원자력발전소 디지털 계측제어계통 고신뢰도 소프트웨어 검증 기술

한국원자력연구소 권기춘* · 차경호 · 이장수*

1. 서 론

소프트웨어 검증은 계통이 실제로 요구된 기능을 완벽하고 신뢰성있게 수행함을 소프트웨어 개발 공정 단계별로 검증(Verification)하는 절차와 그 소프트웨어가 계통의 요구사항대로 설계되었음을 확인(Validation)하는 절차인 확인/검증(V&V)을 포괄적으로 포함하는 개념으로 설정한다.

기존 원자력발전소(원전) 아날로그 계측제어계통은 그 시스템의 노후화와 기술의 낙후성으로 인해 운전 및 유지보수 비용이 증가하고 안전성까지 위협받고 있다. 반면에 컴퓨터 소프트웨어 기술은 급속도로 발전하여 그 성능의 우수성을 인정받고 여러 산업 분야에서 활용되고 있다. 원자력 산업에서도 이러한 추세와 보조를 같이하여 비안전 계측제어계통이 디지털화 되었으며, 소프트웨어 기술의 급격한 발전으로 인해 점차 안전계통에 소프트웨어를 사용하고 있는 추세이다. 그러나 고신뢰도를 요구하는 안전계통을 소프트웨어로 구현하는 과정에는 소프트웨어 공통모드고장(Common Mode Failure)과 같은 위험 요소가 존재한다[1]. 일반 산업체와는 달리 원전에서 발생하는 사고의 여파는 일반 공중에게 방사능 누출과 방사성 물질의 피해를 입힐 수 있는 가능성을 내재하고 있어 이러한 가능성을 배제하기 위한 원전 디지털 안전계통은 다음과 같은 기능을 갖추어야 한다. 디지털 안전계통은 설계된 기본 사건에 대해서 첫째로, 원자로 냉각재 압력 경계의 건전성을 보장하고 둘째, 원자로를 정지시키고 원자로가 안전한 정지조건을 만족하는 것을 보장하고 셋째, 원자로 밖으로 누출되는 사고에 대해서도 그 피해를 최소화시키거나 방지할 수 있는 기능을 보장하는 것이다[2]. 따라서 이러한 디지털 안전계통의 기능을 보장하는 소프트웨어를 개발하기 위해서는 신뢰성(Reliability)과 안전성(Safety) 확보가 그 관건이며 이 두 가지 기능은 원전 계측제어계통 고신뢰도 소프트웨어의 특성상 매우 중요하다.

원전 디지털 안전계통에 적용되는 고신뢰도 소프트웨어는 엄격한 규제요건을 적용받고 있으며, 이러한 규제요건은 원전의 안전성을 확보하기 위해서 필수적인 요소이다. 국내에서는 한국원자력안전기술원이 원전 건설과 운영에 관한 규제를 시행하고 있으며, 디지털 계측제어 소프트웨어에 관한 규제요건 및 지침을 개발중이다. 현재 국내에서도 디지털 안전 소프트웨어 검증은 이와 같은 규제요건에 따라서 수행되고 있다. 고신뢰도 소프트웨어의 검증은 소프트웨어 생명주기 전 단계에 걸쳐서 진행되어야 한다.

2. 고신뢰도 소프트웨어 개발 규제요건

원전 안전계통은 고신뢰도와 고장시 안전을 보장하고 안전기능의 손실이 없도록 하기 위해서 품질보증 개념과 다양성을 갖는 다중방호(Defense-in-Depth) 개념을 가지고 설계되어야 한다. 이러한 개념은 IEEE Std 603-1991, Reg. Guide 1.152[3]와 IEEE 7-4.3.2-1993[4] 등에 잘 나타나 있으며, 규제기관에서 디지털 안전계통을 검토할 때 주요 규제요건으로 사용된다. 그 밖에 많은 Reg. Guide, IEEE 기술기준이 참고로 사용된다. 피규제자는 궁극적으로 IEEE 7-4.3.2를 만족시킬 의무가 있다. IEEE 7-4.3.2는 규제자와 피규제자 사이의 인터페이스, V&V의 독립성, V&V에 사용된 도구와 사람에 대한 자격, 하드웨어와 소프트웨어 및 시스템의 요구사항, 소프트웨어 개발 절차, 상용 소프트웨어의 검증방법, 하드웨어 및 소프트웨어의 통합, 확인 및 검증방법 등을 기술

