원자력발전소 감시제어를 위한 상용 실시간 운영체제 평가시 고려사항

Consideration for the Evaluation of Commercial Real-time Operating System to monitor and control Nuclear Power Plants

이종복, 박근옥, 서용석, 구인수
한국원자력연구소

Abstract

원자력발전소에서 디지털 컴퓨터의 사용이 증가함에 따라 관련 시스템의 안전성, 신뢰성, 무결성, 가용성, 완전성 등을 충족시기기 위한 방안들이 현안으로 대두되고 있다. 특히 원자력발전소의 신경계통이라 할 수 있는 계측제어 계통의 디지털화로 인하여, 기존의 아날로그 하드웨어의 기능을 향상시킨 소프트웨어가 디지털 시스템에 사용되게 됨으로서, 디지털 시스템에 사용되는 상용 소프트웨어 제품의 신뢰도가 원자력발전소의 안전 및 안정 운영과 직결되므로 상용 소프트웨어에 대한 평가 문제가 중요한 관심사로 대두되었다. 본 논문의 서론에서는 원자력발전소에서 상용 소프트웨어제품을 사용하게 된 배경과 감시 및 제어를 위한 상용 실시간 운영체제를 사용하기 위한 고려사항을 기술하고, 본론에서는 상용 실시간 운영체제 선정 시 제공하여야 할 기능에 대한 고려사항과, 상용 소프트웨어 제품 선정에 관한 규제 현황 및 규제 요건에 대한 고려사항을 해결하기 위한 선정 및 평가 절차를 수립하고, 이를 평가에 반영하는 방법과 절차을 제시한다. . 결론에서는 원자력발전소 감시제어를 위한 상용 실시간 운영체제 평가시 고려사항의 해결에 대한 문제점과 해결 방안, 그리고 선정 절차 및 평가방안을 적용하는 데 따른 문제점과 해결 방안을 제시한다.

1. 서론

그 동안 지속적으로 발전되어온 디지털 계통 설계 기술은 산업계의 전 분야에 걸쳐서 다양하게 응용되고 있으며 이로 인한 산업 발달의 파급효과는 매우 큰 것으로 평가되어지고 있다.

원자력발전소 설계분야에 있어서도 디지털 계통 설계 기술의 적용영역은 1970년대 중반이후 점진적으로 증대되어 왔으며 그 중에서도 지난 10년 동안의 디지털 설계기술의 적용범위와 중요성은 급격히 증대되고 있는 추세이다.[2] 또한 최근 원자력발전소 아날로그 계측 제어 시스템은 시스템의 노후화로 인한 운전 및 유지보수 비용의 증가로 점차 디지털화 되어 가는 추세이다.

이러한 추세의 결과 기존의 아날로그 하드웨어의 기능을 향상시킨 소프트웨어가 디지털 시스템에 사용되게 됨으로서, 디지털 시스템에 사용되는 소프트웨어의 신뢰도가 원자력발전소의 안전 및 안정 운영과 직결되므로 소프트웨어에 대한 신뢰도 문제가 새롭게 발생되었다. 따라서 원자력발전소에 사용되는 소프트웨어는 고품질, 고 신뢰도 생산환경의 조성 및 완벽한 소프트웨어 개발 방법 및 확인 검증 기법이 요구되고 있다.[3]

원자력발전소 감시 및 제어 시스템에서 소프트웨어 오류는 심각한 위험 상태를 초래할 수 있기 때문에 시스템을 구성하는 복잡한 소프트웨어에 대한 안전성, 신뢰성, 확실성, 무결성 등은 상용 소프트웨어의 선정 및 소프트웨어 개발 시에 체계적인 확인 및 검증을 수행하여야 할 사항이다.

이에 따라 본 논문에서는 원자력발전소 감시 및 제어를 위한 상용 실시간 운영체제 선정 시, 내외부적인 다음과 같은 고려사항을 해결하기 위한 방법 및 절차를 기술하였다.

첫째, 내부적인 고려사항으로 감시 및 제어 시스템은 경성(hard) 실시간 시스템으로 사용되는 운영체제는 사용자 요구사항을 충족시키는 성능, 기능, 결정성, 응답성, 신뢰성, 안정성을 제공하여야 한다.

둘째, 외부적인 고려사항으로 원자력발전소에서 안전등급으로 분류된 시스템에 사용하는 상용 실시간 운영체제는 원자력 관련 법, 규칙, 지침, 표준 등을 준용하여 선정하여야 한다.

