나 모두 품질 중심의 활동만 수행하고 있었다. 이에 따라 소프트웨어 안전에 대한 명확한 정의와 산업계 대상 확산이 필요하며 소프트웨어 품질과 안전 관련 구체적 활동 내역 구분과 명확화가 시급한 것으로 분석되었다.

소프트웨어 안전 예방점검활동에서는 대부분의 기업이 안전사고 예방활동은 대부분 ‘안전’ 보다는 ‘품질’ 관점이며, 기업 내부 인력/전문가 중심의 예방활동 수행하여 객관성이 확보 될 수 있는 제3자를 활용한 검증은 전체의 25.0% 만 차지하고 있다. 단, 솔루션 개발/판매, 제조 기반 IT 기업 중심으로 품질/안전 관련 객관적이고 구체적인 활동을 수행하고 있었다. Safety-Critical SW 검수에 대하여 기업 내부 표준/지침은 대부분 보유하고 있었으나, 부품공급 업체 등에 이러한 표준/지침 확산/적용은 다소 미흡했다. 이와 더불어 안전성(Safety)을 강화한 제품을 제조/판매하고 있거나 양산할 계획이 있는 기업은 절반 이하(47.4%)이며 대부분 자동차 제조, IT인프라(서버 등) 제조, 우주항공(드론 등) 등 장치제조 기반의 IT 기업들이 다수를 차지하고 있다. 안전성 강화 제품을 추진하는 이유는 고객의 니즈(Needs), 제품 경쟁력 강화/영업 전략, 외부 BMT 통과용 등 외적 요인이 다수를 차지하고 있다. 이에 따라 소프트웨어 품질 및 안전 관련 예방/검증 시 객관적인 방안 고려가 필요하며, 기업의 사업 속성에 따라 소프트웨어 안전 관련 차별화된 추진이 고려되어 한다. 또한, 무엇보다 우선하여 소프트웨어 안전에 대한 민간 기업의 인식 변화가 시급하며, 사업 환경적인 필요에 의하여 기업이 소프트웨어 안전을 자발적 추진하도록 하는 것이 현실적이라 분석되었다.

소프트웨어 안전 대응관리활동에서는 제품(솔루션)과 관련된 사고에 대한 대응 시나리오를 보유하고 있는 기업은 대기업군을 제외하면 자동차 및 서버 제작 등 제조 기

반 ICT 기업들이었으며, 사고 대응 시나리오에 따라 정기적인 대응훈련을 실시하고 있는 기업은 18.2%로 소수였다. 소프트웨어 사고대응 시나리오를 구체적으로 보면, 기업 내부 관점에서의 기본적인 대응 체계는 존재하나, 기업 외부(정부 또는 협력사 등)와의 관계, 의사소통 등에 대한 대응 체계는 극히 취약했다. 이와 더불어 소프트웨어 관련 사고 발생 시 문제해결을 위하여 필요한 요소는 '기술과 비용' (인력, 유사해결사례, 예산-비용)이었는데, 기업의 보안 및 이익 논리 때문에 소프트웨어 안전 사고해결 사례에 대한 기업 간 공유는 불가능하다고 조사되었다. 소프트웨어 품질 및 안전에 대한 검증, 관리 툴(시스템)은 36.8%가 보유하고 있으며, 이러한 툴(시스템) 대부분은 '사업관리/품질관리'에 집중되고 있으며 기술기반의 전문적인 검증 툴은 거의 전무했다. End User 기업의 31.6%가 소프트웨어 안전 테스트 및 사고사례정보를 수집/축적하고 있었으며, 수집/축적 된 안전 테스트 및 사고사례정보는 주로 '테스트 케이스에 적용', '개발인력의 교육/인식 제고'에 활용(76%)되고 있었고, 소프트웨어 안전기능 개선에 활용되는 경우는 극히 드물었다(8%). 이에 따라 소프트웨어 안전 관련 기업의 사업 속성에 따라 차별화된 추진 고려가 필요하며 소프트웨어 안전을 위한 구체적인 행동지침과 강제성이 필요하다고 판단된다. 소프트웨어 사고대응은 기업 내부 및 외부까지 모두 고려한 종합적이 체계가 필요하고 시장 논리로 인하여 추진이 불가능한 부분 중심으로 정부차원의 우선 추진을 고려해야 한다고 분석되었다.

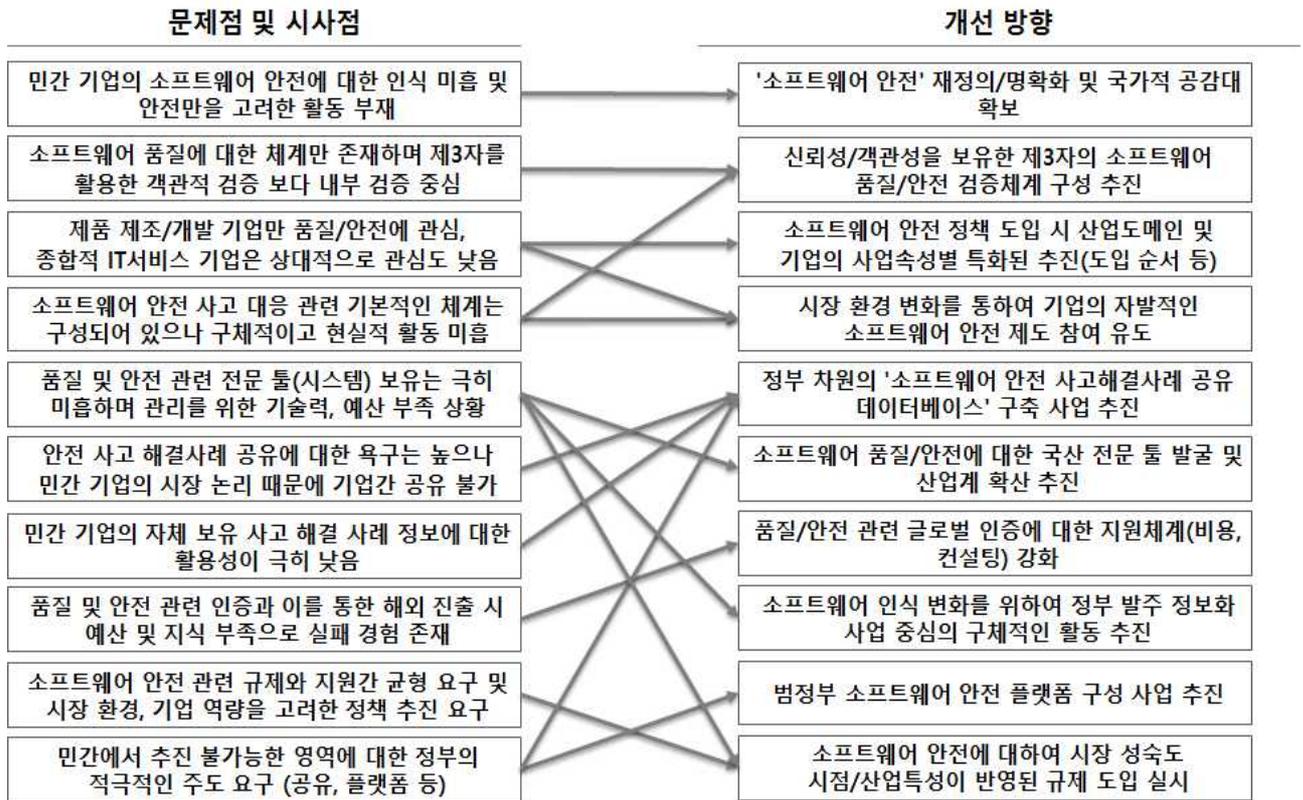
소프트웨어 안전에 관한 정책 요구사항에서는 소프트웨어 품질을 포함한 소프트웨어 안전관련 인증(예: SP인증)을 위한 정부의 정책적인 지원을 받은 경험이 있다는 답변은 11%에 불과했다. End User 기업들의 주된 요구사항을 보면 소프트웨어에 대한 인식 변화 → 소프트웨어 경쟁력 제고 → 범정부 소프트웨어 안전 플랫폼 구성 → 소프트웨어 안전 규제의 순서에 따라 정부의 활동이 이루어져야 한다고 조사되었다. 즉, 시장의 준비 및 각 기업들의 역량을 고려하지 않고 규제 중심으로 소프트웨어 안정 정책이 추진되면 기업들은 정책 추진 방향에 대한 대응이 불가능하다고 조사되었다. 먼저 사회 전반에 걸친 문화와 인식이 변혁되고 소프트웨어 안전에 관련된 기업들(특히, 중소기업)의 취약점이 강화되면서 범정부적인 소프트웨어 안전에 대한 지원체계가 구성 되어야 현실적인 안전 규제가 이루어 질 수 있다고 분석되었다. 특히, 중소기업 중심으로 인증에 대한 현실적이고 구체적인 정부 지원, 소프트웨어 품질 및 안전 강화를 위한 정부의 관련 사업발주, 안전 관련 사고해결사례에 대한 정부 주도의 공유체계 구성, 설계 검증을 위한 기술적 지원 등에 대하여 매우 강력한 요구사항이 도출된 바, 이에 대한 체계적인 대응이 필요 한 것으로 분석되었다.

