'2001 춘계학술발표회 논문집
한국원자력학회

원전 디지털 계측제어계통의 규제 및 안전성 평가방향

Regulatory and Safety Evaluation Approach of Digital Instrumentation and Control Systems

오성헌, 김복렬, 김대일, 고정수, 황희수, 정충희

한국원자력안전기술원
대전광역시 유성구 구성동 19

요 약

원자력발전소의 계측제어분야는 컴퓨터기반 소프트웨어, 통신네트워크 및 인간-기계 연계 기술들을 바탕으로 기술혁신이 급속하게 이루어져 왔으며, 규제기술 적용 및 안전성 평가방법에 있어서도 변화를 요구하고 있다. 동 분야에 대한 규제기술은 미국 등 선진 외국에서도 명확하게 정립되지 않은 상태로써 향후 기술적으로 가장 많은 변화가 있을 것으로 전망되고 있으며, 이에 따라 관련 규제요건 및 기술기준 등이 지속적으로 보완·발전될 것으로 예상된다. 이와같은 상황에서 소프트웨어 확인 및 검증 방법, 심층방어 및 다양성분석, 전자기파 장해 문제, 실시간 성능 및 데이터통신계통 독립성 등이 지속적으로 연구되어야할 주요 규제 현안사항들이다. 본 논문에서는 가동중 원전의 디지털 설비개선이나 신규원전 및 차세대 원전에 적용되고 있는 컴퓨터기반 계측제어 시스템의 기술적인 규제현안사항을 포함하여 전반적인 디지털 계측제어계통에 대한 규제 및 안전성 평가방향을 제시한다.

Abstract

The instrumentation and control system of nuclear power plant has been a drastic change by introducing software-oriented digital system, digital data communication and man-machine interface technology. In response to this change, regulatory methodologies and approaches need to be changed. It is also expected that the regulatory methodology and approach which are not completely justified in the States as well as developed countries will be significantly changed in the future and regulatory requirements and standards will be also modified and supplemented continuously. In this context, the focused issues such as the methodologies of software verification/validation, the analysis of defense-in-depth and diversity, electromagnetic interference, the performance of real time, and the independence of data communication should be studied and resolved consistently. This paper presents regulatory issues and approaches of the digitalized instrumentation and control system which can be applied in the Korea Next Generation Reactor (KNGR), operating nuclear power plant (NPP) for upgrading or a new NPP.

1. 개 요

최근의 계측제어분야는 컴퓨터기반 소프트웨어공학기술, 통신네트워크기술 및 인간-기계 연계기술 등 기술혁신이 급속하게 이루어지고 있는 첨단 신기술분야로서 규제기술 적용 및 안전성 평가방법에 있어서도 현재까지 많은 변화가 있었다. 또한 동 분야에 대한 규제기술은 미국 등 선진 외국에서도 명확하게 정립되지 않은 상태로써 향후 기술적으로 가장 많은 변화가 있을 것으로 전망되고 있으며, 이에 따라 관련 규제요건 및 기술기준 등이 지속적으로 보완·발전될 것으로 예상된다.

오늘날 일반 산업계에서는 컴퓨터 시스템의 사용이 보편화되어 있으며, 최근에는 신규 및 차세대원전 설계분야의 원자력산업계에서도 시스템의 정확성, 보수성, 운전신뢰도의 향상과 기존 아날로그 계통설계의 한계성 극복을 위해 디지털시스템을 사용하고 있다. 특히 가동중인 원전에서도 기존 하드웨어 기기의 성능저하, 노후화된 기기를 교체할 만한 동등한 예비품 및 교체품 구입의 어려움 등으로 설비개선시에 점진적으로 컴퓨터기반 시스템을 도입하고 있다.[1] 지금까지 원자력 분야에서 컴퓨터기술의 적용이 억제되었던 주요 요인은 고장모드가 검증되지 않은 디지털기술이 안전성에 미칠 수 있는 영향을 완전하게 예측하지 못하기 때문이었다. 다시 말하면 컴퓨터기술이 정확하고 이상적으로 구현되면, 운전이득 뿐만 아니라 안전성을 향상시킬 수 있을 것으로 예상되지만, 만약 잘못 구현되면 안전성을 크게 저하시킬 수 있다. 다행히도 지금까지의 컴퓨터-기반 공정제어시스템에서 얻은 운전경험에 의하면, 대다수 설비들이 관련요건에 따라 적합하게 설계될 경우 안전성에 긍정적인 영향을 주고 있다는 점들이 확인되고 있다. 현재까지 관련 규제요건에 따라 디지털 기반 계측제어설비에 대해 주요하게 제기되고 있는 규제현안에는 디지털계통 및 기기의 설계검증, 소프트웨어에 대한 공통모드고장 대책, 심층방어 및 다양성분석, 소프트웨어 신뢰도 및 품질보증, 소프트웨어 확인 및 검증 방법, 전자기파 장해 문제, 실시간 성능 및 데이터통신계통 독립성 등이 있다. 따라서 본 논문에서는 가동중 원전의 디지털 설비개선이나 신규원전 및 차세대원전에 적용되고 있는 컴퓨터기반 계측제어시스템의 기술적인 규제현안사항을 포함하여 전반적인 디지털 계측제어계통에 대한 규제 및 안전성 평가방향을 제시한다.

2. 디지털 I&C계통 주요 현안사항

2.1 디지털 계통 및 기기의 설계검증

디지털 시스템은 시스템 기능구현 관점에서는 아날로그 시스템과 크게 다르지 않지만 동작 또는 운전 관점에서는 근본적으로 다르다. 즉 아날로그 시스템은 병렬적인 동작특성을 갖지만 디지털 시스템은 순차적인 동작특성을 갖고 있다. 이와 같은 동작특성의 차이점 때문에 디지털 계측제어시스템은 아날로그 시스템에 비해서 추가적인 설계 및 검증 방법들을 요구하게 된다. 아날로그 시스템은 정해진 입력범위에 걸쳐서 연속적인 성능을 보일 수 있기 때문에 이러한 특성이 아날로그 시스템과 기기의 설계를 검증할 때 이용되는 형식시험, 인수시험, 그리고 검사 시에 활용될 수가 있다. 만약 어떤 아날로그 시스템이 정해진 범위의 입력조건에서 연속적인 거동을 보이고 각 연속된 범위 내에서 제한된 갯수의 입력 샘플을 취해서 수행한 시험에서 허용 가능한 성능을 보여준다면, 샘플된 시험점들의 중간값에서 성

능은 높은 신뢰도와 허용 가능한 성능을 갖고 있는 것으로 평가할 수 있다.

