원전 MMIS 소프트웨어 응용을 위한 개발 지침에 관한 연구

이종복*, 서용석*, 서상문*, 박근옥*
*한국원자력연구소
e-mail:jblee1@kaeri.re.kr

A Development Guideline for MMIS Software Applications in Nuclear Power Plants

Jong-Bok Lee*, Yong-Suk Suh*, Sang-Moon Suh*, Geun-Ok Park*
*Korea Atomic Energy Research Institute

요 약

원자력 산업계에서는 원전 MMIS(Man-Machine Interface System)의 디지털 기술 적용을 위해 많은 노력을 기울이고 있고, 디지털 MMIS의 핵심기반기술인 고 신뢰도 소프트웨어 개발 방법론이 확립되지 못하여 소프트웨어 공통모드고장 문제, 정량적인 소프트웨어 신뢰도 보장 문제 등이 현안으로 제기되고 있다. 이에 따라 원자력 산업의 특수성인 안전성 확보에 필요한 개발기준과 규제방법 정립에 많은 연구가 수행되고 있다. 또한 이와 같이 원전 MMIS의 디지털화를 성공하기 위해서는 소프트웨어의 고 신뢰도 확보가 관건이며, 고 신뢰도와 품질을 확보하기 위한 소프트웨어 개발 지침의 정립이 요구되고 있다. 본 논문에서는 원전 소프트웨어 개발에 적용되는 규제 요건을 분석하고, SMART(System-integrated Modular Advanced ReacTor) MMIS 소프트웨어 개발에 적용될 소프트웨어 개발 지침을 제시한다.

1. 서론

원자력 산업계에서 디지털 기술의 적용은 다른 응용분야와 마찬가지로 요구되는 시대적 변화라 할 수 있다. 일반적으로 디지털 시스템은 아날로그 시스템에 비하여 처리능력이 월등하고, 적은 표류현상, 정확성, 융통성의 향상, 그리고 각종 자원들을 공유할 수 있어서 자원의 이용도를 높일 수 있다는 장점이 있다. 그러나 디지털 시스템은 주변환경(예, 온도, 습도, 방사선, 전자파 등)에 민감하고 설계 및 프로그래밍 오류에 취약하여 공통유형고장(common mode failure) 가능성이 큰 것으로 지적되고 있으며, 정량적인 소프트웨어 신뢰도 보장 문제 등이 현안으로 제기되고 있다. 이에 따라 원자력발전의 첨단 디지털 계측제어 시스템에 대한 안전성, 신뢰성을 보장하고 품질을 평가할 수 있는 소프트웨어 개발 방법론과 확인 및 검증 방법론을 제공하는 것이 필요하다. 현재 까지 원전의 소프트웨어를 개발하기 위한 개발 방법론에 대한 많은 연구가 있어 왔으나, 원전 소프트웨어 개발 전 단계/범위에 걸쳐 적용한 사례는 없었다. 이에 현재 설계를 진행중인 SMART MMIS 소프트웨어 개발에 적용될 소프트웨어 개발 지침을 제안한다.

본 논문에서는 제 2장에서 SMART MMIS 소프트웨어 개발에 적용되는 규제요건을 살펴보고, 3장에서 SMART MMIS 개발에 적용될 소프트웨어 개발 지침을 제시하고, 4장에서 결론 및 향후 연구방향을 제시한다.

2. 관련 연구 및 소프트웨어 인허가 규제요건

2.1 안전 요건

미국 원자력 법(10 CFR 50), NUREG-0800 7장, BTP(Branch Technical Position)-14, IEEE Std 603, IEEE Std 7-4.3.2은 안전관련 요건은 디지털 안전계통 설계의 안전기준으로도 사용된다. 안전성 소프트웨어의 인허가를 위해서는 안전심사항목중 설계지침의 적합성, 소프트웨어 생명주기 공정, 심층방어 및 다양성, 확인 및 검증, 형상관리, 소프트웨어 개발과 하드웨어/소프트웨어 통합, 기성 소프트웨어, 소프트웨어 도구에 대한 기준과 대책 마련이 요구된다. 디

