안전에 중요한 소프트웨어 개발을 위한 확인 및 검증

이종복*, 서상문, 금종용
한국원자력연구소

Verification and Validation to develop Safety-critical Software

Jong-Bok Lee*, Sang-Moon Suh, Jong-Yong, Keum
Korea Atomic Energy Research Institute

Abstract

Software verification and validation(V&V) is a means to develop high-quality software and assure safety and reliability for software. Also, we can achieve the desired software quality through systematic V&V activities. The software to be applied safety critical system like nuclear power plants is required to setup the V&V methodology that comply with licensing requirements for nuclear power plants and should be performed V&V activities according to it. In this paper, we classified safety-critical, safety-related and non-safety for software according to safety function to be performed and define V&V activities to be applied software grade. Also, we defined V&V activities, procedures and documentation for each phase of software development life cycle and showed techniques and management to perform V&V. Finally, we propose the V&V framework to be applied software development of SMART(System-integrated Modular Advanced ReacTor) MMIS(Man-Machine Interface System) and to comply with domestic licensing requirements.

1. 서론

소프트웨어 개발 생명주기(SDLC : Software Development Life Cycle) 각 단계의 활동에서 생산되는 출력물이 자신의 단계에 설정된 요건을 충족하며 생산되는지 평가하는 과정을 확인(verification)이라 하며, 개발이 완료된 소프트웨어 생산물이 소프트웨어 요건을 만족하는지 평가하는 과정을 검증(validation)이라 한다[1]. 원자력발전소 MMIS는 발전소 공정과 관련 장비들을 감시 및 제어하고, 필요시에 보호기능을 수행함으로써 발전소를 안전하고 신뢰성 있게 운전할 수 있도록 지원한다. 그러한 MMIS의 설계에 소프트웨어 기반의 디지털기술이 사용된 경우, 사용된 하드웨어와 소프트웨어가 주변 환경요인이나 설계 및 프로그래밍 오류에 취약하여 공통유형고장을 일으킬 가능성이 있는 것으로 제기되고 있으며, 그것이 설계 및 규제의 현안으로 제기되고 있다. 그러므로 원자력발전소의 안전계통에 사용되는 소프트웨어는 높은 기능적 신뢰도와 품질을 높일 수 있도록 설계되어야 하고, 또한 원자력산업의 특수성인 시스템의 안전성에 필수적인 요소인 소프트웨어의 신뢰도 보장을 확보하기 위해서는 확인 및 검증(V&V : Verification and Validation) 기술을 정립하고 체계적인 적용이 필수적이다.

본 논문에서는 원자력발전소의 소프트웨어에 적용되는 V&V 관련 인허가 규제요건을 분석하고, 현재 설계를 진행중인 SMART MMIS 소프트웨어 개발에 적용될 V&V를 체계적으로 수행하기 위한 프레임웍을 제시한다.

2. 소프트웨어 V&V 관련 인허가 규제요건

SMART 안전계통 소프트웨어에 대한 V&V에 관련된 규제 체계는 그림 1과 같다. 과학기술부고시 제2001-47호에서는 원자로의 건설 및 운영에 과학기술부고시 제2000-17호로 적용을 고시한 전력산업기술기준(KEPIC)의 원자력품질보증기준(QAP) 또는 이와 동등한 기준을 적용하도록 하고 있다. 과학기술부고시 제 2002-21호에서 안전등급 3의 전기설비에 적용되는 기술기준으로 과학기술부고시 제 2000-17호에 의한 원자로 시설의 기술기준으로 KEPIC EN(원자력전기)과 이에 상응하는 기술기준(IEEE 603, 7-4.3.2)을 제시하고 있다.