이와 비교하여 디지털 계측제어시스템은 설계 및 구현의 사소한 오류에도 예측할 수 없는 거동을 보일 수 있다는 점에서 아날로그 시스템과는 기본적으로 다르다. 디지털시스템의 경우는 일반적으로 샘플된 입력조건에서 수행된 시험만으로는 전구간의 성능을 추론할 수가 없으므로, 디지털 시스템과 기기들의 검사, 형식시험, 그리고 인수시험 자체만으로는 신뢰도가 높은 설계검증이라고 할 수 없다. 따라서 디지털시스템의 설계검증내용에 대한 검토는 신청자가 설계요건에 따른 엄격한 명세서와 이행사항을 반영한 고품질의 개발공정을 채택하여 설계를 수행했는지를 확인하는 데에 중점을 두게 된다.

2.2 공통모드 고장 가능성 및 대비책

디지털 계측제어시스템은 아날로그 시스템에 비해서 코드, 데이터 전송, 데이터, 그리고 공정 장비를 훨씬 많이 공유할 수가 있다. 비록 이러한 공유가 디지털시스템의 커다란 장점이 되고 있지만, 그것은 또한 안전성관점에서 중요한 현안문제점들을 야기할 수 있다. 즉 공유된 데이터 또는 코드를 이용한 설계는 소프트웨어 오류로 인해서 공통원인 또는 공통모드 고장(CMF)을 파급시킬 가능성이 있으므로 하드웨어 구조물로써 달성된 다중성을 파기시킬 수도 있다.

어떤 한 채널에서 여러 가지 기능들을 수행하는 공정 장비를 공유하면 단일 하드웨어모듈의 고장결말이 커지게 되고 단일 안전채널내에서 가용한 다양성의 정도가 줄어들게 된다. 이러한 현안문제들 때문에 디지털 계측제어시스템에 대한 검토에서는 기능단위 내부에서와 기능단위 간의 공통모드고장 파급에 따른 대비책으로서 고품질과 심층방어 및 다양성설계가 강조되고 있다.

2.3 소프트웨어 신뢰도 및 품질보증

컴퓨터-기반 소프트웨어에 대한 신뢰도를 보장하기 위해서는 소프트웨어 개발과정의 수명주기 활동(계획, 요건, 구현, 통합, 검증, 설치, 운전 및 보수활동)에 대한 품질보증활동을 철저하게 평가하고 이를 확인 및 검증하게 된다. 이것은 소프트웨어의 특성상 개발이 완료된 상태에서 제품의 신뢰도를 평가하는 것이 매우 어려운 것으로 인식되고 있기 때문에 소프트웨어의 개발과정에 대한 신뢰성을 확인하기 위한 것이다. 즉 디지털계통의 신뢰도에 크게 영향을 미치는 인자는 소프트웨어 프로그램이며, 이는 기존의 아날로그 계통과는 달리 시험에 의한 방법으로는 신뢰도를 평가하는 것이 거의 불가능하다는 점이다. 따라서 소프트웨어에 대한 신뢰도를 보장하기 위해서는 컴퓨터 소프트웨어의 설계 및 설치단계에서 철저한 품질관리와 체계적인 검토가 이루어져야 하고 이에 대한 내용이 문서화됨으로써 추후 이에 대한 확인이 가능하여야 한다.

2.4 디지털 기기 검증

일반적으로 기존 원자력발전소의 아날로그계통 설계의 경우에도 안전관련 계통 또는 설비는 사전에 엄격한 기기검증 시험이 수행되어져 왔다. 원전기기에 사용되고 있는 성능검증시

험은 지진발생으로 인한 진동조건하에서 설비의 건전성을 보장하기 위한 내진검증시험과 원전 사고로 인한 극한 환경조건하에서 설비의 건전성을 보장하기 위한 내환경 검증시험으로 분류되어 진다. 따라서 이러한 기기검증 시험요건은 디지털설비의 경우에도 동일하게 적용되고 있다. 그러나 디지털설비의 경우에는 특히 낮은 전압레벨에서 운전되고 있어서 전자기파와 같은 주위의 환경인자에 민감하게 영향을 받을 수 있기 때문에 기존의 아날로그설비에서 크게 고려하지 않았던 전자기파 장해(EMI) 영향에 대한 대응능력(EMC)을 갖출 것을 요구하고 있다.

2.5 실시간 성능

실시간 디지털 계측제어계통은 발전소의 공정계통에서 요구되는 시간 제약조건에 응답하여야 하므로, 동 계통의 설계는 엄격한 성능요건을 고려해야 한다. 일반적으로 원자로 보호계통의 성능을 평가하기 위한 최소한의 척도로는 응답시간, 정확도와 측정범위를 들고 있다.

디지털 보호계통은 아날로그 보호계통과는 달리 성능관점에서 추가로 고려되어야 할 몇가지 현안사항들이 있다. 즉, 아날로그 보호계통의 동작모드는 병렬처리인 반면에 디지털계통의 동작은 일반적으로 직렬처리 특성을 갖기 때문에 디지털계통의 구성요소에 대한 타이밍 기준이 사고해석결과 또는 운영기술지침서의 응답시간 제한치를 만족할 수 있도록 엄격히 결정되어야 한다. 또한 디지털 보호계통의 정확도를 평가하는데 있어서도 아날로그계통과는 다른 입력수집방법을 사용하기 때문에 Aliasing 및 워드길이에 의한 영향을 고려해야 한다. 이와 같은 현안들이 디지털 보호계통의 실시간 성능을 떨어뜨릴 수 있으므로 이에 대한 철저한 평가가 필요하다.

2.6 데이터 통신계통 독립성

데이터통신계통은 일반적으로 특수한 하드웨어와 내장(embedded) 소프트웨어, 그리고 모(mother) 계통과 상호 연결된 컴퓨터에서 운영되는 통신규약(protocol) 소프트웨어로 이루어진다. 원자력발전소의 안전계통에 사용되는 데이터통신계통에 대한 규제현안으로는 데이터통신계통의 설계, 통신규약, 그리고 통신 매체(media) 등이 있다.

데이터통신계통의 구조는 일반적으로 동일한 채널의 컴퓨터들간 데이터통신, 다른 채널들간 데이터통신, 또는 안전등급이 서로 다른 컴퓨터들간 데이터통신 등으로 설계될 수 있다. 이와 같은 통신구조가 부적합하게 설계되면 모(mother) 계통(예, 원자로보호계통)의 안전기능 수행에 영향을 미칠 수 있다. 따라서 데이터통신계통은 통신 독립성과 계통 건전성에 관한 요건을 만족하여야 한다. 또한 같은 등급의 안전채널들 간에, 또는 낮은 등급의 통신채널에서 보다 높은 등급의 통신채널로의 고장 파급을 막기 위해 전기적 및 통신 격리기능이 보장되어야 한다.