이러한 고려사항을 충족시키기 위하여 2장에서는 시스템 요건으로부터 만족시켜야 하는 운영체제의 특성 파악하고, 3장에서는 상용 소프트웨어 제품 사용과 관련된 규제 내용을 고찰하였다. 제 4장에서는 선정 및 평가 절차, 방법에 관하여 기술하고, 결론에서는 평가의 문제점과 해결방안을 기술하였다.

2. 감시제어를 위한 실시간 운영체제 요건

원자력발전소 감시제어를 위한 실시간 시스템은 다음과 같은 수행 특성을 가진다.

첫째, 실시간의 관점에서 보면 방대한 발전소 신호를 취득하여 정의된 응답 및 지연시간 이내에 요구되는 기능을 처리하여 결과를 운전 작업자에게 제공하여야 하므로 정확한 타이밍과 빠른 수행주기, 그리고 높은 신뢰성(high reliability)이 요구되며, 정확성, 안정성을 위해 입출력간 고속 응답이 보장되어야 한다.

둘째, 운전 중 시험이나 교정과 같은 유지보수가 용이하도록 모듈화 기법으로 설계되어 있어야 한다.

셋째, 실시간 시스템은 충분한 여유성과 확장성을 유지하여야 한다.

넷째, 시스템은 평균고장발생시간은 전체적으로 만족함으로써 약 99%이상의 이용률을 유지하여야 한다.

다섯째, 실시간 운영체제는 원자력발전소 또는 유사환경에서 충분한 운전 경험이 있는 신뢰성 있는 제품을 사용하여야 하고, 상용제품을 사용할 경우에는 상용제품 인정절차에 따라 확인 및 허가된 제품을 사용한다.

여섯째, 네트웍 기능을 지원하여야 한다.[7][8]

상기의 특성들을 만족시키기 위하여 실시간 운영체제는 고 신뢰성(high reliability), 결정성, 고속 응답성, 엄격 실시간(hard real-time), 안전성(safety-critical), 견고성(robustness), 보안성(security), 가용성(availability), 보수성(maintainability) 등의 요건을 만족시키기 위한 최소한 의 요건으로서 다음의 특성들을 지니고 있어야 한다.

- 멀티 태스킹 지원
- 선점 우선 순위 스케줄링 알고리즘 제공
- 응용시스템의 복잡도에 따라 사용할 수 있는 충분한 우선순위 레벨
- 우선 순위 역전(priority inversion)현상을 방지할 수 있는 기법 제공
- 예측성 있는 쓰레드 동기화 기법 제공
- 다음의 행위가 알려져 있고 예측 가능하여야 한다.
  - interrupt latency time
  - context switching time
  - task switching time
  - memory latency time
  - driver latency time
- 다양한 네트웍을 지원하여야 한다.
- 유사분야에서의 운전이력이 있어야 한다.
- 신뢰성과 고속 응답성, 안전성, 견고성을 제공하여야 한다.

3. 상용 소프트웨어 사용에 대한 규제 요건

다음은 원자력발전소의 감시 및 제어 시스템에서 상용 소프트웨어 제품을 사용할 때, 따라야 할 규제 요건과 사용에 대한 지침을 고찰한다.

3.1 규제요건

원자력발전소에서 상용 제품(Commercial Grade Item)을 사용하기 위해서는 상용제품을 수락(acceptance)할 수 있는 타당한 기준을 설정하고 그 기준에 적합한 제품을 선택하는 절차가 있어야 한다. 이러한 상용제품에 대한 승인(dedication)에 대한 우리 나라 고유의 규제 요건은 아직 없기 때문에 NRC(Nuclear Regulatory Commission)와 IEEE(The Institute of Electrical and Electronic Engineers) 프레임을 준용하고 있다. 이에 따라 상용제품에 적용되는 규제 프레임으로서 다음과 같은 법(code), 표준(standard)이 있다.

표 1 상용제품을 사용하기 위한 법, 표준, 지침

구분	내 용
법	▸10 CFR 21 : 상용제품(Commerical Grade Item)과 승인(Dedication)에 대한 정의 ▸10 CFR 50 Appendix B : 품질보증기준
표준	▸IEEE 7-4.3.2 - "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations", 1993
지침	▸EPRI NP-5652, "Guideline for the utilization of commercial grade items in nuclear safety related applications" ▸EPRI TR-106439, "Guideline on evaluation and acceptance of commercial grade digital equipment for nuclear safety applications", 1996 ▸NUREG/CR-6421, " A proposed acceptance process for commercial off-the-shelf(COTS) software in reactor applications"

이들 소프트웨어 상용제품 측면에서 법과 표준에 따르면, 상용제품에 대한 승인(dedication)요건으로서

첫째, 안전성 요건을 만족하여야 하며,

둘째, 필수 특성이 적절하게 구현되어 있어야 하고,

셋째, 안전기능을 수행할 것이라는 타당한 확신을 제시하기 위한 정립된 승인 절차를 충족시켜야 한다.