지털 MMIS의 소프트웨어는 공통모드 고장의 발생 가능성 때문에 안전 현안으로 제기되고 있으며, 소프트웨어에 의한 공통모드 고장 문제를 해결하기 위해 심층방어(Defense-in-Depth) 및 다양성(Diversity) 설계를 적용하도록 하고 있다. 안전계통 소프트웨어의 신뢰도 분석에 IEEE Std 352를 적용하기 위해서는 척도의 표준화가 필요하며, NUREG/CR-5930, "고-건전성(High-integrity) 소프트웨어에 대한 표준지침"은 기존 지침서들의 문제점을 분석하여 표준화 지침서가 가져야 할 기준을 제시하고 있다. 그리고 소프트웨어의 안전성을 보장하는 방법으로 소프트웨어 위험도 분석(Software Risk Analysis:SRA)을 요구하며, 그 기준도 함께 제시하고 있다. IEC 60880-200, (Part 2) 는 공통원인 고장(Common Cause Failure) 대책, 소프트웨어 도구, 그리고 기성(pre-developed) 소프트웨어의 사용에 따른 안전요건을 규정한다. 또한 미국 원자력 규제위원회는 ITAAC(Inspection, Tests, Analyses and Acceptance Criteria) 항목들이 소프트웨어 구조 및 품질과 같은 설계현안(Design issues)을 반영함으로서 안전규제 요건을 만족하도록 요구한다.

2.2 품질 및 개발공정요건

IEEE Std 7-4.3.2에서 5절의 품질에서 안전계통 디지털 컴퓨터의 소프트웨어 개발, 기존 상용컴퓨터의 인증, 소프트웨어 도구, 확인 및 검증, 소프트웨어 형상관리에 대한 기준을 규정한다. 그리고 신뢰도 목표 달성의 증명은 사용된 소프트웨어도 포함되도록 규정한다. 한편 IEC 가 표준으로 채택한 IEC 60880에서도 안전계통의 컴퓨터 소프트웨어에 대한 기준을 제시한다. IEC-60880-1986은 안전계통의 소프트웨어 개발에 대한 일반 및 품질보증, 요구명세, 설계 및 코딩, 검증, 하드웨어/소프트웨어 통합, 컴퓨터 시스템 확인, 유지보수 변경, 그리고 운영에 대한 요건을 규정하고 있다.

2.3 SMART MMIS 소프트웨어 개발 규제 체계

원자력 규제기관에서 요구하는 고품질의 SMART MMIS 소프트웨어 개발을 위해 기본적으로 참조하는 국내표준은 전력산업기술기준인 KEPIC QAP와 KEPIC ENB 6370, ENB 1100 이다. 이들은 각각 미국 원자력품질보증규격인 ASME NQA와 IEEE Std 7-4.3.2, 603 표준에 상응하는 국내표준이다. SMART MMIS 소프트웨어 개발을 위해 적용되는 국내 원자력법, 규제, 표준체계는 그림 1과 같다. 원자력법, 시행령, 시행규칙, 경수로형 원전 안전심사지침, KEPIC ENB 6370, ENB 1100의 안전관련 요건은 안전기능을 수행하는 계측제어계통 소프트웨어 설계의 안전기준으로도 사용된다. 안전기능을 수행하는 소프트웨어의 인허가를 위해서는 KEPIC ENB 6370의 품질요건을 따라야 한다. 소프트웨어 개발은 소프트웨어 품질보증계획에 따라 개발 또는 수정하여야 하고, 품질보증계획에는 컴퓨터가 동작할 때 컴퓨터에 내재되어있는 모든 프로그램을 언급하도록 요구하고 있다. 소프트웨어 개발에 사용되는 도구는 개발과정에서 식별되고, 소프트웨어 도구를 이용하여 만들어진 소프트웨어가 소프트웨어 도구에 의해 야기되는 결함을 검출하는 확인 및 검증작업을 수행하여야 한다.

