SW안전 주요산업의 관리 현황과 시사점

이중엽, 박태형
소프트웨어정책연구소
ilovebiz@spri.kr, parkth@spri.kr

Current Status and Policy Implications of Software Safety Management in Critical Industries

Lee Joong-Yeup, Park, Tae Hyung
Software Policy & Research Institute(SPRi)

요 약

본 논문은 원자력, 항공, 자동차 등 필수안전 산업을 중심으로 소프트웨어 안전관리의 현황을 분석하고, 제도적 정비 방향을 고찰한다. 산업별로 기준과 지침은 점차 마련되고 있으나, 제도 간 정합성과 정책 연계 측면에서 보완이 필요한 지점이 확인된다. 단기적으로는 지침의 구체화, 적용 대상 명확화, 정보 공유 기반 마련이 중요한 과제로 제시되며, 중장기적으로는 보다 구조적인 대응 방안도 향후 검토될 수 있다. 이를 통해 소프트웨어 안전관리의 일관성과 실효성을 높일 수 있을 것으로 기대된다.

Ⅰ. 서론

소프트웨어 안전(software safety)은 소프트웨어가 인명 피해나 재산 손실과 같은 위해(危害)를 일으킬 수 있는 위험으로부터 자유로운 상태를 의미한다. 원자력·항공·자동차·가스·의료 등 이른바 필수안전 산업에서는 작은 소프트웨어 결함 하나가 대형 사고로 이어질 수 있다. 실제로 이러한 산업 분야에서는 소프트웨어 오류로 인한 원전 제어 시스템 오작동, 항공기 운항 장애, 차량 결함으로 인한 리콜, 의료기기 오동작 사례 등이 보고되면서 소프트웨어 안전의 중요성이 크게 부각되고 있다. 이에 따라 국제적으로 각 산업에 특화된 소프트웨어 안전성 표준과 규제들이 정립되어 왔다 (예: 항공 분야의 DO-178C, 자동차 분야의 ISO 26262, 산업제어 전반의 IEC 61508 등). 우리나라에서도 공공 부문을 중심으로 소프트웨어 안전관리의 필요성이 인식되어 2020년 「소프트웨어안전 확보를 위한 지침」이 제정된 바 있다. 이 지침에서는 공공기관이 안전관리 대상 소프트웨어를 지정할 때 고려해야 할 기준으로, 소프트웨어가 수행하는 업무의 국가·사회적 중요성, 다른 시스템과의 연계성, 사고 발생 시 예상 피해 규모 및 범위, 그리고 사고 발생 가능성 및 복구 용이성 등을 명시하고 있다. 이러한 기준은 소프트웨어의 잠재적 위험도를 평가하여 안전관리 필요 대상을 선별하기 위한 것으로, 소프트웨어 안전관리의 제도적 출발점이라 할 수 있다. 이제 본 논문에서는 주요 필수안전 산업 분야별 소프트웨어 안전관리 현황을 살펴보고, 각 분야의 법·제도적 격차와 문제점을 비교한 뒤, 향후 소프트웨어 안전관리 정책의 강화 방향과 시사점을 논의한다.

Ⅱ. 주요 산업 분야별 소프트웨어 안전관리 현황

각 필수안전 산업 분야에서 소프트웨어 안전을 확보하기 위해 적용되고 있는 주요 제도와 표준의 현황을 분야별로 정리하면 다음과 같다.

원자력: 원자력 발전소와 방사선 시설 등에서는 디지털 계측제어(I&C) 시스템 소프트웨어의 오류가 치명적 결과를 초래할 수 있다. 이를 감안하여 원자력안전법 및 관련 규정에서는 소프트웨어를 포함한 계측제어계통의 품질보증을 엄격히 요구하고 있다. 예를 들어, 「원자로 시설 등의 기술기준에 관한 규칙」 제67조 제2항에서는 중요 소프트웨어에 대한 품질보증 세부 요건을 명시하고 있다. 국제적으로도 원자력 분야에서는 IEC 60880과 IEC 61513 등 원전 소프트웨어 안전에 관한 표준이 활용되며, 국내에서도 한국원자력안전기술원(KINS)을 통해 안전등급 소프트웨어에 대한 검증이 이루어지고 있다.

항공: 민간 항공기의 비행제어, 항전장비 등 항공 소프트웨어는 국제 민항 규정에 따라 엄격한 안전성 검증을 거쳐야 한다. 대표적으로 DO-178C는 항공 소프트웨어 개발에 관한 글로벌 규격으로, 미국 FAA와 유럽 EASA 등 항공당국이 이를 사실상의 인증 기준으로 활용한다. 우리나라의 경우 「항공안전법」 및 관련 규정에서 감항인증과 안전관리체계를 통해 항공기 안전을 보장하고 있으나, 소프트웨어 안전에 대한 구체적인 조항은 직접적으로 명시되어 있지 않다. 따라서 국내 항공 분야에서도 항공기 제작사와 인증기관이 DO-178C 등 국제 표준을 준용하여 소프트웨어 안전성을 확보하는 형식으로 운영되고 있다.