KEPIC ENB 6370에서 소프트웨어의 개발 및 수정과정에서 복귀시험을 포함한 확인 및 검증작업이 수행되어야 하고, 이 작업은 KEPIC QAP-2 II.7의 3 및 4항에 따라 수행할 것을 요구하고 있다. 또한 안전계통 소프트웨어 개발은 공식적으로 정의된 수명주기에

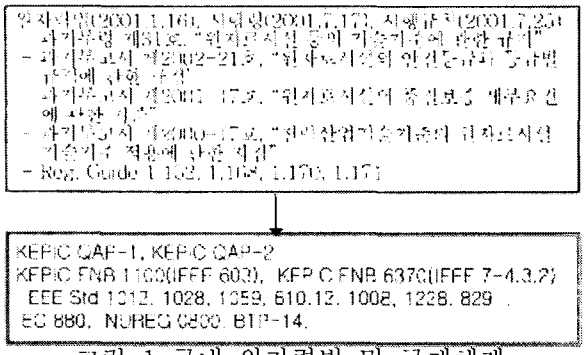

그림 1 국내 원자력법 및 규제체계

따라 이루어져야하고, 그 수명주기에 따른 활동을 정의하고, 생산될 설계문서 또는 제품을 지정하도록 하고 있다. 즉 소프트웨어 개발은 미리 계획되고 정해진 절차에 의해 수행되어야 하고, 확인 및 검증을 통해 안전계통의 요건 및 비정상 상태에 대해 신뢰성있는 처리를 포함하여 각 개발단계에서 규정된 요건이 수행되었는가를 확인하도록 하고 있다. 또한 안전계통 소프트웨어는 설계 및 개발자이외의 자격을 갖춘 개인이나 집단에 의한 독립적인 확인 및 검증작업을 수행하도록 요구하고 있다.

3. MMIS 소프트웨어 V&V 활동

SMART MMIS 소프트웨어 V&V는 소프트웨어 개발 수명주기 개발공정에 따라 수행되는 V&V활동들과 소프트웨어 개발 수명주기 전체에서 V&V활동을 관리하는 V&V 관리가 있다.

SMART MMIS 소프트웨어는 수행되는 안전관련 기능의 중요도에 따라 아래와 같이 세 등급으로 분류한다.

- 안전-필수(SC, Safety-Critical) 소프트웨어
- 안전-관련(SR, Ssafety-Rrelated) 소프트웨어
- 비안전(NS, Non-Safety) 소프트웨어

위와 같은 소프트웨어 등급분류의 목적은 소프트웨어 등급별로 공통유형고장(CMF) 분석요건, 확인 및 검증(V&V)요건과 안전성분석(SA, Safety Analysis)요건을 차등적으로 적용하기 위한 것으로 SMART MMIS 안전-필수 소프트웨어에 한하여 아래와 같은 추가적인 V&V요건이 적용된다.

- 안전성분석과 연계하여 V&V가 수행되어야 한다.
- 소프트웨어 개발팀으로부터 조직, 재정, 책임, 권한, 기술적으로 독립된 검토팀으로부터 독립V&V를 받아야 한다.

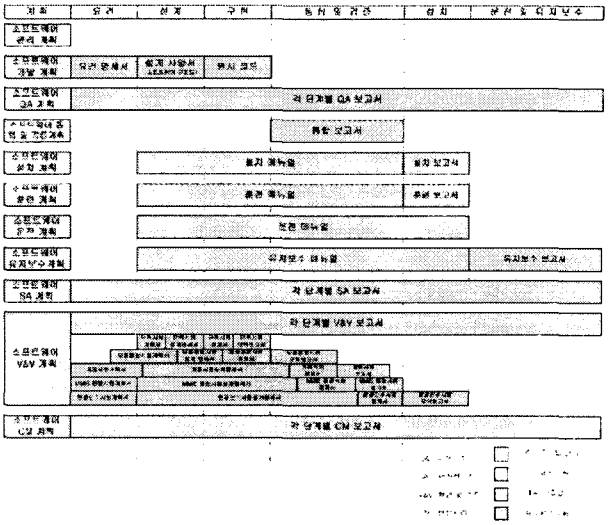

그림 2 MMIS 소프트웨어 개발 수명주기 활동 및 생산물

3.1 소프트웨어 개발 수명주기 공정에 따른 V&V

SMART MMIS 소프트웨어 개발 수명주기는 그림 2와 같이 계획, 요건, 설계, 통합 및 검증, 설치, 운전 및 유지보수로 구성되며, 그 수명주기 공정에 따라 수행되어야 할 V&V활동은 다음과 같다. 이 활동은 표 1과 같이 소프트웨어 등급에 따라 차등 적용된다

