2002 추계학술발표회 논문집
한국원자력학회

소프트웨어 설계검증 승인요건에 대한 일치성 분석

Compliance Analysis of Acceptance Criteria for Verifying Software Design

차경호, 이장수, 손한성, 김장열, 천세우, 권기춘
한국원자력연구소
대전광역시 유성구 덕진동 150

요 약

원전 안전계통 소프트웨어 설계를 검증하기 위해 적용해야하는 인허가 승인요건들 중 과학기술부 고시에서 규정하는 산업표준과 인허가 기관의 규제지침의 관계를 분석하였다. 분석대상인 법적 기준은 과학기술부 고시 "원자로시설의 계측제어계통에 관한 기준" 중에서 안전계통 소프트웨어의 확인, 검증, 검토, 감사를 위한 기준인 별지15에서 규정하는 내용과 관련 산업표준이다. 이에 대한 일치성을 분석하기 위한 비교대상은 한국원자력 안전기술원의 "원자력발전소 컴퓨터-기반 계측제어계통에 개한 안전규제 일반원칙 및 규제지침" 중의 개발 소프트웨어에 대한 평가기준이다. 이러한 분석을 토대로 KNICS 안전계통 소프트웨어 검증에 사용할 원전 안전계통 소프트웨어 설계명세 검증절차서를 개발하였다.

Abstract

This paper presents the analysis of the compliant relationships between the industrial standards to be noticed by the Ministry of Science and Technology (MOST) and the regulatory guidelines to be used by regulatory agencies, with the aim of verifying software design for safety systems in Nuclear Power Plants. The standards and guidelines were selected for the mandatory criteria in design certification. Lawful criteria in the analysis is the content and industrial standards for verifying, validating, reviewing, and auditing safety software (Appendix 15), which is a part of Criteria for I&C systems of nuclear facilities. The evaluation criteria for developing software, which is a part of General principles of safety regulation and regulatory guidelines for computer-based I&C systems in Nuclear power plants, are compared compliantly with the lawful criteria. Recently, the analyzed results had been applied to develop the verification procedure for software design specifications (SDS) of safety software in Korea Instrumentation and Control System(KNICS).

1. 서 론

원전 안전계통 소프트웨어 설계를 검증하기 위해 적용해야하는 인허가 승인요건들 중 과학기술부 고시에서 규정하는 산업표준과 인허가 기관의 규제지침의 관계를 분석하였다. 이러한 승인기준들은 원전 안전계통 소프트웨어 개발공정 전체를 규정하는 기준이며 본 논문에서의 분석범위는 원전 안전계통 소프트웨어 설계만을 대상으로 하며 향후 같은 방법으로 이 분석결과를 전 공정에 확대 적용할 수 있다.

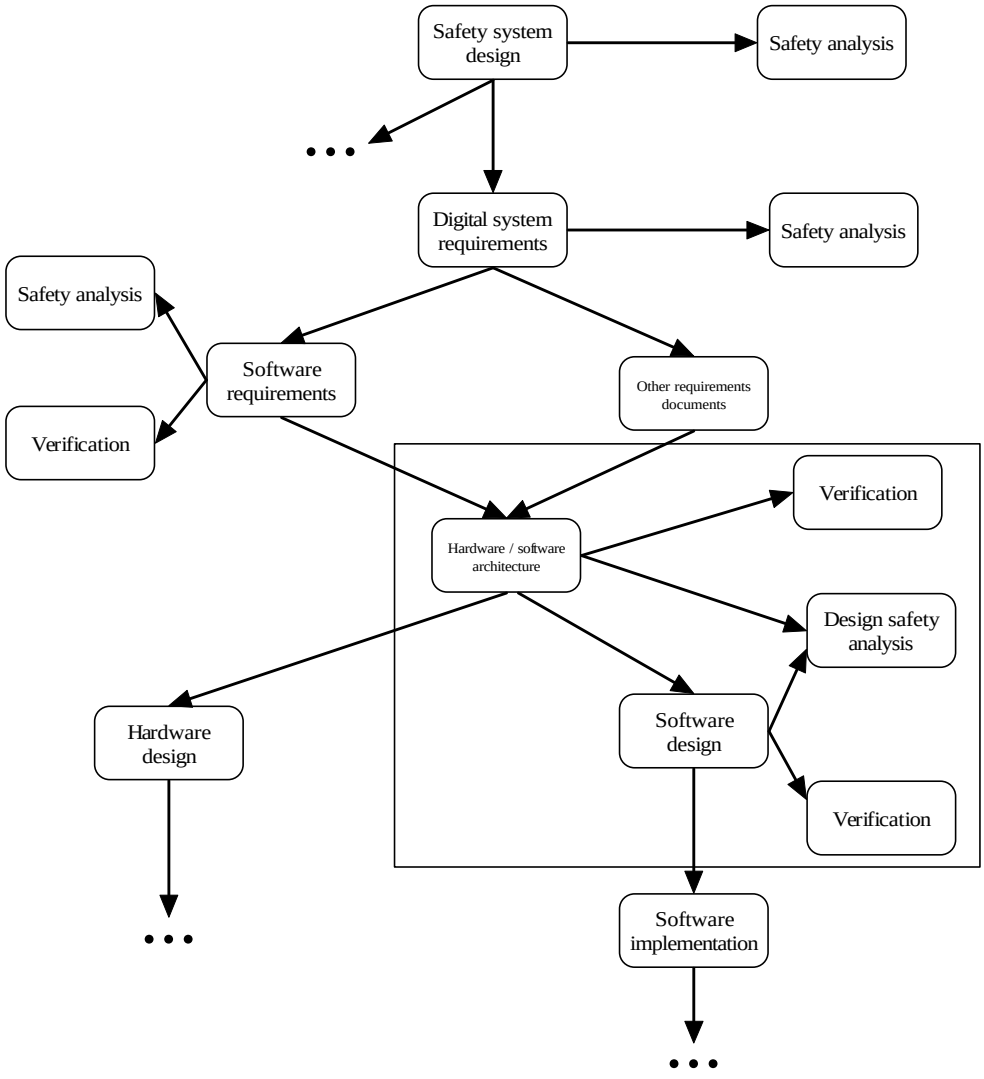

그림 1. 안전계통 개발공정

원전 안전계통 디지털 시스템의 설계는 일반적으로 구조설계와 상세설계의 2단계를 거친다. 소프트웨어 설계는 이를 상위레벨 설계와 상세설계로 구분한다. 실시간 시스템의 경우에는 소프트웨어 구조와 하드웨어 구조의 분리가 어렵기 때문에, 구조설계와 상위레벨 설계를 하나의 공정으로 간주한다.

