'97 춘계학술발표회 논문집
한국원자력학회

Safety-critical 소프트웨어 개발을 위한 V&V 독립성 구현 방안

엄흥섭, 이장수, 김장열, 최유락, 권기춘
한국원자력연구소
305-353 대전광역시 유성구 덕진동 150

요 약

검증 및 확인(V&V)의 속성상 Independent V&V는 반드시 필요 한 것으로 인식되고 실제로 규제 기준이나 여러 표준(Standard)들에서 그 요구사항들이 기술되고 있으나 그 기술 내용이 너무 단순, 추상적인 경우가 많아 구체적인 실현 방법에 있어서는 합의된 해결책이 제시되지 못하고 있는 실정이다. 이러한 문제점들을 해결하기 위해 본 논문에서는 원자력분야는 물론 프로세스와 군사 분야의 표준들과 기타 기술기준 자료들을 조사 분석하고 이를 기반으로 하여 원자력 분야, 특히 계측제어 계통의 Safety-critical 소프트웨어 개발에 따른 안전성과 경제성 문제가 고려되고 기술적, 관리적 측면에서 균형을 갖춘 V&V의 독립성 구현 방안에 대한 가이드를 제시 하였다.

1. 서 론

컴퓨터와 정보처리 기술은 발전소 운영상의 성능을 개선하고 보장하는 경제적 이유로 계측제어계통에 도입되어서 주로 운전분야, 즉 데이터의 수집, 표시, 저장 등의 분야에 적용되기 시작했으나 안전성에 관련된 부분에 대해서는 그 적용이 매우 보수적인 입장이었다. 그러나 이러한 제한은 안전성, 기능성, 신뢰성 향상에 대한 요구 사항이 높아지면서 점차 약화 되기 시작해서 현재는 원자력발전소의 안전성을 담당하는 계통에도 컴퓨터가 사용되기 시작했고 우리나라를 비롯한 수개 국에서 원자로 보호 계통에 컴퓨터가 도입되었다. 이에 따라 타 산업분야, 즉 의료, 항공, 군사 분야등에서 전부터 중요시 되고 있던 안전기능을 담당하는 소프트웨어의 개발에 대한 관심이 원자력 분야에서도 대두 되는 것은 당연하다고 볼 수 있다. 본 논문에서는 IAEA, IEC, NRC등에서 이러한 Safety-critical 소프트웨어의 개발에 핵심적인 요소 중의 하나로 제시하고 있는 소프트웨어의 검증 및 확인(Verification and Validation: V&V) 활동 중에서 그 규제기준이나 관련 표준들에 나타난 내용이 너무 단순하고 추상적이어서 실제로 구현 시 어려움이 있고 논의가 되고 있는 V&V

의 독립성(Independent Verification and Validation: IV&V) 문제에 대해 그 현황을 조사 분석하고 구현을 위한 가이드를 제시하였다.

2. IV&V와 관련된 규제기준, 표준들의 현황

조사, 분석된 자료들은 IEEE/ANS 7-4.3.2-1993, ASME/NQA2a, IEC 987, IEC 880, RTCA DO-178B, UK MOD 00-55, IEC 65A(Sec) 123, IEEE Std 1012-1986이며 이들에 나타나 있는 V&V의 독립성에 대한 요구 사항들을 인용해 보면 다음과 같다.

(1) IEEE/ANS 7-4.3.2-1993
The V&V plan shall specify activities and tests that shall be inspected, witnessed, performed, or reviewed by competent individual(s) or group(s) other than those who developed the original design.

(2) ASME/NQA2a, Part 2.7(1990)
Software V&V shall be performed by individuals other than those who designed the software.

(3) IEC 987 (1989) (nuclear safety system) Par. 6.2
Individuals or groups who perform the design verification shall be independent from those who are involved in the design activity. Persons involved with verification may be from the same organization as the individuals responsible for the design.

(4) IEC 880 (1986) Par. 6.2
The management of the verification team shall be separate and independent from the management of the development team.

(5) RTCA DO-178B (flight critical software)
For software verification activities, independence is achieved when the verification activity is performed by a person(s) other than the developer of the item being verified, and a tool(s) may be used to achieve equivalent coverage of a human verification activity.

(6) UK MOD 00-55 Clause 15
The design authority shall appoint a V&V team, independent of the design team, to verify and validate safety critical software.

