디지털 계측제어계통 규제기술

오성헌, 김복렬 / 한국원자력안전기술원 계측제어실

개 요

최근의 계측제어분야는 컴퓨터기반 소프트웨어 공학기술, 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 보완되고 발전될 것으로 예상된다.

오늘날 일반 산업계에서는 컴퓨터 시스템의 사용이 보편화되어 있으며, 최근에는 신규 및 차세대 원자력발전소 설계분야의 원자력산업계에서도 시스템의 정확성, 보수성, 운전신뢰도의 향상과 기존 아날로그시스템설계의 한계성 극복을 위해 디지털시스템을 사용하고 있다. 특히 가동중인 원전에서도 기존 하드웨어 기기의 성능저하, 노후화된 기기를 교체할 만한 동등한 예비품 및 교체품 구입의 어려움 등으로 설비개선 시에 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 있다는 것이다. 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 규제기술현안에는 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, 데이터통신계통 독립성 및 상용제품인증문제 등이 있다. 이와 관련하여 본 기고에서는 가동중인 원자력발전소(원전)의 디지털 설비개선이나 신규 원전 및 차세대 원전 등에 적용되고 있는 컴퓨터기반 디지털 계측제어시스템에 대한 기술적인 규제기술 현안내용과 이를 해결하기 위한 방안을 제시하고자 한다

디지털 계측제어시스템의 특징

디지털시스템은 기능적 관점에서 보면 아날로그 시스템과 크게 다를 바가 없다. 그러나 운전 특성은 서로 크게 다르다. 예를 들어, 디지털시스템은 소프트웨어를 내장하고 있고 복잡한 기능들을 순차적으

로 수행하는 반면에 아날로그시스템은 병렬로 신호를 처리할 수 있다. 또한 아날로그와 디지털 시스템의 중요한 차이는 발전소 입력신호들을 취득하는 방식이 서로 다르다[2]. 그림 1은 두 시스템의 차이를 나타내고 있다. 아날로그시스템은 발전소 입력신호에 대한 전압 또는 전류 값을 직접 이용하여 결과를 계산한다. 반면 디지털시스템은 발전소 입력신호에 대한 전압 또는 전류 값을 디지털 2진수 값으로 변환하고, 변환된 디지털 신호를 이용하여 계산을 수행하며 계산결과를 필요에 따라 아날로그 신호로 다시 변환하여 사용하고 있다.

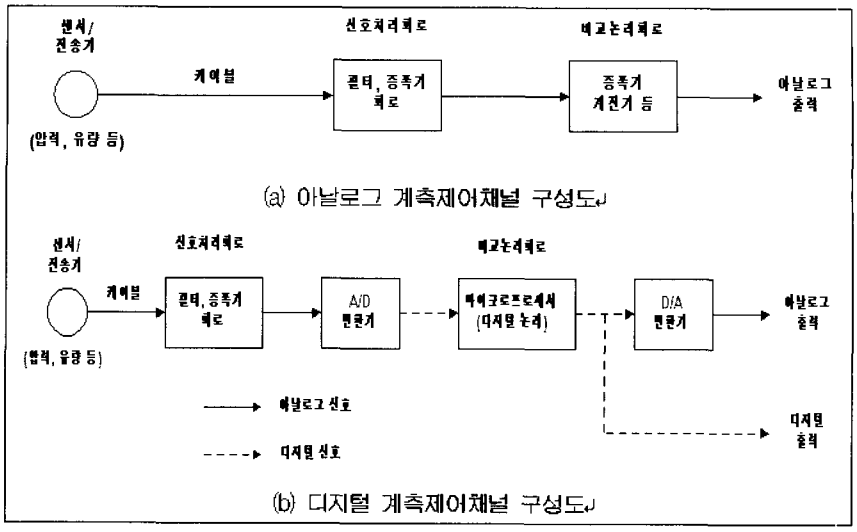
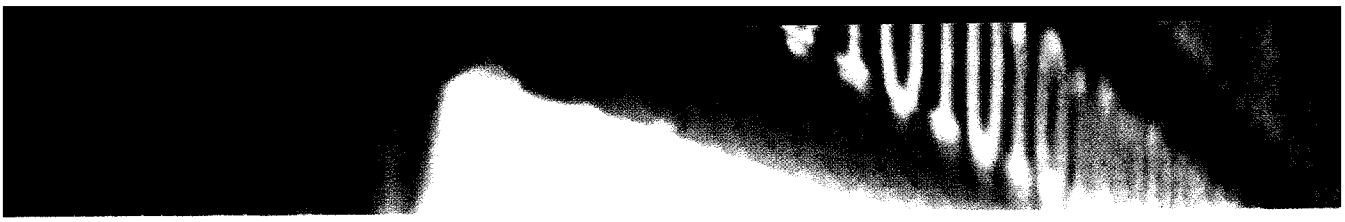