이에 따르면 제품의 개발에 따르는 품질보증 프로그램과 같은 정도의 평가과정을 요구하고 있다.

따라서 소프트웨어가 수행할 안전기능을 규명하고, 이러한 안전기능을 수행하기 위해 소프트웨어가 보유하여야 할 필수 특성(characteristics), 즉 안전기능을 수행할 수 있음을 확신할 수 있는 측정가능한 속성(attribute)을 규명하여, 이러한 필수 특성이 적절하게 구현되어 있음을 보여야 한다.

3.2 상용 소프트웨어 사용에 대한 지침

사용 소프트웨어 선정에 대한 지침으로서 EPRI NP-5652에서는 안전기능을 수행할 상용제품에 대하여 필수 특성을 규명하여 표 2 와 같은 다

표 2 EPRI NP-5652의 상용제품 선정방법

	방 법
1	특별 시험과 검사
2	제품공급자의 자격조사
3	제품개발 현장 확인
4	제품 및 공급자의 성능과 운전이력 확인
5	방법 1,2,3,4가운데 둘 또는 그이상의 방법을 조합

섯 가지의 승인방법을 제시하고 있다.

표 2에서 나타난 다섯 가지 방법 가운데 어떠한 것이 적절한 것인지에 대한 판단은 선정하고자 하는 제품의 특성과 계통의 요건에 따라 다를 수 있다.

방법 1은 특별 시험 및 검사(special tests and inspections)를 통해 제품을 승인하는 것으로 제품 인수 시 또는 설치 후 필요한 경우에 수행하는 방법으로, 제품 공급자가 제품에 대한 기술자료를 충분히 제공하여야 하고, 시험할 수 있는 설비 및 환경이 만들어져야 하고, 제품이 시험 및 검사를 통해 충분히 필수 특성을 확인할 수 있는 특성을 지녀야 한다.

방법 2는 제품 공급자의 자격조사(commercial grade survey of supplier)를 수행하는 것으로, 제품 공급자가 자체적으로 수행하고 있는 품질관리(quality control), 체계, 절차, 사례 등의 정도를 확인하여 승인한다. 방법 3은 제품이 인도되기 전에 현장에서 제품의 품질을 검사하는 것으로, 공급자의 현장에서 품질보증, 형상관리, 소프트웨어의 확인 및 검증 등의 활동에 대한 실사를 통하여 승인을 하는 방법이다.

방법 4는 제품과 공급자의 성능과 수락 가능한 운전이력(acceptable supplier/item performance record)를 통해 제품을 승인하는 것으로 기존의 운전이력(proven historical performance)를 인정하는 것이다. 방법 5는 방법 1에서 4까지의 방법 가운데 제품의 특성에 따라 두 가지 또는 그 이상의 방법을 조합하여 수행함으로써 제품을 승인한다.[4]

EPRI TR-106439에서는 제품의 품질을 강조하며, 상용제품의 필수 특성을 규명하고, 시험, 공급자 평가, 운전이력과 같은 검증(verification)을 통해 상용제품을 승인하는 방법을 사용하고 있다.[5]

표 3 NUREG/CR-6421에서 분류한 상용 소프트웨어 등급

IEC 1226 Category	Example systems
A	-Reactor Protection System(RPS) -Engineered Safety Features Actuation System(ESFAS) -Instrumentation essential for operator action
B	-Reactor automatic control system -Control room data processing system -Fire suppression system -Refueling system interlocks and circuits
C	-Alarms,annunciators -Radwasting and area monitoring -Access control system -Emergency communication system

NUREG/CR-6421에서는 상용 소프트웨어를 응용분야에 따라 A,B,C로 분류하여 다음과 같이 두 단계로 승인절차를 분류하고, 예비자격심사에서는 분류한 등급에 관계없이 모든 상용 소프트웨어에 공통적으로 적용되는 승인 기준을 제시하였고, 상세 자격심사에서는 사용소프트웨어의 안전 등급에 따라 확인하여야 하는 승인 기준을 제시하였다.[6]