1) 계획단계 V&V

소프트웨어 개발 수명주기의 계획단계에서는 소프트웨어 V&V 계획서를 작성한다. 이 계획서는 소프트웨어 품질보증계획서, 소프트웨어 관리계획서와 소프트웨어 개발절차서, SMART MMIS 설계 기준서에서 제시하고 있는 법, 규제, 표준에 따라 작성되며, 소프트웨어 안전성 분석 계획서, 소프트웨어 형상관리 계획서와 서로 양립해야 한다. 이 단계에서 생성된 V&V 계획서는 V&V 관리를 통해 소프트웨어 개발 수명주기 전체에서 지속적으로 수정 및 보완된다.

2) 요건단계 V&V

요건단계에서 V&V활동은 계통별로 소프트웨어 요건명세서(SRS)와 계통 설계문건에 대해 요건추적분석을 수행하고, 소프트웨어 요건에 대한 평가, 소프트웨어 시험 문서 작성 및 평가와 요건단계 소프트웨어 필수성, 위해도,

위험성 분석을 수행한다.

3) 설계단계 V&V

설계단계에서 설계결과물에 대한 V&V활동은 요건 추적 분석, 소프트웨어 설계 평가, 소프트웨어 시험 문서 작성 및 평가와 설계단계 소프트웨어 필수성, 위해요소, 위험성 분석을 수행한다.

확인 및 검증(V&V) 방법	소프트웨어 안전등급			수행단계
	안전-필수	안전-관련	비안전	
소프트웨어 확인 및 검증계획 (SVVP) 수립 및 이행	○	○	○	계획
소프트웨어 요구사항 검토 및 분석	○	○	○	요건
정형적(formal) 요건 및 설계방법의 사용	△	-	-	요건, 설계
정형적(formal) 요건 및 설계검토	△	-	-	요건, 설계
소프트웨어 설계평가	○	○	△	설계
정형적(formal) 언어의 사용	△	-	-	설계, 구현
원시코드 및 원시코드 문서 평가	○	△	△	구현
요건추적 분석	○	△	△	요건, 설계, 구현, 통합/검증
필수성 분석	○	△	-	요건, 설계, 구현
위험요소 및 리스크 분석	○	△	-	요건, 설계, 구현, 통합/검증, 설치, 운전/유지보수
인터페이스 분석	○	○	-	요건, 설계, 구현
고장유형 및 영향분석	○	△	-	설계, 구현
알고리즘 분석	△	-	-	요건, 설계, 구현
데이터베이스 분석	○	△	-	요건, 설계, 구현
통합문서 평가	○	○	○	통합/검증
크기 및 타이밍 분석	○	△	△	요건, 설계, 구현, 통합/검증
제어 및 데이터 흐름분석	○	△	△	요건, 설계, 구현
시스템 확인 및 검증 시험계획 수립	○	○	△	요건, 설계, 구현, 통합/검증
구조 시험	○	○	△	구현, 통합/검증
기능 시험	○	○	○	구현, 통합/검증, 설치
통계 시험	△	-	-	구현, 통합/검증
응력 시험	○	△	△	구현, 통합/검증, 설치
회귀 시험	○	○	△	구현, 통합/검증, 설치
검증 시험	○	○	△	구현, 통합/검증, 설치

범례: ○(요구사항), △(권고사항), —(해당사항 없음)

표 1 MMIS 소프트웨어 등급별 적용되는 V&V항목

4) 구현단계 V&V

구현단계에서 V&V활동은 원시 코드 요건 추적 분석, 원시코드 및 원시코드 문서 평가, 소프트웨어 시험 문건 작성 및 평가, 구현단계 소프트웨어 필수성, 위해도, 위험성 분석을 수행한다.