그림 1과 같이 이 절차서는 엄격한 안전계통 개발공정을 전제로 하며, 전반적인 안전계통 요구사항과 설계가 먼저 수행되어 있다고 가정한다. 이 설계는 안전계통의 디지털 시스템에 대한 요구사항과 디지털 시스템의 소프트웨어 요구사항을 생산한다고 가정한다. 디지털 시스템과 소프트웨어 요구사항은 디지털 시스템의 하드웨어/소프트웨어 구조를 도출하는 데에 사용된다. 이 구조는 다시 하드웨어와 소프트웨어의 상세설계로 이어진다. 이후 소프트웨어의 구현, 시험(testing) 등의 공정이 요구되며 이 각 공정에서 검증과 안전성 분석이 수행되어야 한다.

2. 원전 안전계통 소프트웨어 개발 관련 법적 기준

원전 안전계통 소프트웨어 개발의 법적 기준은 상위 원자력법을 만족하기 위한 과학기술부 고시 "원자로시설의 계측제어계통에 관한 기준" 중에서 안전계통 소프트웨어의 확인, 검증, 검토, 감사를 위한 기준인 별지15에서 규정하는 내용과 관련 산업표준이다. "원자로시설의 계측제어계통에 관한 기준"은 원자로시설등의 기술기준에 관한 규칙 제20조・제25조·제26조・제27조에 의한 원자로시설의 계측제어계통에 관한 사항을 규정함을 목적으로 한다.

이 기준의 별지 15 "원전의 안전계통에 사용되는 디지털 컴퓨터 소프트웨어의 확인, 검증, 검토 및 감사"는 Reg. Guide 1.168을 참조하여, 1986년에 발행된 IEEE Std. 1012 "소프트웨어 확인 및 검증에 대한 기술기준"과 1988년에 발행된 IEEE Std. 1028 "소프트웨어 검토 및 감사에 대한 기술기준"을 다음 항목에 대한 단서 조항을 붙여서 적용하고 있다.

1. 필수 소프트웨어
2. 소프트웨어 신뢰도
3. 소프트웨어 확인 및 검증의 독립성
4. 설계변경
5. 자재의 일치
6. 품질보증
7. 소프트웨어 개발도구
8. 확인 및 검증 작업

IEEE Std. 1012-1986과 IEEE Std. 1028-1988의 여러 절에는 산업코드와 기술기준을 참고하고 있다. 이와 같이 참조된 기술기준들은 개별적으로 처리되어야 한다. 만약 어떠한 참조기술기준이 과학기술부(규제기관)의 법령·고시(규제법규)에 포함된 것이라면 사업자(피규제자)는 해당 법령·고시(규제법규)에 기술된 기술기준을 준수해야한다. 또한, 만약 참조된 기술기준이 별지에서 승인된 것이라면 별지에서 기술된 것과 같은 규제요건을 만족하는 허용 가능한 방법들을 포함하고 있다. 그러나 만약 참조된 기술기준이 별지에서 승인되지도 않고 과학기술부(규제기관)의 법령·고시(규제법규)에 포함된 것이 아니라면 사업자(피규제자)는 참조된 기술기준이 기존의 규제 관행과 일관성이 있고 적절히 검증되었다는 전제하에 참조된 기술기준에 제시된 정보를 이용할 수 있다.

별지 15 "원전의 안전계통에 사용되는 디지털 컴퓨터 소프트웨어의 확인, 검증, 검토 및 감사"가 규정하고 있는 1986년에 발행된 IEEE Std. 1012 "소프트웨어 확인 및 검증에 대한 기술기준"과 1988에 발행된 IEEE Std. 1028 "소프트웨어 검토에 대한 기술기준"은 이미 10년 이상된 산업표준이다. 따라서 본 논문에서는 이 산업표준의 최근판인 IEEE Std 1012-1998과 IEEE Std. 1028-1997을 KNICS 소프트웨어 설계명세에 대한 확인, 검증 및 검토 기술기준으로 선택하였다. 이 표준들이 별지에서 참조된 것은 아니지만 기존 기술기준과 일관성이 있고 소프트웨어 산업의 빠른 발전 속도와, 이 분석을 바탕으로 개발된 소프트웨어 설계명세 검증절차서가 향후 10년 이후에 사용될 소프트웨어의 개발에 사용될 것이므로 가능하면 최근 기술기준을 참고할 필요가 있다.

표1. 설계단계 소프트웨어 확인 및 검증에 대한 기술기준 비교

	IEEE 1012-1986			IEEE 1012-1998
1	소프트웨어 설계 추적성 분석		1	소프트웨어 설계 추적성 분석
2	소프트웨어 설계 분석		2	소프트웨어 설계 분석
3	소프트웨어 설계 연계 분석		3	소프트웨어 설계 연계 분석
4	시험 계획 생성		4	중요도(Criticality) 분석
4a	단위/모듈 시험		5	단위/모듈 시험
4b	통합 시험		6	통합 시험
5	시험 설계 생성 및 평가		7	시험 설계 생성 및 평가
			8	위해도(Hazard) 분석
			9	위험도(Risk) 분석

3. 원전 안전계통 소프트웨어 규제지침

법적 기준인 과기부고시에서 사용하는 산업표준에 대한 규제지침의 일치성을 분석하기 위한 비교대상은 한국원자력 안전기술원의 “원자력발전소 컴퓨터-기반 계측제어계통에 개한 안전규제 일반원칙 및 규제지침” 중 부록 1의 개발 소프트웨어에 대한 평가기준이다. 이 부록은 NUREG-0800, BTP HICB-14의 디지털 컴퓨터-기반 계측제어계통의 소프트웨어 검토에 관한 지침을 기반으로 작성된 것이다.

