원자력 시설에 적합한 안전 필수 소프트웨어의 개발 방법

박재관*
*한국원자력연구원
e-mail : jkpark183@kaeri.re.kr

A Development Method of Safety Critical Software for Nuclear Facilities

Jae-Kwan Park *
*Korea Atomic Energy Research Institute

요 약

원자력 시설에 적용되는 안전 필수 시스템의 소프트웨어는 매우 높은 수준의 신뢰성이 요구되기 때문에 개발 과정은 중요한 인허가 이슈이다. 원자력 안전 필수 시스템에서의 소프트웨어 공학 활동은 산업표준을 준용하는 부분이 있으나, 일부 상이한 부분이 존재하므로 주의해야 한다. 이 논문은 원자력 요건에 적합한 소프트웨어 개발 방법을 제안한다. 원자력 안전 필수 소프트웨어는 기능 및 성능 요건과 더불어, 안전 요건과 보안 요건을 종합적으로 고려하여 계획 수립, 명세화, 확인 및 검증, 시험을 수행하는 것이 중요하다.

1. 서론

원자력 시설은 사고가 발생할 경우 경제적, 사회적 영향이 매우 크기 때문에 원자력 시설에 설치되는 컴퓨터 시스템들은 매우 높은 수준의 신뢰성이 요구된다. 특히, 원자로를 보호하거나 방사능 누출을 방지하는 안전 기능을 수행하는 안전 필수(Safety Critical) 시스템에서 동작하는 소프트웨어의 개발 방법과 수행 과정은 매우 중요한 인허가 이슈이다. 원자력 시설을 운영하려는 사업자는 소프트웨어 개발 계획, 안전성 분석, 확인 및 검증의 산출물들을 법령에 근거하여 제출하고, 원자력 규제기관은 이를 검토 및 승인한다.

원자력 분야에서의 소프트웨어 공학 활동은 IEEE와 같은 산업표준을 승인해왔으나, 최근에는 산업표준에서 요구하는 부분과 원자력 분야의 요건이 상이한 부분이 발생하고 있다. 따라서, 산업표준을 활용하되, 원자력 요건에 적합한 소프트웨어 공학 활동을 계획 및 수행 하는 것이 필요하다.

