'95 추계학술발표회 논문집
한국원자력학회

원전 I&C FSE 분류기준과 이에 따른 상용 소프트웨어의 원전 사용 승인기준

김장열, 권기춘
한국원자력연구소

요 약

본 논문에서는 원전 I&C Function System Equipment (FSE)의 분류기준을 제시하기 위하여 IEEE 730.1, IEEE 828, IEEE 1012 및 IEC 1226 의 관련 표준들을 비교 분석하여 I&C FSE를 근간으로 계측제어 소프트웨어를 원전 I&C 계통의 기능에 따라 Type I,Type II,Type III 및 Type IV로 분류할 수 있는 분류기준, 분류절차 및 예를 제시하였다. 또한, 본 논문의 분류기준을 토대로 하여 최근 이슈가 되고 있는 상용 소프트웨어 (Commercial Off The Shelf Software)의 원전 사용 승인기준을 제시 하였다.

1. 서 론

IEEE 730.1, IEEE 828 및 IEEE 1012를 보면 소프트웨어 범주(category)를 critical 및 non-critical의 2가지 범주(two category)로 크게 분류하였다. IEC 1226에서는 원전 I&C 계통의 기능을 중심으로 category A, category B, category C 및 unclassified의 4가지 범주로 분류하였다. CE의 NUPLEX 80+의 Software Program Manual (SPM)을 보면 IEC 1226을 근간으로 하여 Critical safety(Active protection), Important to safety, Important to availability, General로 분류하고 다시 category를 원본(Original), 수정이 필요한 것(ETBM : Existing to be Modified), 수정이 필요하지 않은것(ENM : Existing not to be Modified)으로 분류(classification)와 범주를 2차원화 하였다. 이는 기존의 NUPLEX 80에서 NUPLEX 80+에로의 upgrade plan에서 운영체제, 컴파일어 등 수정이 필요없는 시스템 소프트웨어는 ENM 범주로 묶고 기존에 NUPLEX 80 프로젝트에서 사용하던 응용 프로그램과 디스플레이 포맷과 같은 수정이 필요한 것들은 ETBM으로 묶었다. 한편 새롭게 개발하여야 할 데이터베이스, 새로운 응용프로그램, 디스플레이 포맷등은 원본(original)으로 묶었다.

상기 표준과 분류된 내용들을 종합하면 모든 원전 계측제어 소프트웨어들은 원전 I&C 계통의 기능에 따라 4가지로 분류가 가능하다. 즉, IEEE 730.1, IEEE 828, IEEE 1012에서 제시한 critical 과 IEC 1226 및 CE NUPLEX 80+의 critical safety를 Type I 으로 분류할 수 있으며 non-critical 부분을 IEC 1226과 CE NUPLEX 80+에서 제시한 것처럼 Type II,Type III,Type IV로 분류할 수 있다. 이러한 Type의 분류는 원자력발전소 계통에 기능(function)적으로 대응되도록 기준을 설정할 수 있는데 대응되는 시스템 level은 Function-> Sub-function -> System -> Sub-system -> Equipment 의 I&C FSE 로 기능분할(function decomposition)을 설정할 수 있다. 본 논문에서는 이러한 I&C FSE에 따른 분류기준, 절차 및 시스템의 예를 제시하고 이에 따른 Commercial Off The Shelf Software (COTS)의 원전사용 승인기준을 제시하고자 한다.

2. I&C FSE의 분류기준

원전 I&C FSE 를 Type I, II, III 및 IV로 분류하는 기준을 제시한다. 만약 I&C FSE가 다음에서 제시한 기준을 충족시키지 못한다면 이를 Type IV로 분류한다.

분류하고자 하는 대상이 여러 군데 중복될 경우는 각 I&C FSE의 Type중 가장 적합한 Type의 I&C FSE에 포함되도록 고려하여 분류한다.

2.1 Type I

I&C FSE가 다음 기준중 어느 하나라도 만족한다면 Type I 으로 분류한다.

① 중대결과를 초래하지 않도록 하는 PIE(Postulated Initiating Events)의 연속적인 완화 조치가 요구되는것.

② PIE에 대응하도록 요구되는 작동으로 인하여 중요 SOE(Sequence of Event) 결과를 초래할 때 고장이 일어날 수 있는것.