End User 기업을 종합적으로 보았을 때 주로 자동차 부문 기업이 안전 개념의 이해, 검증 활동, 사고 정보 축적 등이 잘 이루어지고 있었고, 항공 부문 기업은 일부분이 진행되고 있는 실정이었다. 금융의 경우는 안전 개념 및 활동이 다소 부족해 보이는데 이는 금융의 특성상 안전보다는 보안을 더 중시하기 때문으로 판단된다. 아래 표는 주요 산업도메인(자동차, 항공, 금융)별 차이가 발생하는 조사항목에 대한 비교자료이다.

〈표 3-14〉 산업도메인별 조사항목 비교

특이항목	자동차	항공	금융
소프트웨어 안전 인식	안전 개념 모두 인지 - 안전이 품질보다 큰 개념(50%)	안전 개념 일부 인지 - 안전은 품질과 다름	안전 개념 부재 - 안전은 품질에 포함
Safety-Critical 소프트웨어 검증활동	모두 외부업체 활용	일부 외부업체 활용(33.3%)	외부 업체 사용 안함
안전성 강화 제품 제조, 판매	모두 판매/양산 계획 존재(100%) - 고객 니즈, 회사의 안전 의식 때문	일부 판매/양산 계획 존재(67%) - 고객 니즈, 회사의 안전 의식 때문	판매/양산 계획 부재
제품 사고 대응 시나리오	모두 시나리오 보유 (100%) - 구체적/정기적 대응훈련 없음	일부 시나리오 보유 (33.3%) - 구체적/정기적 대응훈련 없음	모두 시나리오 보유 (100%) - 비정기적 대응훈련 실시
안전 테스트 및 사고사례정보를 수집, 축적	일부 사례정보 수집, 축적 (50%)	사례정보 수집, 축적 없음	사례정보 수집, 축적 없음
안전 사고 수습 필요 요소	1순위: 의사결정/소통 2순위: 인력	1순위: Best Practice 2순위: 인력	1순위: 의사결정/소통 2순위: 인력

[그림 3-23] End User 기업 문제점 및 개선 방향



제4장 비교 분석 및 SWOT 분석

제1절 비교 분석

1. 개요

2015년 전년도와 학계, 소프트웨어 안전 분야 사업 기업, End User 기업을 대상으로 조사한 국내 소프트웨어 안전 산업 현황과 2016년도 기준으로 조사된 현황을 비교하여 변화 포인트를 파악하였다.

2. 2015년 대비 2016년 국내 소프트웨어 안전 산업 비교 분석

먼저 학계 및 정부 부문에서 전년도와 차이가 발생하는 항목은 소프트웨어 안전 개념 측면인데, 전년도에는 소프트웨어 안전이 품질과는 구별된다는 의견이 주를 이루었으나, 2016년도의 인터뷰에서는 사람의 생명 및 건강에 직·간접적으로 연관되어야만 소프트웨어 안전이라고 정의하고 있고 소프트웨어 안전 분야가 정립되면 소프트웨어 안전이 품질을 포함하는 개념으로 발전할 개연성이 있다고 조사되었다.

국내 소프트웨어 안전 분야 사업 기업 부문에서 소프트웨어 안전 개념은 안전에 대한 정의를 추상적이고 일반적인 개념으로 인식하고 있었으며 35% 비율로 안전/품질/보안을 구분한 반면, 2016년도에는 소프트웨어 안전을 보안 관점으로 인식하는 경우가 50%에 달했으나 분석, 설계, 회피 메카니즘 등 전문 엔지니어링 측면으로 인식하는 경향도 40%로 조사되었다. 그리고 자격증 관련된 결과는 전년도와 다르지 않으나 자격 보유 여부가 업무 생산성과 연관도가 낮다고 판단하여 자격증보다는 실무경험을 중시하였고 2015년 자동차에 편중되어 있었던 고객군은 철도, 자동차, 원자력, 우주항공, 의료, 정보통신 산업 고객군으로 고루 분포되어 있었다. 이것은 다양한 고객군으로 확대되었다기보다는 조사 대상이 다양화되었다는데 의의를 두는 것이 적합할 것이며 이로 인해 조사 자료가 전년도보다는 좀 더 객관성을 보유했다고 볼 수 있다. 소프트웨어 안전관련 인증(GS/SP인증)은 안전성 확보에 효과적이지 않다는 인식이 감소(2015년 76% → 2016년 57%)되었으며 정책 요구사항으로 철도, 원자력, 우주항공, 국방 도메인 별로 구체화하여 정부 주도의 기반 구축이 필요하다고 조사되었다.

End User 기업 부문에서는 전년도 5개 업체에서 19개 업체로 조사 대상이 확대되어 기업체 내부의 표준 및 지침 준수, 소프트웨어 안전 관리체계, 관련 제품 개발 계획 등의 다양한 의견을 수집하고 분석할 수 있었다. 주로 장치기반 기업에서는 고객 니즈(수출국 인증) 등의 외적 요인에 의하여 소프트웨어 안전이 강화된 제품을 개발/판매할 계획을 보유하고 있었으며, 안전관련 정책요구사항은 기업 중심의 지원에서 시장 및 범정부적 지원 요구로 확대되어 범정부적인 소프트웨어 안전 플랫폼의 필요성이 제기되었다. 아래 표는 설문항목에 대한 주요 차이점을 비교하였으며 특히 밑줄은 전년도 조사 대비 변화된 부분을 표시한 것이다.