* 종신회원

하고 있다. 그러나 IEEE 7-4.3.2에는 시스템 및 하드웨어와의 통합을 고려하면서 주로 소프트웨어에 관련된 규제내용들이 원칙적인 측면에서 간략하게 기술되어 있다. 즉, IEEE 7-4.3.2의 본문내용에는 다른 규제지침서와 표준들로의 참고부분이 많으며 기술적으로 구체적인 내용은 대부분 부록에 수록되어 있다. 따라서 규제기관에서는 많은 부분을 확대 해석하여 적용하고 있으며, 이에 따라 여러 가지 규제 지침들을 필요로 한다.

고신뢰도 소프트웨어 관련 규제 지침을 살펴보면, 최상위에 10 CFR(Code of Federal Regulations) Part 50(원자력발전소 설계기준)이 있고 그 밑에 안전계통 설계 기준인 IEEE Std 603이 있으며, 안전성과 관련하여 Reg. Guide 1.153(안전계통 규제요건)[5]과 IEEE Std 379-2000(안전계통 단일고장 기준의 표준)[6]가 있다. 소프트웨어 품질과 관련하여 Reg. Guide 1.152(안전계통 디지털 컴퓨터의 규제요건), Reg. Guide 1.168(안전계통 소프트웨어 확인·검증· 검토·감사 규제요건)[7]이 있으며, 이 규제요건에서 승인한 IEEE Std 7-4.3.2가 있다. 그 하위에 소프트웨어 계획관련인 IEEE Std 1058.1-1987(소프트웨어 프로젝트 관리계획을 위한 기준)[8], IEEE Std 828-1998(소프트웨어 형상관리계획 작성을 위한 기준)[9], IEEE Std 1042-1987(소프트웨어 형상관리 기준)[10], IEEE Std. 1012-1986(소프트웨어 확인/검증 계획을 위한 기준)[11], IEEE Std 1228-1994(소프트웨어 안전성 계획을 위한 기준)[12], Regulatory Guide 1.169(안전계통의 디지털 컴퓨터 소프트웨어에 대한 형상관리 계획)[13]이 있다. 그리고 소프트웨어 설계와 관련하여 IEEE Std 830-1993(안전 소프트웨어 요구명세를 위한 기준)[14], IEEE Std 1016-1987(소프트웨어 설계 명세 기준)[15], IEEE Std 1016.1-1993(소프트웨어 설계 명세 안내서)[16], Reg. Guide 1.172(안전계통 소프트웨어 요구명세 규제 지침)[17]이 있으며, 소프트웨어 시험검증과 관련하여 IEEE Std 829-1983(안전계통의 소프트웨어 시험에 관한 문서화 기준)[18], IEEE Std 1008-1987(안전계통 소프트웨어 단위 시험을 위한 기준)[19], IEEE Std 1059-1993(소프트웨어 시험검증 기준)[20], Reg. Guide 1.171(안전계통의 디지털 소프트웨어 단위시험에 대한 규제 지침)[21] 등이 있다. 그 밖에 IEEE Std 730-1998(소프트웨어 품질보증 계획서 작성을 위한 기준)[22], IEEE Std 1074-1997(소프트웨어 생명주기 공정 개발 기준)[23], IEEE Std 1028-1998(소프트웨어 검토 및 감사 기준)[24]이 있다. 이와 같은 규제 기준 또는 지침을 계층적으로 표현하면 그림 1과 같다.