철도: 철도 신호 및 열차 제어 시스템은 소프트웨어 오류 시 대형 사고로 이어질 가능성이 높은 분야이다. 이에 따라 국내 「철도안전법」 하위의 철도차량 및 철도시설 기술기준에서는 전자연동장치, 열차제어시스템 등 핵심 설비에 대한 안전무결성 보장 및 위험도 분석, 그리고 안전 개발 프로세스, 시험과 제3자 검증 등을 요구하고 있다. 유럽에서는 철도 신호시스템에 대한 국제 표준으로 EN 50128/50129 등이 사용되고 있으며, 한국도 철도차량에 대한 형식승인 및 안전성 평가 과정에서 이들 기준을 반영하고 있다.

자동차: 자동차 산업에서는 전자제어장치(ECU)와 자율주행 SW 등의 결함이 운전자의 생명에 직접적인 위험을 줄 수 있다. 국제 표준 ISO 26262

(도로 차량 기능안전)를 중심으로 업계에서는 자발적으로 안전 프로세스를 적용하고 있다. 우리나라는 자동차 제조사들을 중심으로 ISO 26262 준수가 사실상의 표준으로 자리 잡고 있다. 정부 차원에서는 자동차관리법 등 일반 차량 안전 규정과 제조물책임법 등을 통해 간접적으로 소프트웨어 안전을 유도하고 있으며, 최근 자율주행차 안전 규제 논의에서도 소프트웨어 안전성 기준이 포함되고 있다.

가스/석유화학: 정유·화학 플랜트, 가스 생산·공급시설 등에서는 센서와 제어 소프트웨어가 가스 누출, 폭발 등을 방지하는 역할을 한다. 그러나 현재 국내 가스 및 산업안전 관련 법령에는 이러한 안전 시스템의 소프트웨어에 대한 구체적 안전기준에 대해서는 좀 더 살펴볼 여지가 있다. 국제적으로는 공정 산업 분야의 안전을 위해 IEC 61511 등이 활용되고 있으므로, 국내에도 이와 연계한 소프트웨어 안전관리 지침 마련을 살펴볼 수 있을 것이다.

의료: 의료기기 소프트웨어는 환자 진단·치료에 직접 영향을 미치므로 각국에서 별도의 규제와 표준을 적용하고 있다. 우리나라는 의료기기법 체계 아래 의료기기를 위험도에 따라 1~4등급으로 분류하고, 소프트웨어가 포함된 의료기기에 대해서는 식품의약품안전처의 가이드라인에 따라 설계 검증, 특성평가 및 밸리데이션 등을 실시한다. 예를 들어 '의료기기 소프트웨어 허가·심사 가이드라인'과 '의료용 소프트웨어 밸리데이션 가이드라인' 등을 제정하여 개발 단계부터 안전성을 입증하도록 하고 있다. 또한 국제 표준 IEC 62304(의료기기 소프트웨어 생명주기 프로세스)와 ISO 14971(위험관리) 등이 의료 SW 설계에 적용되고 있으며, 미국 FDA 역시 소프트웨어 수준에 따른 요구사항을 운영하는 등 의료 분야의 소프트웨어 안전관리가 강화되고 있다.

Ⅲ. 소프트웨어 안전관리의 주요 과제

소프트웨어 안전은 다양한 산업 분야에서 점차 중요성이 부각되고 있으며, 관련 제도와 기준도 점진적으로 정비되어 가는 추세이다. 그럼에도 불구하고, 기술 발전 속도와 산업 간 융합이 빠르게 이루어지는 현 시점에서는 보다 체계적이고 일관된 정책적 대응이 요구된다. 이를 위해 단기적으로 접근 가능한 개선 과제와 중장기적으로 검토할 수 있는 제도적 보완 방향을 구분하여 고찰해볼 필요가 있다.

우선, 각 산업 분야별로 존재하는 소프트웨어 안전 관련 지침이나 기준의 적용 대상을 보다 명확히 하고, 관련 내용을 구체화하는 노력이 필요하다. 현재 일부 제도는 권고 수준에 머물러 있거나 구체적인 기술적 기준 없이 운영되는 경우도 있어, 산업 현장에서의 적용에 어려움이 있을 수 있다. 이에 따라 단기적으로는 기존 지침이나 가이드라인의 실효성을 높이기 위한 세부 기준 보완과 기술 적용 범위의 명확화가 중요한 과제로 제기된다. 또한, 관계 부처 간 정책의 연계성을 강화하기 위한 정보 공유 체계의 마련도 고려해볼 수 있다. 산업별로 개별적으로 관리되고 있는 소프트웨어 안전 관련 정보나 평가사례, 기술자료 등을 공유할 수 있는 플랫폼을 구축하면, 부처 간 정책 일관성을 높이고 중복을 방지할 수 있다. 이러한 협력 기반은 향후 보다 구조적인 거버넌스 논의로 확장될 수 있는 기반이 될 수 있다.