3. 디지털 I&C 계통 평가방침

3.1 기본적인 평가방침

원자력발전소의 원자로 보호계통을 포함한 안전계통에 디지털기술을 이용한 컴퓨터-기반

계측제어시스템을 채택할 경우 동 시스템에 대한 안전성 검토와 평가를 위한 접근방식은 기존 원전의 계측제어설비에 적용된 규제요건(TMI, GSI요건 등 포함)을 포함하여 각종 규제문서에서 승인한 산업표준과 관례(IEEE Std. 등), 그리고 국내·외 규제기관의 인허가 사례·교훈 및 디지털기술에 관한 규제입장(Reg. Guide, SECY, NUREG Report 등)들을 추가로 적용해서 신청된 디지털시스템에 대한 안전성을 검토하고 평가한다. 이들 시스템에 대한 검토절차와 내용은 신청된 디지털시스템의 규모와 복잡성에 따라 다르게 적용될 수 있다.

3.2 일반 검토절차 및 내용

디지털 계측제어시스템의 일반적인 검토절차는 기존 원전의 경우와 크게 다르지는 않지만 신청된 디지털 설비에 대한 기술내용의 범위 및 복잡성, 국내 원자력관련법에 따른 변경허가절차, 그리고 특정기술주제보고서의 승인 신청 등을 고려해서 검토유형을 구분할 수 있으며, 이를 그림 1에 나타내었다. 그림에 나타나 있는 바와 같이 국내 원자력법에 따른 인허가사항들은 크게 신규원전의 건설/운영허가, 변경허가, 그리고 특정기술주제보고서의 승인 등으로 구분할 수 있다.[2]

원자력발전소에 대한 인허가신청서가 제출되면 그 신청서의 유형을 결정하고, 실질적인 검토가 이루어지기 이전에 그 신청서가 검토할 만한 충분한 정보를 담고 있는지를 확인한다. 특히 신규원전의 경우 안전성분석보고서는 안전심사지침서 7장 및 부록(7.0-1 등) 등의 세부 지침을 참고하여 작성·제출되어야 하고, 디지털 계측제어시스템에 대한 상세한 안전성검토는 동 지침서에 따라 수행된다.

어떠한 유형의 신청서에 대해서도 디지털시스템에 대한 안전성검토는 안전심사지침서[3,4]에 따라 모든 적용 가능한 소프트웨어 수명주기 활동들(계획, 요건, 설계, 구현, 통합, 검증, 설치, 운전 및 보수활동)에 대해서 검토한다. 이와 같은 검토에서는 시스템 요건의 적합성과 최종시스템이 요구되는 규제요건들을 만족하고 있는지를 확인한다. 컴퓨터를 사용하지 않은 시스템에 대해서는 기기와 시스템의 요건, 설계결과, 그리고 검증내용(예, 형식시험) 등에 중점을 두고 검토되며, 컴퓨터-기반시스템에 대한 검토에서는 소프트웨어 수명주기 활동에 따른 수락성과 정확한 이행내용을 확증하는 데에 검토의 중점을 두고있다. 신청서 유형별로 중점적으로 검토되는 내용을 요약하여 기술하면 다음과 같으며, 디지털 계측제어계통 개발 단계별 검토내용을 그림 2에 나타내었다.

(1) 건설허가(CP) 신청서 검토

신규 원전에 대한 건설허가 단계에서는 개념설계내용의 적합성 검토를 수행하며, 세부단계별 주요 검토범위 및 내용은 표 1과 같다.

(2) 운영허가(OL) 신청서 검토

신규원전에 대한 운영허가단계에서의 검토는 건설허가단계에서 확인된 개념설계내용에 따라 설계된 상세설계내용에 대한 검토를 수행한다. 따라서, 운영허가 단계에서 검토는 다음과

같은 항목들과 건설허가(CP) 심사시 준수사항에 대한 변경내용 등을 검토한다. 세부단계별 주요 검토범위 및 내용은 표 2와 같다.

(3) 변경허가 신청서 검토

가동중 원전의 디지털 설비개선을 위해 기존의 설계내용을 변경하는 경우, 신청자는 그 변경사항이 안전한 것인지를 안전성분석보고서 작성을 통하여 검토 및 평가함과 동시에 변경내용이 적용 가능한 규제법규를 만족하는지를 확인하고, 발전소 인허가 기술기준에 미치는 영향을 판단하여야 한다. 변경허가와 관련해서 중요한 것은 그 변경내용의 범위와 복잡성이며 변경내용이 미검토 안전성문제(USQ)를 제기하는지의 여부에 따라 심층 평가할 것인지 혹은 그렇지 않을 것인지를 결정하게 된다. 그렇지만 변경사항에 대한 평가에서는 시스템에 대한 개념설계내용 검토에서부터 운영/보수에 이르기까지 전 과정을 다루게 되며, 주요 검토사항은 변경된 부분의 안전성 평가뿐만 아니라 그 부분이 변경되지 않은 부분에 미치는 영향을 심층 평가한다.

(4) 특정기술주제보고서 검토

특정기술주제보고서는 건설허가, 운영허가 또는 변경허가와는 무관하게 원자력법 제 104조의 2에 따라 특정한 기술사안에 대해서 규제기관의 검토·승인을 받기 위해 제출될 수가 있다. 예를 들면 여러 발전소에서 반복하여 사용될 것으로 계획된 계통 및 기기에 대한 설계내용과 설계방법론 등이 검토를 위해 제출될 수가 있지만, 특정기술주제보고서의 범위는 매우 다양하므로 그 대상 항목에 따라 신청서에 맞는 검토범위를 선정하여 검토하게 된다. 검토대상 신청서내용과 관련해서는 상기의 모든 논의사항들이 신청서내용에 따라 적절히 고려되어야 한다.

4. 주요 평가기준 및 내용

4.1 평가기준 및 주제

계측제어시스템에 관한 기본적인 허용기준 및 지침은 국내 원자력관련 법규(원자력시설 기술기준에 관한 규칙), 안전심사지침서 7장 및 10CFR 50.55a, ANSI/IEEE Std 279 및 603, IEEE Std. 7.4.3.2를 승인한 Re. Guide 1.152, IEEE Std 603을 승인한 Reg. Guide 1.153, 그리고 10CFR 50, App. A(일반설계기준: GDC) 등이 있다.[1,2,3] 10CFR 50, App. B(품질보증기준)에는 안전관련 계측제어시스템의 설계, 제작, 설치, 그리고 시험 등에 적용되어야 할 품질보증프로그램에 관한 기준들이 제시되어 있으며, 10CFR 50의 기준들은 디지털 계측제어시스템에도 적용된다. 새로 개발된 안전심사지침서 7장 7.1절(표 7-1)에는 안전성분석보고서 각 절의 검토에 적용되는 허용기준 및 지침이 기술되어 있다.[3]

디지털 계측제어시스템의 몇 가지 특성들은 10CFR 50의 기본적인 허용기준을 따르고 있는지를 평가하는 데에 있어서 검토방식을 강화하고 새로운 검토관점을 고려하여 평가되고 있다. 이러한 특성들은 컴퓨터를 이용할 때 새롭게 보증되어야 하는 디지털시스템의 설계검증, 공통모드고장에 대한 대비책, 그리고 IEEE Std 603과 일반설계기준(GDC)에서 선정된

기능적 요건들을 평가하는 데에 중요한 것들이다.