3. 고신뢰도 소프트웨어 검증의 기술적 측면

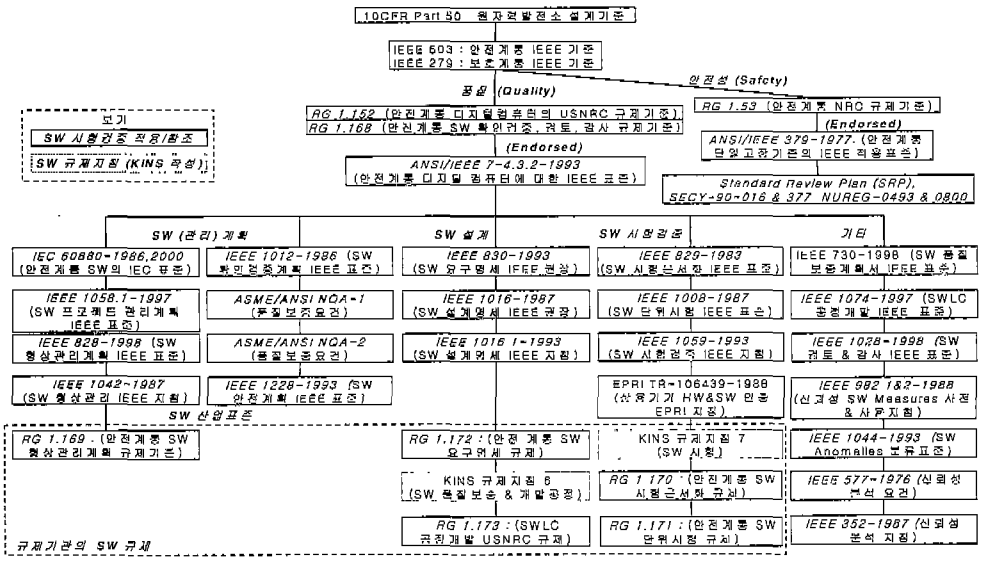

그림 1 고신뢰도 소프트웨어 규제요건 계층도

원전 디지털 계측제어 소프트웨어는 그 중요도(Criticality)의 정도에 따라 안전계통 소프트웨어, 제어계통 소프트웨어, 감시계통 소프트웨어와 그 외 여러가지 운전보조계통 등으로 나눌 수 있다. 이들은 다시 안전관련 소프트웨어와 안전에 관련이 없는 소프트웨어로 나누어지며, 이들 소프트웨어를 개발하고 인허가를 수행할 때 현재 쟁점으로 부각되고 있는 것은 대중의 안전과 직결되는 안전관련 소프트웨어의 품질(Quality)과 신뢰도(Reliability)의 보장 문제이다.

구체적으로 말하자면 안전계통 소프트웨어의 공통모드고장 극복이 관건이며 이를 위해 소프트웨어 다중성(Diversity), 주요 소프트웨어 격리, 소프트웨어 위험도 분석, 고장허용(Fault-tolerant) 소프트웨어 개발, 정형기법(Formalism)의 도입 등 다양한 방법들이 제시되고 있다. 또한 원전에서 사용되는 모든 소프트웨어는 상당히 높은 수준의 품질과 신뢰도를 요구하고 있다.

고신뢰도 소프트웨어를 개발하고 확인 및 검증을 수행하여 이에 대한 인허가를 수행하기 위해서는 소프트웨어 개발공정 전단계에 걸쳐서 기존의 소프트웨어 공학에서 연구되고 실용화되어 있는 소프트웨어 개발 방법론들이 매우 엄격하게 적용되어야 하며, 이에 대해서 규제기관에서는 그림 2와 같이 소프트웨어 생명주기에 대한 업무를 정의하고 있다. 이러한 엄격함에도 불구하고 현재 소프트웨어의 신뢰도 측면에서 소프트웨어 공통모드고장 문제를 완전히 해결하자 못하고 있으며 한편으로는 인공지능 기법, 객체지향 프로그래밍, 실시간 프로그래밍 등 소프트웨어 관련 기술이 급속도로 발전하고 있다.

급격한 기술 발전은 소프트웨어 개발자에게 새로운 개발방법의 사용을 요구하며 규제기관에게는 새로운 규제요건의 개발과 새로운 규제방법을 요구하고 있다. 또한 소프트웨어 공학의 학문적인 측면에서도 고신뢰도 고품질의 소프트웨어를 적은 비용으로 효율적으로 개발할 수 있고 소프트웨어 공통모드고장을 극복하여 신뢰도를 보장할 수 있는 이론 정립과 도구 개발에 많은 노력을 하고 있으며, 이를 바탕으로 한 새로운 개발 방법론들을 제시하고 있다.