5) 통합 및 검증단계 V&V

통합 및 검증단계에서 V&V활동은 통합문서 평가, 소프트웨어 시험 문건 작성 및 평가, 통합 및 검증단계 소프트웨어 위험요소 및 위험성 분석을 수행한다.

6) 설치단계 V&V

설치단계에서의 V&V활동은 계통별 소프트웨어 설치 형상감사와 정확한 소프트웨어가 설치되었는지를 확인하는 소프트웨어 설치 형상감사와 현장인수시험을 수행한다. 소프트웨어 시험 문건 작성 및 평가, 설치단계 소프트웨어 위험요소, 위험성 분석을 수행하고 V&V 최종 요약보고서를 작성한다.

7) 운전 및 유지보수단계 V&V

운전 및 유지보수단계의 V&V활동은 실제로 소프트웨어를 운전하면서 필요한 개선이나 발생된 문제점 등을 평가하고 수정하는 활동으로 운전 중 새로이 발생된 제약조건 평가, 운전절차 평가, 소프트웨어 변경 평가, 위해요소 및 위험성 분석을 수행하며, 이것은 유지보수 계획에 따른다.

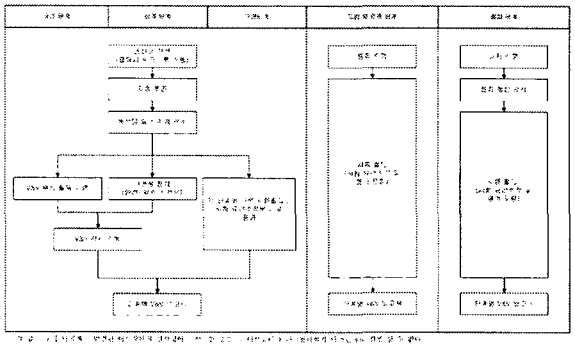

그림 3 소프트웨어 개발생명주기에 따른 V&V 절차

3.2 MMIS 소프트웨어 V&V 절차

SMART MMIS 소프트웨어는 소프트웨어 개발 수명주기 공정에 따라 V&V를 수행하게 된다. 또한 소프트웨어 개발 수명주기 공정에 따라 이루어지는 V&V활동을 수행하는 중에 발생한 이상상태는 이상상태 보고서로서 작성되며, 그 이상상태의 심각성이 '상'이라면 그 이상상태가 해결되기 까지는 다음 단계로 넘어갈 수 없다. 요건, 설계, 구현단계에서 V&V 절차는 그림 3과 같다. 생산물 작성 중에 필요에 따라 워크스루를 수행한다. 워크스루는 생산물에 대한 최종 초안이 완성되면, 개발자는 요건 추적 분석을 하여 요건 추적 매트릭스를 작성하고, 그 결과를 V&V업무보고서로서 작성한다. 요건 추적 분석이 완료되면, 이 요건 추적 분석 자료와 생산물은 각종 V&V 분석 및 시험, 그리고 안전성 분석의 입력으로서 사용된다. 각 분석은 안전-필수, 안전-관련 및

비안전 소프트웨어에 대해 차등적으로 이루어지며, 안전성 분석은 안전-필수 소프트웨어에 한해서 안전분석계획서에 따라 이루어진다. V&V 분석 업무와 안전성 분석 업무의 결과는 검사를 위한 자료로서 사용지고, 검사절차를 수행한다. 시험활동은 각 단계의 시험문서와 SMART MMIS 시험 지침서를 참조하고, 시험문서에 대한 V&V를 수행한다. 모든 V&V검사가 수행되고 시험관련 업무가 완료되었다면 그것은 V&V보고서로서 작성한다.

