'99 춘계학술발표회 논문집
한국원자력학회

SMART MMIS를 위한 상용소프트웨어 선정절차 개발
Development of COTS Software Selection Procedure for SMART MMIS

서용석, 장귀숙, 허 섭, 성승환, 이철권
한국원자력연구소

요 약

원자력발전소 안전관련계통에 상용소프트웨어 사용에 대한 고려가 점차 증가되고 있으나 상용소프트웨어 인정방법이 정립되어 있지 않은 실정이다. 디지틀기기 중심의 SMART MMIS 설계를 위해 3단계로 구성된 상용소프트웨어 선정절차를 개발하였다. 단계 1에서는 상용소프트웨어에 대한 조사를 통해 필수특성과 기술기준을 도출한다. 단계 2에서는 선정기준을 설정한다. 단계 3에서는 시험 및 분석을 통해 안전성이 확인된 상용소프트웨어를 선정한다. 본 논문에서 개발한 선정절차는 현재 SMART MMIS 설계과정에 적용되고 있다.

Abstract

Although the use of COTS(commercial off-the-shelf) software in the safety-related systems of nuclear power plants has been considered, a methodology of COTS software dedication is not well established. A three-phase COTS software selection procedure for the design of digitalized SMART MMIS was developed. The critical characteristics and technology criteria of the COTS software are identified through investigating the COTS software in step one. The selection criteria is documented in step two. A COTS software is selected in step three after the safety of the COTS software is assured through testing and analyzing the COTS software. The developed selection procedure is being applied for the design of the SMART MMIS.

1. 서론

기존의 원자력발전소의 안전관련계통에는 10CFR50 App. B의 품질보증요건을 만족한 원

자력등급품목을 사용했으나 GL 89-02에서 지적한 바와 같이 안전관련계통에도 상용등급품목(CGI, commercial grade item)을 사용하려는 추세이다[1]. 이러한 추세는 안전관련계통에 상용등급품목을 사용함으로써 기기단종 해결, 용이한 유지보수, 설계비용 절감 등의 장점을 얻을 수 있기 때문이다. 상용등급품목에 대한 정의는 10CFR21 및 IEEE 7-4.3.2에 기술되어 있으며 상용등급품목을 안전관련계통설계에 사용하기 위해서는 상용등급품목에 대한 인정절차(dedication process)를 수행하여 상용등급품목이 원자력등급품목과 동등한 품질을 만족할 수 있음을 증명하거나 확신을 제시하여야 하며 이것을 상용등급품목의 인정(dedication)이라 한다. 안전관련계통에 사용하는 상용소프트웨어는 상용등급품목의 범주에 속한다. 이것은 상용소프트웨어 역시 상용등급품목과 동일한 인정절차를 통해 품질을 인정해야 함을 의미한다.

상용소프트웨어는 pre-existing 소프트웨어로써 원자력산업에 국한하지 않는 일반적인 분야에 적용할 목적으로 개발된 상용, 연구용, 공개용 소프트웨어를 포함한다. 디지틀시스템 기반의 SMART(System integrated Modular Advanced ReacTor) MMIS(Man Machine Interface System)의 설계기술개발과제를 수행하는 과정에서 상용소프트웨어를 안전관련계통에 사용하기 위한 상용소프트웨어 인정절차의 개발이 요구되었다. 또한 비안전계통에 사용하는 상용소프트웨어에 대해서도 품질보증측면에서 인정절차에 따라 상용소프트웨어를 선정할 필요가 있다. 원전 상용기기 승인 및 평가 방법론[2]이 제시된바 있으나 본 논문은 상용소프트웨어 인정절차의 선결사항인 선정절차를 개발하여 상용소프트웨어를 선정하는 데 목적을 둔다.

본 논문의 구성은 제 2장에서 SMART MMIS 각 계통에서 필요로 하는 소프트웨어의 종류를 기술하며, 제 3장에서 본 논문에서 제시한 3 단계 선정절차에 대해 기술하며, 제 4장에서 각 단계별 선정방법에 대해 기술한다.