<표 4-1> 2015년 vs 2016년 국내 SW 안전 산업 현황 비교

구분	대상	비교 분석
학계, 정부	소프트웨어 안전 개념	<u>소프트웨어 안전의 개념의 확대 (SW안전 내 품질 및 보안 포함 유형 등장¹⁰³)</u>
	소프트웨어 산업	소프트웨어의 설계/개발보다는 여전히 코딩을 중시하며 개발환경은 열악
	소프트웨어 안전산업	소프트웨어 안전 산업의 법제도적 기반 및 시장 여건 미조성
국내 소프트웨어 안전 분야 사업 기업	일반현황	소프트웨어 안전 개념은 추상적으로 이해하는 수준이며, <u>보안 관점 강세(50%)</u> <u>분석, 설계, 회피 메카니즘의 엔지니어링 관점으로 이해(40%)</u>
		단기 용역위주의 컨설팅 사업을 수익 확대 및 사업 영속성 취약
		자동화 도구는 사내 활용 수준으로 해외 규격 기준의 도구 국산화 개발 필요
		품질검증 자격증보다는 <u>실무경험 중시 성향 강조</u>
		<u>고객군은 자동차뿐 아니라, 철도/자동차/원자력/우주항공/의료/정보통신 등 다양한 고객군으로 확대</u>
소프트웨어 안전프로세스	여전히 안전 메커니즘 설계, 위해도 분석 활동 중요하다고 인식	
	<u>소프트웨어 관련인증(GS/SP인증)은 안전성 확보에 효과적이지 않다는 인식 감소('15, 76% -> '16, 57%), 기존 인증 보완 또는 신규 인증 필요 의견 제시</u>	
인프라 및	법제도 개정이 필요하다는 것은 여전히 동의하나, 기	

	요구사항	존 법제도 내 “소프트웨어 안전 “ 항목 추가 또는 점진적 적용 등으로 법제도적 접근 방법이 구체화되고 있음
		소프트웨어 품질측정용 매뉴얼/툴 중심이며, 업무상황에 맞게 작성/개선하는 수준 지속
		소프트웨어 전문가와 도메인 전문가 교류가 미흡하여 업무 전문성을 가진 소프트웨어 전문가 희소, 소프트웨어 안전 전문가보다 인증심사원으로 인력 쏠림
		소프트웨어 안전산업의 활성화를 위해 공공성과 안전요구가 필요한 철도, 원자력, 우주항공, 국방 도메인으로 구체화하여 정부 주도 기반 구축 필요
End User 기업	소프트웨어 안전 일반 현황	전년도 대비 5개 업체에서 19개 업체 다양한 도메인으로 조사 확대
		소수(32%) 기업만 안전 개념 인지, 대다수 품질과 관련된 것으로 인식
		소프트웨어 안전/품질 관리체계를 보유하나 실제 활동 미흡
		소프트웨어 안전/품질 전담인력은 품질활동 수행/소프트웨어 안전 활동 전무
	소프트웨어 안전 예방점검 활동	안전보다는 품질 위주로 제3자 검증 25% 수준. 단, 솔루션 개발, 판매, 제조기반 IT 기업은 객관적이고 구체적 활동 수행
		대기업은 대부분 Safety-Critical 소프트웨어 검수 표준/지침 보유하나, 부품업체는 미흡한 수준임
		고객 니즈 등 외적 요인(수출국 인증 등)에 의하여, 자동차 제조, IT인프라(서버 등) 제조, 우주항공(드론 등) 등 장치제조 기반 IT 기업에서 소프트웨어 안전강화 제품 개발/판매/계획 보유(47.4%)
	소프트웨어 안전 대응관리 활동	제품 사고 대응 시나리오를 보유하고 있으나 정기 모의 훈련 실시(18.2%) 및 기업 외부 연계 대응 체계 취약
		사고사례 수집/축적(31.6%)하고 축적된 정보는 테스트케이스 적용/교육 등에 활용하나, 소프트웨어 안전 기능 개선 활용 미흡
	소프트웨어 안전관련 정책 요구사항	기업내 중심의 정책 요구사항에서 시장/법정부적 지원 요구로 확대 -개발자의 업종/업무 사례중심의 교육 지원 또는 업

		체의 사업 참여시 최소한의 자격요건 필요 -시장환경을 고려한 단계적 소프트웨어 안전 제도 도입 및 정부의 공통서비스와 민간 특화서비스로 구성된 범정부 소프트웨어 안전 플랫폼 필요성 제시
--	--	--

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 파악하였다.

2. SWOT 분석

1) 강점

국내 소프트웨어 안전 시장의 강점으로는, 상당수의 규모 있는 국내 자동차, IT인프라, 우주항공 등 장치제조 기반의 기업들은 소프트웨어 품질과 안전 관리 규정/조직 등의 체계를 구축하고 있으며 안전이 중요한(Safety Critical) 소프트웨어 검수 표준/지침, 제품관련 사고 대응 시나리오를 보유하고 있었는데, 이것은 대부분이 고객의 니즈, 제품 경쟁력 강화 및 영업 전략적 차원, 외부 BMT 통과용 등의 외적 요인에 의한 것이었다. 국내 소프트웨어 안전 사업 분야의 기업들은 소프트웨어 안전 관련 고객 요구 사항으로부터 테스트에 이르기까지 소프트웨어 생명주기 전과정을 점검할 수 있는 토탈 솔루션을 제공하고 있고, 과감하고 지속적인 투자로 전문인력확보를 통한 핵심 도구를 개발하고 있었다. 이러한 기업들은 해외 진출을 희망하고 있으며 시장을 선점할 기회가 많은 아시아태평양 지역으로 우선 진출하기를 원하며 이를 발판으로 미국, 유럽 등지로 진출하고자 한다.

2) 약점

국내 TIC(Testing, Inspection and Certification) 업체는 용역 위주의 사업 구조로 매출 및 수익 확대에 한계가 있으며, 소프트웨어 안전 사업의 법/제도적 기반이 미흡하고 소프트웨어 개발 환경은 여전히 열악한 상태다. 또한 대다수 소프트웨어 개발 사용자 기업은 안전사고 및 해결 사례에 대하여 데이터베이스화 하지 않으며 데이터베이스화 한 기업조차 기업 내부 공유 및 활용이 크지 않은 편이었다. 이를 해소하기 위한 방법으로 소프트웨어 안전에 대한 개념을 정립하고 안전사업을 강화하기 위하여 현재의 법제도 측면에서 추가적인 제정 또는 개정이 필요하며, 국가 차원의 소프트웨어 안전을 위한 공통기반 사업을 추진하고 학계 및 산업 도메인별로 소프트웨어 안전이 필수 사항으로 고려되어 분석/설계되도록 하는 정책 지원이 필요하다. 즉 소프트웨어 안전 관련 법규정의 제개정 및 인증/해외 판로 지원과 안전 사고 해결 사례에 대한 공유 데이터베이스를 제공하고 설계에 대한 안전 메커니즘을 검토하는 시스템을 제공하는 등 범정부 차원의 지원과 기업의 안전 활동이 요구된다.