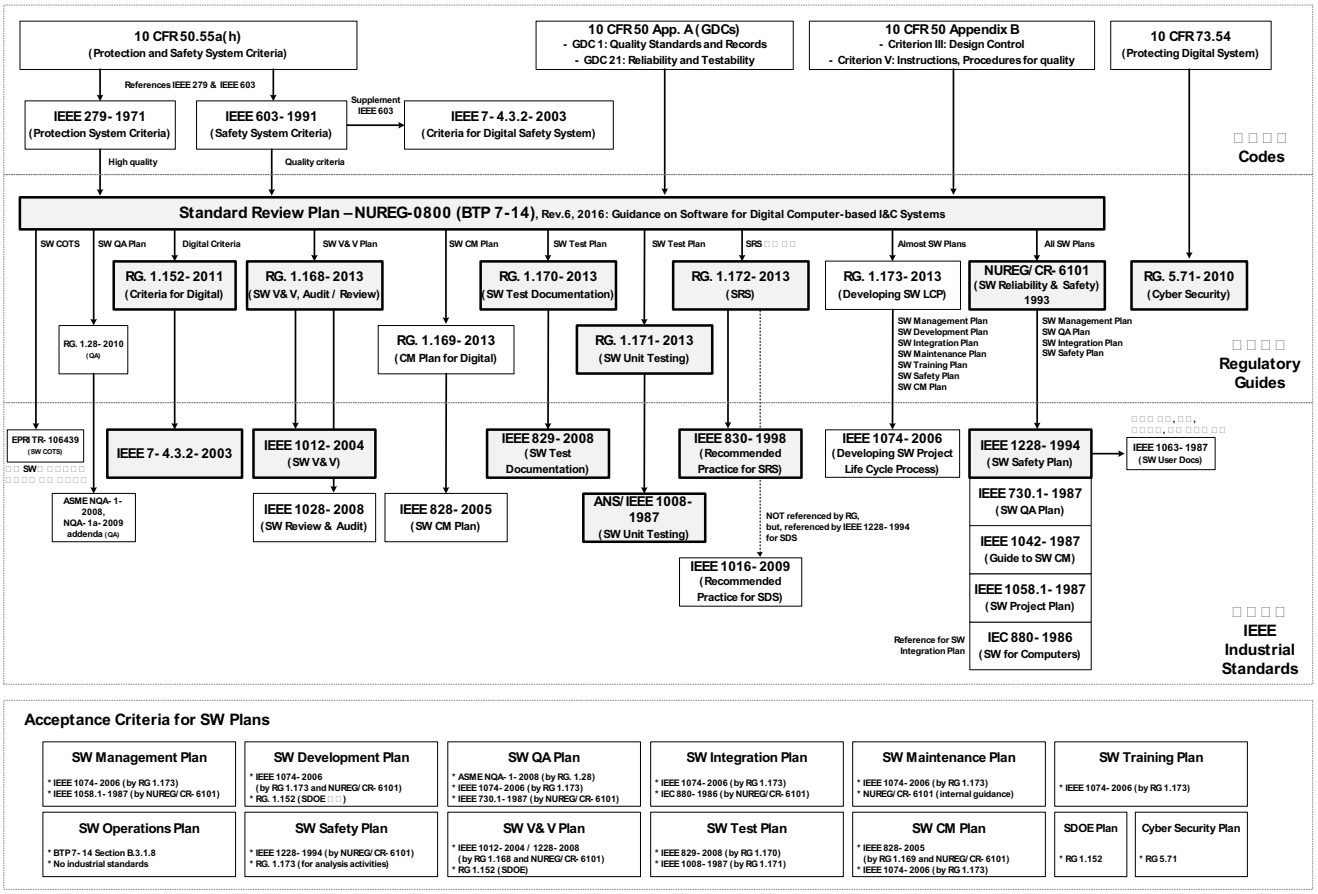
이 논문은 원자력 규제 요건에 적합하도록 안전 필수 시스템의 소프트웨어를 개발하는 방법을 제안한다. 원자력 분야는 소프트웨어 공학에서도 보수적인 접근법을 적용되는 분야이지만, 최근 이슈가 되고 있는 보안이 적용된 개발 환경과 운영에서의 내재적인 안전 강화, 그리고 외부 침투에 대응하는 사이버보안 등이 소프트웨어 개발 과정에서 함께 고려되어야 하며, 이를 통해 더 안전한 소프트웨어 개발할 수 있을 것으로 기대한다.

2. 원자력 안전 필수 소프트웨어 개발 과정

대한민국을 포함한 많은 나라의 원자력 규제는 미국의 규제법 및 규제지침을 준용한다. 따라서, 이 논문에서는 미국 원자력위원회(Nuclear Regulatory Commission)의 규제지침(Regulatory Guide)과 산업표준(IEEE)을 기반으로 분석한다. 안전 기능을 수행하는 시스템의 소프트웨어에 대한 요건은 두 개의 부분, 시스템 내부의 기능, 성능, 신뢰성과 관련된 표준심사지침의 소프트웨어 요건[1]과 외부로부터의 사이버 공격에 대비한 요건[2]이 존재한다. 안전 필수 소프트웨어는 프로젝트 관리, 개발 계획, 형상 관리, 품질, 안전성 분석, 확인 및 검증, 시험 요건이 중요하게 요구된다. 이 논문에서는 이러한 요건들의 상관 관계와 법령, 규제지침, 산업표준 간의 인용 관계에 대한 이해도를 높이기 위해서 그림 1 을 작성하였다.

안전 필수 소프트웨어 요건을 만족하기 위해서 수행해야 할 기본 소프트웨어 활동은 아래와 같다.

- 프로젝트 관리: IEEE 1058.1-1987[3]에 기반하여 프로젝트의 위험을 관리
- 개발 계획 수립: IEEE 1074-2006[4]에 기반하여 소프트웨어 생명주기 공정 계획을 수립
- 형상 관리: IEEE 828-2005[5]를 활용하여 소프트웨어의 형상을 관리
- 품질 관리: ASME NQA-1-2008[6]을 준용하여 소프트웨어 산출물이 높은 품질을 유지