2. SMART MMIS를 위한 상용소프트웨어 분류

SMART MMIS의 설계목표는 디지틀시스템 기반의 계통을 설계하는 것이다[3]. 상용소프트웨어를 선정하기 앞서 SMART MMIS의 각 계통에서 디지틀시스템 기반의 계통을 개발하기 위해 필요로 하는 소프트웨어 기능을 조사하고 종류를 파악하여 종류별로 분류할 필요가 있다. 이러한 작업은 산업계에 산재되어 있는 상용소프트웨어를 종류별로 묶어 공통적인 특성을 체계적으로 조사하기 위함이며 기술기준을 체계적으로 도출하기 위함이다. 표 1은 SMART MMIS 각 계통의 안전등급과 계통에서 필요로 하는 소프트웨어 기능을 보여준다.

표 1. SMART MMIS 각 계통의 안전등급과 필요로 하는 소프트웨어 기능

계통	등급	필요한 소프트웨어 기능
정보처리	NS	준경성 실시간 스케쥴링을 지원하는 Unix계열 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, GUI도구를 이용하여 화면설계를 수행하며, 이력데이터저장기능을 지원하는 데이터베이스를 사용하며, 통신망을 통해 타 계통과 연계한다. 가능한 CASE도구를 사용하여 요구분석을 수행한다.
경보/상태 표시	IS	준경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, GUI도구를 이용하여 화면설계를 수행하며, 통신망을 통해 타 계통과 연계한다. 경보시스템 구축을 지원하는 도구를 사용한다.
대형화면	IS	준경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, GUI도구를 이용하여 화면설계를 수행하며, 통신망을 통해 타 계통과 연계한다.
보호/안전제어	S	경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 저급언어를 사용하여 응용프로그램을 개발하며, 통신망을 통해 타 계통과 연계한다.
제어	NS	준경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, 통신망을 통해 타 계통과 연계한다.
소프트 제어기	NS	준경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, GUI도구를 이용하여 화면설계를 수행하며, 통신망을 통해 타 계통과 연계한다.
특정감시	IS	경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, 통신망을 통해 타 계통과 연계한다.
	NS	준경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, 통신망을 통해 타 계통과 연계한다.
계측	S	경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 저급언어를 사용하여 응용프로그램을 개발하며, 통신망을 통해 타 계통과 연계한다.
	NS	준경성 실시간 스케쥴링을 지원하는 마이크로프로세서 계열의 운영체제위에 고급언어를 사용하여 응용프로그램을 개발하며, 통신망을 통해 타 계통과 연계한다.
통신망	S	결정론적 프로토콜을 지원하는 통신방식을 사용한다.
	NS	비결정론적 프로토콜을 지원하는 통신방식을 사용한다.

참고) S : Safety-related, IS : Important to safety, NS : Non-safety, G : Generic

표 1에서 조사한 바와 같이 SMART MMIS에서 필요로 하는 소프트웨어를 기능별로 구분하였을 경우, 운영체제, 프로그래밍 언어, GUI(Graphic User Interface) 도구, 데이터베이스, CASE(Computer-Aided Software Engineering), 통신망과 같이 5가지로 분류하였다.

3. 상용소프트웨어 선정절차

현재 산업계에는 무수히 많은 상용소프트웨어가 생성되며 소멸되고 있다. 그 가운데 사용자요건에 부합되는 상용소프트웨어를 선정하는 작업은 사실상 완벽할 수 없다. SMART MMIS 설계과정에서 상용소프트웨어 선정작업을 얼마나 자세히 수행할 것인가에 대한 결정과 그에 따른 비용과 기간을 예측할 필요가 있으며 설계수행차원에서 위험요소를 최대한 줄일 수 있는 효과적인 선정방법이 제시될 필요가 있다. 이러한 목적하에서 본 논문은 그림 1