3) 기회

2020년까지 글로벌 TIC 시장은 매년 약 5%씩 증가하여 2022년까지 1,132억 달러 규모로 성장할 전망이다. 국내 시장에서는 소프트웨어 안전 개념 및 중요성 또한 점차 확산되고 있는 추세이다. 특히 자동화를 통한 자율비행, 자율주행의 국내 자동차 산업, 항공 및 철도 분야를 중심으로 시스템 및 소프트웨어 안전 수요가 증가하고 있다. 또한 제품이 다양해지고 글로벌 무역이 증가하면서 자국민의 안전을 보장하기 위하여 제품 안전에 대한 정부 규제가 강화되고 신규 기술 개발로 인해 관련 표준은 점차 상세화되며 정부나 기업 내 전문성을 보유한 내부인력 부족으로 인하여 제3자를 통한 소프트웨어 안전 테스트, 인증 등이 점차 증가하게 되었다. 이러한 시장에서 국내 소프트웨어 안전 사업 분야 기업들은 주로 자동차, 항공 등의 기능안전 측면으로 관련 대기업과의 신뢰성을 기반으로 꾸준한 관계를 형성해 왔고 고객의 산업 특성에 맞는 검증 도구를 자체 개발하여 안전 검증에 활용해 왔다. 그러나 소프트웨어의 기능 안전은 산업 도메인의 전문 지식 및 기술과 소프트웨어의 전문 지식이 동시에 요구되는 영역이므로, 도메인 중심의 전문가와 소프트웨어 공학 중심의 전문가 간의 상호 정보 공유의 장과 안전 관련 인력의 양성이 필요하다.

4) 위협

글로벌 TIC 업체의 활발한 활동으로 인한 시장규모와 제공 서비스는 기존 시장을 포

합하여 신규 시장인 중국 등 아시아권으로 확대되고 있으며, 안전 표준 융복합화 및 타 산업 분야 규제에 대한 분석 및 활용이 증가하고 있으며, 안전 표준 제정에도 여러 분야의 전문가가 참여하고 있고 이러한 표준은 점차 상세화되고 있는 추세이다. 국내에서는 현재 소프트웨어 안전 관련 국제표준을 기반으로 소프트웨어 안전 분야 사업 기업 및 각 산업 도메인 기업에서 적용할 수 있는 매뉴얼/가이드, 관련 도구를 개발하여 사용하고 있으나 개별적으로 활용하고 있으므로, 이러한 정보를 상호간에 공유하고 교류함으로써 개별적 지식을 통합하여 시너지 효과를 발휘한다면 이러한 표준화 추세에 유연하게 대응할 수 있을 것이다.

위의 강점, 약점, 기회 및 위협에 대하여 종합적으로 분석한 SO, WO, ST, WT전략은 아래 [그림 4-1]과 같다.

[그림 4-1] 국내 소프트웨어 안전 산업의 SWOT 분석 결과

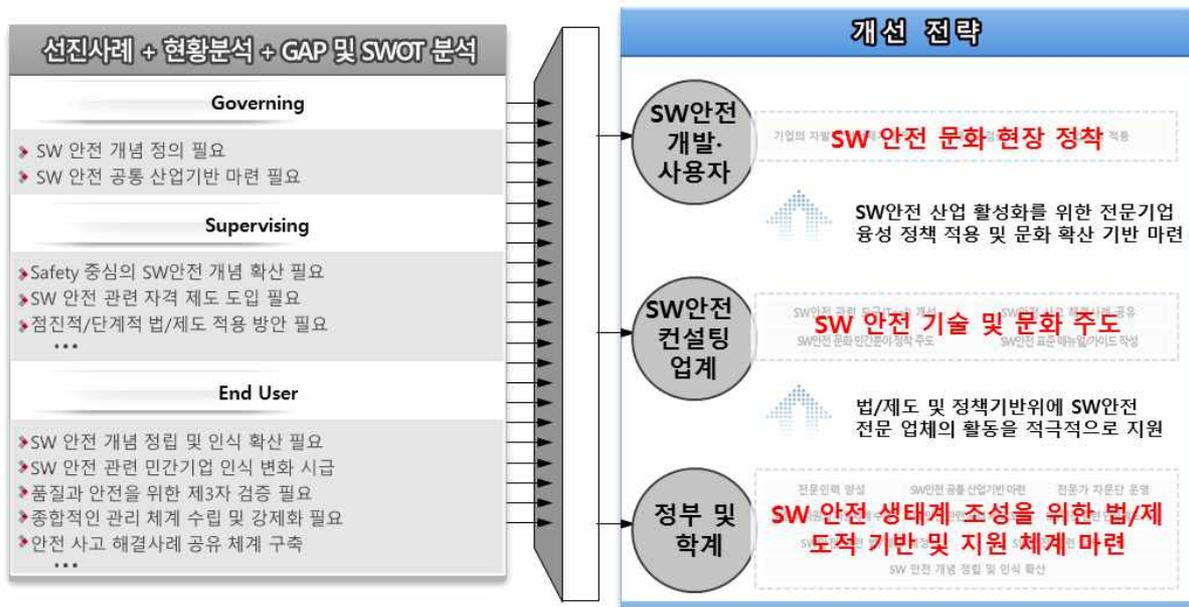
강점 / 약점 기회 / 위협		강점 (Strength)	약점 (Weakness)
		<ul style="list-style-type: none"> 상당수 규모 있는 국내 자동차, 우주항공 관련 제조기업은 SW 품질/안전 관리 체계(규정 및 조직) 및 Safety Critical SW 검수 표준/지침, 제품관련 사고 대응 시나리오 보유 	<ul style="list-style-type: none"> 국내 TIC 업체는 용역 위주의 사업 구조로 매출 및 수익 확대에 한계 SW안전사업 법/제도적 기반 미흡 열악한 SW 개발 환경 대다수 SW개발사용자 기업은 안전사고/해결 사례 DB화 않음. DB화 해도 공유하지 않음
기회 (Opportunity)	<ul style="list-style-type: none"> 2020년까지 글로벌 TIC 시장 성장 전망(매년 5.15%) 국내 SW안전 개념 및 중요성 확산 국내 자동차, 우주항공, 철도 분야 제조업 분야를 중심으로 시스템 및 SW안전 수요 증가 	<p>SO전략</p> <ul style="list-style-type: none"> 지속적인 고객 신뢰 관계를 통한 국내 소프트웨어 안전 시장 수성 자동차, 우주항공 등 SW 안전 검수 노하우 활용 및 해외 규격의 도구 개발 	<p>WO전략</p> <ul style="list-style-type: none"> SW 안전 개념 정착 및 SW 안전 생태계 지원 체계 마련 업종별 SW 안전 사고 및 해결 사례 공유 및 활성화 활동 추진
	위협 (Threats)	<ul style="list-style-type: none"> 글로벌 TIC 업체의 활발한 규모 및 제공 서비스 확대 안전 표준 융복합화 및 타 산업 분야 규제 분석/활용 증가 안전 표준 제정에 여러 분야 전문가 참여, 안전 표준 상세화 	<p>ST전략</p> <ul style="list-style-type: none"> 국내 SW 안전 공통 기반 구축을 위한 업종별 관리체계 및 지침에 대한 상호 보완 및 개선 활동 추진 관련 업종 전문가와 SW 안전 컨설팅업체 간의 지식 교류 및 전문가의 국내외 활동 지원

제5장 국내 소프트웨어 안전 산업 개선 전략 및 과제

제1절 개요

비교 분석 결과와 SWOT분석을 통해 도출된 개선 전략을 비교/종합한 후, 선진사례 주요 시사점을 반영하여, 정부 및 학계 부문, 소프트웨어 안전 컨설팅 부문, 소프트웨어 안전 개발·사용자 부문의 3대 부문으로 구분하여, 개선 전략을 도출하고 도출된 개선 전략 별 주요 개선 과제를 Mapping 및 Grouping 하였다. 확정된 개선 전략 및 개선 과제를 통해 미래 모형을 제시하였다.