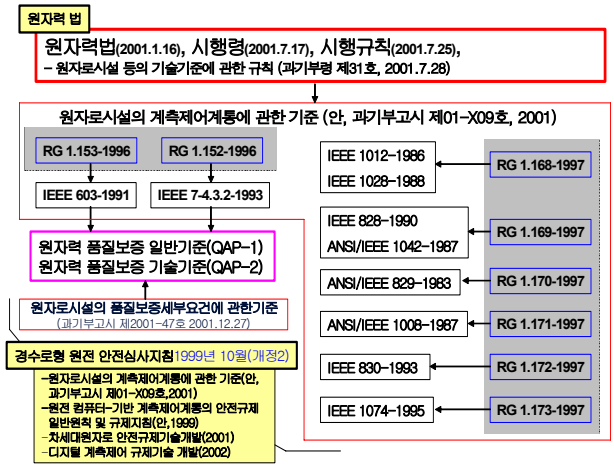

그림 1 국내 원자력 법 및 규제체계

RG	제 목
1.168	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

↓인준

IEEE Std
IEEE Std 610.12-1990, IEEE Std730-1998, IEEE Std730.1-1995, IEEE Std 828-1998, IEEE Std 829-1998, IEEE Std 830-1998, IEEE Std 982.1-1988, IEEE Std 982.2-1988, IEEE Std 1008-1993, IEEE Std 1012-1986, IEEE Std 1016-1987, IEEE Std 1016.1-1993, IEEE Std 1028-1997, IEEE Std 1042-1993, IEEE Std 1044-1993, IEEE Std 1044.1-1995, IEEE Std 1045-1992, IEEE Std 1058-1998, IEEE Std 1059-1993, IEEE Std 1061-1998, IEEE Std 1062-1998, IEEE Std 1063-1987, IEEE Std 1074-1997, IEEE Std 1074.1-1995, IEEE Std 1209-1992, IEEE Std 1219-1998, IEEE Std 1220-1998, IEEE Std 1228-1994, IEEE Std 1233-1998, IEEE Std 1298-1992, IEEE Std 1348-1995, IEEE Std 1362-1998, IEEE Std 1420-1995, IEEE Std 1420.1a-1995,

그림 2 SMART MMIS 소프트웨어 개발에 적용될 IEEE 표준

소프트웨어 개발 및 수정과정에서 복귀시험(regression testing)을 포함한 확인 및 검증작업이 수행되어야 하며, 이를 통해 안전계통의 요건 및 비정상 상태의 신뢰성 있는 처리를 확인하고, 소프트웨어에 대한 형상관리를 하도록 요구하고 있다. 또한 기성 소프트웨어에 대한 승인 기준과 대책이 요구된다. 디지털 계측제어계통의 소프트웨어는 공통모드 고장의 발생 가능성 때문에 안전 현안으로 제기되고 있으며, 이에 따른 공통원인 고장(Common Cause Failure) 대책이 요구된다. 안전계통 소프트웨어의 신뢰도 분석과 소프트웨어의 안전성을 보장하는 방법으로 소프트웨어 위험도 분석(Software Risk Analysis:SRA)이 요구된다.

현재 국내 표준단체에서 제시하는 소프트웨어 표

준들은 원자력 규제기관에 의해 인준되어 있지 않은 실정이다. 반면에 경수로형 원전 안전심사지침은 원자력 플랜트 안전계통에 동작하는 소프트웨어 개발에 적용할 수 있는 표준으로서 그림 2와 같은 IEEE 소프트웨어 표준을 언급함에 따라 SMART MMIS 소프트웨어 개발 시 이를 준용한다.

3. 원전 소프트웨어 개발 지침

3.1 소프트웨어 등급분류

SMART MMIS 소프트웨어의 등급은 안전관련 기능의 중요도에 따라 아래와 같이 세 등급으로 분류한다.