에 제시된 바와 같이 3단계 선정방법을 개발하여 SMART MMIS 설계에 적용하고 있다. 상용소프트웨어 선정절차의 단계 1은 상용소프트웨어의 종류를 분류하고 필수특성(critical characteristics)을 파악하며 기술사항을 분류하는 단계이며, 단계 2는 계통에 적용될 규제요건과 단계 1의 결과물을 바탕으로 선정기준을 설정하는 단계이며, 단계 3은 단계 2의 선정기준에 적합한 소프트웨어를 선택하여 기준에 적합한 소프트웨어를 선정하며 특별한 시험 및 분석이 필요로 하는 경우 이를 프로토타입 환경을 통해 수행하는 단계이다. 안전관련계통에 적용할 상용소프트웨어에 대한 확신은 정량적이어야 하며 비안전계통에 대해서는 정성적인 확신도를 산출한다.

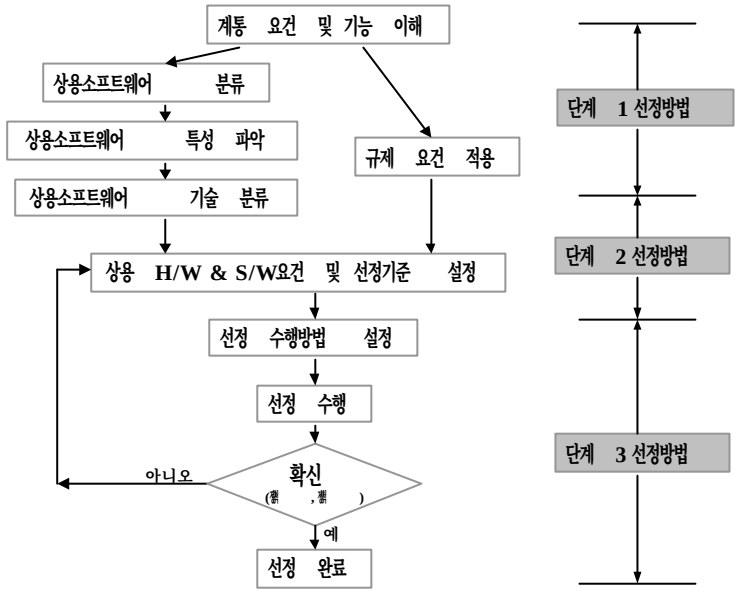

그림 1. 상용소프트웨어 선정절차

그림 1의 선정절차는 EPRI NP-5652[4]의 CGI 인정절차와 KEPIC QAP-1996 추록 6,[5] 일반규격 품목의 승인방법에 기술된 다음과 같은 4가지 방법과 유사하다: (1) 특별시험 또는 (및) 검사, (2) 공급자의 일반규격 실사, (3) 현장 검증, (4) 공급자/품목 성능 기록. EPRI NP-5652의 CGI 인정절차와 유사한 선정절차를 개발한 이유는 소프트웨어의 안전성을 증명할 수 있는 방법론이 현재 정립되어 있지 않기 때문이다. 즉, 상용소프트웨어 자체의 품질보증만으로 그 소프트웨어가 안전하다고 할 수 없다. 안전관련계통에 사용할 상용소프트웨어는 계통시험에 적용하여 계통의 안전성을 확인하는 과정을 통해서 인정될 수 있는 필수특성이 있을 수 있다. 본 논문에서 제시한 선정절차는 시험 및 분석을 요구하는 필수특성을 프로토타이핑을 통해 확인하는 범위까지이다. 이러한 선정절차는 인정절차의 일부분으로써 사용될 수 있을 것이다. 그림 1의 상용소프트웨어 선정절차에서 각 단계별 수행할 내용 및 방법은 제 4장에서 기술한다.