그림 3은 디지털 계측제어시스템에 대한 주요 검토내용 및 절차를 개략적으로 보여주고 있다. 이 검토내용 및 절차는 건설/운영허가 신청서, 특정기술주제보고서, 변경허가신청서에서 제안된 어떠한 디지털 계측제어시스템에도 적용된다.

검토절차는 모든 계측제어계통의 안전성 기능확인에 대해 동일하지만, 단순히 몇 개의 안전성요건이 적용되는 계통에 대한 검토내용 및 절차와 비교해서 통합이 완료된 디지털 안전계통 등에 대한 검토절차는 매우 복잡할 수 있다. 규제측면에서의 검토 중점사항은 주어진 계통의 안전성 중요도 또는 검토대상 계통의 설계내용에 적합하도록 선정되며, 이에 따라 대상계통의 적합성을 검토한다.

그림 3의 검토내용 및 절차에 따른 다음과 같은 7가지 검토주제들이 디지털 계측제어시스템의 검토에서 주요하게 다루어진다.

① **신청된 시스템에 적용되어야 할 상세설계기준과 지침의 적합성:** 안전심사지침서 7.1절의 표 7-1 및 부록 7.1-1의 내용을 만족하고 있는지를 확인한다. 새로운 디지털계통이 IEEE Std 7-4.3.2-1993을 승인한 Reg.Guide 1.152의 지침, 소프트웨어 개발공정을 상세히 기술한 일련의 소프트웨어공학 표준 및 소프트웨어관련 신규 규제요건(Reg. Guide 1.168~1.173) 등을 준수하고 있는 가를 확인한다.

② **검토주제의 확인:** 확인된 검토주제에 대한 검토내용 및 절차는 신청된 계측제어시스템의 설계내용 등에 따라 달라진다. 이에 대한 내용은 다음 절(검토대상 시스템 및 범위)에 기술되어 있다.

③ **심층방어 및 다양성:** 원자로 정지계통(RTS) 또는 공학적 안전설비 작동계통(ESFAS)과 관련된 신청서에 대해서는 공통모드고장에 대처하는 계측제어계통의 종합적인 능력을 검토한다. 즉 원자로 보호계통이나 공학적안전설비 작동계통에 디지털 컴퓨터 기술을 채택한 안전등급 계측제어계통은 SECY-93-087, 규제요건메모(SRM)의 심층방어(D-I-D) 및 다양성에 대한 규제요건을 적용한다. 이 검토에서는 심층방어 및 다양성 설계가 안전심사지침서 7.1절과 부록 7.16의 지침을 따르고 있는지를 확인한다.

④ **각 개별 계측제어시스템에 대한 시스템 기능요건과 준수사항의 적합성:** 각 계측제어계통의 기능요건과 준수사항들은 국내 원자력법(원자력시설기술기준에 관한 규칙)과 안전심사지침서 7.1절 및 안전심사지침 관련 절에 기술된 10 CFR 50의 요건들을 만족하고 있는지를 검토한다. 디지털 컴퓨터시스템의 경우, 새롭게 부과된 현안사항에 대해서는 IEEE 603의 기능요건들과 일반설계기준에 따라 검토된다. 또한 안전심사지침서 7.1절의 디지털 컴퓨터기반 안전계통에 대한 추가지침에서는 디지털계통에서 신중히 고려되어야 할 사항들을 기술하고 있으며, 이에 대한 내용(실시간 성능, 자기 및 감시시험 등) 등이 안전심사지침서 부록 7-14와 7-17을 기준으로 중요하게 검토된다.

⑤ **수명주기 공정계획:** 컴퓨터시스템 개발공정, 특히 디지털시스템의 소프트웨어 수명주기 활동계획들이 검토된다. 그림 4는 검토시에 고려되어야 할 소프트웨어 수명주기계획의 주제들을 나타내 주고 있다. 소프트웨어 수명주기계획 검토에서는 안전심사지침서 부록

7.13의 II.3.1절에 기술된 바와 같이 각 활동그룹들의 유기적인 연계활동과 개발과정에서 확인되어야 할 제품 및 공정특성에 대한 단계별 점검내용 등이 적절하게 관련계획에 포함되어 있는 지를 확인한다.

⑥ **소프트웨어 수명주기 공정이행의 적합성:** 신청자의 수명주기 활동들이 계획대로 이행되어 왔는지를 확인하기 위해 여러 수명주기 단계들에 대한 확인 및 검증(V&V), 안전성분석, 그리고 형상관리(CM) 문서들을 임의로 선정하여 검토 및 감사(Audit)한다. 그림 4는 공정이행 검토 및 실사(감사)시 고려되는 소프트웨어 수명주기 이행주제들을 나타내주고 있으며, 안전심사지침서 부록 7.13의 II.3.2절에는 이러한 감사를 수행하기 위한 지침으로서 허용기준과 검토절차가 기술되어 있다. 감사활동의 범위와 깊이는 신청된 디지털계통의 범위와 복잡성 그리고 계통의 고장에 따른 안전성 영향에 알맞게 선정된다. 개발공정의 감사에서는 계획된 절차가 실제로 사용되었는지와, 적절한 안전성분석, 확인 및 검증, 그리고 형상관리 활동들이 수행되었는지를 확인한다.

