'97 춘계학술발표회 논문집
한국원자력학회

Safety-critical 소프트웨어 V&V 지침서 개발 방법론

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

요 약

본 논문에서는 Safety-critical 소프트웨어를 위한 V&V 지침서(guideline) 개발 방법론을 제시한다. 즉, 기존의 산업계 표준인 IEEE Std-1012, IEEE Std-1059에서 논의되고 있는 개념을 근간으로 "독립성(independence)", "소프트웨어 안전성 분석(software safety analysis)", "COTS 평가(evaluation) 기준", "다른 보증(assurance) 조직들간의 관련성(relationship)" 등의 필수 안전 항목들을 추가하여 원전 안전성 시스템(NPP safety system)을 위한 V&V 지침서 개발 방법론을 제시하였다. 제시된 방법론에는 V&V 지침서의 범위(scope), 승인기준(acceptance criteria) 부분인 지침서 프레임(guideline framework), V&V activities 및 methods 부분인 타스크(task) entrance 및 exit 기준(criteria), 리뷰 및 감사(review and audit), 테스팅 그리고 V&V material의 QA 레코드(records) 및 형상관리, 소프트웨어 검증 및 확인 계획서(Software Verification and Validation Plan : SVVP) 생성 등의 내용을 기술하고, Safety-critical 소프트웨어 V&V 방법론도 함께 제시하였다.

I. 서 론

Safety-critical 소프트웨어란 잘못된 소프트웨어의 사용으로 인하여 그 결과가 사람 또는 장비(equipment)의 안전성에 크게 영향을 미쳐 경제적, 사회적으로 큰 손실을 초래할 수 있는 필수 안전 소프트웨어를 의미한다. 이러한 필수 안전 소프트웨어가 사용되는 시스템을 예를 들면 원자력발전소 보호계통에 장착되는 소프트웨어를 비롯하여 항공기 제어 시스템, 화학공장의 프로세스 제어 시스템, 방사선조사를 이용한 의료기기 시스템, 엘리베이터 시스템 등을 들 수 있다.

현재 산업계 표준으로 나와 있는 IEEE Std-1012, "Software Verification and Validation Plans", 1986 및 IEEE Std-1059, "IEEE Guide for Software Verification and Validation", 1993은 원자력발전소 보호계통 및 계측제어계통에 사용되는 Safety-critical 소프트웨어에 적용하기에는 USNRC에서 제시하는 규제요건을 충족시키지 못한다.

산업계의 표준인 IEEE Std-1012 및 IEEE Std-1059는 앞서 기술한 바와 같이 의료분야 및 엘리베이터 시스템 등의 주로 산업계에서 사용되는 Safety-critical 소프트웨어 등의 전형적인(typical) 시스템에 적용할 수 있는 표준으로써 안전성이 보다 엄격히 요구되는 원전 안전성 시스템(NPP safety system)에 적용하기 위해서는 첫째, IEEE Std 7-4.3.2, BTP-14, IEEE Std-1228에서 제시하고 있는 소프트웨어 안전성(software safety) 요건을 만족시켜야 한다. 둘째, 이러한 V&V activities들은 여러 보증조직(Software Verification and Validation : SVV, Software Quality Assurance : SQA, Software Configuration Management : SCM, Software Safety Analysis : SSA) 의 분담수행 또는 SQA 조직을 중심으로 수행하여야 하는 바, 이들 보증조직들간의 관련성(relationship)을 기술하여야 한다. 셋째, NUREG/CR-6421의 Commercial Off the

Shelf (COTS) 소프트웨어의 평가기준 요건을 만족시킬 수 있어야 한다. 넷째, 기술적(technical), 관리적(management), 재정적(financial) 형태를 고려한 독립성(independence) 요건이 추가되어 한다. [표 1]

본 논문에서는 원전 안전성 시스템의 규제요건을 충족시킬 수 있는 지침서 프레임(guideline framework)을 설정하고 이러한 지침서 프레임을 토대로 Safety-critical 소프트웨어를 위한 V&V 지침서 개발 및 V&V 방법론을 제시 하였다.