원전 계측제어 소프트웨어들은 그 중요도의 정도와 소프트웨어의 종류에 따라 분류되며 이러한 분류에 따른 각각의 소프트웨어는 서로 다른 패러다임과 개발 방법론들이 적용되어야 한다. 이를 위해 IEEE Std 7-4.3.2, IEEE Std 1228 등에서와 같이 체계적인 요건들의 개발 및 보완 작업이 진행 중에 있다. 그러나 규제요건 및 표준들이 급격한 기술 발전을 효율적

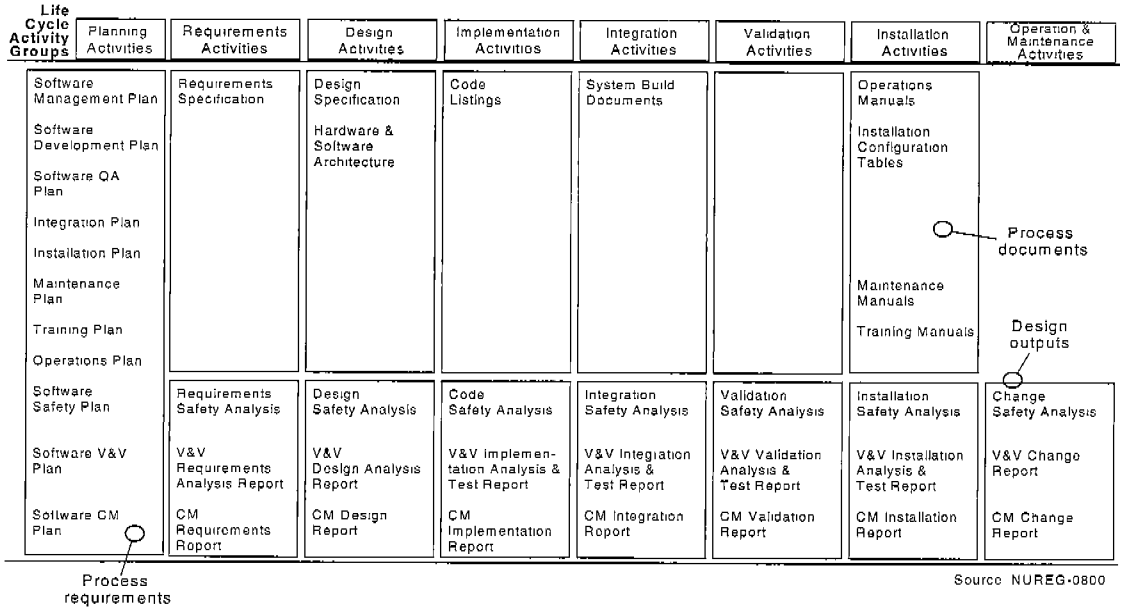

그림 2 소프트웨어 생명주기 업무 정의

으로 수용하기 위해서는 각각의 요건들이 유연성과 확장성을 갖도록 보완되어야 하며 IEEE, ASME 등 타 산업 표준들과 개발자 내부 지침서, 규제요건들의 유기적인 연계 체제를 갖추어야 한다.

3.1 품질과 안전성 보장을 위한 문제점 고찰

3.1.1 품질측면

3.1.1.1 계획 단계

이 단계에서는 프로젝트 관리 계획(Project Management Planning), 형상관리계획(Configuration Management Planning), 소프트웨어 안전성 확보 계획(Software Safety Planning), 소프트웨어 검증 및 확인 계획(Software Verification and Validation Planning), 소프트웨어 품질보증 계획(Quality Assurance Planning) 등이 수행되며 이와 관련하여 IEEE Std 1058.1, IEEE Std 828, IEEE Std 730.1-1989[25], IEEE Std 1012, IEEE Std 1228 등의 규제요건들이 있다. 규제기관에서는 소프트웨어 생명주기 전단계에 대하여 감사와 검토를 수행하며 이 때 필요한 문서의 종류를 밝히고 있다.

그러나 규제기관에서는 IEEE 7-4.3.2를 중심으로 상하의 관련된 기술기준(Codes and Stds)을 참고하여 규제를 시행하며 검토에 필요한 문서의 종류를 밝히고 있으나, 세부 기술적인 면에서 애매하고 추상적인 부분에 대해서는 현재 명확한 기준과 한계를 세우지 못하고 있는 실정이다. 예를 들면 프로젝트 관리 계획에서 개발팀과 V&V팀의 독립성에 대한 명확한 정의, 소프트웨어 안전성 확보 계획에서 모든 종류의 소프트웨어에 대한 정량적인 신뢰도 명시, 요구되어지는 문서들이 가져야 할 세부적인 기술사항에 대한 구체적인 언급이 없다.