4. 상용소프트웨어 선정방법

상용소프트웨어 선정에 대한 상세요건은 IEEE 7-4.3.2으로부터 출발한다. 본 논문은 제 3장에서 제시한 선정절차가 IEEE 7-4.3.2의 요건을 최대한 반영하면서 현실적인 방법을 제시하고자 한다. 안전관련계통에 사용될 상용소프트웨어의 인정은 최대한 정량적인 평가기준을 통해 이루어져야 하지만 IEEE 7-4.3.2에 기술된 바와 같이 평가깊이는 평가자의 판단에 의해 결정된다[6].

4.1 단계 1 선정방법

단계 1 선정방법에서는 제 2장에서 분류한 상용소프트웨어의 종류를 파악하고 각각의 소프트웨어가 갖고 있는 공통적인 필수특성을 도출한다. 필수특성이 도출되면 그 특성을 구현하기 위한 기술사항이 도출될 수 있으며 안전한 소프트웨어에 대한 기술적 요건이 작성될 수 있다.

안전관련계통에 사용할 상용소프트웨어에 대한 필수특성은 EPRI TR-106439[7]으로부터 출발한다. EPRI TR-106439는 디지틀기기에 대한 필수특성을 물리적 특성, 성능 특성, 종속성 특성과 같이 크게 3가지로 구분하였다. 이를 토대로 SMART MMIS에서 분류한 상용소프트웨어에 대한 필수특성을 재정립할 필요가 있다. 표 2는 운영체제를 예로 들었을 경우, 소프트웨어 필수특성을 세가지로 구분하여 제시하였다. 표 2의 일반적인 특성은 EPRI TR-106439의 물리적 특성과 대응되며, 기능적인 특성은 성능 특성과 대응되며, 메트릭 특성은 종속성 특성과 대응된다. 안전한 소프트웨어에 대한 상세한 필수특성을 본 선정절차를 수행하면서 도출할 것이다.

표 2. 소프트웨어 특성분류

일반적인 특성	기능적인 특성	소프트웨어 메트릭 특성
확장성, 안정성, 용이성, 호환성 등	성능, 스케쥴링 능력, 메모리 관리, 주변장치 관리 등	복잡도, 무한루프, 데드락(deadlock), 등

단계 1을 수행하는데 있어서 가장 큰 애로사항은 업체의 협조와 안전한 소프트웨어 필수특성에 대한 기술기준 설정이다. 단계 1에서는 SMART MMIS 각 계통에서 요구하는 기능을 만족하는 소프트웨어를 일차적으로 선정하고 그 가운데 단계 2 선정방법을 수행하는데 있어서 충분한 자료를 제공할 수 있는 업체를 우선적으로 선정하여 단계 2를 수행할 수 있도록 한다.

4.2 단계 2 선정방법

단계 2 선정방법에서는 단계 1에서 선정한 후보 상용소프트웨어들이 공통적으로 갖고 있는 필수특성과 규제요건을 적용하여 선정기준을 작성한다. 선정기준은 다음과 같은 네가지 항목을 수행하는 과정에서 설정된다.

1) 선정기준서 작성 : 선정기준서에는 단계 1에서 도출한 소프트웨어의 기술적 세부사항과 업체의 명성에 관한 내용을 포함한다. 기술적 세부사항은 소프트웨어의 안전성을 평가할 수 있는 항목들에 대한 기준을 기술하며 업체의 명성을 통해 제품의 단종문제 및 지원능력 등을 평가한다. 평가전문회사인 OVUM, www.realtime-info.be, Gartner로부터 생산된 상용 평가보고서를 참조할 수 있다.

2) 운전이력 : 원자력 안전관련계통에 사용될 상용소프트웨어는 운전이력이 검증되어야 한다. 운전이력에 대해 원자력 안전관련계통과 유사한 환경에서 NUREG/CR-6421[8]에는 최소 1년의 운전이력을, EPRI ALWR URD[9]에는 최소 3년의 운전이력을 요구할 것을 기술하고 있다. 상용소프트웨어 개발업체는 자사의 사용자에 대한 정보를 체계적으로 관리하고 있지 않는 실정이다. 이것은 범용 소프트웨어인 경우에는 더 심하며 특수분야에 적용을 목표로 개발한 소프트웨어인 경우 일부 운전이력을 제시하는 경우가 있다. 운전이력 확인방법은 상용소프트웨어 사용자를 접촉하여 오류발생을 포함한 문제점, 운전이력 등에 관한 문서를 직접 확인하여야 한다. 운전이력 확인이 불가능한 경우 정부기관 또는 규제기관의 지침으로 대신할 수 있다. 예를 들어, 프로그래밍 언어에 대한 사용은 NUREG/CR-6463[10]의 지침을 따르도록 권고하는 것이다.