표 1. 원전 안전성 시스템을 위한 관련 표준요건

구 분	관 련 표 준	적 용 분 야	비 고
산업표준	IEEE Std-1012	전형적인(typical) V&V	
	IEEE Std-1059	전형적인(typical) V&V	
원전 안전성 시스템	IEEE Std 7-4.3.2	원전 안전성시스템을 위한 고려사항들	
	BTP-14	SVV,SQA,SCM 및 SSA 조직간의 관련성	
	IEEE Std-1228	소프트웨어 안전성 분석	
	NUREG/CR-6421	COTS 소프트웨어 평가	
	NUREG/DG-1054	독립성, 감사, 형상관리	

II. Safety-critical 소프트웨어 V&V 지침서 개발 방법론

2.1 지침서 범위 설정

원전 Safety-critical 소프트웨어 V&V 지침서를 개발하기 위해서 가장 먼저 고려하여야 할 사항은 지침서의 범위(scope)를 설정하는 것이다. 소프트웨어란 그 자체만으로는 고유의 기능을 발휘할 수 없는 객체로써 결국 소프트웨어는 하드웨어에 장착(embeded)되고 이들 하드웨어는 다시 원전이라는 시스템으로 통합되기 때문에 소프트웨어 V&V 지침서의 범위를 기술할 때 이를 원전 계측제어 시스템으로 한정하기 보다는 원전의 포괄적인 관점(fom the global point of view)에서 기술하여야 한다. 즉, 원전 계측제어 시스템의 시스템 엔지니어링 관점과 소프트웨어 엔지니어링의 개념이 상호 연계되도록 지침서가 개발되어야 한다.

2.2 승인 프레임 기준

개발하고자 하는 소프트웨어 V&V 지침서의 규제요건 일치성을 체크하기 위한 "Acceptance criteria with Framework"을 구축하여야 한다. 이 부분에서는 각국의 특성을 고려한 규제상황을 기술하고 소프트웨어 엔지니어링의 개념을 추가한다. 이때 기존의 산업계 표준인 IEEE Std-1012 및 IEEE Std-1059를 근간으로 하고 여기에 현재 새롭게 논의되고 있는 개념들 즉, 다음 사항들을 승인 프레임(acceptance famework)에 추가하여야 한다.

- 10 CFR 50의 인용 및 각국의 자체 원자력 법령(nuclear code) 도입
- NUREG/DG-1054의 독립성, 감사, 형상관리 개념, IEEE Std-1074에서 제시하고 있는 소프트웨어 생명주기 모델 및 activity 들의 사상(mapping)
- 원전 안전성 시스템을 고려한 사항들의 추가
  - IEEE Std 7-4.3.2 : 원전 안전성 시스템 고려사항들
  - BTP-14 : SVV,SQA,SCM 및 SSA 조직간의 관련성(relationship)
  - IEEE Std-1228 : 소프트웨어 안전성 분석(software safety analysis)
  - NUREG/CR-6421 : COTS 소프트웨어 평가 기준

2.3 V&V 및 다른 보증 조직들간의 관련성

V&V와 다른 보증조직 들과의 관계를 정의한다. 이를 위하여 ASME/NQA-1에서 기술한 설계결과물(design output)에 대한 정의를 내린다. 소프트웨어 생명주기 모델에 따라 설계결과물(design output)이 약간 상이할 수 있으나 하드웨어 및 소프트웨어에 대한 설계결과물(design output)을 ASME/NQA-1을 기준으로 예를들어 제시해 보면 표2와 같이 정의할 수 있다.

표 2. 하드웨어 및 소프트웨어에 대한 설계결과물(design output)의 정의

하 드 웨 어	소 프 트 웨 어
Hardware Requirement	Software Requirement Specification
Functional Block Diagram	Architecture Design
Schematic Diagram	Detailed Design
Assembly Drawing	Code, Build description
Operations & Maintenance Manual	Manuals

표2에서 정의된 소프트웨어 설계결과물(design output)에 대하여 각 보증 조직들간의 V&V 업무를 명확히 정의하여야 하는데 다음과 같이 보증팀별 책임사항(Define of Responsibility)을 정의할 수 있어야 한다.