소프트웨어가 안전계통 소프트웨어에 중요한 각 특성을 갖고 있는지를 결정하기 위해 사용되어야 할 기준을 기술한다. 기준은 먼저 생명주기 활동그룹별로 이루어져 있고, 그 다음에는 설계 결과물 별로 그리고 특성 별로 이루어졌다. 이 절에서 기술된 설계 결과를 마련하기 위해 정형 또는 준 정형 방법이 사용될 수 있다. "NUREG 0800 SRP Section C.3 of Appendix 7.0-A"는 그러한 방법의 장점과 그 방법으로 작성된 설계 결과물 검토의 주의점을 기술하고 있다. 수용기준은 아래 표에 나타난 바와 같이 만족해야 할 기능상 특성과 공정상 특성 집합으로 구분된다.

표2. 안전계통 소프트웨어 수용기준 특성

기능 특성	공정 특성
정확성	완전성
기능성	일관성
신뢰성	정확성
강인성	스타일
안전성	추적성
보안성	명확성
타이밍	확인성

이러한 개발 소프트웨어에 대한 평가기준은 소프트웨어 수명주기 공정계획에 대한 기준, 소프트웨어 수명주기 공정이행에 대한 기준과 소프트웨어 수명주기 공정 설계결과물에 개한 기준으로 구성되어 있다. 여기서 소프트웨어 수명주기 공정 설계결과물에 개한 기준은 다시 요구사항활동, 설계활동, 구현활동, 통합활동, 설치활동 등으로 구성되어 있다. 본 논문에서는 아래 표 3와 4에서와 같이 설계활동에 대한 규제지침을 비교대상으로 한다.

표3. 안전계통 소프트웨어 구조설계 승인기준

소프트웨어 구조설계	
(가) 기능적 특성	각 기능적 특성에 대해서 그 특성에 맞게 소프트웨어에 부과된 요건이 소프트웨어 구조에서 만족되어야 한다. 소프트웨어 구조 검토는 하드웨어 구조 검토와 병행해서 이루어져야 한다. 소프트웨어 구조내용에서 다루어질 기능적 특성은 신뢰도, 안전성, 보안성, 그리고 타이밍이다.
신뢰도	요건은 통합된 하드웨어와 소프트웨어 구조에서 각 개별 소프트웨어 구성분의 고장이 안전성을 해치지 않도록 해야 함을 요구한다. 소프트웨어 구조에서는 오류 검출시에 취해야 할 동작을 파악해야 한다. 하드웨어와 소프트웨어 구조는 그 검토를 통해서 오류의 파급이 잘 체계화된 모듈 설계로서 통제되고 있음을 확인해야 한다.
안전성	요건은 소프트웨어 구조가 새로운 위험요소을 안전계통에다 넣어서는 안됨을 요구한다. 안전성 기능은 정상운전 및 정상적인 기능과는 잘 정의되고 엄격히 통제된 인터페이스를 통해서 분리되어야 한다. 어떠한 기동중 보수설비도 포함되어야 한다. 하드웨어와 소프트웨어 구조는 그 검토를 통해서 단일고장, 채널분리와 등급 1E와 비등급 1E 시스템의 분리와 같은 기준을 위반하지 않음을 확인해야 한다. 그 검토에서는 구조배치의 결과로서 안전계통에 새로운 위
보안성	요건은 그 구조가 확인된 보안 위협요소을 정확하게 처리하고, 그리고 새로운 보안 위협요소를 만들지 않아야 함을 요구한다.
타이밍	요건은 구조 설계에서 모든 타이밍 제한사항, 각각을 처리하기 위한 전략, 요구된 여유도, 그리고 그러한 여유도를 측정하는 방법을 기술해야 함을 요구한다. 각 구조 요소에 대한 타이밍 명세서, 즉 실행을 위한 최소와 최대 시간이 주어져야 한다. 스케쥴링 메카니즘과 공정간 통신방법이 기술되어야 한다. 그 구조는 작동이 정확한 순서에 따라 수행되도록 해야 한다. SRP 7.9절에는 디지털 데이터 통신시스템에 관한 추가지침을 제시하고 있다.
(나) 개발공정 특성	소프트웨어 구조내용이 갖추어야 할 소프트웨어 개발공정 특성은 완전성, 일관성, 추적성, 그리고 확인성이다.
완전성	요건은 모든 소프트웨어 요건이 구조에서 만족되어야 함을 요구한다. 소프트웨어 구조내용은 초기화, 운전, 정지, 보수, 그리고 시험 모드들을 비롯한 소프트웨어 요건명세서에 정해진 모든 동작모드들을 다루어야 한다.
일관성	요건은 각 소프트웨어 구성분이 소프트웨어 요건명세서, 하드웨어 구조, 문서화된 내용과 운전 및 하드웨어 환경과, 기타 소프트웨어 구성분의 알려진 특성과 적합해야 함을 요구한다. 각 소프트웨어 구성분의 타이밍 명세서는 그것이 서로 작용하는 다른 구성분의 명세서와 시스템 전체의 예상된 성능과 일치해야 한다. 균일하고 일관된 용어, 기호법, 그리고 정의가 사용되어야 한다.
스타일	요건은 소프트웨어 구조내용이 이해할 수 있어야 함을 요구한다. 그 구조내용은 개발자의 스타일 지침을 따라야 한다. 구조명세서는 구조 결정에 합당한 이유를 제시해야 한다.
추적성	요건은 소프트웨어 요건명세서의 각 요건과 구조의 성분 간에 양방향 추적이 가능해야 함을 요구한다. 구성분과 상세한 설계 요소 간의 양방향 추적이 되어야 한다. 각 구조 성분에서부터 그 성분이 정확하게 설계되었는지를 확인하기 위한 특정한 검사, 분석 또는 시험에 이르기까지 전방향 추적을 할 수 있어야 한다.
확인성	요건은 그 구조가 소프트웨어 요건을 만족하고 있는지를 확인하기 위한 특정한 분석, 검토, 또는 시험을 가능하게 해야 함을 요구한다.