- 안전-필수(SC, Safety-Critical) 소프트웨어
- 안전-관련(SR, Safety-Related) 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 것이다.

1) 안전-필수 소프트웨어

SMART 안전-필수 소프트웨어는 KEPIC QAP-1, KEPIC QAP-2 II.7, KEPIC ENB 6370에서 요구하는 가장 엄격한 소프트웨어 품질보증요건 및 설계기준을 적용하며 설계되는 소프트웨어이다. 안전-필수 소프트웨어는 공통유형고장 방지를 위한 소프트웨어적 심층방어(Defence in Depth) 및 다양성(diversity)분석이 수행되고 반영되어야 한다. 안전-필수 소프트웨어는 안전계통에 미치는 위험요소 및 위험도 분석들을 수행하여 공통유형고장 발생 가능성을 최소화해야 한다. 안전-필수 소프트웨어는 SDLC 전체에 걸쳐 안전성분석이 수행되며 이에 대한 결과 보고서가 작성해야 한다. 안전-필수 소프트웨어 산출물에 대해 두 단계의 V&V활동이 이루어진다. 첫 번째 단계는 소프트웨어 개발팀 내에서 구현자가 아닌 다른 개발자에 의해 V&V되는 것이다. 두 번째 단계는 첫 번째 단계에서 V&V활동을 수행한 소프트웨어 산출물(product)이 소프트웨어 개발팀과는 기술, 조직, 책임, 권한 및 재정적으로 독립된 검토팀에 의해 독립적인 V&V활동이 수행된다.

2) 안전-관련 소프트웨어

SMART MMIS 안전-관련 소프트웨어는 안전-필수 소프트웨어보다는 완화된 품질보증요건 및 기술기준을 적용하며 설계되는 소프트웨어이다. 안전-관련 소프트웨어에 대한 공통유형고장 방지를 위한 분석 및 안전성분석은 요구되지 않지만, 만약 그 소프트웨어가 안전-필수 소프트웨어에 영향을 미칠 수 있는 위험요소가 내재되어 있다면 이를 찾아서 명시하고 시정한 결과를 문서화해야 한다.

3) 비안전 소프트웨어

SMART MMIS 비안전 소프트웨어는 원자력 플랜트 안전운전에 적합한 수준의 품질보증요건 및 기술기준을 적용하며 설계되는 소프트웨어 이다. 비안전 소프트웨어에 대한 공통유형고장 방지를 위한 분석 및 안전성분석은 요구되지 않지만, 만약 비안전 소프트웨어가 안전-필수 또는 안전-관련 소프트웨어와 함께 동일한 컴퓨터-기반시스템에서 실행된다면 그 소프트웨어가 다른 상위 소프트웨어들에게 미칠 수 있는 위험요소를 분석하고 필요하다면 적절한 보완조치(예, 격리)를 하여야 한다.

3.2 소프트웨어 개발수명주기 및 산출물

SMART MMIS 소프트웨어 개발에 적용되는 소프트웨어 개발수명주기(SDLC)는 KEPIC QAP-2 II.7 및 IEEE Std 1074을 기반으로 그림 3과 같이 7단계로 수립하며 SDLC 각 단계별 활동 및 산출물은 그림 3과 같이 제시한다. 이는 원자력 규제기관의 경수로형 원전 안전심사지침에서 언급하는 SDLC 수립에 대한 심사방향을 만족하며 SMART MMIS 소프트웨어 개발에 적용한다.

SMART MMIS 계통의 기능, 성능, 요건 설계 등이 status 개념을 적용하여 개발되며, 소프트웨어 개발에 대해서도 status 개념이 적용되어 수행된다. Status-1 설계내용에 대해서 그림 2의 SDLC는 폭포수(waterfall) 모델을 적용하여 수행하는 것을 원칙으로 한다. 그러나 status-3 및 status-2 설계내용에 대해서는 점진적 증가형(increment)과 반복형(iteration) 모델로 융통성 있게 수행될 수 있으며, SMART MMIS 계통의 기능, 성능, 요건 확인을 위해 프로토타입 개발이 전략적으로 채택된다면 프로토타이핑 모델이 적용될 수 있다.