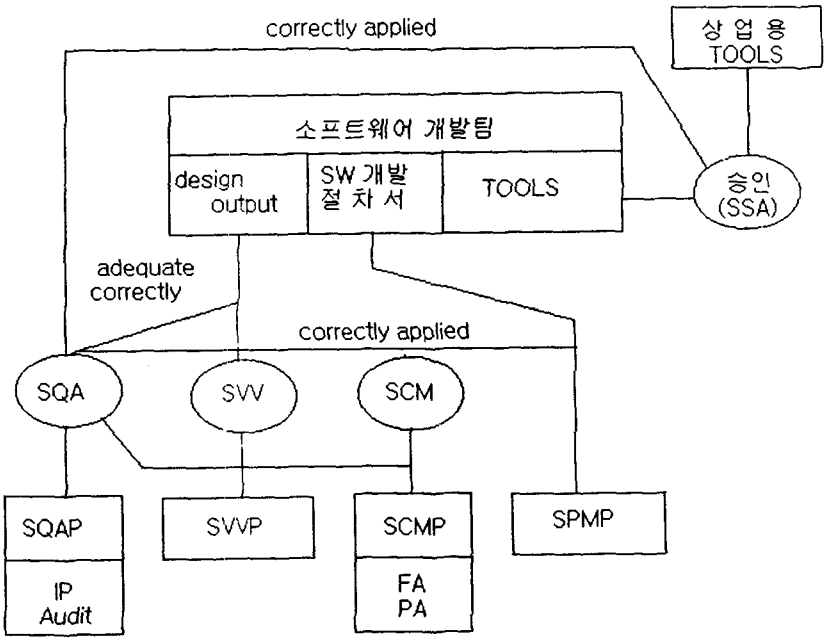
- ㅇ SQA 팀
  - 소프트웨어 품질보증 계획서(Software Quality Assurance Plan : SQAP) 작성
  - Review 수행
  - 인-프로세스 감사(in-process audit) 수행
- ㅇ SCM 팀
  - 소프트웨어 형상관리 계획서(Software Configuration Management Plan : SCMP) 작성
  - 기능적 감사(functional audit) 및 물리적 감사(physical audit) 수행
- ㅇ SVV 팀
  - 소프트웨어 검증 및 확인 계획서(Software Verification and Validation Plan : SVVP) 작성
  - 추적성(traceability) 분석
  - 테스팅
  - SQA팀의 Review 수행 지원
  - SSA팀의 COTS 소프트웨어 도구(tools) 평가 지원
- ㅇ SSA 팀
  - SVV로 부터 받은 추적(tracing) 정보를 토대로 소프트웨어 안전성 분석 (Software Safety Analysis) 수행
  - COTS 소프트웨어 도구 평가

이러한 보증(assurance) 팀별 책임사항은 프로젝트를 관리하는 총책임자의 정책(policy)에 따라 SQA팀을 주축으로 하여 약간의 변형된 형태로 구성할 수도 있으나 본 논문에서 제시하는 조직도는 한국적 상황을 고려하여 구성해 보았다.
상기 보증 조직들간의 업무 범위 및 관련성 그리고 소프트웨어 개발 도구에 대한 승인과정의 관련성 등을 도식화 하면 그림 1과 같다.