(7) IEC 65A(Sec)123 Functional Safety of Electrical/Electronic/Programmable Systems: Generic Aspects(Draft 7, 1992) Clause 11, Functional Safety Assessment

	CONSEQUENCES		
LEVEL of INDEPENDENCE	MARGINAL	CRITICAL	CATASTROPH
Independent Person	HR#	NR	NR
Independent Department	HR*	HR#	NR
Independent Organization	-	HR*	HR

Legend: HR= highly recommended, -= not recommended or against, NR= not recommended, HR*= applies to programs of high complexity of new design, or using new technology. In all other cases HR# is applicable.

IEEE Std 1012 (1993)는 소프트웨어 V&V 계획서의 작성에 대한 기준을 제시하고 있는 중요한 표준인데 여기에는 디자인 기능과 V&V 기능 사이의 보고 관계에 대한

기술(description)만을 요구하고 있고 독립성의 정도에 대한 권고안은 없어서 분석 대상에서 제외 하였다.

이렇게 다양한 내용과 형태의 독립성에 대한 요구 사항이 나오게 된 배경과 각 내용이 내포하고 있는 특성을 분석해 보면 다음과 같다.

첫째, 발전소의 조달(procurement) 형태가 서로 달라 생기는 차이인데 (1), (2), (3)의 경우는 사용자가 개발을 직접 관리하지 않고 시스템을 구매하는 경우로서 개발자가 IV&V의 책임을 지고 있으므로 단지 개인이나 그룹 차원의 독립성을 요구하고 있다. 한편 (6)의 경우는 군수 분야의 조달 형태에 적용되는 기준인데 이는 사용자(또는 구매자)가 개발에 직접적으로 참여, 관리하는 형태로서 디자인 팀과는 별개의 IV&V 팀을 지정 할 수 있고 또 그 대가를 지불 할 수 있는 경우이다[1].

둘째, 독립성의 주체에 대한 차이들을 발견 할 수 있는데 (1), (2), (3), (5), (6)의 경우는 독립성의 주체가 인원, 즉 개인 또는 그룹,이고 (4)의 경우는 관리의 측면에 두었는데 이는 IV&V에 대한 시각의 또 다른 한 면을 열었다는데 그 의의가 있다고 볼 수 있다.

셋째, 독립성의 요구 조건을 만족 시키기 위해 Tool의 사용을 도입한 경우로 (5)가 이에 해당 된다. V&V는 관리적인 면과 기술적인 면이 합쳐진 종합적 활동인데 대부분의 경우 독립성 문제를 단지 관리적 측면, 특히 조직의 측면에서만 해결하려고 시도한 반면 이 기준은 한걸음 나아가 Tool 사용의 개념을 도입해서 보다 총체적으로 독립성의 구현 방안을 제시하고 있다. V&V 활동에 있어 V&V조직의 높은 독립성 정도가, 이는 Verifier가 개발팀에 참여하지 않는 제3자로서 조직적 측면에서 아주 독립 되어 있는(외부 기관 등)것을 의미하는데, 보다 신뢰성 있는 소프트웨어를 개발하는데 충분한 조건이 될 수 없다는 연구[2,3]와 조사 결과[1]는 V&V가 속성으로 가지고 있는 독립성에 대한 구현 방법으로 Tool의 사용에 보다 많은 관심을 기울일 필요성을 제시해 준다. 물론 이에 사용되는 Tool들에 대한 적절한 평가가 선행 되어야 할 문제이며 이 평가 문제에 대해서는 이미 원자력 분야에서도 Software Safety, V&V, QA 등의 분야와 관련된 표준들에서 나타나고 있다[4,5,6]. 이 기준에서 제시하는 Tool 사용에 대한 또 하나의 사항은 V&V 활동에서 사용되는 Tool의 개발자가 사용하는 Tool에 대한 독립성이며 이는 Verifier와 개발자가 같은 Tool을 사용해서는 안된다는 것을 암시한다.

넷째, 독립성의 정도를 Consequences of Failure에 비례하여 정의한 경우로 (7)이 이에 해당 된다. 위에서 언급된 표준들과는 다른 기준에서 독립성의 정도를 시도한 것으로 이 방법은 프로세스(process)와 군사(military) 분야에서는 많이 사용 되었지만 원자력 분야에서는 아직 그 예가 없다.

3. IV&V의 구현 방안

Safety-critical 소프트웨어의 V&V 활동에 있어서 V&V의 독립성을 적절히 구현하는데 필요하다고 생각되는 점을 위에서 고찰한 여러 표준들로부터 도출해 보면 다음과 같다.