① 예비 자격심사(preliminary qualification)
② 상세 자격심사(detailed qualification)

4. 상용 실시간 운영체제 평가 및 승인 절차

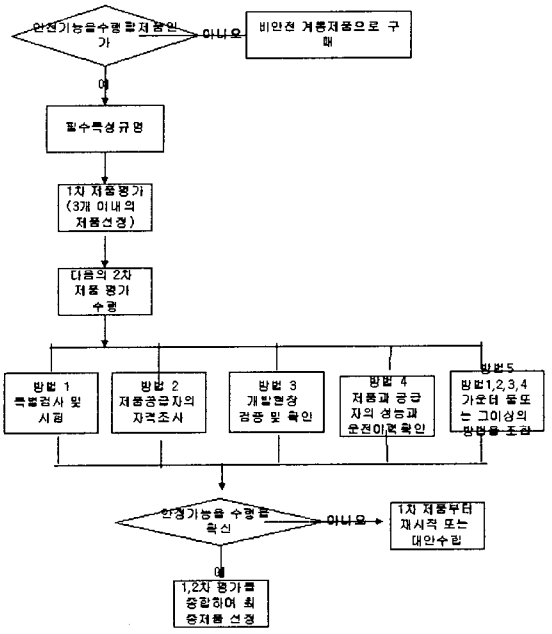

그림 1 상용 소프트웨어 선정 절차

원자력발전소 감시제어를 위한 상용 실시간 운영체제를 선정하기 위하여 EPRI NP-5652를 기반으로 그림 1과 같은 절차를 수립하고 평가를 수행중에 있다.

먼저 안전기능을 수행하는 실시간 시스템의 필수 요건을 파악하고, 이에 따라서 제공하여야 할 실시간 운영체제의 필수 특성을 파악하였다.

파악된 필수 특성과 일반적으로 실시간 운영체제가 가지는 표 4와같은 특성에 대해 1차 선정 평가 메트릭(metric)을 개발하였다.

1차 평가에서는 다단계 가중치 방법을 사용한다. 각 항목에는 상대적인 중요도(요구되는 필수특성)에 따라 전체 100%을 기준으로 가중치를 부여한다. 개개의 항목은 100점을 만점으로 하여 배점을 하고, 전체적인 배점은 100점을 만점으로 하여 평가한다.

1차 평가에서 후보제품을 3 제품 이내로 선정한 다음 2차 평가를 실시한다.

2차 평가에서는 제품의 특성에 따라 방법 1에

표 4 실시간 운영제의 특성 요소

구분	특성 항목 요소
기술특성	Kernel ROM(Min,Max), Kernel RAM(Min,Max), Min RAM per Process, Min RAM per thread, Min RAM per Queue, Multithreading scheduling policy, Number of priorities, Priority inversion protection method, Max. number of thread, Multiprocess support, Multithread support, Multiprocessor support, MMU support, Autocoder 등
성능특성	Thread switching time,Process switching time System clock's Min. resolution, Guarenteed Max. interrupt latency, Thread creation, Thread switch latency, Thread deletion, Interrupt latency, Context switching, task switching, Memory latency ,Driver latency 등
개발특성	개발호스트, 지원프로세서,지원보드/컴퓨터,컴파일러,RTOS구조,설치와 구성의 용이성,개발도구,지원네트웍,지원표준,개발환경,RTOS개발언어,GUI,API,사용가능한 컴포넌트, RTOS제공형태, 기술문서와 지원,개발방법론 등
비용	최소가격, 가격과 라이센싱 정책, 유지보수 비용
기타	교육지원, 유지보수지원,업그레이드 지원, 및 기술지원, 기술문서지원, 국내외 시장 점유율,개발사 안정성,개발사의 명성,국내공급사의 안정성, 제품의 타켓 시장, 유사분야에서의 사용업체의 수 등

서 방법 4까지의 가운데 하나 또는 그 이상의 방법을 조합하여 수행한다. 각 방법은 다음과 같다.

방법 1. 특별검사 및 시험
제품이 검사 및 시험을 통하여 충분히 안전기능을 수행할 수 있음을 확인할 수 있는 특성을 지닌 제품에 대하여 적용한다.

방법 2. 제품 공급자 자격조사
제품 공급자가 제품의 개발 과정에 공인된 품질보증 체계를 유지하고 있음을, 공급자 측의 품질보증 프로그램이나, 절차서 등을 확인한다.

방법 3. 개발 현장 검증 및 확인
상용 제품 개발 현장에서 제품의 품질보증, 확인 및 검증, 형상관리 체계를 확인한다.