2.4 독립성 요건

독립성(independence) 요건은 V&V 속성상 반드시 확보되어야 하는 것으로서 IEEE Std

7-4.3.2, ASME/NQA 2a part 2.7, IEC 987 part 6.2, IEC pub. 880, RTCA DO-178B, UK MOD 00-55 Clause 15, IEC 65A(sec) 123, IEEE Std 1012 등에서 요구사양을 기술하고 있다. 이의 실현 방법(Independence Parameter : Technical, Management, Financial, Independence form : Classical IV&V, Modified IV&V, Internal iV&V, Embeded V&V)에 있어서는 독립성의 정도를 개인, 조직, 경제적 그리고 관리적 측면을 고려한 후, 이를 다시 안전성 정도에 따라 구분할 수 있도록 하고 있다. Classical IV&V란 기술적, 경제적, 관리적, 계약적으로 개발조직으로 부터 완전히 분리된 조직이 수행하는 제3자 수행 IV&V를 의미한다. Modified IV&V와 Internal iV&V란 예를들어 하나의 설계결과물(design output)에 대하여 별도의 V&V 조직이 개발팀과 상호 연계하여 개발팀의 중간결과물에 대하여 V&V를 수행한다고 가정하면 이는 Internal iV&V에 해당되며 개발팀과 V&V팀이 상호연계(interaction)되지 않은 채 개발팀의 결과물에 대하여 독립적으로 별도의 V&V를 수행 할 경우에는 Modified IV&V에 해당된다. Embeded V&V는 V&V 요원이 개발조직과 함께 검사(inspection), 워크스루(walkthrough), Review를 수행하는 것으로서 독립성의 parameter가 없는 경우이다. 현재 미국의 USNRC 규제요건을 보면 Safety-critical 소프트웨어의 경우 Modified IV&V나 Internal iV&V를 만족하도록 규정하고 있으나 각 국가의 원전 구매형태(턴키 계약, 공동설계, 독자설계)와 규제기관, 개발자, 사용자 등 모든 이해당사자들의 입장이 현실적으로 반영된 형태(다양한 독립성 매개변수가 반영된 independence form의 조합형태)가 모색되도록 해야 한다.



주) design output : SRS, SDD, Code, User Doc., Test Plan, Test Result Plan

그림 1. SQA, SCM, SVV 및 SSA팀간의 V&V 업무수행 관련 구성도

2.5 생명주기상에서의 V&V 타스크(task) entrance 및 exit 기준

V&V activities 들을 소프트웨어 생명주기 단계별로 기술한다. 이때 생명주기 모델(waterfall model, sprial model, increment model)을 설정하고 생명주기 모델에 따른 각 단계를

확정한 다음 IEEE Std-1074를 참조하여 생명주기 각 단계의 activity 항목(item) 들을 생명주기 모델에 적합하게 사상(mapping) 시킨다. 그 다음 각 생명주기 단계별로 V&V 타스크 entrance 및 exit 기준을 설정한다. 이러한 entrance/exit 기준을 생명주기의 한 단계인 단위 테스트(unit test) 단계를 하나의 예로써 제시해 보면 표 3과 같다.

생명주기 끝 부분(유지보수 단계 다음 부분)에는 실제 ongoing V&V activities 수행을 위하여 다음 activities 들을 별도로 추가한다.

- ㅇ Ongoing V&V activities
  - SVVP 유지(maintain SVVP)
  - V&V 평가 기준선 설정(baseline change V&V assessments)
  - V&V 활동의 평가(reviews of V&V activities)
  - V&V 활동중 SQA팀의 review 지원(support related activities)

표 3 단위테스트(unit test) 단계에서의 V&V 타스크 entrance 및 exit criteria

생명주기 단계	entrance 기 준	exit 기 준
단위테스트 (unit test)	ㅇ 코딩 완료 ㅇ Unit Test Plan(UTP) 완료 - Unit Test Coverage(UTC) 준비 - 테스트 데이터 준비 - 테스트 소프트웨어 . Drivers . Stubs ㅇ Test Platform/Tools	ㅇ 모든 test coverage가 성공적일 때 ㅇ PATH coverage를 만족했을 때 - branch coverage를 달성

2.6 V&V material 및 형상관리, 패키징 정책(packaging policy)

V&V material 관리 부분을 형상관리와 함께 기술한다. 이러한 모든 사항들은 앞서 기술한 지침서 프레임(guideline framework)에 사상(mapping)하여 원전 안전성 시스템 규제요건에 맞도록 일관성을 반드시 유지하도록 한다. 그런다음, 계획단계에서의 각 문서들(SQAP, SVVP, SCMP, SO&MP 등)을 종합하여 원전설계 Design Certification (DC) 요건중의 하나인 SVVP를 생성한다.

이상을 종합하여 본 논문에서 제시했던 V&V 지침서 개발 방법론을 토대로 원전 안전성 시스템을 위한 Safety-critical 소프트웨어의 V&V 방법론을 제시하면 표 4와 같다.