[그림 5-1] 국내 소프트웨어 안전 산업 개선 전략 도출



제2절 개선 전략 및 개선 과제 도출

상기 분석을 통해 도출된 개선 전략으로 ‘소프트웨어 안전 생태계 조성을 위한 법/제도적 기반 및 지원 체계 마련’ 전략과 9개의 개선 과제가 정부 및 학계 부문에서 도출되었고, ‘소프트웨어 안전 기술 및 문화 주도’ 전략과 4개의 개선 과제가 소프트웨어 안전 컨설팅 업계 부문에서 도출되었으며, ‘소프트웨어 안전 문화 현장 정착’

전략과 3개의 개선 개선과제가 소프트웨어 안전 개발·사용자 부문에서 도출되었다.

1. 정부 및 학계 부문

정부 및 학계 부문에서 도출된 개선 전략은 ‘소프트웨어 안전 생태계 조성을 위한 법/제도적 기반 및 지원 체계 마련’인데, 이는 법/제도 및 정책 기반위에 소프트웨어 안전 산업의 활성화 및 소프트웨어 안전 개발·사용자의 안전 문화 정착이 필요하기 때문이다. 지원 체계 마련을 위해 필요한 주요 과제는 각 부문별 조사된 요구 사항을 종합하여 Grouping하여 도출하였는데, 우선순위가 높은 순서대로 나열하면 아래와 같다.

- 소프트웨어 안전 개념 정립 및 확산: 2015년에 비해 많이 개선되긴 하였으나, 소프트웨어 안전 개념이 아직 미 정립된 상황이며, 소프트웨어 안전 컨설팅 업계 및 소프트웨어 안전·개발 사용자가 안전에 대한 개념을 모르거나 명확히 알지 못하는 경우가 많았다. 따라서 정부 및 학계에서 일관된 소프트웨어 안전 개념을 정립하고, 이를 일반 업계에 확산이 가장 우선적으로 필요할 것으로 판단된다.
- 소프트웨어 안전 관련 정책 수립: 정립된 소프트웨어 안전 개념을 토대로, 일관적이고 중장기적인 소프트웨어 안전 관련 정책 수립이 필요하다.
- 소프트웨어 안전 관련 법/제도 제정: 정부의 일관적이고 중장기적인 소프트웨어 정책을 토대로, 현실을 고려한 체계적이고 포괄적인 소프트웨어 안전 관련 법/제도 제정이 필요하다. 특히, 소프트웨어 안전은 비용 및 시간이 소모되는 비자발적인 분야이므로, 현실을 감안한 법/제도 없이는 일부 산업 도메인(자동차 등)을 제외하고는 자율적인 준수가 쉽지 않다.
- 소프트웨어 인증제도 개선: 법/제도 체계 위에 소프트웨어 안전을 고려하여 소프트웨어 인증제도 개선이 필요하다. 일부 산업 도메인(자동차, 철도, 원자력 등)에서는 기능 및 소프트웨어 안전에 대한 인증을 요구하고 있으나, 전반적인 산업 도메인에서 생산되는 안전에 중요한 제품 및 시스템 등에 대한 안전을 담보하지 못한다. 따라서 소프트웨어 안전이 중요한 제품 및 시스템의 안전에 대한 인증을 담보할 수 있도록, 기존 소프트웨어 인증제도를 개선할 필요가 있다.
- 소프트웨어 안전 자격 제도: 소프트웨어 인증제도가 발맞추어 이를 수행하는 인력 육성 및 처우 개선 등을 위해 소프트웨어 안전 자격 제도가 필요하다.
- 범정부 차원의 지원체계 수립: 정부 정책, 법/제도 제정, 소프트웨어 안전 인증 및

자격 제도의 기반위에 이러한 요소들이 제대로 선순환 할 수 있도록 범정부 차원의 지원 체계 수립이 필요하다. 본 조사에서 도출된 대표적인 지원 요청 사항으로는 인력(교육 포함), 자금지원, 정부 발주 사업에 소프트웨어 안전 부분 포함 등이 있었다.

- 전문인력 양성: 범정부 차원의 지원체계 수립 후, 점차 유입되기 시작할 소프트웨어 안전 인력에 대한 중장기적이고 체계적인 양성 방안이 필요하다.
- 소프트웨어 안전 공통 산업 기반: 개별 기업 간에 소프트웨어 안전 정보 공유가 어려운 특성을 감안하여, 정부 주도하에 주요 산업 도메인에서 공통으로 활용 가능한 기반을 마련 및 제공하여, 소프트웨어 안전 기반 조성을 촉진할 필요가 있다. 미국의 경우 자율주행차 정책에서 도로교통안전국(NHTSA)은 자율주행차 관련 주요 데이터를 각 업체로부터 취합하여 DB화 하겠다고 밝혔다.
- 전문가 자문단 운영: 소프트웨어 안전 정책, 법/제도, 지원체계 및 소프트웨어 안전 산업이 제대로 운영되는지 수시로 확인하고 가이드하기 위해 정부, 학계, 산업계를 아우르는 전문가를 모아 자문단을 구성하고 운영하는 것이 필요하다.

도출된 9개 과제를 실행 순서에 따라 정리해 보면, 소프트웨어 안전 개념 정립 및 확산을 기반으로 한 소프트웨어 안전 관련 정책 수립 및 법/제도 제정하고 소프트웨어 안전 인증 및 자격 제도 수립 하여 안전 관련 인력이 유입될 수 있는 기반을 확보하고 범정부 차원의 지원 체계 수립을 통해 정책, 법/제도, 인증/자격 제도가 원활하게 운영될 수 있도록 지원하고, 안전 전문 인력 양성을 지원하고, 산업계가 공통으로 활용할 수 있는 소프트웨어 안전 기반을 제공하고, 전문가 자문단을 운영하여 수시로 자문을 통해 ‘소프트웨어 안전 생태계 조성을 위한 법/제도 기반 및 지원 체계 마련’ 개선전략을 달성하는 것이다.

2. 소프트웨어 안전 컨설팅 부문

소프트웨어 안전 컨설팅 부문에서 도출된 개선 전략은 ‘소프트웨어 안전 기술 및 문화’ 이다. 정부 및 학계 부문에서 조성된 소프트웨어 안전 생태계 조성을 위한 법/제도적 기반 및 지원 체계를 토대로 소프트웨어 안전 컨설팅 업계는 소프트웨어 안전 검증, 교육, 인증 활동 등을 통해 소프트웨어 안전 개발·사용자 부문에서 소프트웨어 안전 문화가 정착될 수 있도록 주도해야 하는 역할을 수행할 필요가 있다. 이를 위해 필요한 주요 과제를 우선순위 별로 나열하면 아래와 같다.