③ I&C FSE에 있어서의 결함이나 고장이 다른 Type I FSE에 의해서 완화되지 않고 중요 SOE를 직접적으로 일으키는 것

④ 중대 결과를 초래하지 않도록 PIE의 연속적인 완화 조치를 수동적으로 이루어 질 수 있도록 하는 정보 또는 제어능력의 제공이 요구되는것

2.2 Type II

I&C FSE가 다음 기준 중 어떤것이라도 부합된다면 Type II로 분류하고 부합되지 않을 경우 Type I 으로 분류한다.

① 발전소가 제어 가능하고 프로세스 변수는 안전성 분석에서 가정한 제한치 범위 내에서 유지되는것.

② 중대한 결과를 회피하기 위한 Type I FSE의 운전을 위한 요건이 Type II FSE의 결함 또는 고장의 결과를 초래하는것.

③ 원전 설계 기준 내에서의 사소한 방사능 누출 또는 사소한 핵연료 파손의 방지 또는 완화를 위해서 사용되지만 중요 SOE 보다는 중요도가 낮은것.

④ Type I FSE에서의 고장을 제어실 요원에게 알려주기 위하여 제공되는 것.

⑤ 안전의무 이행을 위하여 Type I FSE의 이동성을 연속적으로 감시해 주는 것.

⑥ 안전성 분석의 요구로써 PIE 빈도를 상당히 줄이는데 사용되는 것

2.3 Type III

I&C FSE가 다음 기준 중 어떤 것이라도 부합된다면 Type III로 분류한다. 그렇지 않으면 Type I 또는 Type II로 분류한다.

① PIE 빈도를 기대치로 줄이는데 사용되는 것.

② Type I FSE의 성능개선이나 요구를 줄이는데 사용되는것

③ 안전상태를 결정하기 위하여 특히, 오동작이 PIE를 유발할 수 있는 것 등 FSE의 상태 기록이나 감시를 위하여 사용되는 것.

④ 원전 설계 기준범위내에서 (예를들면, 화재 또는 홍수) 내적인 위험도(hazard)의 완화조치나 감시를 위해서 사용되는 것

⑤ 발전소 내에서의 방사선 피폭 위험 또는 방사능 누출로 인한 사건 동안 요원의 안전을 보장하기 위하여 사용되는 것

⑥ 방사능 누출 위험이나 발전소에서 중대한 방사능 누출시 발전소 요원에게 경고 메시지를 주기 위해서 사용되는 것

⑦ 천재지변(지진, 해일 등)에 따른 완화조치나 감시를 위해서 사용되는 것

⑧ 발전소 내부 접근제어를 위한 것

여기서, Type I, Type II, Type III의 기준에 해당되지 않는 I&C FSE는 Type IV로 분류한다.

3. I&C FSE 분류절차

I&C FSE의 분류절차는 그림 1과 같다.

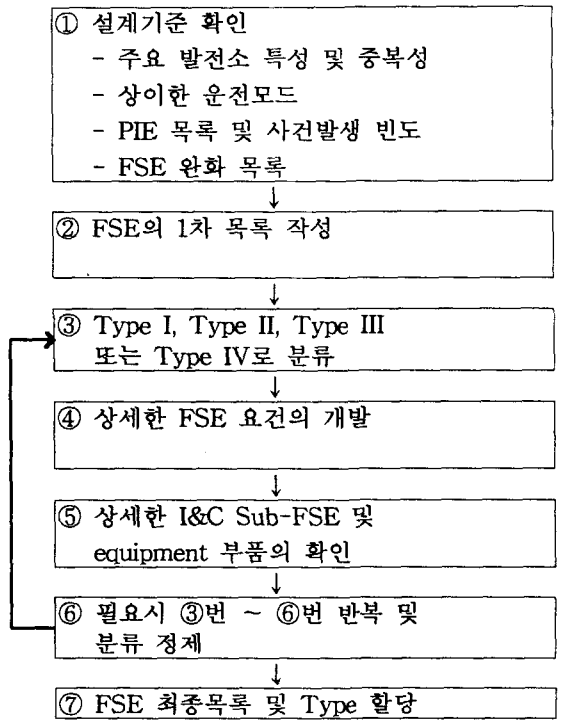

그림 1. I&C FSE 분류절차

3.1 범주화(categories)의 예

3.1.1 Type I

가. 일반적인 기능

Type I으로 분류된 I&C FSE는 다음과 같은 기능을 가져야 한다.