통합 및 검증단계에서는 통합 및 통합시험이 주된 활동이다. 대부분의 V&V활동이 시험문서를 작성하고 시험을 수행하며, 그에 대해서 요건 추적 분석을 수행하고, 평가를 수행한다.

설치단계에서는 소프트웨어 설치계획에 따라 설치를 수행하고, 형상 관리 업무와 협조하여 설치 형상 감사를 수행한다. 이 설치 형상 감사를 통해 설치된 소프트웨어의 정확함을 판단한다. 형상감사가 완료되었다면, 안전성 분석 계획에 따라 안전성 분석을 수행하며, 소프트웨어 인수시험을 수행하고 보고서를 작성하고, 보고서에 대해서 평가한다.

3.3 문서화

1) V&V계획서

소프트웨어 개발책임자는 아래 사항을 포함하는 V&V계획을 수립하여 그에 따라 V&V업무를 수행하여야 한다.

- SDLC 각 단계별로 수행할 V&V항목
- SDLC 각 단계별로 확인할 검사목록 작성계획
- 시험문서 작성 및 수행 계획
- 이상상태 시정조치 결과추적
- V&V결과에 대한 관리 및 보고서 작성계획

2) V&V 업무보고

V&V 업무보고는 검토자가 수시로 수행하는 V&V 수행결과를 개발책임자에게 보고한다. 그러한 V&V활동으로는 V&V를 위한 분석업무(인터페이스 분석, 데이터 흐름 분석, 제어 흐름 분석 등)와 워크스루 등 이다.

3) 이상상태보고서

V&V활동 과정 중에 이상상태(anomaly)가 예상치 못한 상황에서 발생하거나 발견될 수 있다. 이 경우 이상상태의 심각성이 아래와 같이 구분되어 이상상태보고서가 작성되어야 한다.

- 상 : 시정되지 않으면 치명적인 결과를 야기하므로 즉시 시정되어야 하는 이상상태.
- 하 : 사소한 이상상태이거나, 시정되지 않는다 하여도 치명적인 결과를 야기하지 않는 이상상태.

이상상태보고서에는 이상상태 발생시간, 상황, 관련 하드웨어 또는 소프트웨어 요소, 발생빈도, 소프트웨어 개발 수명주기 단계 등이 명시된다. 개발책임자는 이상상태보고서를 분석한 후 개발자에게 전달하여 개발자로 하여금 이상상태가 해결될 수 있도록 한다. 개발책임자는 이상상태의 시정이 완료되었는지 추적 및 기록하여야 한다.

4) V&V보고서

SDLC의 각 단계가 종료되기 전에 그 단계에서 수행한 모든 V&V활동이 종합적으로 정리된 V&V보고서가 작성된다. V&V보고서는 수행된 V&V활동을 요약하고, 그 수행 과정 중에 발견된 이상상태와 그에 대한 조치 결과가 요약되어야 한다.

3.4 V&V 관리

V&V관리는 소프트웨어 개발 수명주기 공정 전체에 걸쳐 수행되는 활동으로, V&V활동을 검토하고, 소프트웨어 확인 및 검증 계획서를 개정하며, 품질보증이나 형상관리와 같은 다른 지원활동과 연계하여 수행한다.

1) V&V 계획서 작성 및 수정

소프트웨어 개발 수명주기의 계획단계에서는 V&V 계획서를 작성한다. 이 계획서는 소프트웨어 개발 책임자가 작성하게 되며, 소프트웨어 개발 수명주기 단계를 거치면서 지속적으로 수정 및 보완되어야 한다. 이러한 업무는 형상관리에 따라 정해진 절차를 통해 이루어 진다. 예를 들면, 소프트웨어 확인 및 검증 계획서 및 절차서의 개정의 필요성이 있으면 소프트웨어 형상통제위원회(CCB)가 개최되고 이에 따라 변경이 결정되고, 형상 저장소에서 Check-Out을 한 다음, 변경을 수행하고, 다시 변경내용을 검토하여 Check-In을 수행함으로서 변경이 완료된다.