⑦ **소프트웨어 수명주기 공정에 따른 설계결과물:** 하드웨어 및 소프트웨어가 설계기준에서 도출된 기능 및 공정 요건들을 따르고 있는지를 검토/감사하고, 설계결과물(그림 4 참조)이 소프트웨어에 구현된 기능요건들을 기술하고 있는 지와, 그리고 요구되는 소프트웨어 개발공정 특성들을 설계결과물이 갖추고 있는지를 확인하기 위해 소프트웨어 설계결과물을 샘플로 취해서 검토한다. 검증 및 설치 활동들에 대한 검토에서는 시스템의 기능들이 의도대로 발휘되는지를 보증하는 시스템 시험절차서와 시험결과(검증시험, 현장 허용시험, 사용전 및 기동 시험)의 적합성을 확인한다. 안전심사지침서 부록 7.13의 II.3.3절에는 이와 같은 검토 및 감사에서 확인되어야 할 기능적인 특성들과 소프트웨어 개발공정의 특성들이 기술되어 있다. 설계결과물의 감사(audit)에서는 기능요건들이 모든 중간단계의 설계문서들을 걸쳐서 최종제품에 이르기까지 추적 가능한지를 확인한다. 설계결과물에 대한 감사는 또한 필요한 소프트웨어 개발공정 특성들과 필요한 소프트웨어 필수특성들이 있는지를 확인한다. 심층방어 및 다양성(상기 ③번의 주제) 설계검토는 전체 계측제어계통의 설계 기능들이 공통모드고장에 대비해서 어떻게 서로 작용하는지를 결정하기 위해 여러 가지 계측제어계통들을 검토한다. 본 사항에 대한 검토는 컴퓨터를 채택하지 않은 시스템과 컴퓨터-기반 시스템 모두에 해당될 수 있으며, 상기 ④, ⑤, ⑥번의 주제들에 대한 검토는 다중계통에 공통된 설계공정을 평가하기 위해 한 번만 수행할 수도 있다. 그리고 ⑦번 주제에 대한 검토는 신청자의 안전성분석보고서 7장의 각 디지털 계측제어계통에서 샘플로 취해서 수행한다.

상용 디지털기기를 이용하는 계통의 경우에도 원칙적으로 상기한 7가지 주제가 적용되지만, 세부 검토방법에서는 이와는 다른 특성들(예, 운전이력 등)이 고려되어 검토가 수행될 수 있다. 또한 계통내에 설치된 상용제품에 대해서는 이의 사용을 위해 적절한 인증절차가 적용되었는지를 확인한다. 여기서 인증절차는 동 제품이 요구되는 안전기능을 수행할 수 있고 10 CFR 50 부록 B를 만족하는 품질보증절차서에 따라 설계/제작된 제품과 동등하다는 것을 확신함으로써, 이의 사용을 인증하게 되는 과정을 말한다. 인증절차는 10 CFR 50, 부록 B의 적용 가능한 조항을 따라야 한다. 이러한 절차는 상업용

기기의 종류에 따라 또는 적용내용에 따라 달라질 수 있으나 어떤 경우에도 요구되는 보증사항을 만족해야 한다. 이와 같은 상용제품 인증에 대해서는 Reg. Guide 1.152 (개정 1)와 EPRI TR-106439을 준용하여 검토한다.

4.2 평가대상 시스템 및 범위

평가대상 시스템은 원자로 보호계통(RPS, ESFAS), 기타 안전계통, 제어계통, 다양성 계측제어계통 및 데이터 통신계통이 있으며, 이들 시스템에 대한 검토수준은 안전성 중요도에 따라 표 3과 같이 달라진다. 신청자가 기 승인된 디지털 계측제어계통을 신청하는 경우, 검토범위는 크게 줄어들게 되고 변경과 관련된 특정한 현안들(예, 환경검증, 형상관리)에 대해서만 중점적으로 검토하게 된다. 그리고 신청된 설계의 일반사항, 즉 소프트웨어 개발공정, 제품, 그리고 문서들에 대해서는 만약 이들 사항들이 발전소의 특정한 차이점에 의해서 변경 혹은 영향을 받지 않았다면 반복적으로 검토하지는 않는다. 그러나 예전에 승인된 것과 차이점들이 있다면 이와 같은 사항은 확인되어야 한다.

원자로 보호계통은 디지털시스템의 검토주제들을 모두 적용해서 검토되고 기타 안전계통은 심층방어 및 다양성 평가를 수행하지 않아도 된다. 제어계통은 그 계통의 고장이 보호 및 기타 안전계통의 기능에 악영향을 주지 않음을 확인하기 위해 제한된 범위만을 검토한다. 제어계통의 검토에서는 특히 제어계통과 안전계통의 독립성 유지와 품질 및 제어계통의 고장으로부터 안전계통의 적절한 격리설계내용을 확인한다. 계측제어계통의 디지털설계와 관련하여 새롭게 추가된 다양성 계측제어계통과 데이터 통신계통에 대한 주요 검토내용은 다음과 같다.

ATWS 관련법규, 10CFR 50.62와 국내 원자력법(원자로시설등의 기술기준에 관한 규칙)에서는 센서 출력에서부터 최종작동장치에 이르기까지 기존의 원자로 정지계통과는 독립적이고 다양한 기능을 갖는 다른 설비를 갖추도록 요구하고 있다.[2,5] 동 법규에 따른 다양성 계측제어계통을 아날로그 또는 디지털 계측제어시스템으로 새롭게 설치할 경우 신청자는 적절한 다양성을 보증해야 한다.

이 경우에 있어서 다양성 계측제어계통의 제작자와 원자로 보호계통의 제작자가 서로 다르고, 두 계통에 사용된 하드웨어 및 소프트웨어가 서로 다르면 다양성 요건을 만족한 것으로 평가되며, 기존의 ATWS 완화시스템을 디지털시스템으로 변경하고자 할 경우에도 동일한 요건을 만족하도록 설계되어야 한다.

다양성 평가에서는 하드웨어, 사용된 소프트웨어 언어, 전반적인 설계 또는 구조, 작동신호, 그리고 각 시스템에서 수행된 기능들과 같은 항목들을 검토한다. 어떤 다양성 계측제어계통이 적절한 다양성을 유지하고 “있다” 또는 “없다”의 결정은 NUREG-0494 또는 NUREG/CR-6303 과 같은 지침을 참조해서 사안별로 공학적인 판단에 따르지만, 중요하게 검토되는 사항은 두 계통들이 어떤 공통모드고장으로 인해서 소정의 기능들을 상실할 가능성이 있는지를 평가하는 것이다.[6,7] 다양성 계측제어계통에 대한 상세한 안전성검토는 안전심사지침서 7.8절에 따라 수행된다.

데이터 통신계통은 원자로 보호계통, 기타 안전계통, 다양성 작동계통, 또는 제어계통을

지원하는 시스템으로서 동 계통에 의해 지원을 받는 계측제어시스템에 적용된 검토주제들을 통신시스템에도 그대로 적용해서 검토한다. 데이터 통신계통에 대한 상세한 안전성검토는 안전심사지침서 7.9절에 따라 수행된다.

5. 결 론

디지털 계측제어시스템에 대한 규제 및 안전성평가 방향을 요약하여 기술하면 다음과 같다. 첫째, 디지털 계측제어계통에 대한 안전성평가는 기존 원전의 계측제어설비에 적용된 규제요건, 각종 규제문서에서 승인한 산업표준과 관례, 국내·외 인허가 사례 그리고 외국 규제기관의 디지털기술에 관한 규제방침들을 추가로 적용하고, 특히 새로 개정된 안전심사 지침서 7장의 검토절차, 규제요건, 허용기준 및 규제지침에 따라 수행한다.