표 4. 안전계통 소프트웨어 상세설계 승인기준

소프트웨어 상세설계	
(가) 기능적 특성	각 기능적 특성에 대해서 그 특성에 맞게 소프트웨어에 부과된 요건이 소프트웨어 설계에서 충족되어야 한다. 소프트웨어 설계명세서에서 다루어질 제품의 기능적 특성은 정확도, 신뢰도, 강인성, 안전성, 보안성, 그리고 타이밍이다.
정확도	요건은 모든 계산이 그 계산을 위한 정확도 요건이 만족될 수 있도록 지정되어야 함을 요구한다. 특히, 부동소수점 산술은 피해야 하며; 만약 그럴 수가 없다면 계산의 정확도를 유지하기 위해 특별한 주의가 요구된다. 설계에서는 입력 변수의 값이 적절한 범위내에 있는지를 결정하기 위한 방법, 소프트웨어가 적절한 범위내에 있지 않은 입력 변수의 값을 검출해 낼 방법, 그리고 후자의 경우 취해져야 할 동작을 지정해야 한다. 모든 계산은 수렴, 반올림 오차
신뢰도	요건은 상세한 소프트웨어 설계에서 각 개별 구성분의 단일 고장이 안전계통의 고장을 일으키지 않도록 해야 함을 요구한다.
강인성	요건은 설계에서 예상치 못한, 부정확한, 애매한, 그리고 부적당한 (1) 입력, (2) 하드웨어 거동, 혹은 (3) 소프트웨어 거동이 생길 때 소프트웨어가 정확하게 동작할 것인지를 요구한다. 특히 소프트웨어가 그러한 조건에서 고장나서는 안되며, 부정확한 출력을 만들어서도 안된다. 비록 적용하는 데에 있어서 논리적으로 불가능할지라도 장치에 물리적으로 가능한 입력변수의 값에 신중을 기해야 한다.
안전성	요건은 상세한 설계에서 새로운 안전성 위험요소가 안전계통에 들어가지 않도록 해야 함을 요구한다.
보안성	요건은 무단 변경이 금지되고, 검출 또는 적절히 완화되게 요구한다.
타이밍	요건은 입력과 응답 간의 시지연이 결정적이어야 함을 요구한다.
(나) 개발공정 특성	소프트웨어 설계명세서는 다음과 같은 각 소프트웨어 개발공정 특성: 완전성, 일관성, 정확성, 스타일, 추적성, 명확성 그리고 확인성을 갖추어야 한다.
완전성	요건은 상세 설계에서는 각 입력변수의 전체구간(예, 계기 입력 또는 클럭/캘렌더 시간의 전범위)에서 각 소프트웨어 단위의 동작을 지정해야 함을 요구한다. 설계는 구현이 가능할 만큼 충분히 완벽해야 한다. 소프트웨어 요건명세서에서 예상된 모든 상황에서의 동작이 지정되어야 한다. 장비, 인간, 하드웨어, 그리고 소프트웨어 인터페이스들이 정확하고 철저하게 지정되어야 한다. 방정식, 알고리즘, 그리고 제어논리가 정확하고 철저하게 지정되어야 한다.
일관성	요건은 상세 설계가 구조 설계와 일치하고, 그리고 상세한 설계 요소들이 상호간에 일치하도록 요구한다. 설계 요소들은 소프트웨어가 실행하게 될 운전환경의 문서화된 내용과 알려진 특성과 일치해야 한다. 소프트웨어 설계에서 정해진 입력과 출력 명세서는 하드웨어 또는 기성 소프트웨어 제품에 부과된 인터페이스 요건과도 일치해야 한다. 각 상세한 설계요소의 타이밍 명세서는 그것이 일부인 구조 요소의 타이밍 명세서와 일치해야 한다. 소프트웨어 설계에서 정해
정확성	요건은 모든 방정식, 알고리즘, 그리고 제어논리가 예상 가능한 오류에 대해서 평가되어야 함을 요구한다. 모든 방정식과 알고리즘은 코딩이 될 만큼 충분히 상세하게 정의되어야 한다. 데이터 체제설계에서는 코드 요소들이 정확하게 데이터를 초기화하고, 정확하게 저장된 데이터로 접근하고, 그리고 정확하게 데이터를 스케일할 것임을 보장해야 한다. 상세 설계에서는 데이터 항목이 초기화 되기 전에 사용될 수 없게 하고, 그 값이 예상치 못하게 변하지 않게 하고
스타일	요건은 상세한 설계문서의 기술내용이 개발자의 스타일 지침을 따라야 함을 요구한다. 상세 설계의 각 요소가 지정되어야 한다. 상세한 설계문서는 설계결정에 합당한 이유를 수록해야 한다. 프로그래밍 언어의 표준이 명시되어야 한다. 상세한 설계문서에서는 정당성이 없이는 사용되지 않을 언어특성을 명시해야 한다.
추적성	요건은 상세 설계의 요소들과 구조의 요소 간에 양방향 추적이 가능해야 함을 요구한다. 상세한 설계요소들과 코드 요소 간에도 양방향 추적이 되어야 한다. 각 상세한 설계요소에서부터 그 요소가 정확하게 설계되었는지를 확인하기 위한 특정한 검사, 분석 또는 시험에 이르기까지 전향 추적을 할 수 있어야 한다.
확인성	요건은 그 설계가 소프트웨어 구조를 만족하고 있는지를 확인하기 위한 특정한 분석, 검토, 또는 시험을 가능하게 해야 함을 요구한다.

4. 과학기술부 고시 지정 산업표준과 규제지침 승인 기준의 비교

과학기술부 고시인 법적 기준과 인허가 기관의 규제지침을 모두 만족하는, KNICS 안전계통 소프트웨어 검증에 사용할 원전 안전계통 소프트웨어 설계명세 검증절차서를 개발하기 위해서는 법적기준, 산업표준, 규제지침 등을 상호비교 할 필요가 있다.