3.1.1.2 요구분석 단계

이 단계에서는 요구사양을 작성하고 분석할 때 수학적인 정형기법을 도입하여 품질과 신뢰도를 높여보고자 하는 것이 최근의 추세이다. 요구사양을 형식에 맞게 작성함으로써 다음 단계인 설계를 수행할 때 보다 완벽하게 요구사항을 반영할 수 있고 요구분석을 수동 혹은 자동으로 수학적인 증명을 할 수 있다. 그리고 오류를 개발공정 초기에 발견 수정할 수 있음으로써 개발비용을 절감할 수 있는 장점이 있다. 그러나 이 단계의 주목적이 사용자 혹은 시스템 엔지니어와 소프트웨어 엔지니어사이의 의견교환을 통해서 정확한 요구사항을 수립하는 것인데, 이러한 수학적인 정형기법의 도입은 자연 언어를 사용한 통신보다는 의사 전달이 부자유스러운 단점이 있다. 이러한 정형화된 요구조건으로부터 테스트 케이스를 자동생성할 수 있고 요구사양 자체를 실행할 수 있는 자동화 도구를 만들어 요구분석 단계에서 개발하고자 하는 시스템의 동작을 시뮬레이션해 봄으로써 오류를 조기에 발견, 해결하고자 하는 노력을 진행 중에 있다. 이외에도 요구사항 분석에 대한 추적성의 완벽한 시행 및 자동 점검방법 등에 대한 연구와 상품화가 진행 중에 있다.

3.1.1.3 설계 단계

여기서도 앞 단계에서와 같은 수학적인 정형기법의 도입이 시도되고 있으며 설계 방법론에서도 이제까지의 구조적 설계 방법론에서 점차 객체지향 설계 방법론으로 바뀌어 가고 있다. 모듈 결합도(Module Coupling), 모듈강도(Module Cohesion), 모듈화(Modularity), 정보은닉(Information Hiding) 등 그동안의 소프트웨어 공학에서의 연구 결과들이 점차 객체지향 설계 방법론으로 초점이 맞춰지고 있다. 이러한 객체지향 설계방법은 재사용성을 높여 개발하는 소프트웨어 시스템의 신뢰도를 높이고 V&V 비용을 감소시킬 수 있다.

3.1.1.4 구현 단계

개발시 사용되는 프로그래밍 언어가 점차 어셈블리 언어에서 C, Ada와 같은 고수준 언어로 바뀌어 가고 있으며 앞으로는 C++과 같은 객체지향 언어가 사용될 전망이다. 이러한 프로그래밍 언어의 선택과 소프트웨어 공통모드고장 극복을 위한 다양성을 언어와 컴파일러에 적용하고 있다. 또한 컴파일러, 운영체제, 시험 도구, 에디터 등 개발에 사용되는 모든 도구들에 대한 사전 자격심사(Prequalification)가 문제가 되고 있다. 소프트웨어 개발 회사들은 자체적으로 코딩 지침서등을 작성하여 사용하고 있으나 표준화가 되어 있지 못한 형편이다. 완벽한 예외사항 처리등 고장허용 프로그래밍이 요구되고 있으며 고장허용 소프트웨어의 개발은 요구분석 단계부터 고려되어야 할 기술적인 사항이 매우 많다. 이를 위해 현재 시도되고 있는 기술들 중 대표적인 것으로 소프트

웨어 생명주기 전 단계에 걸쳐 다양성을 고려하는 N-version 프로그래밍 기법과 Recovery Block 기법이 사용되고 있으나 소프트웨어 복잡도 증가에 따른 안전성 위해요소가 있어 많은 논란이 제기되고 있다.