둘째, 디지털 I&C 검토범위와 검토의 정도는 신청되는 시스템의 중요도 및 변경내용의 복잡성에 따라 선택적으로 결정하고, 기존에 승인된 설계에 대해서는 연속 적용에 따른 차이점과 발전소 특정 사안에 대해서만 검토한다. 셋째, 소프트웨어 품질에 대한 안전성평가에서는 수명주기 공정과정의 품질활동 내용에 대한 확인 및 검증평가에 검토의 주안점을 두고 있으며, 특히 디지털 시스템에 대한 현안 사항을 중점적으로 검토한다. 끝으로, 디지털 계측제어계통에 관한 설계 및 규제목표는 공통모드고장 발생을 최대한 억제하는데 있으며, 만약 그러한 고장이 발생하더라도 동 계통의 기능상실 정도를 가능한 한 최소화시키는 방향으로 설계가 되어야 한다. 이와 같은 설계 및 규제 쟁점현안을 해결하기 위한 가장 최선의 방안으로는 철저한 품질보증과 심층방어 및 다양성설계기법을 들 수 있다. 즉, 철저한 품질보증은 설계 및 운전과정에서 인적실수로 인한 공통모드고장의 발생가능성을 최소화할 수 있으며, 각 장비 및 전체계통(소프트웨어 포함)의 신뢰도를 증대시켜 원전의 안전성을 확보하여 원전산업의 지속적인 발전을 기대할 수 있다고 본다.

참고 문헌

[1] KINS/GR-125 "디지털 계측제어시스템 안전성 평가기술 개발", KINS, 1997.9

[2] "원자력관계법령집", KINS, 2000. 6

[3] KINS/G-001(개정 2) "경수로형 원자력발전소 안전심사지침서" , KINS, 1999.10

[4] NUREG-0800, "Standard Review Plan", Chapter 7 I&C, Rev. 4, June 1997

[5] 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants", January 1987

[6] NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System", March 1979

[7] NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems", December 1994

표 1. 건설허가단계 주요 검토범위 및 내용

세부 평가 단계	검 토 내 용
시스템 개념적 합성 평가	○ 10CFR50의 기능과 사고해석에 따른 전반적인 I&C 시스템 설계사항 ○ 시스템 또는 기기 설계에 따른 현안의 해결방안 ○ 기술관련 USI와 중/고-순위 GSI 해결방안
시스템 요건 적합성 평가	○ 10CFR50.55a(h), IEEE 279, 603, 10CFR50, App. A&B 등의 설계상세기준 ○ 설계기준과 설계상세기준과의 상관성
시스템 설계 적합성 평가	○ 시스템의 중요한 특성, 기능 및 성능요건, 일반 배열/배치 등 ○ 기술지침서의 I&C 기능과 변수 확인 ○ 기본적인 설계기준과 성능요건을 입증하는 신청자 해석사항과 기술적 타당성 평가
하드웨어 및 소프트웨어 계획 적합성 평가	○ 시스템 개발에 따른 관리와 이행, QA, 통합, 설치, 보수, 훈련, 운전, 안전성분석, 확인 및 검증, 형상관리(CM) 계획

표 2. 운영허가단계 주요 검토범위 및 내용

세부 평가 단계	검 토 내 용
H/W와 S/W 요건, 설계, 제작, 시험, 통합적합성 평가	○ 개발계획의 이행 ○ 시스템 요건에 따른 설계결과물 확인 ○ 설계결과물에 포함된 설계공정 특성들의 확인 ○ 건설허가 단계에서 확인된 안전성 현안들에 대한 해결방안
시스템검증 적합성 평가	○ 기본 설계기준과 성능요건을 포함한 계측제어시스템 설계가 소정의 안전성 기능들을 수행할 수 있는지를 입증하는 신청자의 시험, 해석과 기술적 타당성 평가 ○ 참조표준설계의 경우 인터페이스요건의 준수
설치, 운전 및 보수적합성 평가	○ 사용전 시설 및 성능검사의 수행 ○ 심사 이행사항 확인

표 3. 평가대상 시스템과 검토주제

주 제	**보호계통 (7.2～7.3절)**	**기타 안전계통 (7.4～7.6절)**	**제어계통 (7.7절)**	**다양성 I&C계통 (7.8절)**	**데이터 통신계통 (7.9절)**
심층방어 및 다양성	검토	*(1)	*(1)	*(1)	*(2)
개발공정	검토	검토	제한 검토	검토	*(2)
기능현안	검토	검토	제한 검토	검토	*(2)
공정이행	검토	검토	제한 검토	검토	*(2)
설계결과물	검토	검토	제한 검토	검토	*(2)

주) * :

(1) 원자로 정지계통과 공학적 안전설비 작동계통 이외의 기타 계측제어시스템에 대해서는

심층방어 및 다양성 분석이 요구되지는 않지만, 기존의 디지털 원자로 정지계통과 공학적안전설비 작동계통을 갖는 발전소에서 기타 계측제어계통을 디지털설비로 변경하는 경우는 그 변경내용이 기존의 심층방어 및 다양성 분석에서 고려된 가정사항과 준수사항들에 영향을 주지 않음을 확인하기 위해서 검토한다.

(2) 데이터 통신계통은 지원 받는 시스템과 동일한 수준으로 검토한다.