첫째 Software Integrity Level을 정하는 것이다. Software Integrity level 문제는 비단 V&V 분야에만 영향을 주는 것은 아니다. 요구 사항 분석, 설계, QA, 유지 보수, 시험 등 Safety-critical 소프트웨어의 전 생명주기에 걸쳐 그 설계자, 사용자, 그리고 규제 관련자들에게 각 단계별로 투여해야 할 주의 정도를 제시 하기 때문이다[7]. 같은 이유로 V&V의 독립성에 대한 규제, 표준 수준의 요구 사항을 만족 시키면서 현실적 여러 조건들(예를 들면 경제성, 전문 인력의 적시 투여 등)을 고려한 구현 방안을 마련코자 한다면 Integrity Level은 필요 하다고 본다. Integrity Level을 정하는 방법에는 정량적인 방법, Risk-based ranking에 의한 방법 등 여러 가지가 있다. 현재 원자력 분야의 표준들 중 IEC 1226은 FSE(Functions, Systems, Equipments)을 대상으로 그 수행되는 안전 기능이 PIE(Postulated Initiating Events)의 완화에 어느 정도 기여하느냐에 따라 4개의 단계를 정량적으로 정하고 있고 타 분야, 특히 프로세스(process)와 군사(military) 분야의 표준들은 대부분 Multi-Level의 Risk-based Ranking 방법을 취하고 있는데 보통 4개의 Safety-relevant Risk 범주를 정하고 있다. 이미 언급된 표준 (5), (6)외에도 MIL-STD-1629 "Failure Mode, Effects and Criticality Analysis", MIL-STD-882 "System Safety Programs" 등이 이의 예에 속한다. Software Integrity Level을 정하는데 있어 Multi-Level의 채택은 V&V의 요구 사항과 수행에 필요한 자원을 감소 시킬 수 있는 체계적인 근거를 제공하고 이는 V&V의 독립성 구현에 있어서도 같이 적용된다. 또한 적절한 Multi-Level을 구현하기 위해서는 Risk-based 분류 방법을 채택하는 것이 현재의 최선이라고 본다[1,7].

둘째, 위에서 분석된 표준들에서 나타났던 "독립성"의 의미에 대한 보다 세분화된 요구이다. 이미 살펴 본 것처럼 이 의미는 인원, 조직을 의미하기도 하고 또는 관리적 측면을 의미하기도 하며 한편 Tool 사용의 개념이 도입되기도 하였는데 이에 대한 보다 보편화, 구체화가 모든 이해 당사자(사용자, 개발자, 규제 관련자 등)에게 보다 이해를 높일 것으로 본다. 여기에서는 2장에서 나타난 바 있는 (7) "IEC 65A(Sec)123 Functional Safety of Electrical/Electronic/Programmable Systems"에서와 같이 독립성의 정도에 대한 세분화를 Independent Person, Independent Department, Independent Organization으로 나눈 경우도 있지만 이는 조직적 측면에서 만의 세분화가 강조되어 있다. 보다 종합적이고 포괄적인 관점에서 시도된 기술적 독립성, 관리의 독립성, 그리고 재정의 독립성으로 나누는 방법이 보다 타당하다고 본다.[8]

1) 기술적 독립성(Technical Independence:TI)

이는 개발에 참여하지 않으며, 대상 시스템에 대해 충분한 지식을 가지고 있거나 관련된 분야에서의 경험과 배경이 충분하여 그 대상 시스템을 빨리 이해 할 수 있는 능력을 가진 사람(또는 그룹)이 대상 시스템이 문제를 해결 하는 방법을 이해 함과 동시에

그와는 다른 방법으로 문제 인식 및 해결 능력을 가져야 하는 "Fresh Viewpoint", 즉 기술적 측면에서의 독립성 역할을 의미한다.

2) 관리의 독립성(Managerial Independence:MI)

V&V 조직의 책임이 개발팀의 관리 조직이 아닌 별개의 조직에 귀속되어야 하는 관리, 조직상의 독립성 역할을 의미 한다. V&V 수행에 필요한 기술의 선택, V&V 활동 일정의 결정, 발견된 문제의 처리 및 해결에 대한 방안의 선택 등은 이런 관리의 독립성과 관련된 것들이다.