3.1.1.5 통합, 확인 및 검증 단계

검증이란 소프트웨어 개발의 각 단계에서 그 소프트웨어가 요구사항을 만족하는가를 평가하는 것이며, 확인은 소프트웨어 개발공정 전체 단계에서 해당 단계의 결과물이 전단계의 결과물과의 일관성, 완결성, 정확성을 만족하는가를 확인하는 것이다. 요구분석 단계, 설계 단계, 구현 단계를 거치면서 세부 모듈의 프로그래밍이 되고 나면, 이러한 Break-down의 역순으로 모듈들을 통합하여 시스템을 완성하고 통합 순서에 따라 확인과 시험이 이루어진다. 이러한 시험은 모듈시험, 통합시험, 기능시험, 시스템 시험, 인수시험, 설치시험의 순서로 이루어진다. 시험의 각 단계에서 사용될 수 있는 기법과 도구가 많으며, 관련 연구 논문들이 계속해서 나오고 있기 때문에 이들의 선택과 사용에 세심한 주의를 기울여야 하며, 요구되는 신뢰도에 따라 시험계획 작성과 시험종료시점이 달라지며 고신뢰도 소프트웨어일수록 시험비용이 올라간다. 근본적으로 소프트웨어의 완벽한 시험은 불가능하며 확인 및 검증의 독립성, 자체시험, 확인 및 검증의 정도 등이 주 관심사이다. 현재 사용중인 시험관련 규제지침에는 IEEE Std 829와 IEEE Std 1008이 있으며 확인 및 검증과 관련하여 IEEE Std 1012가 있다. 원전 안전계통 소프트웨어와 같은 고신뢰도 소프트웨어의 시험을 위해서는 이러한 기존의 표준을 바탕으로 엄격하고 명확하며 객관적인 기준이 제시되어야 하며, Reg. Guide 1.171에서 이러한 기준의 일부를 명시하고 있다.

3.1.1.6 설치, 운영 및 유지보수 단계

이 단계에는 설치문서, 운전 및 유지보수 지침서, 훈련지침서등 각종 문서들을 정확히 갖추어야 하며 개발과정에서 발견하지 못한 결함을 보완하기 위한 유지 및 보수계획, 회귀분석(Regressing) 시험계획과 이에 따른 형상관리 수정, V&V 이상 보고서, 안전성 분석 수정 등이 중요하다. 특히 소프트웨어 유지보수는 계측제어계통이 하드웨어에서 소프트웨어로 바뀜에 따라 현장에서 느끼는 가장 심각한 애로 사항으로 부각되고 있어 소프트웨어 시스템에 대한 시험가능성 여부는 새로운 문제로 제기되고 있다.

3.1.2 안전성측면

원전 디지털 안전계통이 개발되면서 소프트웨어 공통모드고장 극복과 같은 소프트웨어 안전성 보장 문제가 쟁점으로 부각되고 있다. 품질보증 측면에서의 노력에도 불구하고 공통모드고장이 발생할 가능성이 있기 때문에 다중방호 보장을 위한 설계에서의 다양성 제공이 필요하다. 원전 안전계통의 신뢰도 분석에 대한 일반적인 원칙은 IEEE Std 352에 소개되어 있으며 고장모드 영향분석과 고장수목분석과 같은 정성적인 신뢰도 분석방법과 수학적 모델링에 의한 정량적인 신뢰도 분석원칙을 설명하고 있다. 즉 신뢰도 분석에 대한 시스템 차원에서의 이론들을 표준화한 것이다. 이렇게 표준화된 시스템 차원의 이론들은 소프트웨어에 그대로 적용될 수 없으며 소프트웨어의 신뢰도 분석을 위한 정성적, 정량적 방법과 척도가 표준화되어야 한다.

이러한 표준화를 위한 노력의 일환으로 NUREG/CR-5930[26]와 IEEE Std 1228 등이 만들어 졌다. NUREG/CR-5930에서는 고신뢰도 소프트웨어의 표준화 지침서들이 가져야 할 기준을 설명하고 기존 지침서들의 문제점을 분석하고 있다. 여기서는 고신뢰도를 요하는 소프트웨어의 안전성을 보장하기 위한 방법으로 소프트웨어 위험도분석에 대한 기준을 제시하고 있으며 이러한 기준 전체에 대한 설명은 다음 절에서 기술하고자 한다. IEEE Std 1228은 소프트웨어 안전성계획에 대한 방법들을 서술하고 있다.

3.2 고신뢰도 소프트웨어 확인검증 기준

고신뢰도의 소프트웨어 시스템을 개발하기 위해서는 개발자, 감리자, 사용자가 공동으로 사용할 수 있는 고신뢰도 소프트웨어 공학 분야의 지식이나 기술적 근거가 있어야 한다. 그러나 타 공학분야와는 달리 소프트웨어 공학 분야의 이러한 지식은 규제지침이나 핸드북 형태의 체계적이고 종합적인 문서화가 미흡한 실정이다. 본 절에서는 규제지침이 체계적으로 문서화되고 대상 소프트웨어의 객관적인 측정도구로 사용될 수 있기 위한 기준을 설명하고자 한다. 이에 대한 연구 결과인 NUREG/CR-5930 내용 중 기준에 관련된 핵심적인 것만을 요약하여 정리하였다.