III. 결 론

본 논문은 현재 산업계 표준으로 사용하고 있는 IEEE Std-1012와 IEEE Std-1059를 근간으로 하여 원전 안전성 시스템에 사용될 수 있도록 "독립성(independence)", "소프트웨어 안전성 분석(software safety analysis)", "COTS 평가(evaluation)", "다른 보증 조직들간의 관련성(relationship)" 등의 필수 안전 항목들을 추가하여 Safety-critical 소프트웨어 V&V를 위한 새로운 지침서 개발 및 V&V 방법론을 제시하였다. 본 논문에서 제시한 Safety-critical 소프트웨어를 위한 지침서 개발 및 V&V 방법론을 토대로 한국 실정에 알맞는 V&V 지침서 및 방법론을 개발할 수 있을 뿐만아니라 원전설계 DC를 위한 SVVP 생성의 초석이 될 수 있다.

Safety-critical 소프트웨어 V&V 분야는 NPP I&C 분야의 디지털화에 따라 전세계적으로 hot issue가 될 만큼 활발한 연구가 진행되고 있는바 앞으로 이러한 연구에 대한 지속적인 관심과 보다 많은 연구가 필요하다.

표 4. Safety-critical 소프트웨어를 위한 V&V 방법론

생명주기 / V&V 타스크	분 석 (SRS)	설 계 (SDD)	구 현 (소스코드)	테스팅 (test plan,test doc등)	유지/보수 (메뉴얼)	역할분담
o 리뷰(review)	R	R	R			SQA
o 리뷰 지원	r	r	r			SVV
o 감사(audit)						
- 기능적 감사			FA	FA	FA	SCM
- 물리적 감사				PA	PA	SCM
- 인-프로세스 감사	IA	IA	IA	IA	IA	SQA
o 감사활동 지원			a	a	a	SVV
o 테스팅	V	V	V	V	V	SVV
o 평가(evaluation)	V	V	V	V	V	SVV
o 추적(tracing)	V	V	V	V	V	SVV
o SW 안전성 분석						
- 추적정보 이용	S	S	S	S	S	SSA
o COTS 평가	C	C	C	C	C	SSA
o COTS 평가 지원	c	c	c	c	c	SVV

주) R : Major review, r : Minior review(support review), a : Minior audit(support audit),
V : Verification and Validation, C : Major COTS evaluation,
c : Minior COTS evaluation(support evaluation), S : Software Safety Analysis
FA : Functional Audit
PA : Physical Audit
IA : In-process Audit

IV. 참고문헌

[1] 10 CFR PART 50 *"Domestic Licensing of Production and Utilization Facilities"*

[2] 10 CFR PART 52 *"Early Site Permits ; Standard Design Certification ; and Combined Licenses for Nuclear Power Plant"*

[3] Reg. Guide 1.53 *"Application of the single-failure criterion to Nuclear Power Plant Protection System"*.

[4] ANSI/IEEE 730, *"IEEE Standard for Software Quality Assurance Plans"*, Institute of Electrical and Electronics Engineers, 1990.

[5] ANSI/IEEE 1012, *"Software Verification and Validation Plan"*, Institute of Electrical and Electronics Engineers, 1986.

[6] ANSI/IEEE 1059, *"IEEE Guide for Software Verification and Validation"*, Institute of Electrical and Electronics Engineers, 1993.

[7] NUREG/CR-6101, *"Software Reliability and Safety Nuclear Reactor System"*, 1993.

[8] NUREG/CR-6263, *"High Integrity Software for Nuclear Power Plants"*, 1995.

[9] NUREG/CR-6421, *"A Proposed Acceptance Process for Commercial Off the Shelf (COTS) Software in Reactor Applications"*, 1996.

[10] IEC 880, *"Software for Computers in the Safety Systems of Nuclear Power Stations"*, International Electrotechnical Commission, 1986.

[11] IEC 1226, *"The Classification of Instrumentation Control Systems Importance to Safety for Nuclear Power Plants"*, 1993.