3) 품질보증 확인 : 업체가 소프트웨어 개발에 적용하고 있는 품질보증표준 또는 인증(certification)을 조사한다. 일반산업계에는 ISO 9000-3, 12207, 15504(일명 SPICE:Software Process Improvement and Capability dEtermination), ISO/IEC 9126, 14598 및 SEI사의 CMM(Capability Maturity Model) 등을 통해 소프트웨어 품질을 인증하고 있다. 이들의 인증은 원자력 안전관련계통에 사용될 소프트웨어에 대해서는 필요할 수 있지만 충분치 않다. 따라서 평가자는 IEEE, IEC, NUREG에서 제시한 소프트웨어 개발지침을 참조하여 품질보증확인사항을 작성하여 업체의 품질보증체계를 확인할 수 있어야 한다. 업체는 상용소프트웨어에 대해 white-box 시험를 수행하여야 하며 최소한의 시험범위는 NUREG/CR-6421를 벗어나지 않도록 한다. 또한 평가자는 특별히 업체에게 원시코드에 대한 미국표준기관(NIST)에서 제시한 맥케이브(McCabe) 방식의 cyclomatic 복잡도 분석결과 및 오류주입(fault injection) 시험결과를 요구할 수 있다. 안전관련계통에 사용할 상용소프트웨어인 경우, 업체는 자사의 소프트웨어에 대해 SFMEA(Software Failure Modes and Effects Analysis)와 SFTA(Software Fault Tree Analysis)를 포함한 소프트웨어 위해도분석

[11](software hazard analysis)을 수행해야 한다. 이러한 시험결과는 개발업체를 방문하거나 문서를 통해 확인할 수 있어야 한다.

4) 표준 준수 : 상용소프트웨어가 ISO, IEC와 같은 국제표준을 준수함으로써 얻을 수 있는 장점은 호환성이다. 표준이 안전하다고 인정할 수 없지만 범용적으로 신뢰성을 인정받았다고 말할 수 있다. 특정 국제표준 또는 산업계표준을 준수한 상용소프트웨어인 경우 표준기구 산하기관 또는 제 3의 기관에서 인증하는 표준준수시험 인증서[12]를 요구할 수 있다.

4.3 단계 3 선정방법

비안전계통에 사용할 상용소프트웨어인 경우, 단계 2에서 작성된 선정기준에 대한 만족도를 서류상으로 확인한 후 최종적으로 선정작업을 완료할 수 있다. 필요하다면 상용소프트웨어 평가버젼등으로 기능시험을 통해 선정여부를 결정할 수 있다. 그러나 안전관련계통에 사용할 상용소프트웨어는 단계 3을 통해 분석 및 시험을 수행하여야 한다. 이것은 소프트웨어가 수학적인 방법을 통해 안전성을 입증할 수 없는 특성이 있기 때문이다.

10CFR21에 의하면 상용등급품목 인정은 그 품목을 계통에 적용한 후, 계통이 수행하여야 할 안전기능을 완벽하게 수행할 수 있다는 증명 또는 확신을 얻음으로써 종료된다. 따라서 인정절차에는 계통시험을 통해 상용소프트웨어 품질을 확신할 수 있는 방법이 제시되어야 한다. 본 선정절차에서는 계통시험을 수행할 수 없기 때문에 계통을 프로토타이핑하여 분석 및 수행한다.