3.2.1 중요도/보증의 수준

인적, 물적 중요도의 정도에 따라 개발하고자 하는 소프트웨어의 요구사항, 개발에 사용된 도구, 방법론 등이 달라져야 한다. 이와 같은 것들은 중요도 이외에도 인공지능 기법과 같은 신기술의 사용, 소프트웨어가 가지는 임무의 중요도, 프로젝트의 크기 등에 의해서도 달라진다.

3.2.2 Life Cycle Phases

규제지침이 생명주기의 단계를 갖는 것이 각 문서의 범위를 분명히 하기에 용이하다. 여러 가지 생명주기 모델이 있고 각 모델에서의 단계에 대한 표현도 다양하다. 일반적으로 계획(초기) 요구분석, 설계, 구현, 통합 및 시험, 설치, 운영 및 유지보수 등으로 이루어진다.

3.2.3 문서화

소프트웨어 문서화는 개발자, 사용자, 감리자, 검사자, 인허가자 각각에게 서로 다른 여러가지 목적을 가진다. 따라서 규제지침은 문서의 요구사항이 얼마나 철저한가?, 문서화에 묘사되어야 할 내용과 항목이 제대로 명시되어 있는가?, 정량적인 특성 묘사가 있는가? 등을 반영하여야 한다.

3.2.4 위험대비 소프트웨어 기능성

시스템 위험도분석은 시스템 동작에 급작스럽게 영향을 줄 수 있는 위험요소의 종류에 대한 정보를 제공한다. 특정 소프트웨어는 이러한 위험요소를 발견하고 완화하며 극복하는 기능을 가질 수 있으며 고신뢰도 소프트웨어 규제지침에서는 이와 같이 위험요소를 대비하기 위한 소프트웨어의 방호 기능을 고려하여야 한다.

3.2.5 소프트웨어 공학 실행

소프트웨어 공학의 실제 기술들의 적절한 사용이 고신뢰도 소프트웨어 개발에 필수적이며 규제지침에도 정확하게 명시되어야 한다. 즉 정형화된 명세서, Component Isolation, Modularity, 언어와 컴파일러 선택, 부동 소수점 계산과 인터럽트를 사용하지 않는 프로그래밍, Quality Attributes 등이 반영되어야 한다.

3.2.6 보증활동

여기서는 소프트웨어 개발공정 전체에서의 문제점 발견을 위한 활동들인 소프트웨어 확인 및 검증, 소프트웨어 품질보증, 소프트웨어 형상관리, 소프트웨어 위험도 분석 등에 관하여 규제지침이 가져야 할 기준을 명시한다.

4. 결 론

지금까지 원전 디지털 안전계통에서 사용되는 고신뢰도 소프트웨어의 개발과 규제의 기술적인 측면을 소프트웨어 품질과 안전성 보장 측면에서 문제점들을 논하였다. 이러한 기술적 현안을 해결하기 위한 연구 노력들을 살펴보았고, 고신뢰도 소프트웨어 규제요건이 갖추어야 할 기준을 서술하였다. 이와 같은 규제요건이 가져야 할 기준은 곧 고신뢰도 소프트웨어 개발방법과 규제방법의 기준이 될 수 있을 정도로 직접적인 관계가 있다.

고신뢰도 소프트웨어의 품질보증 관련 현안들을 소프트웨어 개발단계별로 알아보았고 각 단계별 기술 추세를 소프트웨어 개발방법, 규제방법, 규제기준의 측면에서 제시하였다. 그리고 소프트웨어 공통모드고장 대책과 같은 안전성 보장 관련 현안에 관하여 논하였다.

이와 같이 소프트웨어 안전성 보장이라는 목표를 달성하기 위해 현재 각계 각층에서 많은 노력을 기울이고 있다. 즉 산업표준을 정립하는 IEEE, ASME, IEC, ISO 등에서는 소프트웨어 안전관련 요건 정립 노력을 진행 중이며 규제를 시행하는 외국의 규제기관들에서도 규제시행 측면에서 소프트웨어 안전성 보장을 위한 연구를 수행 중에 있다. Lawrence Livermore National Laboratory와 National Institute of Standard and Technology 등 NRC 자문기관들에서는 원자력 분야 소프트웨어의 안전성 보장을 위한 광범위한 연구와 디지털 시스템 안전성 평가 업무를 수행 중이며 관련 기술이 가장 많이 축적된 것으로 알려지고 있다.