그림 1 아날로그 및 디지털 채널의 구성도

디지털시스템의 장 단점을 살펴보면 아날로그시스템에 비해 데이터 전송과 처리능력이 월등하고, 드리프트(drift) 현상이 적으며, 정확도, 신뢰도, 유연성 향상 그리고 무엇보다도 각종 자원(resource)들을 공유할 수 있어서 자원의 활용도를 높일 수 있다는 장점을 갖고 있다. 반면에 디지털시스템은 아날로그시스템에 비해 주변환경(예, 온도, 습도, 방사선, 전자파, 연기 등)에 민감하고 설계 및 프로그래밍 오류에 취약하여 공통모드고장 가능성이 큰 것으로 지적되고 있다[3]

그림 2는 그림 1의 디지털 계측제어채널에서 마이크로프로세서의 내부상태를 모델링한 것이다[4]. 컴퓨터-기반 시스템은 크게 하드웨어, 소프트웨어, 그리고 인간-기계 인터페이스(MMI)로 구분된다. 하드웨어는 프로그램 또는 데이터를 처리, 저장, 송신 및 수신하기 위한 시스템의 본체를 말한다. 소프트웨어는 시스템의 동작을 위한 프로그램, 프로시저, 그리고 데이터를 말하며 내장된 펌웨어(firmware)를 포함한다. 개발 관점에서 소프트웨어는 이미 개발되었거나 상용화된 기성 소프트웨어와 특정한 응용분야에 적합하게 새롭게 개발된 신개발 소프트웨어로 구분된다. 따라서 그림 2의 중앙에 있는 소프트웨어는 기성 또는 신개발 소프트웨어일 수 있다. 그리고 인간-기계 인터페이스는 계측제어계통 또는 장비와 운전원, 보수요원, 또는 엔지니어링 요원간의 접속부분, 즉 표시기, 제어기(누름 버튼 포함), 시험 패널, 구성 터미널 등이 포함된다.

컴퓨터-기반 시스템은 그림 2에서 보는 바와 같이 그 채널의 다른 부분과의 경계가 확실하게 구분된다. 그 경계의 각 입력은 고유한 식별 명칭과 번호가 부여되며 이를 감시변수(monitored variable)라고 부르고, 그 경계의 각 출력에도 고유한 식별 명칭과 번호가 부여되는데 이를 제어변수(controlled variable)라고 한다[5]. 컴퓨터-기반 시스템 내부에서 실행되는 소프트웨어간의 경계가 또한 확실하게 구분된다. 그 경계선의 각 입력은 고유한 식별 명칭과 번호가 부여되며 이를 입력변수(input variable)라고 하고, 그 경계선의 각 출력에도 고유한 식별 명칭과 번호가 부여되는데 이를 출력변수(output variable)라고 한다.