표 5. 안전계통 소프트웨어 설계의 확인 및 검증을 위한 산업 표준의 승인기준

추적성분석	**요건(SRS 및 IRS)에 대한 설계요소(SDD 및 IDD)와 설계요소에 대한 요건을 추적하고, 정확성, 일관성, 그리고 완전성을 분석한다. 직무기준(Task Criteria)는 아래에 설명된다.**
정확성	**각 설계요소와 소프트웨어 요구 사항 사이의 관계를 검증한다.**
일관성	**설계요소와 소프트웨어 요구 사항 사이의 관계성이 일정한 상세수준까지 명세되는지를 확인한다.**
완전성	**모든 설계요소가 소프트웨어 요구사항으로부터 추적되고, 모든 소프트웨어 요구사항 들은 설계요소까지 추적할 수 있는지를 확인한다.**
소프트웨어 설계평가	**정확성, 일관성, 완전성, 정밀도, 가독성, 그리고 시험가능성에 대한 설계요소(SDD 및 IDD)를 평가하며, 직무기준(Task Criteria)는 아래에 설명된다.**
정확성	**원시코드 컴포넌트가 (1) 소프트웨어 설계를 만족하는지, (2)표준, 참조, 규제, 정책, 법규, 그리고 영업전략을 따르는지 확인검증하고, 그리고 (3) 논리나 데이터 흐름을 사용하는 상태들과 상태변경의 원시코드 컴포넌트 순서가 전문기술, 시제품 결과, 공학원리, 그리고 성능요건과 합쳐지는지 확인검증한다.**
	(4) 데이터 및 제어흐름이 기능 및 성능요건을 만족하는지 검증한다.
	(5) 데이터 사용과 형식을 검증한다.
	(6) 코딩방법과 표준의 적절성을 평가한다.
일관성	**모든 용어 및 코드 개념들이 일관되게 문서화되는지 검증하고, 원시코드 컴포넌트 사이에 내부 일관성이 유지되는지를 확인한다.**
완전성	**(1) 계통의 가정들과 제한 내에서 SDD에 다음 요소들이 있는지 확인한다.**
	- 기능성(즉, 알고리듬, 상태/모드정의, 입출력 검증, 예외처리, 보고 및 로깅)
	- 공정정의 및 스케쥴링
	- 하드웨어, 소프트웨어, 그리고 사용자 인터페이스 명세
	- 성능기준 (즉, 타이밍, 크기, 속도, 용량, 정확도, 정밀도, 안전성, 보안성)
	- 필수 형상데이터
	- 계통, 디바이스, 그리고 소프트웨어 제어(즉, 초기화, 트랜잭션과 상태 모니터링, 그리고 자체시험)
	(2) SDD 및 IDD가 명세된 형상관리 절차를 만족하는지 확인한다.
정밀도	**논리, 계산, 그리고 인터페이스 정밀도(즉, 버림과 올림)가 계통환경에서 요건을 만족하는지 검증하고, 모델된 물리적 현상이 계통 정확도 요건과 물리 법칙을 따르는지 점검한다.**
가독성	**문서화가 의도된 독자에게 읽기에 쉽고 이해할 수 있으며 애매모호하지 않은지 검증하고, 모든 두문자어, 연상(mnemonics), 약어, 기호, 그리고 설계 언어를 정의하는지 검증한다.**
시험가능성	**각 소프트웨어 설계요소가 계통설계를 검증하기 위한 객관적인 승인기준이 있는지 확인하고, 각 소프트웨어 설계요소가 객관적인 승인기준에 대하여 시험 가능한지 확인한다.**
인터페이스 분석	**소프트웨어 설계가 하드웨어, 사용자, 운전원, 소프트웨어, 그리고 다른 계통들과 정확성, 일관성, 완전성, 정확도, 그리고 시험가능성에 대하여 연계하는지 확인검증한다. 직무기준은 아래와 같다.**
정확성	**계통요건의 문맥표현으로 외부 및 내부 소프트웨어 인터페이스 설계를 검증한다.**
일관성	**인터페이스 설계가 SDD와 IDD 사이에 일관성이 유지되는지 확인한다.**
완전성	**각 인터페이스가 명세되고 데이터 형식과 성능기준(즉, 타이밍, 대역폭, 정확도, 안전성, 보안성)을 포함하는지 확인한다.**
정밀도	**각 인터페이스가 요구 정밀도를 갖는 정보를 제공하는지 확인한다.**
시험가능성	**인터페이스 설계를 검증하기 위한 객관적인 승인기준이 있는지 확인한다.**

표 5. 안전계통 소프트웨어 설계의 확인 및 검증을 위한 산업 표준의 승인기준(계속)