① 원자로 정지 및 미임계 유지

② 궁극적인 heat sink가 되도록 붕괴열의 전송

③ 격납 용기 분리

④ 운전원이 취득해야 할 필수정보

나. 시스템의 예

① 원자로 보호계통

② 안전 작동 계통 및 안전계통 지원

③ 발전소 안전성을 보장하기 위하여 요구되는 것으로 발전소운전 지침서에 정의된 운전원이 조치할 수 있도록 허용된 주요 계측 및 디스플레이 장치들

3.1.2 Type II

가. 일반적인 기능

Type II로 분류된 I&C FSE는 다음과 같은 기능을 가져야 한다.

① 발전소 1차 및 2차계통의 순환상태, 안전성 분석을 가정한 한계치에서의 변수유지, 사고의 상승효과, 사건방지 등의 자동제어

② 사고후 단계동안 조치해야 할 조기경보의 수집과 ALARA개념에 입각한 방사능 누출

의 유지 등 사고후의 각 시스템 및 장비들의 성능 감시 및 제어
③ 내적인 위험도(internal hazard)의 연속발생 제한
④ 고장으로 사소한 방사능 누출이 유발될 수 있는 핵연료 취급의 감시 및 제어

나. 시스템의 예
① 원전 자동제어 계통 또는 예방적인 보호계통
② 제어실 자료처리 시스템
③ 화재방지 계통
④ 원자로 정지시 사용되는 핵연료처리 시스템의 안전순환 및 연동장치(interlocks)

3.1.3 Type III

가. 일반적 기능

Type III로 분류된 I&C FSE는 다음과 같은 것을 내포할 수 있다.
① 내적 및 외적인 위험도 (화재, 홍수, 폭발, 지진 등)를 경보하는데 필요한 것들
② 운전실수로 인한 경미한 방사능 누출이나 운전요원에 의하여 방사능 누출 위험도를 야기할 수 있는 것들
③ 접근 통제시스템. 비상 계획의 이행을 목적으로 부지내 또는 부지외의 방사능 누출 경보를 위한 통신 시스템

나. 시스템의 예
① 경보시스템
② 방사성폐기물 유통감시 및 연동장치, 지역 방사선 감시
③ 접근 통제시스템
④ 비상통신시스템

4. 상용 소프트웨어의 원전사용 승인기준

상용 소프트웨어(COTS : Commercial Off The Shelf Software)의 원전사용 승인기준은 앞절에서 제시한 I&C FSE 분류 기준에 따라 승인 기준을 설정하게 되는데 다음과 같이 크게 1,2 단계 과정을 거친다.

ㅇ 1단계 : Preliminary qualification phase
- 안전성 관련 정도와 무관하게 모든 COTS 제품에 적용
- COTS 제품 확인 및 이해 수준
- 차기 qualification procedure의 엄격한 적용의 결정
- COTS 제품의 분석 및 문서화

ㅇ 2단계 : Detailed qualification phase
- Preliminary qualification phase의 결과 내용에 따라 다양하고 엄격한 승인기준의 적용

4.1 1 단계 : Preliminary qualification phase
① 시스템 수준에서 요구되는 안전기능의 확인을 위하여 위험도 분석(hazard analysis)을 한다.
② COTS 제품이 수행해야 할 안전기능(만약 존재한다면)을 확인한다.
③ COTS 제품은 형상 및 변경제어가 가능하도록 한다.
④ COTS 제품의 안전성 관련 정도를 다음 4가지의 기준에 따라 결정한다.

(1) 만약, COTS 제품이 안전관련 시스템에 직접적으로 사용된다면 COTS 안전성 범주는 IEC 1226의 기준에 따라 결정한다.

(2) 만약, 직접적으로 COTS 제품을 생산하거나 안전관련 시스템에서 사용중인 실행가능한 소프트웨어 제품의 형상을 제어한다면 COTS 제품의 결과물을 검증할 수 있는 방법은 존

재 하지 않는다.
직접적으로 생산하는 Type I 또는 Type II의 COTS 소프트웨어는 다음절에서 제시하는 Type I 또는 Type II의 승인기준에 의해서 검증되어야 한다.