- 소프트웨어 문화 민간분야 정착 주도: 소프트웨어 안전 컨설팅 업계는 소프트웨어 안전 문화 민간 분야 정착 주도의 의무를 인지해야 하며, 이를 위해 다양한 교육, 포럼, 세미나 등을 통해 비단 주요 산업 도메인의 소프트웨어 안전 개발·사용자 뿐만 아니라 사회전반에 걸친 소프트웨어 안전 문화 정착 활동에 매진해야 할 필요가 있다.
- 소프트웨어 안전 표준 매뉴얼/가이드 작성: 소프트웨어 문화 민간분야 정착 주도를 위해 소프트웨어 안전 컨설팅 업계는 소프트웨어 안전 준수를 위해 필요한 다양한 표준 매뉴얼/가이드를 작성하여 배포하고 교육해야 한다.
- 소프트웨어 안전 관련 도구 개선: 소프트웨어 안전 표준 매뉴얼/가이드를 토대로 실제 사용자들이 소프트웨어 안전 활동 수행 할 수 있도록 소프트웨어 안전을 분석하고 개선할 수 있는 도구를 개발/개선해야 한다.
- 소프트웨어 안전사고 해결 사례 공유: 민간차원의 소프트웨어 안전사고 관련 정보는 공유가 쉽지 않으므로, 소프트웨어 안전 컨설팅 업계 차원에서의 해결 사례 공유를 통해 소프트웨어 안전 지식 기반 확대가 필요하다.

도출된 4개 과제를 실행 순서에 따라 정리해 보면, 소프트웨어 안전 컨설팅 업계는 소프트웨어 안전 문화 민간분야 정착 주도에 대한 인식 및 활동이 필요하며, 이를 위해 소프트웨어 안전 표준 매뉴얼/가이드 작성과 도구(Tool) 개발 및 개선 활동이 필요하다. 또한, 소프트웨어 안전 지식 기반 확대를 위해 안전 컨설팅 업계 간 소프트웨어 안전사고 해결 사례가 공유되어야 한다.

3. 소프트웨어 안전 개발·사용자 부문

소프트웨어 안전·개발 사용자 부문에서 도출된 개선 전략은 ‘소프트웨어 안전 문화 정착’이다. 정부 및 학계 부문에서 조성된 소프트웨어 안전 생태계 조성을 위한 법/제도적 기반 구축 및 지원 체계와 소프트웨어 안전 컨설팅 업계의 소프트웨어 안전 및 문화 주도 노력이 중요하지만, 결국 소프트웨어 안전을 실현하는 주체는 소프트웨어 안전·개발 사용자이며, 이들이 중심이 된 소프트웨어 안전 문화의 현장 정착 이야말로 소프트웨어 안전의 최종적인 목적이라 할 수 있다. 이를 위해 필요한 주요 과제를 우선순위 별로 나열하면 아래와 같다.

- 기업의 자발적 안전체계 도입: 소프트웨어 안전·개발 사용자의 자발적인 소프트웨어 안전을 위한 노력 및 이에 대한 문화 정착이 가장 중요한 최종적인 모습이

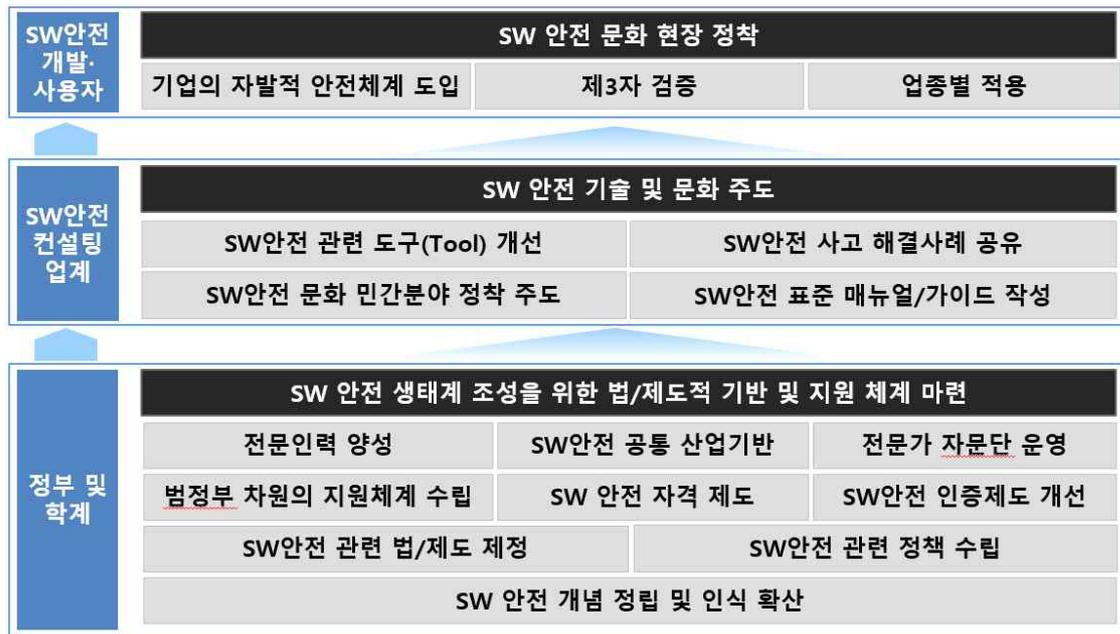
다. 이를 위해, 사용자는 소프트웨어 안전의 필요성을 자각하여 자발적으로 안전을 위한 체계를 도입하고 이를 준수해야 한다.

- 제3자 검증: 국내 현황 조사 결과 소프트웨어 안전을 인식하거나 중요시하는 상당수의 기업들도 비용 및 시간 등의 이유로 소프트웨어 안전을 자체적으로만 실시하는 경우가 많았다. 자체적으로 실시하는 안전 검증은 자칫하면 안전 점검의 원래 취지를 벗어날 유혹에 빠지기 쉽기 때문에 제3자 검증을 통한 객관적인 소프트웨어 안전 점검을 실시하도록 해야 한다.
- 업종별 적용: 선진 사례 조사 결과 업종별 위험, 위해요소 등에 대한 정의가 달랐고 위험 평가를 하는 방법도 달랐다. 따라서 산업도메인별 특성을 반영한 위험, 위해요소 및 소프트웨어 안전에 대한 접근 방법이 다르기 때문에, 소프트웨어 안전을 각 업종별로 적용할 경우 업종의 특성을 고려한 적용 방법이 필요하다.

도출된 3개 과제를 실행 순서에 따라 정리해 보면, 기업이 자발적으로 안전 체계를 도입하기 시작하고 좀 더 객관적인 안전 검증을 위해 제3자 검증이 확대되며, 안전체계 및 안전 가이드 등이 산업도메인의 특성을 고려하여 업종별로 적용되어야 한다.

위에서 도출된 각 부문별 개선 전략 및 개선 과제를 도식화하면 아래와 같다.