이와 같은 종합적인 노력에 의해서 디지털 소프트웨어 시스템의 안전성이 보장될 수 있고 원전에서 디지털 계측제어 기술이 정착할 수 있을 것이다. 후속기 원전에서 계측제어계통을 디지털화하고 기술자립을 추구하고 있는 우리도 이러한 상황에서 고신뢰도 소프트웨어 안전성 보장 기술과 확인 및 검증 기술과 같은 핵심 기반 기술의 확보가 필수적이다.

참고문헌

[1] 이장수 외, "원전 계측제어 고신뢰도 소프트웨어

개발 및 확인검증의 기술적 고찰," '94춘계학술발표회 논문집, 한국원자력학회.
[2] IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.
[3] Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Rev. 1, U.S. Nuclear Regulatory Commission, January 1996.
[4] IEEE Std 7-4.3.2-1993, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
[5] Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," Rev. 1, U.S. Nuclear Regulatory Commission, 1996.
[6] IEEE Std 379-2000, "IEEE Std. Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems".
[7] Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, 1997.
[8] IEEE Std 1058.1-1987, "Standard for Software Project Management Plans."
[9] IEEE Std 828-1983, "Standard for Software Configuration Management Plans."
[10] IEEE Std 1042-1987, "Guide to Software Configuration Management."
[11] IEEE Std 1012-1992, "Standard for Software Verification and Validation Plans."
[12] IEEE Std 1228-1994, "Standard for Software Safety Plans."
[13] Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, 1997.
[14] IEEE Std 830-1984, "Guide for Software Requirements Specifications."
[15] IEEE Std 1016-1987, "Recommended Practice for Software Design Descriptions."
[16] IEEE Std 1016.1-1993, "Guide to Software Design Descriptions."
[17] Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, 1997.
[18] IEEE Std 829-1983, "Standard for Software Test Documentation."
[19] IEEE Std 1008-1987, "Standard for Software Unit Testing."
[20] IEEE Std 1059-1993, "IEEE Guide for Software Verification and Validation."
[21] Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, 1997.
[22] IEEE Std 730-1990, "IEEE Standard for Software Quality Assurance Plans."
[23] IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."
[24] IEEE Std 1028-1988, "Standard for Software Reviews and Audits."
[25] IEEE Std 730.1-1989, "Standard for Software Quality Assurance Plans."
[26] NUREG/CR-5930, "High Integrity Software Standards and Guidelines," NIST, U.S. DoC, September, 1992.
[27] NUREG-0800, "Standard Review Plan," U.S. Nuclear Regulatory Commission, June 1997.

권 기 춘

1980 경북대학교 전자공학 학사
1989 한국과학기술원 전자전산학과 석사
1999 한국과학기술원 전자전산학과 박사
1980~현재 한국원자력연구소 책임연구원
관심분야 : 소프트웨어 확인검증, 인공지능기법 원전 적용, 실시간 시뮬레이션
E-mail:kckwon@kaeri.re.kr

차 경 호

1983 경북대학교 전자공학과 학사
1985 한국과학기술원 전산학과 석사
1985~1990 한국원자력연구소 연구원
1990~현재 한국원자력연구소 선임연구원
관심분야:Real-Time Computing, Wearable Computing, Multi-Agent Systems, Interface Agents
E-mail:khcha@kaeri.re.kr

이 장 수

1983 경북대학교 전자공학 학사
1986 한국과학기술원 전산학과 석사
1991 정보처리기술사.
1994~현재 한국과학기술원 박사과정
1986~현재 한국원자력연구소 책임연구원
관심분야:소프트웨어 안전성분석, 실시간 소프트웨어, 정형기법
E-mail:jslee@kaeri.re.kr

• 정정기사 •

♠ 정보과학회지 제19권 제10호(52~61쪽)의 "기고"로 게재된 원고에 저자의 요청으로 아래의 지원문구를 추가합니다.

"본 연구는 한국학술진흥재단의 2001년도 광대역 무선 접속 시스템 프로토타입 구현 협동연구과제로 수행되었습니다."

• 제19회 정보산업리뷰 심포지움 •

- 일 자 : 2001년 12월 14일(금)
- 장 소 : 전경련회관
- 주 최 : 한국정보과학회
- 문 의 처 : 한국정보과학회 사무국
  Tel. 02-588-9246/7
  E-mail : kiss@kiss.or.kr