필수성 분석	SDD와 IDD를 사용하여 이전의 필수성 직무분석보고서로부터 현존 필수성 분석결과를 검토하고 수정한다. 구현방법과 연계방법론은 미리 부여된 소프트웨어 무결성 수준이 주어진 소프트웨어 요소(요구사항, 모듈, 함수, 하부계통, 다른 소프트웨어 분할)에 대하여 높이거나 낮출 수 있도록 한다. 일관되지 않거나 요구되지 않는 소프트웨어 무결성 결과들은 개정된 소프트웨어 무결성 수준을 검토함으로써 개입되지 않음을 검증한다.
컴포넌트 확인검증 시험계획 생성 및 검증	*(소프트웨어 무결성 수준 3과 4에 대하여)* 소프트웨어 컴포넌트(즉, 단위, 원시코드, 모듈)가 정확하게 컴포넌트 요구사항을 구현하는지 검증하기 위한 컴포넌트 확인검증 시험을 계획한다. 직무기준은 (1) 설계요건과의 일치성, (2) 타이밍, 크기, 그리고 정밀도 평가, (3) 경계와 인터페이스, 그리고 스트레스와 오류조건에서의 성능, 그리고 (4) 요구사항 시험범위와 소프트웨어 신뢰성 및 유지보수성 측정 등이다. 시험설계, 케이스, 절차, 그리고 결과에 대한 설계요건 추적을 계획하고, 시험직무와 결과의 문서화를 계획한다. 컴포넌트 확인검증 시험계획이 프로젝트에서 정의된 시험문서화 목적, 형식, 그리고 내용(즉, IEEE Std. 829-1983)과 일치하는지 확인하고, 컴포넌트 확인검증 시험계획이 다음 기준을 만족하는지 검증한다.
	(1) 소프트웨어 요구사항과 설계에 추적가능
	(2) 소프트웨어 요구사항 및 설계와 외부 일관성
	(3) 단위 요구사항 사이에 내부 일관성
	(4) 단위 요구사항의 시험범위
	(5) 소프트웨어 통합과 시험가능성
	(6) 운영과 유지보수 가능성(즉, 사용자 요구사항에 부합하여 운영되고 유지되는 능력)
통합 확인검증 시험계획생성 및 검증	*(소프트웨어 무결성 수준 3과 4에 대하여)* 각 소프트웨어 컴포넌트(즉, 단위나 모듈)가 다른 각각의 컴포넌트와 점진적으로 통합되는 것으로써 정확하게 소프트웨어 요구사항과 설계를 구현하는지 검증하는 통합 시험을 계획한다. 직무기준은 (1) 각 통합단계에서 기능요건의 매우 큰 집합과 일치성, (2) 타이밍, 크기, 그리고 정밀도 평가, (3) 경계들과 스트레스 조건에서의 성능, 그리고 (4) 요구사항 시험범위와 소프트웨어 신뢰성 측정 등이다. 시험설계, 케이스, 절차, 그리고 결과에 대한 요구사항 추적을 계획하고, 시험직무와 결과의 문서화를 계획한다. 통합 확인검증 시험계획이 프로젝트에서 정의된 시험문서 목적, 형식, 그리고 내용(즉, IEEE Std. 829-1983)과 일치하는지 확인하고, 통합 확인검증 시험계획이 다음 기준을 만족하는지
	(1) 계통 요구사항에 추적가능
	(2) 계통 요구사항과의 외부 일관성
	(3) 내부 일관성
	(4) 소프트웨어 요구사항의 시험범위
	(5) 사용된 시험표준과 방법의 적절성
	(6) 예상된 결과에 대한 일치성
	(7) 소프트웨어 자격시험의 가능성
	(1) 운영과 유지보수 가능성(즉, 사용자 요구사항에 부합하여 운영되고 유지되는 능력)
확인검증 시험설계 생성 및 검증	*(소프트웨어 무결성 수준 3과 4에 대하여)* (1) 컴포넌트 시험, (2) 통합시험, (3) 계통시험, 그리고 (4) 승인시험을 위한 시험(test)을 설계하고, 확인검증 시험계획서가 요구하는 추적을 한다. 확인검증 시험설계가 일치하는지 확인한다.
위해도 분석	논리 설계와 관련 데이터 요소가 필수 요구사항을 정확하게 구현하고 새로운 위해요소를 추가 하지 않았음을 검증한다.
위험도 분석	지금까지의 문서를 토대로 위험도 분석을 검토하고 수정한다. 과제 위험을 완화, 제거, 감소하기 위한 권고사항을 제공한다.

분석대상인 법적 기준은 과학기술부 고시 "원자로시설의 계측제어계통에 관한 기준" 중에서 안전계통 소프트웨어의 확인, 검증, 검토, 감사를 위한 기준인 별지15에서 규정하는 내용과 관련 산업표준이다. 이에 대한 일치성을 분석하기 위한 비교대상은 한국원자력안전기술원의 "원자력발전소 컴퓨터-기반 계측제어계통에 개한 안전규제 일반원칙 및 규제지침" 중의 개발 소프트웨어에 대한 평가기준이다.

안전계통 소프트웨어 설계명세서의 확인 및 검증을 위한 산업 표준과 규제지침에서의

승인기준 특성을 비교하면 표 6과 같다. 이 표에서 알 수 있는 것은 규제지침에서는 소프트웨어 설계를 구조설계와 상세설계로 나누어 각각의 기능적 측면과 개발공정 측면에서의 승인 기준을 제시하고 있는 반면에, 산업표준에서는 소프트웨어 설계를 하나의 단계로 보고 필요한 확인 검증 행위별로 승인기준 특성을 제시하고 있는 점이 다르다.

표 6. 산업 표준과 규제지침 승인기준 특성 비교

	산업표준(IEEE 1012-1998)	승인기준특성
1	소프트웨어 설계 추적성 분석	
		정확성
		일관성
		완전성
2	소프트웨어 설계 분석	
		정확성
		일관성
		완전성
		정보의 정확성
		가독성
		시험성
3	소프트웨어 설계 연계 분석	
		정확성
		일관성
		완전성
		정보의 정확성
		시험성
4	중요도(Criticality) 분석	
5	단위/모듈 시험	
		정확성
		일관성
		완전성
		정보의 정확성
		타이밍
		강인성
		신뢰성
6	통합 시험	
		정확성
		일관성
		완전성
		정보의 정확성
		타이밍
		강인성
		신뢰성
7	시험 설계 생성 및 평가	
8	위해도(Hazard) 분석	
		안전성
9	위험도(Risk) 분석	
		신뢰성

규제지침(BTP-14)	승인기준 특성
소프트웨어 구조설계	
(가) 기능적 특성	
	신뢰도
	안전성
	보안성
	타이밍
(나) 개발공정 특성	
	완전성
	일관성
	스타일
	추적성
	확인성
소프트웨어 상세설계	
(가) 기능적 특성	
	정확성
	신뢰도
	강인성
	안전성
	보안성
	타이밍
(나) 개발공정 특성	
	완전성
	일관성
	정확성
	스타일
	추적성
	확인성

그러나 산업표준과 규제지침에서 제시하고 있는 승인기준 특성들은 유사한 점이 많았다. 이러한 유사성을 연결 매개체로 활용하여 산업표준과 규제지침을 모두 만족시킬 수 있는 안전계통 소프트웨어 설계명세 검증 절차서를 개발할 수 있었다. 즉, 규제지침 승인

기준에서 제시하는 각각의 기능적 측면과 개발공정 측면에서의 기준들을 산업표준에서의 확인 검증 행위별로 승인기준에 일치시킴으로서 두 가지 체계에서 요구되는 승인기준을 모두 만족시킬 수 있었다.

5. 원전 안전계통 소프트웨어 설계명세 검증절차서

규제지침(BTP-14)에는 설계검토 단계에서 활용할 수 있는 승인기준(acceptance criteria)을 가지고 있다. 이 관점은 특성(characteristics) 으로 정의되는 14개의 카테고리로 나눌 수 있다. 원전 안전계통 소프트웨어 설계명세 승인기준으로 구조설계 관련하여 9개 승인항목과 상세설계 관련한 12개 항목별로 승인기준을 만족하기 위한 지침으로 250여개의 질문의 조합을 개발하였다.