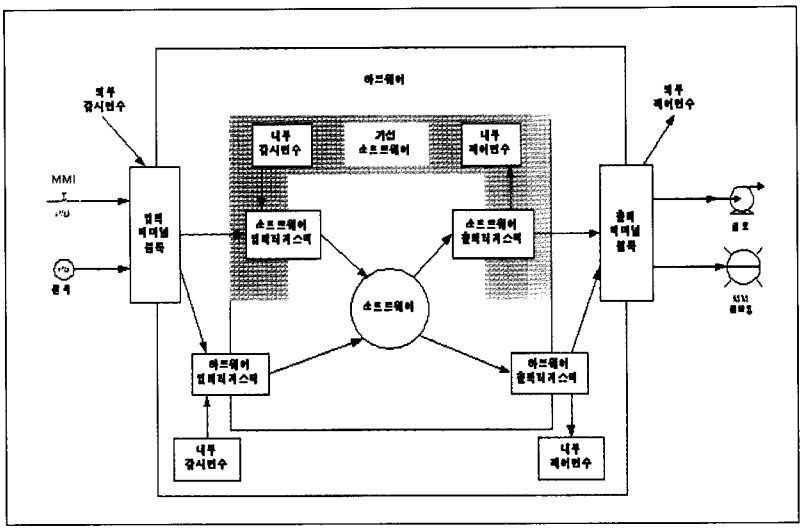


그림 2 컴퓨터-기반 시스템의 내부 구조

주요 규제기술 현안사항

기술적 고유현안 규제기술은 원전의 안전계통(예: 원자로정지계통, 공학적안전설비작동계통 등)에 디지털기술을 사용할 경우 기술적으로 해결되어야 할 규제현안들을 평가하고 규제하기 위한 기술로서 다음과 같은 기술들이 있다.

계측제어시스템은 발전소 장비와 공정들을 감시, 제어, 그리고 보호하며 발전소를 안전하고 신뢰성 있게 운전할 수 있도록 지원하는 기능을 갖고 있다. 발전소 보호 및 제어시스템에 디지털기술을 이용할 경우 그 소프트웨어와 하드웨어가 공통모드고장을 일으킬 수 있는 설계 및 프로그래밍 오류들에 취약한 것으로 평가되고 있다. 즉, 디지털시스템은 아날로그시스템에 비해서 데이터 전송, 기능, 그리고 공정 장비 등을 상당히 많이 공유하게 되며, 그 같은 공유는 다중성 장비에서 공통원인(common cause) 혹은 공통모드(common mode) 고장들을 일으킬 수 있다는 것이다. 그 외에도 중대한 안전현안은 소프트웨어 프로그래ald 오류가 하드웨어로써 달성된 다중성을 파괴시킬 수 있다는 것이다. 따라서, 디지털시스템에 관한 설계 및 규제요건의 목표는 공통원인과 공통모드고장의 발생 가능성을 억제하고, 만약 그 같은 고장이 여전히 발생하더라도, 계측제어시스템의 기능 상실 정도를 억제하자는 데에 있다. 이 같은 현안문제에 대한 규제기술은 크게 세 가지로 구분된다. 그중 하나는 시스템 관련사항, 즉 심층방어 및 다양성, 통신시스템 성능 및 독립성, 실시간 시스템, 그리고 자동 주기시험설비에 관한 사항들이고 다른 하나는 소프트웨어 관련사항으로서 소프트웨어 개발공정에 관한 품질보증, 소프트웨어 안전성 및 신뢰성, 소프트웨어 확인 및 검증 및 형상관리 등이고 다른 하나는 상용제품인증 문제이다.

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 성능은 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 평가는 설계요건에 따른 엄격한 명세서와 이행사항을 반영한 고품질의 개발공정을 채택하여 디지털시스템 설계를 수행했는지를 확인하는 데에 중점을 두게 된다.

심층방어 및 다양성

이 규제기술은 예상운전과도사건 또는 사고 시에 원자로를 안전하게 정지시키고 공학적안전설비를 동작시키는 원자로 보호계통과 공학적 안전설비 작동계통의 심층방어 및 다양성을 평가하기 위한 기술이다. 현행 규제요건[6,7]에 의하면, 원자로 보호계통과 공학적 안전설비계통은 고도의 기능적인 신뢰도를 달성하고, 계통이 고장나면 안전한 상태로 진입하게 하며, 그리고 정상 운전, 보수 및 가상된 사고조건들이 보호기능의 상실을 초래하지 않도록 다양성 설계에 따른 심층방어개념을 만족해야 한다고 규정하고 있다. 디지털시스템의 설계 다양성은 비록 철저한 품질공정에 따라 개발된 하드웨어와 소프트웨어를 사용할지라도 여전히 공통모드고장 가능성이 충분히 있는 것으로 인식되고 있기 때문에 반드시 필요하다.[6,7] 다양성 설계를 달성하기 위한 효과적인 방법들 중의 하나는 어떤 공통모드고장이 한 세트 이상의 기능들을 동시에 상실시키지 않도록 미리 선정된 기능 세트들에 몇 가지 형태의 기능적 다양성을 추가하는 것이다.