2) V&V 관리 및 기술 검토

V&V 관리 검토는 V&V 활동에 대한 노력, 기술적 성과, 자원의 사용, 장래의 계획, 위기

관리의 주기적인 검토를 실시하는 것을 의미한다. 이 관리 검토에서는 각 수명 주기 단계의 작업과 V&V 보고서를 검토하고, 개발 수명주기의 다음단계 활동을 진행할 것인가를 결정한다. V&V 보고서를 검토할 때 아래의 사항을 고려한다.

- 보고서가 기술적으로 정확한가?
- 보고서가 적절하게 작성되었는가?
  - 기술적 문제만으로 제한하여 작성하였는가?
  - 업무 방향을 제한하고 있는가?
  - 명확하게 작성되었는가?
  - 성공적인 개발이 되도록 지원하고 있는가?
- 관리적 차원에서의 의사결정을 할 수 있도록 효과적으로 지원하는가?
- 이상상태가 명확하게 식별되었으며, 그 수준을 구별하는가?
- 이상상태 해결의 접근 방법을 제안하는가?

소프트웨어 요구사항 검토, 주요 설계 검토와 같은 관리와 기술적인 검토를 하기 위해 공식 검토 회의를 수행한다.

3) 기준선 변경 평가

소프트웨어 확인 및 검증을 통한 소프트웨어의 변경과 그에 따른 기준선 변경은 소프트웨어 형상관리에서 중요하므로 V&V 통제절차, 품질보증절차 및 형상관리절차와 연계하여 수행한다.

3.5 V&V 기법

SMART MMIS 소프트웨어 V&V 활동을 수행하는 데에는 여러 가지 방법을 사용한다. 그 중 검토기법에는 검사, 워크스루를 사용한다. 분석기법으로는 알고리즘 분석, 제어 흐름 분석, 데이터베이스 분석, 데이터 흐름 분석, 인터페이스 분석, 크기 및 타이밍 분석, 회귀분석 및 시험, 모사(simulation) 분석, 요건 추적 분석 등이 있으며, 소프트웨어 개발 수명주기에 따라 이루어져야 하는 분석활동은 표 1과 같다. 시험 기법에는 구조시험, 기능시험, 성능시험, 인터페이스시험, 부하시험, 통계시험, 검증시험 등이 있다. 안전성 분석 기법으로는 소프트웨어 고장 모드, 영향 및 필수 분석, 소프트웨어 고장수목 분석, 필수성 분석, 소프트웨어 위험요소 분석, 위험도 분석 등이 있다. 이것은 V&V와 밀접한 관계를 가지고 있으며 안전성 분석에서 수행하게 된다.

SMART MMIS 소프트웨어 시험은 계통별 단위시험, 계통별 기능시험, 계통별 계통시험, MMIS 통합시험, 계통별 현장인수시험, MMIS 시운전시험으로 구분한다. 원자력규제기관에서 제시하는 V&V활동으로서 수행되어야 하는 시험기법으로서 표 1에 나타난 바와 같이 구조적 시험, 기능적 시험, 통계적 시험, 응력(stress) 시험, 검증시험, 회귀시험이 있다.

통계적 시험은 원자력규제기관에서 권고하는 시험이므로 SMART MMIS 소프트웨어에 대해서는 수행하지 않는다. 소프트웨어 개발책임자는 SDLC의 각 단계에서 생산되어야 하는 시험문서 작성자를 지정해야 한다. 소프트웨어를 개발한 담당자가 자신의 소프트웨어를 시험하지 않는 것이 원칙이다. SMART MMIS 소프트웨어 등급별로 수행되는 시험의 강도와 기법이 달라질 수 있다.