이러한 질문 리스트는 원전 안전계통 소프트웨어 설계검토를 위해 과학기술부 고시가 지정하는 산업표준인 IEEE Std. 1028-1997을 만족하기 위한 검토 항목으로 사용된다. 하드웨어/소프트웨어 구조와 소프트웨어 설계명세에 대해서는 정형검토(formal reviews)를 권고한다. 설계 검토를 위한 일반적인 방법론은 US NRC Reg. Guide 1.168로 인증한 IEEE Std. 1028에서 찾을 수 있다. 이 표준에서는 다섯 가지의 검토유형에 대하여 논하고 있다. IEEE Std. 1028의 용어정의에 따르면, 설계검토는 기술적인 검토를 의미한다. 정형검토는 요구사항(requirements)을 평가하는 전형적인 방법론이다. 이 방법은 노동집약적이며, 따라서 비용이 많이 드는 작업이다. 그러나, 이 방법은 개발 후반부까지 설계오류가 발견되지 않는 방법보다 비용 측면에서 더 효율적이다.

검토자는 다양한 전문지식을 가지도록 선택되어야 한다. 예를 들어, 해당분야 전문가, 개발자, 안전해석가, 그리고 시험자(tester)를 선택해야 한다. 각 검토자는 그들의 특정한 관점과 관련된 특정한 문제에 대해서 원전 안전계통 소프트웨어 설계명세 검증절차서에서 제시하고 있는 질문들을 사용하여 심사한다.

추가적으로 이러한 검토 질문 항목 중에서 보다 상세한 검증을 필요로 하는 핵심항목들을 골라 산업표준 (IEEE Std. 1012-1998)에서 제시하고 있는 원전 안전계통 소프트웨어 설계명세 검증행위별 승인기준에 반영하였고 이를 위한 구체적인 검증 방법을 개발하고 있다. 현재 이러한 검증방법의 하나로서 모델체킹과 같은 정형적 검증기법을 개발하고 있다.

표 7. 상세 검증 항목

S/W 설계 추적성 분석 검증 절차	
정확성 추적	• 소프트웨어 구조설계 설명서에는 소프트웨어 구조설계의 각 기능을 유일하게 확인할 수 있는 식별자(ID)를 가지고 있어서 구현(implementation)시 이들 식별자를 가지고 추적
	• 소프트웨어 상세설계 명세는 소프트웨어 상세설계 내의 각 기능을 특정하게 식별하도록 되어 있어 구축 시 특정하게 참조 될 수 있도록 되어 있는가?
일관성 추적	• 소프트웨어 구조설계 요소가 소프트웨어 요구사항 명세서와 일치하는지 확인하는데 사용하는 기법인 특별시험(specific tests) 또는 검증기준(validation criteria)을 이용하여 전향 추적을 할 수 있는가?
	• 각 소프트웨어 구조설계 요소는 소프트웨어 요구사항 명세서의 특별한 요소(specific elements)를 후향추적(backward trace) 할 수 있는가?
	(NPP 시스템 요건과 소프트웨어 요구사항 명세서간에 요건추적 매트릭스를 이용하여 추적성을 확인할 수 있다.)
	• 각 상세설계 요소는 특정시험 또는 상세설계 요소가 만족되었는가에 대한 요구사항을 확증하는데 이용될 검증 기준으로 전방향 추적기록이 가능한가?
	• 각 상세설계 요소가 소프트웨어 요구사항 명세(Software Requirements Specification)내 특정 요소들로 역방향 추적기록이 가능한가? 선호 대상 방법들로는 각 요구사항을 식별하고, 요구사항을 구축하는 계통부품(system component)을 식별하고, 요구사항을 발생시키는 계통 설계요소(system design elements)를 식별하고, 그리고 요구사항이 만족되었는지에 대한 시험을 식별하는데 사용되는 요구사항 추적기록 매트릭스(requirements tracing matrix) 등이
완전성 추적	• 소프트웨어 구조설계 설명서에 소프트웨어 요구사항 명세서에 기술된 요건의 범위를 벗어나는 어떤 기능을 포함하고 있다는 정당한 근거가 있다면 요건의 범위를 벗어난 소프트웨어 구조설계 설명서의 정당성 결과가 요구사항명세서와 일치하는가?
	• SRS에서 기술된 요구사항 범위가 아닌 기능들을 포함하는데 대해 정당성이 입증되어 있는가?
S/W 인터페이스 검토/분석 절차	
정확성	• 소프트웨어 구성요소간의 인터페이스가 정확하게 설계되었는지를 결정하기 위한 인터페이스 분석이 수행되었는가?
일관성	• 그 구조가 각 인터페이스의 요구되는 행동을 허용하는가?
	• 상세설계가 연계요소들에 대한 문서화된 기술이나 알려진 특성과 일관성이 있는가?
완전성	• 안전에 중요한 기능이 잘 정의되고 엄격하게 통제되는 연계에 의하여 정상운전 및 부가기능과 분리되어 있는가?
	• 소프트웨어 상세설계가 단위들 간의 규칙적이고 문서화된 연계를 사용하는가?
	• 모든 내부 및 외부연계가 완전하게 정의되었는가?
	• 소프트웨어 상세설계가 각 연계사항에 대하여 요구되는 프로그램의 행위를 구현하고 있는가?
정보의 정확성	• 인터럽트가 정확하게 처리되고 입출력 타이밍이 정확하며, 그리고 단위들이 정확하게 연계되는지 확증하기 위해 중요한 인터페이스(potential interface)와 타이밍 문제가 분석
	• 센서 및 구동기 설계연계가 신호의 동적범위, 정확성, 타이밍, 인터럽트 및 분해능을 포함하는가?
	• 상세설계 요소들 사이의 연계가 정확하게 설계되었는가를 결정하기 위한 설계 연계분석이 수행되었는가?
	• 자료 전송에 대한 표준연계가 있는가?
시험성	• 상세설계 요소들 사이의 인터페이스가 적절히 설계되고 안전위험(safety hazard)을 생성하지 않음을 결정하기 위해 수행되고 문서화된 설계 인터페이스 분석이 있었는가?