프로토타이핑을 통해 분석하고 확인할 사항은 IEEE 7-4.3.2에서 제시한 범위에 근접하도록 한다. 수행방법은 ACE(Abnormal Conditions and Events)를 규명하고 해결하기 위한 기술로써 FMEA(Failure Modes and Effects Analysis)와 FTA(Fault Tree Analysis) 방법을 이용한다. 많은 상용소프트웨어 업체가 자사의 소프트웨어에 대한 위해도분석 수행여부에 대한 의문점을 내재하고 있다. 그러한 경우, 평가자는 black-box 시험을 통해 상용소프트웨어의 안전성을 시험할 수밖에 없다. 단계 3을 수행하는데 있어서 가장 큰 애로사항은 상용소프트웨어에 대해 black-box 시험을 수행하기 위한 프로토타이핑 환경을 ACE를 규명할 수 있는 규모로 구성하는 것이다.

본 논문에서는 FMEA와 FTA의 상세 방법론은 언급하지 않으며 선정절차를 수행하는 과정에서 추후 방법론을 정립할 것이다. 단계 3에서 상용소프트웨어에 대한 안전성을 증명 또는 보장할 수 없다면 계통차원에서 다양성 및 다중방어개념을 도입하여 안전성요건을 해결해야 할 것이다.

5. 결론

본 논문을 통해 전력산업기술기준의 원자력 품질보증과 IEEE 7-4.3.2의 상용소프트웨어 품질보증을 토대로 SMART MMIS 설계기술개발에 사용할 상용소프트웨어 선정절차를 3단계로 개발하였다. 본 논문에서 제시한 선정절차는 EPRI NP-5652이 제시한 인정절차를 벗어나지 않도록 하였다. SMART MMIS 설계기술개발에서 본 논문을 통해 제시된 선정절차에 따라 상용소프트웨어 선정작업을 수행 중이며 그 과정에서 상용소프트웨어에 대한 필수특성을 개발할 것이다. 현재 상용소프트웨어 선정에서 중요한 현안사항은 소프트웨어 안전성에 대한 필수특성을 포함한 기술기준을 설정하는 것과 소프트웨어 위해도분석 방법론 설정이다. 안전관련계통에 사용할 상용소프트웨어인 경우, IEEE 7-4.3.2 요건에 따라 계통의 기능시험에 접목하여 FMEA와 FTA를 통해 위해도분석을 수행해야 하므로 그에 대한 방법론 설정이 향후 연구과제이다.

Acknowledgement

본 연구는 과학기술부의 원자력연구개발사업 일환으로 수행되었음.

[참고문헌]

1. USNRC GL 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products", U.S. Nuclear Regulatory Commission, 1989.
2. 김장열 외, "원전 상용기기(Commercial Grade Item) 승인 및 평가 방법론", '97 한국원자력학회 추계학술발표회, pp. 239-243, 1997.
3. 구인수 외, "The Development of Man Machine Interface System Design for SMART", KAERI/RR-1706/96, 한국원자력연구소, 1997.
4. EPRI NP-5652, "Guidelines for the Utilization of Commercial Grade Items in Nuclear Safety-related Applications(NCIG-07)", Electric Power Research Institute, 1988.
5. KEPIC QAP-1996 추록 6, "품질보증 기술기준 원자력 품질보증의 일반규격 품목의 승인방법", 전력산업기술기준(KEPIC), 대한전기협회(KEA), 1996.
6. IEEE 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations", 1993.
7. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", Electric Power Research Institute, 1997.

8. NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications", 1996.
9. EPRI ALWR URD, "Advanced Light Water Reactor Utility Requirements Document", Vol. III, Chapter 10, Man-Machine Interface Systems, Electric Power Research Institute, 1992.
10. NUREG/CR-6463, Rev. 1, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems", 1997.
11. NUREG/CR-6430, Ver. 2.0, "Software Safety Hazard Analysis", 1995.
12. Yongsuk Suh, et al., "A Proposal of International Standard Software Dedication for the Nuclear Industry", International Software Assurance Certification Conference, Mar., 1999.