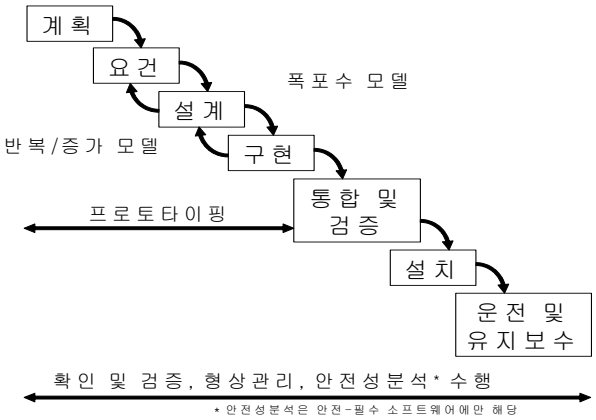

그림 3 SMART MMIS 소프트웨어 개발발수명주기 모델

SMART MMIS 소프트웨어 개발수명주기에서는 단계별 시험과 관련된 활동을 계통별 단위시험, 계통별 모듈통합시험, 계통별 계통시험, MMIS 통합시험, 계통별 현장인수시험, MMIS 시운전시험으로 구분한다. 그림 3의 SDLC 각 단계마다 형상관리보고서, 확인 및 검증(V&V: Verification and Validation) 보고서, 소프트웨어 안전성분석보고서를 생산한다.

3.3 소프트웨어 개발절차

SMART MMIS의 소프트웨어 개발은 규범적인

지침과 절차를 먼저 작성하고 그러한 지침과 절차에 의거하여 소프트웨어 개발을 수행한다. 소프트웨어 개발팀은 각 단계에서 요구되는 산출물을 생산하고 V&V활동을 수행한다.

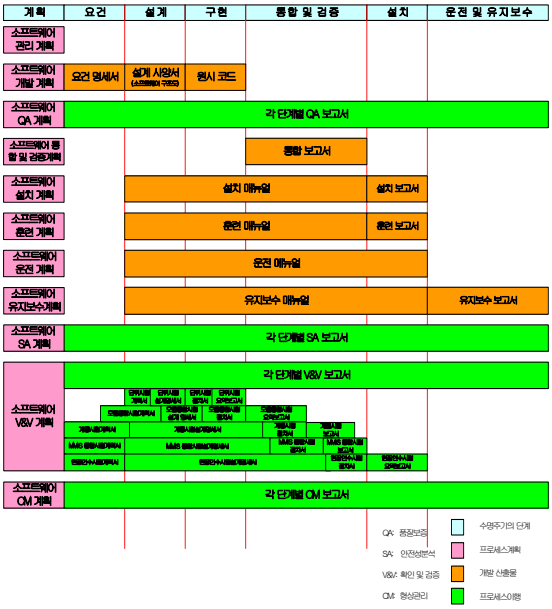

그림 4 SMART MMIS 소프트웨어 개발수명 주기 활동 및 산출물

안전-필수 소프트웨어에 대해 소프트웨어 개발팀은 소프트웨어 안전성관점에서 안전성분석과 V&V활동을 수행한다. 단, 안전-필수 소프트웨어에 대해서는 독립검토팀에 의해 독립적인 확인 및 검증(IV&V)을 받아야 한다.