(□□ 1) □□ □□ □□□□□ □□

- 안전성 분석: IEEE 1228-1994[7]에 기반하여 시스템에 고장을 발생시키거나, 성능 저하를 유발하는 인자를 도출하고 제거
- 확인 및 검증: IEEE 1012-2004[8]의 소프트웨어 신뢰성 수준 4 에 해당하는 소프트웨어 활동이 수행되며, 각 생명주기 단계에서 결과물에 대한 확인 및 검증을 수행
- 시험: IEEE 829-2008[9]에 기반하여 시험 계획, 시험 설계, 시험 절차를 수립하고 문서화하며, IEEE 1008-1987[10]에 기반하여 소프트웨어 단위 시험을 수행

안전 필수 소프트웨어를 개발하는 과정의 첫 단계는 소프트웨어 계획서(Software Plan)를 준비하는 것이다. 그림 1 의 소프트웨어 계획의 허용기준에 정리한 바와 같이, 기본적인 계획들 이외에 소프트웨어 안전성 계획(Software Safety Plan), 보안성 환경 계획(Secure Development and Operational Environment Plan), 사이버보안 계획(Cyber Security Plan)이 소프트웨어의 신뢰성 있는 작동을 보장하기 위해서 중요하게 준비되어야 한다. 안전성 분석 계획은 위험요소 분석(Hazard Analysis)를 수행하여 시스템의 위험상태(Hazard)를 식별하고 중요도 분석(Criticality Analysis)을 통해 위험의 중요도를 분류하며, 안전 요건을 도출한 뒤, 설계항목 및 시험을 통해 위험을 제거하기 위한 계획을 수립하는 것이다. 보안성 환경 계획과 사이버보안 계획은 산업표준을 인용하지 않고 독자적인 원자력 규제요건을 적용한다. 보안성 환경 계획은 소프트웨어를 안전한 개발과정에서 개발하고 설치 및 운영환경을 분석하여 예상되는 오작동을 설계단계부터 고려하여 대처하기 위한 안전 강화 요건이다. 사이버보안 계획은 시스템의 물리적인 접근성과 디지털 연계성을 기반으로 악의적인 의도를 가진 사람에 의한 사이버 공격으로부터 필수 시스템을 보호하기 위한 수단을 마련하기 위한 계획을 세우는 것이다.

계획 수립이 완료되면, 요건 명세서를 작성하는 것이 중요하다. 소프트웨어가 수행해야 하는 기능 및 성능을 개별 요건으로써 정확하게 명시한다. 요건은 추적성, 완전성, 일관성, 확인성, 수정성, 명료함 특성을 만족하도록 요건 명세서에 기술된다. 이에 더하여 원자력 추가 요건으로써, 소프트웨어에 대한 안전성, 보안성, 강인성 요건이 요건 명세서에 명시되어야 한다. 즉, 초기 안전성 분석 결과인 예비 안전성 분석 보고서, 보안성 분석 결과인 잠재적 민감도 분석 보고서와 원자력 사이버보안 요건이 요건 명세서에 기술되어야 한다.

다음 과정은 소프트웨어 계획에 기반하여 개발을 진행하면서, 소프트웨어 확인 및 검증(Software Verification and Validation)을 수행하는 것이다. 이때, 독립된 조직에서 확인 및 검증을 수행하는 것이 필수적이다. IEEE 1012-2004[8]에서는 영향성을 평가하는 조건부 독립성 개념을 정의하고 있으나, 원자력 규제지침에서는 인정되지 않으며, 기술적, 관리적, 경제적으

로 독립된 조직이 수행해야 한다. 확인 및 검증은 기능 및 성능 요건, 안전 요건, 보안성 요건 등이 누락없이 설계, 시험 과정을 통해 정확하게 구현되는지를 보장하기 위한 활동들이 개념단계, 요건단계, 설계단계, 구현단계, 시험단계까지 진행되어야 하고 각 단계마다 개별 확인 및 검증 보고서가 발행되어야 한다. 현재까지의 규제입장에 따르면, 사이버보안을 위해 요구되는 기술적인 소프트웨어 부분은 확인 및 검증 보고서에 포함될 수 있다. 그러나, 안전 요건 및 보안성 요건에 대한 확인 및 검증 활동의 결과는 별도의 안전성 분석 보고서 및 보안성 환경 보고서로 발행되어야 한다. 이것은 기능 및 성능 요건과 안전 요건을 구분하고, 안전 요건을 더 명확하게 검토하기 위한 것이다.