3) 재정의 독립성(Financial Independence:FI)

V&V 업무에 배정된 자금이 다른 용도로 배정되어 V&V에 필요한 분석이나 시험을 수행할 수 없게 되거나 또는 재정적인 압력으로 인해 V&V 수행 결과가 적절한 시간내에 적절한 방법으로 보고되지 못하는 것을 방지하기 위해 요구되는 독립성 역할을 의미한다.

이상에서 논의된 Multi-Level Software Integrity Level들에 대하여 세분화된 독립성 구성 요소를 각각 적용하면 다음의 표-1과 같은 형태로 표현 될 수 있으며 이 방법은 현재의 표준들에서 나타난 간단하고 추상적인 요구 사양을 실제로 프로젝트에 적용할 IV&V 구현 시 하나의 가이드가 될 것으로 본다. Software Integrity Level을 몇 단계로 나눌 것인가, 그리고 독립성을 구성하는 요소를 어떤 형태로 선택하느냐에 따라 여러 가지 구현 방안이 나올 수 있지만 여기에서는 지금까지 살펴본 표준들과 기타 자료들의 조사, 분석 과정에서 도출된 가장 일반적이고 타당하다고 보여지는 4개의 Integrity Level과 독립성의 구성요소로 TI, MI, FI를 채택하여 작성된 것이다. 특히 Software Integrity Level 문제는 IV&V에 국한된 문제가 아니고 Safety-critical 소프트웨어 개발과 이를 위한 QA 활동 전체에 영향을 미치는 사항으로 개발 방법론 분야, QA분야 등에서 계속 연구되는 상황인바 이의 연구 결과를 예의 주시하여 상황에 따라 해당 프로젝트에 적합한 형태를 도입하는 것이 바람직하다고 본다.

[표-1. Multi-Level Software Integrity Level과 독립성 구성요소를 이용한 IV&V 구현 예]

SW Integrity Level Independence 구성요소	Level 4 (Severe)	Level 3 (Major)	Level 2 (Minor)	Level 1 (Negligible)
기술적 독립성	HR	HR	HR	R
관리의 독립성	HR	HR	R	-
재정의 독립성	HR	R	-	-

Legend: HR = Highly Recommended, R = Recommended, - = not Recommended

이 표-1에서 관리의 독립성 부분은 다른 요소에 비해 그 정도의 차이를 이해하는데 애매한 점이 있을 수 있다. 이를 보완하기 위해 관리의 독립성 요소를 다시 (7) "IEC 65A(Sec)123 "에서 본 바와 같이 개인, 팀, 조직으로 2차 세분화 하여 적용 하는 것도 가능하다고 본다.[8]

4. 결론

원자력 분야에서 사용되는 표준들에 나타난 IV&V에 대한 요구 사항은 단순하고, 추상적인 내용으로 기술되어 있어 실제로 프로젝트에 적용 시 여러 가지 해석이 가능하여 그 구현 시 혼란이 생기기 쉽고 또한 관련자들 간의 이의 해석에도 어려움이 있다. 본 논문에서는 원자력 분야와 타 분야의 표준들을 조사하고 기타의 기술 자료들을 검토하여 IV&V에 있어서의 Tool의 역할, Software Integrity Level 개념의 도입, 표준들에 나타난 "독립성"에 대한 의미의 세분화 및 구성요소 도출, 이들의 조합에 의한 IV&V의 구현 방법을 제시하여 원자력 분야의 계측제어계통에 사용되는 소프트웨어 특히 Safety-critical 소프트웨어를 고려하여 이들 소프트웨어의 개발 시 적용될 IV&V의 구현에 대한 하나의 가이드를 제시 하였다.

참 고 문 헌

[1] NUREC/CR-6293 "*V&V Guidelines for High Integrity Systems*" 1995

[2] J.C.Knight and N.G.Leveson, "*An Experimental Evaluation of the Assumption of Independence in Multiversion Programming.*" IEEE Trans. Software Eng., Jan 1986.

[3] "*The Project on Diverse Software,*" OECD Halden Reactor project, June 1985

[4] IAEA Tech. Report No. 367 "*Software Important to Safety in Nuclear Power Plants*", 1994

[5] NUREC/CR 6421 "*A Proposed Acceptance Process for Commercial Off-the-Shelf Software in Reactor Applications*", 1996

[6] IEC 880 Supplement-1 "*Software for Computers Important to Safety for NPP*", 1996

[7] IEC 1226 "*Nuclear Power Plant-Instrumentation and Control Systems Important for Safety- Classification*" 1993

[8] KAERI Software Safety Guideline for Developing Safety Critical Software in Digital I&C Systems of NPP, 1997