방법 4. 제품과 공급자의 성능과 운전이력 확인
최소한 1년 이상이면서 독립된 2개 이상의 운영위치에서 중대한 오류가 없는 운전 이력 데이터 등의 보고서를 기반으로 확인한다.[1]

2차 평가에서 하나 이상의 제품이 선정되면 1차와 2차 평가를 고려하여 최종 선정한다. 2차 평가에서 선정된 제품이 없으면 1차부터 다시 시작하거나, 대안을 수립하여야 한다.

2차 평가는 시간과 비용이 많이 들고, 상용 소프트웨어 공급자의 우호적인 협조 하에 이루어져야 하는 어려운 작업이다. 현재 세부적인 지침 및 절차 개발을 진행하고 있다.

5. 결론

원자력발전소의 감시 및 제어에 사용되는 상용 실시간 운영체제의 선정 시, 가장 고려하여할 문제는 완성된 소프트웨어 제품인 "실시간 운영체제의 신뢰성, 안정성, 정확성을 어떻게 보장하는가?" 하는 문제로 볼 수 있다. 이러한 신뢰성, 안정성, 정확성을 보장하기 위해 선정 시 엄격한 원자력 관련, 규칙, 지침, 표준에 따라 안정성 및 신뢰성을 보장하자는 데 있다.

본 논문에서는 감시 및 제어 시스템으로부터 운영체제가 선정 시 고려사항인 필수 특성을 파악하여 보았고, 외부적인 고려사항인 원자력 관련 법, 규칙, 지침, 표준을 따르는 선정 및 평가 절차를 수립하였다. 선정 및 평가 절차에서 제시한 1차 평가로는 요구되는 기본적인 기능을 제공할 수 있다는 것을 확인하고, 완성된 소프트웨어 제품의 신뢰성과 안정성은 2차 평가에서 확인된다. 문제점은 2차 평가에서 제품공급자의 자격조사나 개발현장 검증 및 확인 등은 실제적으로 비용이 많이 들고, 수행하기에 어렵고, 많은 부분이 평가자의 판단에 의존하게 될 것이다. 또한 특별 검사 및 시험도 많은 부분을 평가자의 판단에 의존하게 될 것이다

이에 따라 방법 1, 2, 3에 대한 평가를 보다 객관화할 수 있는 평가 세부 지침의 개발이 요구되고, 보다 근본적인 대책은 공급자가 엄격한 품질관리 프로그램에 따라 개발하고, 이를 안전 등급에 따라 인증하는 체제를 갖추는 것이 필요하다고 할 수 있다. 또한 완성된 상용 소프트웨어 제품을 검증하고, 평가하는 기법 개발에 대한 체계적인 연구가 있어야 할 것이다.

본 논문에서는 원자력발전소 감시제어를 위한 상용 실시간 운영체제에 대한 내/외부적인 고려사항을 고찰하고, 선정 및 평가 절차를 수립함으로서, 평가 방법론을 확립하는 기반이 될 것으로 판단된다. 그리고 논문에서 제시한 선정 절차 및 평가 방안은 원자력발전소 계측제어 계통의 디지털화에 따른 상용 소프트웨어 제품의 선정 및 평가에 활용할 수 있을 것이다.

(본 연구는 과학기술부에서 시행하는 원자력연구개발 사업으로 수행되었음)

참고문헌

[1] 김장렬외,"원전상용기기(Commercial Grade Item) 승인 및 평가 방법론, 한국원자력학회, 추계학술발표회,1997
[2] "고신뢰도 소프트웨어 생산기법 개발에 관한 연구", 한국원자력연구소, KAERI/CM-018/93, 1994
[3] 윤원영,"원자력발전소 디지털 계통 설계의 안전성", 제어.자동화.시스템공학회지 제2권, 제5호,pp10-15,1996,9
[4] EPRI NP-5652, "Guideline for the utilization of commercial grade items in nuclear safety related applications",1988
[5] EPRI TR-106439, "Guideline on evaluation and acceptance of commercial grade digital equipment for nuclear safety applications", 1996
[6] NUREG/CR-6421, " A proposed acceptance process for commercial off-the-shelf(COTS) software in reactor applications", 1996
[7] 한국원자력연구소,"정보처리계통 설계요건서", SMART-MM- SR231-00, Rev1, 2000
[8] 한국원자력연구소, "제어계통 설계요건서", SMART-MM- SR242-00, Rev1, 2000