확인 및 검증 과정에서 요구되는 원자력 보안 분석(Secure Analysis)은 산업표준에서의 보안 분석과 상이하다. 산업표준에서 보안 분석의 범위는 우연히 또는 악의적인 행위(Accidental and malicious activities)를 다루고 있으나, 원자력에서는 비-악의적인(non-malicious) 행위에 대하여 보안성 분석을 통해 확인 및 검증 활동을 수행해야 한다. 다만, 악의적인 행위에 대한 사이버보안 규제가 적용되나, 개발과정에서의 확인 및 검증을 필수적으로 요구하지는 않는다.

소프트웨어 개발의 마지막 단계는 최종 구현 결과물의 기능 및 성능을 확인하기 위한 시험이다. 시험은 개발팀이 아닌, 확인 및 검증팀이 수행한다. 시험 항목 설계는 소프트웨어 요건 및 설계 항목이 어떤 시험과 연결되는지를 확인할 수 있는 추적성(Traceability)과 소프트웨어의 모든 모드(Mode)에 대하여 모든 기능이 시험될 수 있도록 완전성(Completeness)을 고려하여 작성한다. IEEE 1008-1987[10]에 따르면, 시험 항목은 각 소스코드 문장을 포함하는 구문 커버리지(Statement coverage)를 인정하고 있으나, 원자력에서는 코드 기반의 구문 커버리지와 분기 커버리지(Branch Coverage)가 모두 요구된다. 또한, 시험은 안전 기능 시험, 보안성 환경 시험, 사이버보안 시험을 포함하여 수행한다. 단, 사이버보안 시험은 사이버보안 기능이 동작할 경우, 고유의 안전 기능 수행에 악영향을 주지 않는지 확인해야 한다.

3. 결론

최근, 국내에서는 원자력 시설에 대한 안전이 더욱 강화되고 있다. 또한, 해외에서는 사이버 공격에 의한 제어시스템의 오작동 사례가 발생하여 이에 대응하는 규제가 강화되는 등 원자력 안전 필수 시스템의 소프트웨어에 대한 중요성이 강조되고 있다. 이 논문은 원자력 시설에 적합한 안전 필수 소프트웨어에 요구되는 필수 공학 활동을 제시하였다. 먼저, 최근 강화된 보안 요건을 포함한 원자력 소프트웨어 공학 활동 체계를 분석하여 도식화 하였다. 프로젝트 전반에 걸쳐 기본적인 품질관리, 형상관리가 적용되며, 소프트웨어 계획, 요건 명세서 작성, 확인 및 검증, 시험은 산출물의 신뢰성을 결정짓는 매우 중요한 활동이다. 뿐만 아니라, 안전성 분석, 보안성 환경 분석, 사이버 보안 활동은 시스템 개발 과정에 포함되어 수행되어야 하며, 안전 필수 소프트웨어의 위험이나 취약점을 배제하는데 필수적이다. 제시된 소프트웨어 공학 활동은 계획부터 시험까지 유기적으로 수행되어야 한다.

참고문헌

[1] US Nuclear Regulatory Commission. “Guidance on Software Reviews for Digital computer-Based Instrumentation and Control Systems”, NUREG-0800 BTP 7-14, 2016

[2] US Nuclear Regulatory Commission. “Cyber Security Programs for Nuclear Facilities”, RG 5.71, 2010

[3] IEEE. “IEEE Standard for Software Project Management Plans”, IEEE Std. 1058.1, 1987

[4] IEEE. “IEEE Standard for Developing a Software Project Life Cycle Process”, IEEE Std. 1074, 2006

[5] IEEE. “IEEE Standard for Software and System Test Documentation”, IEEE Std. 828, 2005

[6] ANS. “Quality Assurance Requirements for Nuclear Facility Applications”, ASME NQA-1, 2008

[7] IEEE. “IEEE Standard for Software Safety Plans”, IEEE Std. 1228, 1994

[8] IEEE. “IEEE Standard for Software Verification and Validation”, IEEE Std. 1012, 2004

[9] IEEE. “IEEE Standard for Software and System Test Documentation”, IEEE Std. 829, 2008

[10] ANS. “IEEE Standard for Software Unit Testing”, ANSI/IEEE Std. 1008, 1987