이와 함께, 산업계에서 자율적으로 적용하고 있는 국내외 표준 및 인증 사례들을 수집·정리하여, 소프트웨어 안전성 확보에 실질적인 도움이 될 수 있는 표준화된 참조 자료집 또는 사례집을 마련하는 것도 단기적으로 실현 가능한 과제 중 하나다. 또한 SW안전 산업에 대한 정의를 명확히 하고 분류체계를 구성하여 향후 관련 산업에 대한 지속적인 실태조사 방안을 마련하는 것도 후속 정책을 위한 기반이 될 수 있다.

중장기적으로는 소프트웨어 안전성 확보를 위한 보다 제도적인 장치들을 검토할 필요가 있다. 예컨대, 안전 관련 소프트웨어를 대상으로 한 제3자 인증제도나 안전등급 분류 체계의 도입은 정책 실행력을 높이는 하나의 대안이 될 수 있다. 이러한 제도는 소프트웨어의 위험도에 따라 요구되는 검증 수준을 구분하고, 개발 초기부터 안전성을 고려하도록 유도하는 데 기여할 수 있다. 다만, 이러한 체계는 업계의 수용성과 기술 수준, 인증 역량 확보 등을 종합적으로 고려하여 중장기적으로 단계적으로 추진하는 방식이 바람직할 것이다.

또한, 부처 간 정책 조율과 일관성 확보를 위한 협의체나 조정기구의 구성을 검토해볼 수 있다. 현재 소프트웨어 안전과 관련된 업무가 여러 부처에 분산되어 있어, 정책 방향이나 규제 적용 방식에 있어 일관성이 저하될 가능성이 있다. 따라서 중장기적으로는 부처 간 역할 정립과 정책 정합성을 확보할 수 있는 협력 구조를 마련하는 것이 중요하다. 이는 새로운 법령 제정이나 지침 개정 시에도 상호 충돌을 방지하고, 산업계에 보다 명확한 기준을 제공하는 기반이 될 수 있다.

아울러, 기술 융합이 빠르게 이루어지는 신산업 분야(예: 자율주행, 스마트플랜트, AI 기반 시스템 등)에서는 기존 제도의 적용 범위나 기준이 충분하지 않을 수 있다. 이에 따라 국제 표준의 변화 흐름과 주요국의 정책 사례를 모니터링하고, 국내 제도를 지속적으로 점검·보완하는 체계를 마련하는 것이 필요하다.

Ⅳ. 결론

소프트웨어가 다양한 산업 시스템과 공공 인프라의 핵심 구성요소로 자리 잡으면서, 이에 대한 안전관리의 중요성도 점차 확대되고 있다. 특히 필수안전 산업 분야에서는 소프트웨어의 신뢰성과 기능안전 확보가 전체 시스템의 안전성과 직결되기 때문에, 정책적 대응의 필요성이 꾸준히 제기되어 왔다.

본 논문에서는 원자력, 항공, 자동차, 가스·화학, 의료 등 주요 산업 분야를 중심으로 소프트웨어 안전관리의 제도적 현황을 살펴보고, 관련 법령 및 정책 체계에서의 정비 필요 요소들을 점검하였다. 국내외 표준과 지침이 점차 정비되고 있음에도 불구하고, 산업 특성과 적용 환경에 따라 제도적 접근 방식에는 여전히 다양성이 존재하며, 이를 보다 체계적으로 연결할 수 있는 방안에 대한 논의가 필요하다는 점을 강조하였다. 또한 이를 위해 단기 및 중장기적으로 대응해나갈 방안에 대해서도 고려하였다.

이러한 노력은 궁극적으로 산업 현장의 안전 수준 제고는 물론, 기술 신뢰성 확보와 국민 수용성 향상에도 긍정적인 기여를 할 수 있을 것이다. 지속적인 제도 보완과 정책 연계를 통해 소프트웨어가 안전하게 기능할 수 있는 기반을 마련하는 것이 앞으로의 중요한 과제가 될 것이다.

* 본 논문은 2025년 과학기술정보통신부 SW공학경쟁력강화사업의 지원을 받아 수행된 연구의 일부 내용을 바탕으로 작성되었음.

참 고 문 헌

[1] 과학기술정보통신부, 소프트웨어안전 확보를 위한 지침 (고시 제 2020-77호), 2020.

[2] 박태형, 이중엽 & 손효현, 소프트웨어 안전 사고 사례로 보는 소프트웨어 안전 체계 필요성, 소프트웨어정책연구소(SPRi), 2024.

[3] 이중엽 & 박태형, 미래 모빌리티 동향 및 SW안전 시사점, 소프트웨어정책연구소(SPRi), 2024.

[4] 한국정보통신기술협회 소프트웨어시험인증연구소, 소프트웨어 안전 진단 가이드(공통), 2018