3.4 소프트웨어 형상관리

SMART MMIS 소프트웨어 형상관리의 목적은 소프트웨어 개발 과정에서 생산되는 산출물에 대한 보관 및 수정 절차를 명확히 설정하여 그러한 절차를 통해 산출물이 보전 및 개정될 수 있도록 하는 것으로 그림 1에 나타난 바와 같이 소프트웨어 형상관리는 SDLC 모든 단계에서 이루어진다. 형상관리는 소프트웨어 개발책임자가 지정한 소프트웨어 개발팀의 형상관리자에 의해 수행되며 형상관리항목을 QA팀과 협의하여 개발이 시작되기 전에 결정하여야 한다. 소프트웨어 개발책임자는 형상관리항목을 관리하고 통제하는 총제적인 업무를 책임진다. QA팀은 소프트웨어 개발책임자의 형상관리활동을 감사한다. 소프트웨어 개발팀의 형상관리자는 소프트웨어 개발책임자의 업무지시에 따라 형상관리상태를 점검 및 확인하고 그 결과를 보고하기 위해 SDLC 각 단계마다 형상관리보고서를 작성하여 개발책임자에게 제출한다.

3.5 소프트웨어 확인 및 검증

SMART MMIS 확인 및 검증 활동은 그림 1에 나타난 바와 같이 소프트웨어 V&V는 소프트웨어 개발수명주기 모든 단계에서 이루어진다. 또한 소프트웨어 V&V를 통해 SMART MMIS 소프트웨어의 품질속성이 확인되어야 한다.

소프트웨어 개발수명주기 각 단계에서 수행되어야 할 V&V항목들을 정의하고, 또한 SMART MMIS 소프트웨어 등급별로 V&V항목들을 구분한다. SMART MMIS의 V&V 방법은 아래와 같이 세 가지 유형으로 구분되며 V&V절차에 따라 수행된다.

- 워크스루(walk-through)
- 검사(inspection)
- 시험(test)

3.6 기성 소프트웨어 사용

SMART MMIS 소프트웨어를 개발하기 위해 필요한 도구는 계통설계요건서 또는 계통설계사양서에서 지정될 수 있다. 소프트웨어 개발팀은 위의 기성 소프트웨어를 사용할 때는 일련의 인정과정(dedication process)에 따라 평가된 후 선정한다. 특히, 안전-필수 소프트웨어 개발 또는 동작에 기성 소프트웨어를 사용하기 위해서는 10CFR21의 요건을 만족하여야 한다. 10CFR21 요건은 원자력 플랜트 안전기능을 수행하는 계통 또는 구성품을 상용 등급(commercial grade)으로 설계 및 구현하고자 할 경우, 그 상용 등급이 요구되는 계통 및 구성품이 안전기능을 수행할 수 있음을 확인할 수 있는 적절한 인정과정을 수행하여야 함을 요구하고 있다.

SMART MMIS 안전-필수 소프트웨어 개발 및 동작에 기성 소프트웨어를 사용하기 위해서는 10CFR21에서 요구하는 인정과정에 의거 기성 소프트웨어를 선정하며, 안전-관련 소프트웨어를 위해서는 권고사항이며, 비안전 소프트웨어 경우에는 설계자 또는 개발자의 소프트웨어 개발지원과 품질향상을 고려하여 선택적으로 적용할 수 있다.

4. 결 론

본 논문에서는 현재 설계를 진행중인 SMART MMIS 소프트웨어와 관련된 규제요건을 분석하고, 원전 소프트웨어 개발에 적용될 소프트웨어 개발 지침을 제안하였다.

향후에는 제시한 개발 지침을 SMART MMIS 소프트웨어 개발에 적용하고, 나타나는 문제점을 보완하여 원전 소프트웨어 개발 방법론을 정립하고, 나아가서 개발도구와 통합된 자동화된 개발환경을 제공하기 위한 지속적인 연구를 수행하여야 할 것이다.

참고문헌

[1] KEPIC QAP-1, “원자력 품질보증계획 일반기준”, 대한전기협회, 2000.
[2] KEPIC ENB 6370, “안전계통 디지털 컴퓨터”, 대한전기협회, 2000.
[3] IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Process", 1997.
[4] “경수로형 원전 안전심사지침”, 개정 2, 한국원자력안전기술원, 1999. 10.
[5] 이장수 , “원전계측제어고신뢰도소프트웨어 확인/검증기술현황”, JKNS, 1994