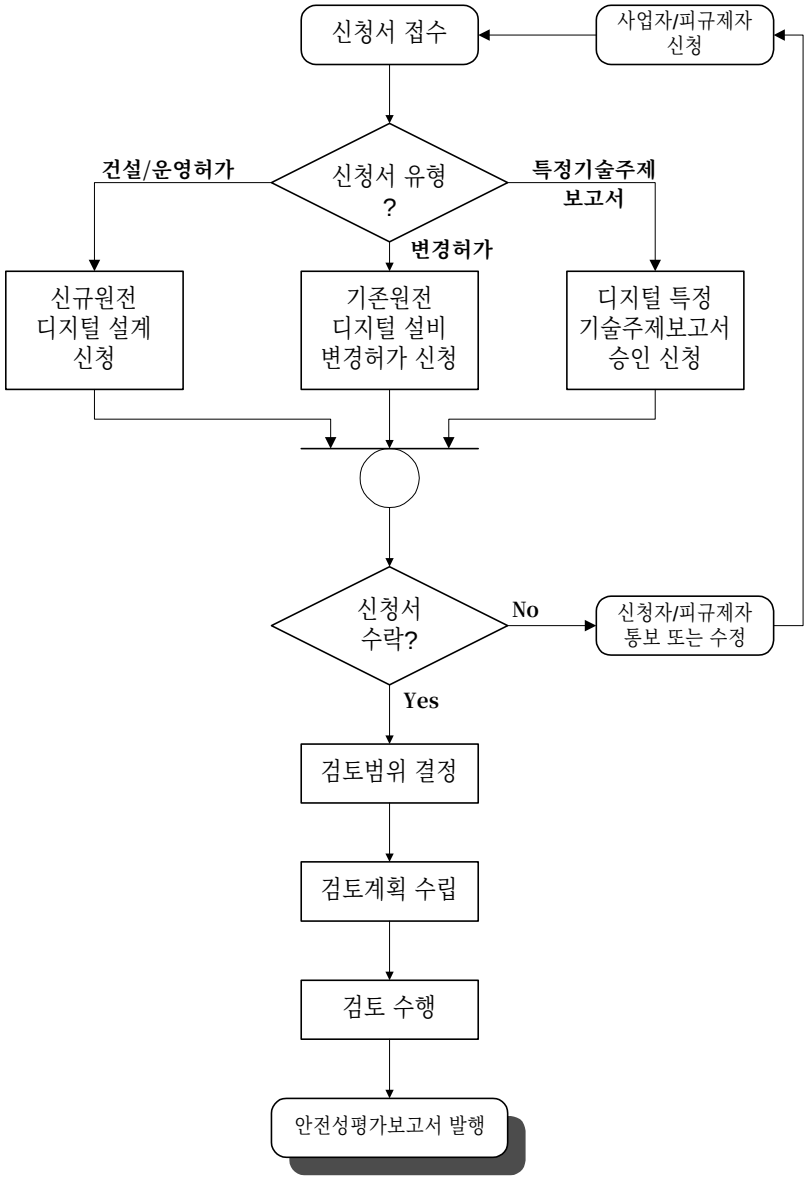


그림 1. 디지털 계측제어시스템의 신청서 유형 및 일반 검토절차

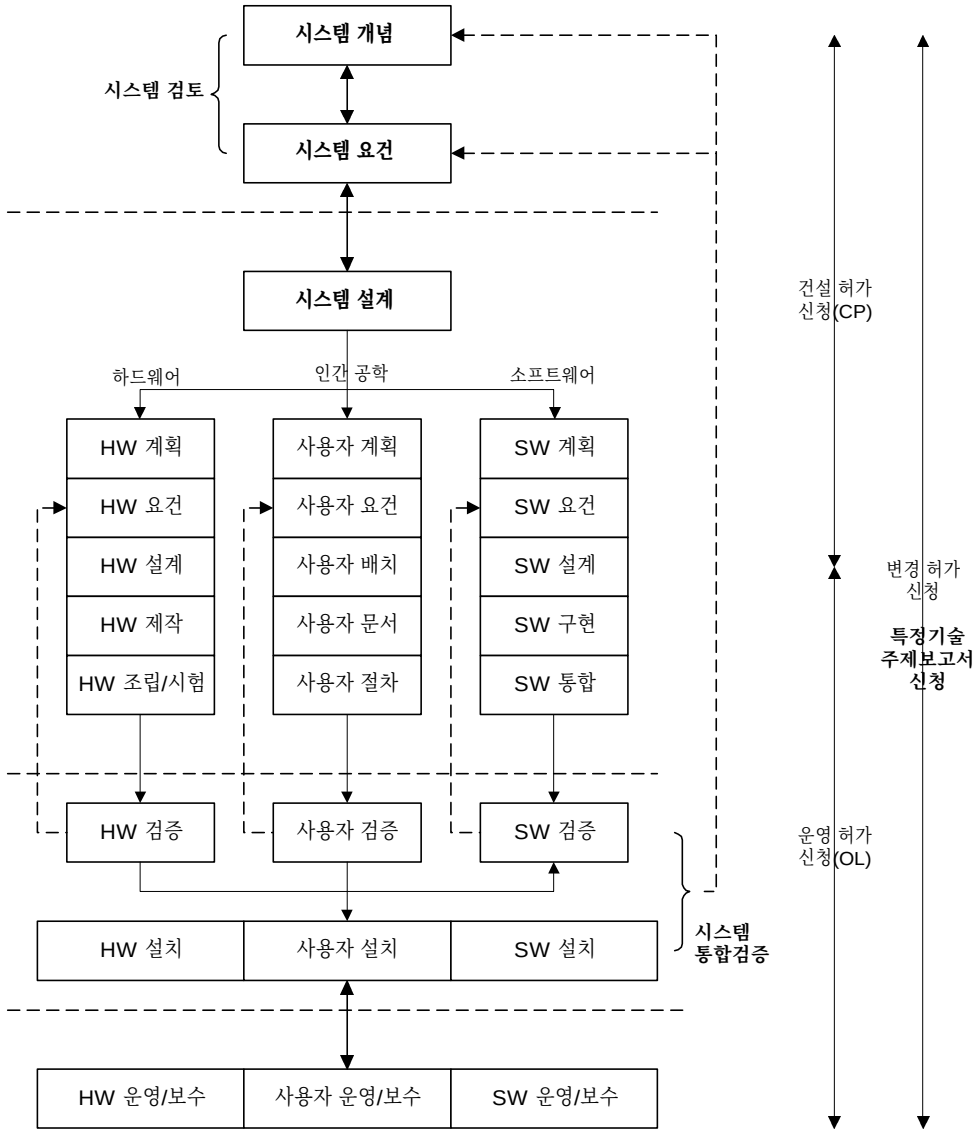


그림 2. 디지털 계측제어계통 개발 단계별 검토사항

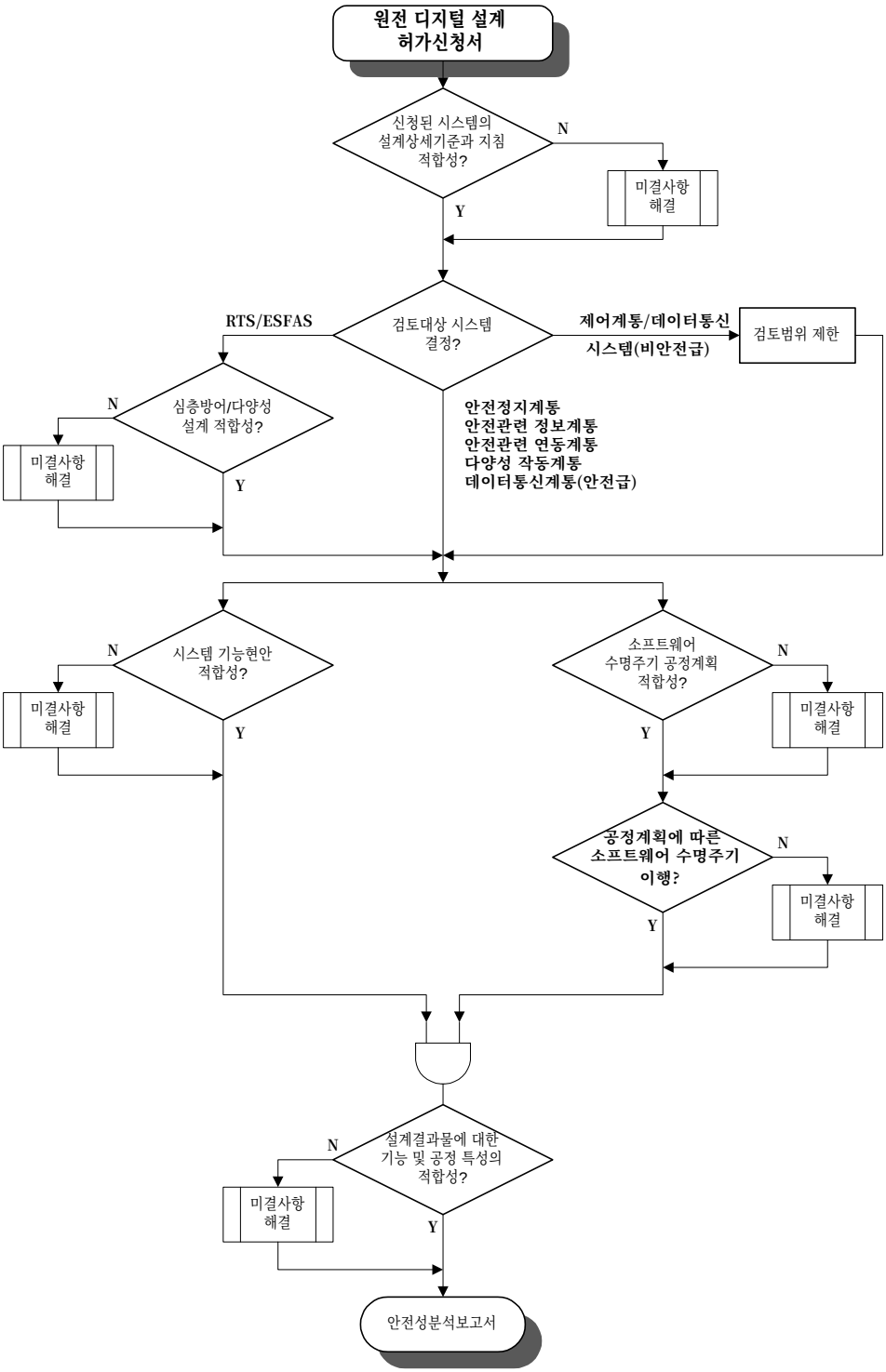