표 7. 상세 검증 항목(계속)

	• 상세설계 요소들 사이의 연계가 정확하게 설계되었는가를 결정하기 위한 설계 연계분석이 수행되었는가?
	• 자료 전송에 대한 표준연계가 있는가?
시험성	• 상세설계 요소들 사이의 인터페이스가 적절히 설계되고 안전위험(safety hazard)을 생성하지 않음을 결정하기 위해 수행되고 문서화된 설계 인터페이스 분석이 있었는가?
S/W (정형)설계 검증 절차	
정확성	• 모든 공식 및 알고리즘이 코딩이 시작될 수 있을 정도로 정확하게 또 충분히 상세한 수준까지 정의되어 있는가?
일관성	• 소프트웨어 구조설계에서 사용된 하나 이상의 정형기법(formal method)은 이들 상호간의 일치성을 유지하고 있는가?
	• 표현 스타일이나 상세정도가 소프트웨어 상세설계명세서 전반에 걸쳐 일관성이 있는가?
	• 소프트웨어 상세설계가 하드웨어 및 소프트웨어 구조와 일관성이 있는가?
완전성	• 소프트웨어 구조가 소프트웨어 설계명세, 안전성분석보고서, 요구사항명세서 등에 있는 모든 예상되는 상황과 조건을 고려하는가?
	• 모든 자료채널에 대한 개수, 크기, 자료속도, 샘플링 빈도 및 응답시간이 소프트웨어 상세설계 명세서에 정의되는가?
	• 소프트웨어 상세설계 명세서가 소프트웨어 요구사항 명세와 소프트웨어 구조설계 명세서에 기술된 시스템 요구사항 및 모든 제약조건들(기능, 성능, 안전성, 신뢰성 및 유지보수성 요구사항 포함)을 만족하는 소프트웨어 상세 설계를 기술하는가?
정보의 정확성	• 소프트웨어 상세설계에서 사용한 모든 계산들은 계산에 대한 정확성 요건을 만족하는가?
시험성	• 소프트웨어 구조설계 설명서는 각 소프트웨어 설계요소의 기능에 대하여 테스트할 수 있는 방법을 기술하고 있는가?
	• 소프트웨어 상세설계 명세에서는 시험 가능한 방법으로 각 소프트웨어 요소의 기능들을 기술하고 있는가?
가독성 (Readability)	• 소프트웨어 구조설계 설명서는 구조설계 요소들간의 관계성(relationship)을 기술하고 있는가?
	• 소프트웨어 상세설계 요소가 어떤 절차를 수행하면서 요소가 기능을 수행하는 방법에 대해서 소프트웨어 상세 설계명세에서 기술하고 있는가?
	• 소프트웨어 상세설계 명세에서 소프트웨어 상세설계의 일환으로 기술되는 구축 제약사항(implementation constraints)들에 대해서 모두 열거하고 있는가?
필수성 분석 (Criticality Analysis) 절차	구조설계, 상세설계, 인터페이스 설계 과정에서 전 단계 소프트웨어 요구명세 시 결정한 필수성 분석 결과를 재 조정한다.
S/W 시험 설계/ 절차	
컴포넌트 시험 계획 생성 및 검증	소프트웨어 유닛(Units) 및 모듈(Modules)이 정확하게 요구사항을 만족하는지 결정하는 단위시험을 계획한다. 이 평가의 기준은 경로(Path) 및 분기(Branch) 시험범위(Coverage)를 만족하도록 하며, 최소한 다음의 4가지를 포함해야 한다.
	- 설계 요구사항과의 부합성.

6. 결론

과학기술부 고시인 법적 기준과 인허가 기관의 규제지침을 모두 만족하는, KNICS 안전계통 소프트웨어 검증에 사용할 원전 안전계통 소프트웨어 설계명세 검증절차서를 개발하기 위해서는 법적기준, 산업표준, 규제지침 등을 상호비교 하였다.

이와 같은 비교분석을 바탕으로 원전 안전계통 소프트웨어 설계명세 승인기준으로 구조설계 관련하여 9개 승인항목과 상세설계 관련한 12개 항목별로 승인기준을 만족하기 위한 지침으로 250여개의 질문의 조합을 개발하였다.

추가적으로 이러한 검토 질문 항목 중에서 보다 상세한 검증을 필요로 하는 핵심항목들을 골라 산업표준 (IEEE Std. 1012-1998)에서 제시하고 있는 원전 안전계통 소프트웨어 설계명세 검증행위별 승인기준에 반영하였고 이를 위한 구체적인 검증 방법을 개발하고 있다. 현재 이러한 검증방법의 하나로서 모델체킹과 같은 정형적 검증기법을 개발하고 있다. 또한 새로운 기법의 개발과 병행하여 기 개발된 테스팅 기법과 검증 기법을 활용하여 가장 효과적인 상세 검증을 할 수 있는 절차서 개발이 필수적이다.

(알림)
본 연구는 원전 계측제어시스템 개발사업의 디지털 계측제어 인허가 기술개발 과제에서 수행되었음.

7. 참고문헌

[1] "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", IEEE Std 7-4.3.2-1993, Sep. 15, 1993.
[2] "IEEE Standard for Software Verification and Validation Plans", ANSI/IEEE Std. 1012-1986, 1987.
[3] "IEEE Standard for Software Verification and Validation Plans", ANSI/IEEE Std. 1012-1998, 1998.
[4] "IEEE Standard for Software Reviews", ANSI/IEEE Std. 1028-1988, 1988.
[5] "IEEE Standard for Software Reviews", ANSI/IEEE Std. 1028-1997, 1997.
[6] NUREG-0800, Standard Review Plan: Chapter 7. Instrumentation and Controls , 1997
[7] IEEE Std. 610.12-1990, Standard Glossary of Software Engineering Terminology

[8] IEEE Std. 1074-1997, Standard for Developing Software Life Cycle Processes
[9] IEEE Std. 830-1998, Recommended Practice for Software Requirements Specifications
[10] IEEE Std. 1016-1998, Recommended Practice for Software Design Descriptions
[11] 과학기술부 고시(안) 제01 - X09호, 원자로시설의 계측제어계통에 관한 기준, 2001.
[12] 원자력발전소 컴퓨터-기반 계측제어계통에 대한 안전규제 일반원칙 및 규제지침, 초안 0, 한국원자력안전기술원, 1999.
[13] KNICS원전 안전계통 소프트웨어 설계 명세 검증 절차서, 초안, 한국원자력연구소, 2002.