[그림 5-2] 소프트웨어 안전 개선 전략 및 과제



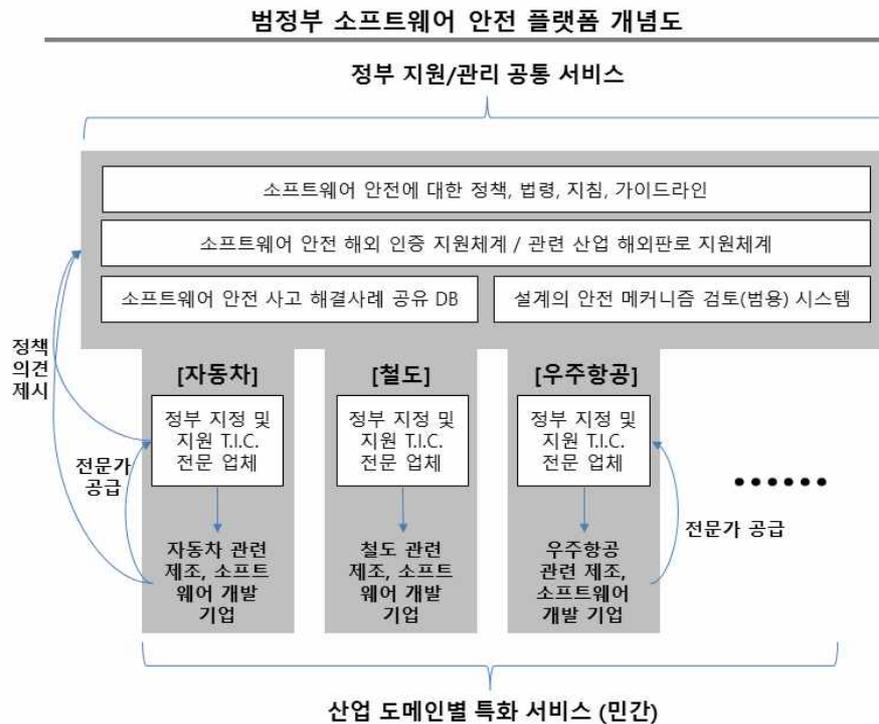
제3절 미래모습: 범정부 소프트웨어 안전 플랫폼 구성(안)

앞에서 도출된 개선 전략 및 과제를 통해 미래모습으로 범정부 소프트웨어 안전 플랫폼(안)을 제시해 본다. 이 미래모습은 국내 소프트웨어 안전 산업 생태계 활성화를 위한 선순환적인 구조로, 앞에서 도출된 개선 전략 및 과제를 모형화한 것이다.

정부 차원에서는 소프트웨어 안전에 대한 정책, 법령, 지침, 가이드라인을 수립하고 관련 인증 지원, 해외 판로 지원 뿐 아니라 안전 사고 해결사례에 대한 공유 데이터베이스 제공, 설계에 대한 안전 메커니즘을 검토하는 시스템(범용적인 부분 중심, 업종별 특화 영역은 제외) 등을 제공한다.

이러한 정부의 서비스를 기반으로, 각 산업 도메인별로 정부가 지정한 소프트웨어 안전 컨설팅 전문 업체가 안전 컨설팅 및 검증 작업을 지원하며, 이를 기반으로 제조 및 소프트웨어 개발 기업에서는 소프트웨어 안전이 강화된 제품을 생산하게 된다.

[그림 5-3] 범정부 소프트웨어 안전 플랫폼 개념도(안)



일선의 제품 생산 기업은 소프트웨어 안전 컨설팅 업체에게 전문가를 공급하게 되고, 이와 더불어 정부를 대상으로 안전 관련 정책 등에 대한 의견을 제시한다.

제6장 결론

2016년 국내 소프트웨어 안전 산업 동향 분석의 특징은 세계적으로는 기능 및 소프트웨어 안전 표준이 특정 산업도메인에 국한되지 않고 필요한 분야 어디서나 도입되고 활용되고 있었고, 요구되는 안전 수준에 따라 다양한 안전 표준 및 가이드가 복합적으로 사용되고 있었다. 해외 선진 TIC 업체들은 2015년 조사와 마찬가지로 세계 각국 및 주요 산업 도메인으로 서비스 영역을 계속적으로 확대하고 있었는데 주요 방법 중 하나는 인수합병을 통해서였다. 또한 이들 업체는 주요 산업도메인의 안전 표준 제정에 직접 참여하는 방법으로 영향력 및 기존 서비스 영역을 공고히 하고 있었다.

국내에 명확하게 안전 개념을 파악하고 있지는 못하더라도 상당수의 주요 소프트웨어 안전·개발 사용자 기업은 소프트웨어 안전 행위를 품질 보증 활동 등을 통해 부지불식간에 수행하고 있었다. 그리고 본 연구를 위해 기업의 관련 담당자와 대면 및 설문 인터뷰 방법이 일선 기업에 소프트웨어 안전을 홍보하고 전파하는 역할을 하였다. 이러한 상황으로 판단컨대 명확한 소프트웨어 안전 개념 및 가이드를 정립하고, 교육 및 홍보할 경우, 소프트웨어 안전에 대한 인식이 빠르게 심을 수 있을 것으로 판단된다. 소프트웨어 안전 활동의 경우 상당수 활동이 품질 보증 영역 안에 포함되어 수행되고 있었으나, 안전에 대한 명확한 표준 및 가이드 그리고 이를 수행할 전문 인력은 부족하였다. 종합적으로 국내 상황을 판단하면, 2015년과 큰 차이가 없으나 안전에 대한 인식 및 활동은 느리게나마 점진적으로 확산되고 있는 것은 분명하다.

현재, IT 기술의 발전 속도는 놀랍게 증가하고 있는데, 요원하게 보였던 인공지능의 발달과 이를 통한 사물의 조정 및 운영(자율주행차, 사물인터넷을 통한 가전제품 제어 등)이 가시적인 범위내로 들어오기 시작하면서, 전자 제품에 대한 기능 안전, 특히 소프트웨어 안전에 대해서는 더 이상 안일하게 대응할 수 있는 상황이 아닌 것으로 나타나고 있다.

따라서 국내 소프트웨어 안전 분야를 빠르게 활성화하기 위해서는 정부가 정책적, 법/제도적 기반 구축부터 조속한 실행을 해야 할 것으로 판단된다. 특히, 소프트웨어 안전 특성상 정부 주도의 수행이 유리하거나 정부 주도의 수행만이 가능한 분야가 있으므로, 정부의 정책적, 법/제도적인 기반 구축이 우선 수행되어야 소프트웨어 안전 분야가 보다 빠르게 활성화될 것으로 보인다. 동시에 국내 산업 환경을 충분히 고려하여

경차륙할 수 있는 소프트웨어 안전 발전 기반이 마련되어야 한다. 앞 장에서 제시한 ‘범정부 소프트웨어 안전 플랫폼’은 단지 하나의 ‘안’으로써 본 안을 토대로 범 정부적인 소프트웨어 안전 정책 모형을 논의의 주제로 삼아 구체적이고 현실 상황을 반영하는 정책 모형을 빠른 시간 내에 만들 수 있다면 그것으로 큰 의미가 될 것이다.