(3) 만약, COTS 제품이 Type I, II 또는 Type III 소프트웨어 생산을 지원하지만 직접적인 생산을 하지 않거나 그러한 소프트웨어 모듈의 형상을 제어한다면 이러한 COTS 소프트웨어 제품은 Type IV로 분류한다.

(4) COTS 제품이 Type I, II 또는 Type III 소프트웨어 또는 시스템에 영향을 주지 않는다면 이러한 COTS 제품 역시 Type IV로 분류한다.
위와같이 결정된 Type I, II, III에 따라 각각 4.2.1절, 4.2.2절 및 4.2.3절로 분기하여 승인기준을 적용한다.

4.2 2단계 : Detailed qualification phase

4.2.1 Type I COTS의 승인기준

I-5 : COTS 제품은 IEEE 730.1, ISO 9000-3 또는 IEC 880에서 정의한 엄격한 소프트웨어 품질보증계획서하에서 개발된 것이어야 한다. 여기에는 충분한 V&V가 포함되어야 한다. 규제자는 임의시험(random testing)과 같은 방법을 통해서 결함 제거(fault sweep)를 요구할 수 있어야 한다.

I-6 : 충분한 소프트웨어 엔지니어링의 이행을 입증하고 검토할 수 있는 문서(documentation)들이 존재하는지 검토한다. 즉, 최소한으로 요구되는 검토(review)를 수행했다는 증거를 이용할 수 있어야 한다.

I-7 : COTS 제품이 1단계에서 확인된 요건에 부합되는지를 입증해야 한다.

I-8 : COTS 제품이 시스템 안전성 요건이나 제약사항을 위반하지 않았다는 것을 입증해야 한다.

I-9 : COTS 제품과 다른 시스템 또는 소프트웨어 사이의 인터페이스가 확인되어야 하고 명확히 정의되어야 하며 형상관리하에 있어야 한다.

I-10 : COTS 제품은 1년이상의 운영시간(operating time) 경험 데이터가 있어야 한다.
동일한 버전 및 배포제품과 운영 플랫폼(operating platform)을 이용하여 최소한 2개의 독립된 운영 위치에서 중대오류가 없다는 운영 데이터가 확보되어야 한다.
이 운영경험은 제안된 사용법과 같거나 거의 똑같아야 한다. 두개의 운영위치에서 역효과 보고서(adverse report)가 없다고 가정 하더라도 역효과보고서(adverse report)를 고려해야만 한다.

I-11 : 모든 오류, 중대한 오류든 아니면 사소한 것이든 간에 COTS 공급자에 의해서 보고되고 분석되어야 한다. 모든 절차들은 고수준의 입증요구를 보장할 수 있어야 한다. 또한 COTS 공급자는 이러한 요구에 대해 오류보고시스템 기록에 의거 납득할만한 통계적 확실성을 입증할 수 있어야 한다.
오류추적, 문서화 및 해결책 절차는 각각 오류에서부터 해결에 이르기까지 문서로 기록되어 있어야 한다.

I-12 : 만약, 사소한 문서의 누락이나 형상변경으로 인하여 보상이 필요할 때는 추가의 검증 및 시험이 수행되어야 한다.

4.2.2 Type II COTS의 승인기준

II-5 : COTS 제품은 IEEE 730 및 IEEE 1012의 품질보증계획 및 시스템적 소프트웨어 개발과정하에서 개발되어야 한다.

II-6 : ANSI/ANS-10.4 요건에 따라 개념정립 문서, 요구사항 명세서, 설계 명세서, 시험계획서 및 시험결과 문서 등 최소한 4가지 문서가 확보되어야 한다.

II-7 : COTS 제품이 1단계에서 확인된 안전기능을 충족시킬수 있는것인지 입증되어야 한다.
COTS의 신뢰도는 Type I에 준하는 높은 빈도가 나타나지 않도록 충분해야 한다.

II-8 : COTS 제품은 시스템 안전성 요건과 일치해야 한다.