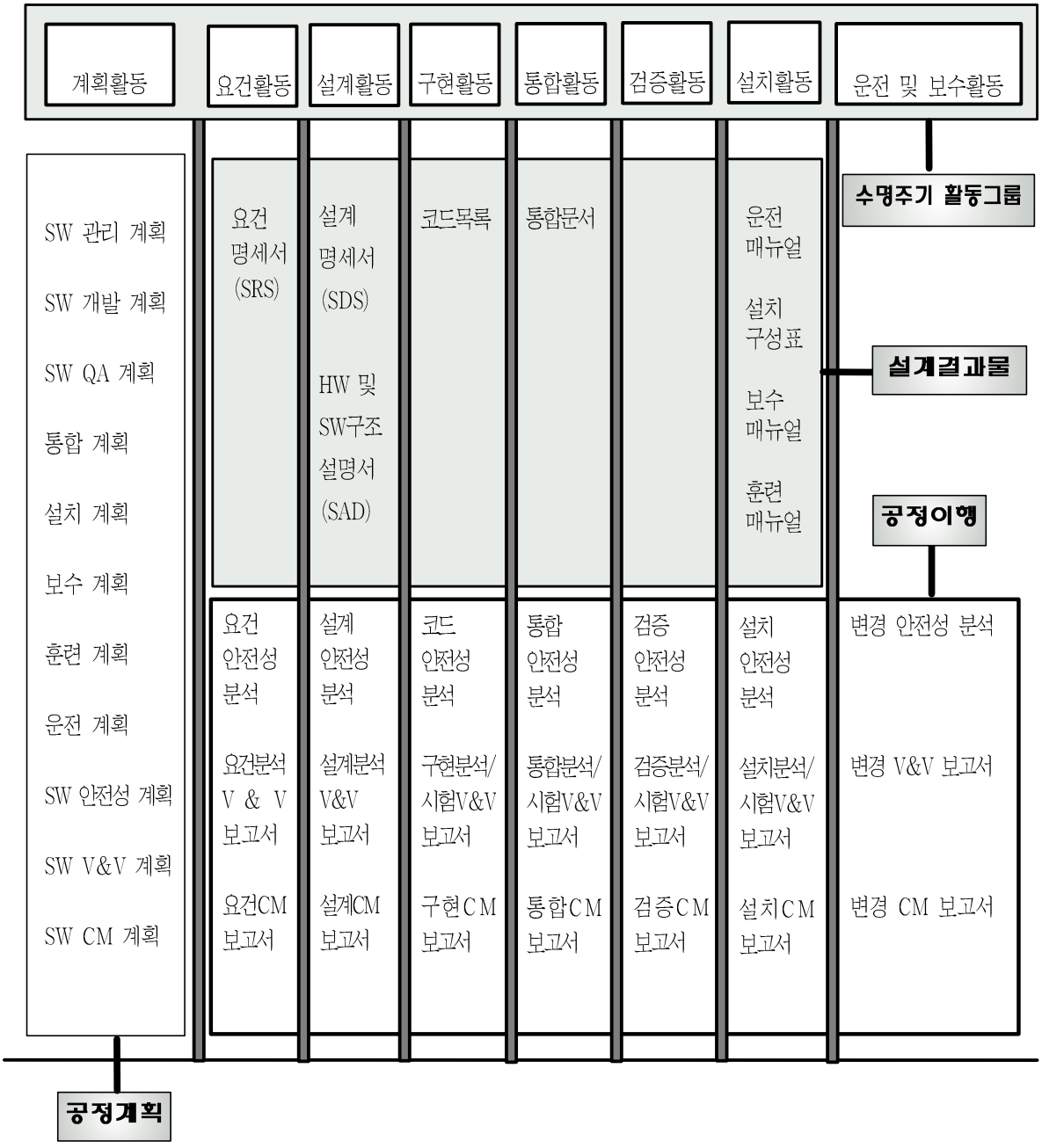


그림 3. 디지털 계측제어시스템에 관한 주요 검토내용 및 절차



(주) 1. 명시된 각 주제에 대해 개별적인 문서를 작성할 필요는 없으나, 프로젝트 문서 내에는 모든 주제를 다루고 있어야 한다.

2. V&V : 확인 및 검증

3. CM : 형상관리

그림 4 소프트웨어 수명주기 활동