소프트웨어 안전 토대를 마련하기 위한 구체적인 방안으로, 소프트웨어 안전 지표를 개발하고 1~2년 단위로 주요 산업 및 기업을 대상으로 소프트웨어 안전 지표를 측정하여 그 결과를 발표하고 정책 수립에 반영한다면, 사회 및 산업계에는 소프트웨어 안전을 수치적으로 제공함으로써 안전에 대한 인식 확산 및 정량화가 가능하고, 정책적 측면에서는 이러한 결과를 정책 수립에 정기적으로 반영할 수 있으므로 보다 현실적인 정책 수립 및 정책 변경에 도움이 될 것으로 본다. 구체적으로 상기 내용을 정의해보자면 향후 1. 소프트웨어 안전 지표 개발 및 측정/관리 방안 수립, 2. 소프트웨어 안전 지표 정책 반영 체계 수립이라는 과제가 필요할 것이며, 각 과제별 주요 내용은 아래와 같다.

- 소프트웨어 안전 지표 개발 및 측정/관리 방안 수립

과제 정의: 측정 가능하고 객관적인 소프트웨어 안전 지표 개발 및 객관적인 측정을 위한 측정 대상, 시기, 기법, 산정 방식 등 정의

주요 측정 항목

- 소프트웨어 안전 인식: 개념, 인식 수준 등
- 소프트웨어 안전 프로세스: 소프트웨어 안전 예방, 탐지, 대응, 사후활동 현황
- 소프트웨어 안전 인프라: 표준/매뉴얼, 인력/조직, 시스템/툴(Tool)

주요 고려 항목

- 측정 대상: 소프트웨어 개발·사용자, 소프트웨어 안전 컨설팅 기업
- 측정 시기: 측정 주기, 측정 일자 등
- 측정 기법: 대상 및 시기에 따른 측정 기법 제시
- 산정 방식: 지표 산정 방식 정의
- 지표 관리 방안: 관리 주체 및 프로세스 정의

- 소프트웨어 안전 지표 정책 반영 체계 수립

과제 정의: 소프트웨어 안전 지표의 소프트웨어 안전 정책 반영에 대한 체계 수립

주요 고려 항목

- 프로세스: 소프트웨어 안전 지표 측정 후, 정책 반영 프로세스 및 역할자 정의
- 정책 평가 프로세스: 정책 평가 프로세스 및 역할자 정의
- 정책 평가 지표: 소프트웨어 안전 지표

참 고 문 헌

국내 문헌

- 김희성, 『항공용 소프트웨어 인증을 위한 DO-178C 적용절차 개관』, 한국항공우주연구원
박무혁 (2007), 『항공용 S/W 개발 및 인증 기술동향』, 항공우주산업기술동향 5권1호 pp. 15~24
심재복 (2011), 『Software Verification & Validation Medical device(IEC 62304)』 한국산업기술시험원
식품의약품안전처 (2007), 『의료기기 소프트웨어 밸리데이션 가이드라인』
식품의약품안전처 (2014), 『의료기기 소프트웨어 안전 관리』
식품의약품안전처 (2015), 『의료기기 소프트웨어 허가·심사 가이드라인』

해외 문헌

- SAE(Society of Automotive Engineers), “Automated Driving Levels of Driving Automation are Defined in New SAE International Standard J3016”
NHTSA, “Federal Automated Vehicles Policy, U.S. Department of Transportation”
Assessment of Safety (2016), “Standards for Automotive Electronic Control Systems”
U.S. Department of Defense (2012), “MIL-STD-882E Standard Practice System Safety”
U.S. Department of Defense (2010), “Joint Software Safety Engineering Handbook” , version 1.0
- Thomas K. Ferrell & Uma D. Ferrell (2001), “RTCA DO-178B/EUROCAE ED-12B” , CRC Press LLC
Stephen A. Jacklin, “Certification of Safety-Critical Software Under DO-178C and DO-278A” , *American Institute of Aeronautics and Astronautics*
Sven Nordhoff, “White Paper DO-178C/ED-12C the new software standard for the avionic industry:goals, changes and challenges” , *SQS*
Frédéric Pothon (2012), “DO-178C/ED-12C versus DO-178B/ED-12B Changes and Improvements” , *ACG Solutions*
Cognizant (2012), “The Impact of RTCA DO-178C on Software Development” , *Cognizant 20-20 Insights*
Shou-Yu Lee, W. Eric Wong, Ruizhi Gao (2014), “Software Safety Standards: Evolution and Lessons Learned”
<http://www.faaconsultants.com/html/do-178c.html>
https://en.wikipedia.org/wiki/Medical_software
<http://www.iso.org/>
MD101 Consulting, <http://blog.cm-dm.com/post/2013/04/04/IEC-62304-vs-IEC-60601-1-and-IEC-61010>
<http://blog.cm-dm.com/post/2011/11/01/ISO-and-IEC-standards-explained-to-software-engineers-and-quality-managers>
<http://blog.cm-dm.com/post/2016/01/15/IEC-82304-1-latest-news-about-the-standard-on-Health-Software>
MDDI (2010), <http://www.mddionline.com/article/developing-medical-device-software-iec-62304>
Justin McCarthy, “Medical Device and Health Software: Standards and regulations now and in the future” , *Clin Eng Consulting Ltd*

Sherman Eagles (2013), "Medical Device Software Standards for Safety and Regulatory Compliance" , *SoftwareCPR*

FDA, "<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/default.htm#pma>"

FDA, "<http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820>"

John F. Murray Jr (2010), "CDRH Regulated Software" , FDA

CDRH (2015), "Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff"

Bruce A. MacFarlane (2009), "FDA Regulation of Mobile Medical Apps" , *NAMSA*

EU commission, "COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993"

European Commission DG Health and consumer, "MEDDEV 2.4/1 Rev.9 June 2010, MEDICAL DEVICES: Guidance document - Classification of a medical devices"

European Commission, "<https://ec.europa.eu/growth/>"

mbc (2014), "Basic Information about the European Directive 93/42/EEC on Medical Devices " Version 1.17 (09-2015), "Manual on borderline and classification in the community regulatory framework for medical devices "

European Commission DG Enterprise, "MEDDEV 2.10-2 Rev.1 April 2001, Designation and monitoring of notified bodies "

The European Association for Medical Devices of Notified Bodies (2014), "Code of Conduct for Notified Bodies, version 3.2"

Market and market(2016), "Testing, Inspection and Certification (T.I.C.) Market"

Catalyst Corporate Finance LLP(2016), "Global Testing, Inspection and Certification Summer 2016"

KPMG(2016), "Test and measurement newsletter Q4 2015"

연구보고서 2016-022

소프트웨어 안전(Safety) 산업 동향 조사

2017년 05월 인쇄

2017년 04월 발행

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

ISBN : 978-89-6108-383-6

주 의

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

ISBN : 978-89-6108-383-6



[소프트웨어정책연구소]에 의해 작성된 [SPRI 보고서]는 공공저작물 자유이용허락 표시기준 제 4유형(출처표시-상업적이용금지-변경금지)에 따라 이용할 수 있습니다.

(출처를 밝히면 자유로운 이용이 가능하지만, 영리목적으로 이용할 수 없고, 변경 없이 그대로 이용해야 합니다.)