II-9 : COTS 제품은 유사한 응용에 있어서도 만족되도록 작동해야 하며, 일치된 형상관리 프로그램과 잘 관리된 갱신프로그램으로 추적과 변경제어를 할 수 있어야 한다.

II-10 : 오류보고, 추적 및 해결책은 일관성이 있어야 하며 버젼 및 배포처, 절차서 들은 버젼이 배포된 후 1년동안 입증요구가 있을 때 보증되어야 한다. 제안된 버젼 및 배포는 해결되지 않은 중요한 문제들을 내포하지 않아야 한다. 현재의 버그리스트는 지원선택사항(support option)으로서 COTS 구매자들이 이용할 수 있어야 한다.

4.2.3 Type III COTS의 승인기준

III-5 : COTS 제품은 좋은 소프트웨어 엔지니링 이행사항에 따라 개발되어야 한다. ANSI/ANS-10.4의 요건에 따른 최소한 4가지 문서를 이용할 수 있어야 하며 IEEE 1012 에서 제시하고 있는 최소한의 Verification and Validation (V&V) 업무를 수행할 수 있어야 한다.

III-6 :V&V 타스크 문서를 포함한, 상기 III-5항에서 기술한 최소한의 4가지 문서는 검사(inspection)를 위하여 이용할 수 있어야 한다.

III-7 : COTS 제품은 감시의 개선, 발전소 상태에 대한 운전원의 이해력, 유지보수 활동의 지원, Type I 또는 Type II 시스템에 관한 요구에의 감소, 모니터링 또는 방사능 누출 효과 감소 또는 유사한 목적에 따라 안전성을 개선할 수 있어야 한다.
COTS 제품에 대하여 의도한 효과에의 제품성능이 검증(verified)되어야 한다.

III-8 : COTS 제품이 Type I 또는 Type II 시스템 또는 소프트웨어에 대하여 안전기능 역효과를 낼 수 없다는 것과 운전원을 중대하게 잘못 인도하는 일이 없다는것이 입증되어야 한다.

III-9 : COTS 제품이 즉각적인 응용(instant application)에 있어 중대한 오동작(malfunction) 없이 작동될 수 있다는 것을 보여야만 한다.

III-10 :오류보고 스킴(error reporting scheme)이 계획되어야 하며 COTS 제품의 적절한 오동작 추적이 가능해야 한다. 문서 및 품질보증기록 자료들은 5년 또는 서비스기간 동안 보존되어야 한다.

5. 결 론

원전 I&C FSE를 안전성 관련 정도와 기능에 따라 Type I, Type II, Type III 및 Type IV의 분류기준을 제시하였다. 이러한 분류기준에 따라 발전소 설계자와 운영자 그리고 규제기관에서는 안전성 관련 정도의 클래스별로 적용기준을 달리 설정하므로써 예산 및 인력투입 절감과 함께 소프트웨어 확인 및 검증 업무의 효율을 기할 수 있다. 또한, 상용 소프트웨어의 이점을 활용하기 위해 이를 원전에 사용시 문제가 되는 COTS의 안전성문제와 품질보증 문제를 해결하기 위한 일환으로 그 평가 요건과 기준을 관찰해 보았다.

앞으로의 연구과제는 이와같은 분류기준에 따라 I&C 소프트웨어를 재분류하고 소프트웨어 생명주기별로 QA 계획서, 소프트웨어개발절차서, 형상관리절차서, V&V 절차서 들이 본 논문에서 제시한 분류 기준을 근간으로 하여 우리나라 고유의 절차서들이 작성되어야 할 것이다.

[참고문헌]

[1] IEEE 730-1989, Software Assurance Plans (ANSI)
[2] IEEE 828-1990, Standard for Software Configuration Management Plans (ANSI)
[3] IEEE 1012-1986, Standard for Software Verification and Validation Plans (ANSI)
[4] IEEE 1228-1994, Standard for Software Safety Plans (ANSI)
[5] NPX80-SQP-0101.0, Rev. 0, Software Program Manual for NPX 80+
[6] NPX80-IC-QP790-02, Rev. 0, NPX 80+ Software Safety Plan Description
[7] IEC 1226, Nuclear Power Plants - Instrumentation and Control Systems Important for Safety - Classification