3.6 안전성분석과 V&V

소프트웨어 안전성분석(SA, Safety Analysis)은 SMART MMIS 안전-필수 소프트웨어에만 해당된다. SMART MMIS 안전계통의 안전기능을 무효화시킬 가능성이 있는 비정상적 조건 및 사건(ACE, Anomaly Condition and Event)을 식별하고 고장을 유발할 수 있는 소프트웨어 결함 및 위해요소를 안전성 관점에서 최대한 분석하는 것이 안전-필수 소프트웨어에 대한 안전성분석이다. 안전성분석을 통해 도출된 비정상적 조건 및 사건과 결함 및 위해요소는 안전-필수 소프트웨어의 V&V활동에서 확인할 검사목록(Checklist)을 작성하기 위한 입력으로써 활용된다. 그림 3에 나타난 바와 같이 안전-필수 소프트웨어에 대한 안전성분석은 소프트웨어 개발수명주기 모든 단계에서 수행된다. 소프트웨어 개발책임자는 소프트웨어 안전성계획을 수립하고 안전성분석을 수행할 안전성분석가를 지정하여야 한다.

안전성분석을 수행하는 안전성분석가는 비정상적 조건 및 사건 식별과 결함 및 위해요소를 도출하고 안전-필수 소프트웨어에의 V&V활동을 위한 검사목록을 작성하여 안전-필수 소프트웨어 V&V활동의 입력으로 제공한다. 안전-필수 소프트웨어에 대한 안전성분석을 완료한 안전성분석가는 소프트웨어 개발수명주기 각 단계별 V&V보고서를 분석하여 최종적으로 안전-필수 소프트웨어에 비정상적 조건 및 사건과 결함 및 위해요소가 존재하지 않음을 보여주는 각 단계별 안전성분석보고서를 작성한다.

비정상적 조건 및 사건(ACE)을 식별하기

위한 소프트웨어 안전성분석 방법으로는 KEPIC ENB 6370에서 제시하는 소프트웨어 고장수목분석(SFTA, Software Fault Tree Analysis), 소프트웨어 고장유형 및 영향분석 (SFMEA, Software Failure Mode and Event analysis) 방법을 따른다.

4. 결론

원자력분야의 안전 시스템이 소프트웨어 기반의 디지털시스템으로 이루어지는 경우에 하드웨어를 사용하는 것보다 오류의 발견이 어려워, 디지털 시스템의 적용에 많은 어려움이 있어왔다. 이러한 안전성 및 신뢰성을 확보하는 문제가 중요한 현안으로 제기되고 있으며, 이러한 문제를 해결하기 위해 소프트웨어 V&V에 관한 많은 연구가 진행되어왔다.

본 논문에서는 현재 설계를 진행중인 SMART MMIS 소프트웨어를 개발하기 위해 적용되는 V&V 규제요건을 분석하고, 소프트웨어 개발생명주기에 따른 V&V를 체계적으로 수행하기 위한 프레임웍을 제시하였다.

향후 과제로는 적용하기 위한 세부지침을 개발하고, 적용에 따른 문제점 보완 및 소프트웨어 개발 방법론과 연계하여 궁극적으로 체계화된 원전 소프트웨어 개발 방법론으로 발전시키는 일이다.

참고문헌

[1] IEEE Std 1012, "IEEE Standard for Software Verification and Validation", IEEE, 1998.

[2] KEPIC QAP-2 II.7, "원자로시설용 전산 소프트웨어의 품질보증요건", 대한전기협회, 2000.

[3] 이장수 , "원전계측제어 고신뢰도 소프트웨어 확인/검증기술현황", Journal of Korean Nuclear Society, 1994

[4] Safety-critical 소프트웨어 V&V 지침서 개발 방법론

[5] EEE Std 1059, "IEEE Guide for Software Verification and Validation Plans", IEEE, 1993.

[6] 과기부령 제31호, "원자로시설 등의 기술기준에 관한 규칙", 2001.

[7] 과기부고시 제2002-21호, "원자로시설의 안전등급과 등급별 규격에 관한 규정", 2002.

[8] KEPIC ENB 6370, "안전계통 디지털 컴퓨터", 대한전기협회, 2000.