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, 이것은 또한 안전성관점에서 중요한 현안문제점들을 야기할 수 있다. 즉 공유된 데이터 또는 코드를 이용한 설계는 소프트웨어 오류로 인해서 공통원인 또는 공통모드 고장(Common Mode Failure: CMF)을 파급시킬 가능성이 있으므로 하드웨어 구조물로써 달성된 다중성을 파괴시킬 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.

소프트웨어 품질 및 신뢰도

소프트웨어는 원자로 정지기능에 사용된 것과 같은 비교적 단순한 결합논리, 또는 공학적 안전설비의 작동 또는 공정 제어 및 감시를 위해 사용된 것과 같은 보다 정교한 순차논리를 수행하는데 사용될 수 있다.

소프트웨어 품질을 보장할 수 있는 한 가지 방법은 그것을 생산해 내는 공정(process)들을 면밀히 조사해서 승인해 주는 것이다. 또 다른 방법은 소프트웨어의 특성들을 직접적으로 평가하는 것이다. 소프트웨어 특성에는 정확성, 신뢰성, 그리고 안전성이 포함된다. 소프트웨어는 만약 그것이 관련요건에 따라 거동하면 정확한 것으로 정의할 수 있다. 소프트웨어의 정확성 보증은 프로그램시험을 통한 실험적 방법 또는 정형적 확인기법을 통한 해석적 방법으로 이루어질 수 있으며, 소프트웨어 신뢰도는 어떤 프로그램이 어떤 정해진 환경에서 정해진 기간 동안 정확하게 동작할 확률이다.

소프트웨어는 만약 그것이 시스템의 위험을 초래하는 거동들(예, 어떤 주어진 환경에서 고장 또는 사고를 일으킬 수 있는 상태)을 나타내지 않으면 안전

한 것으로 본다. 디지털 계측제어시스템에서는 소프트웨어를 사용한다는 것이 아날로그 계측제어시스템과의 중요한 차이이다. 소프트웨어의 품질은 소정의 기능들을 수행해 내는 능력으로서 이것은 소프트웨어 명세서와 구현에 이르기까지 추적 가능해야 한다. 소프트웨어 개발공정을 관리하고 최종제품을 확인하는 전통적인 방식들 중 어느 것도 적절한 소프트웨어 품질을 완전하게 만족할 것으로 볼 수는 없다. 디지털 계측제어시스템에 필요한 소프트웨어를 명세하고, 제작하고, 그리고 관리하는 데에 어느 정도의 인정된 기술적인 해법이 필요한지가 이 현안의 핵심과제이다. 따라서, 설계자 및 운영자는 표 1과 같이 디지털 계측제어시스템의 설계 수명주기에 걸쳐서 소프트웨어 및 하드웨어의 품질을 확보하기 위한 소프트웨어/하드웨어에 대한 통합된 개발계획 등을 수립하고 이를 각 수명주기 활동단계별로 이행해야 한다. 이 같은 계획에는 설계, 구현, 통합, 설치, 운전 및 보수단계에서 소프트웨어 및 하드웨어를 검사하고 시험하는 방법들이 정의되고 관리계획, 형상관리계획, 확인 및 검증계획, 소프트웨어 품질보증계획 및 안전성계획 등이 포함된다.[8]

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 확인 및 검증활동에 대한 검토가 이루어져야 하고 이에 대한 내용이 문서화됨으로써 추후 이에 대한 확인이 가능하여야 한다.

소프트웨어의 공통모드고장 대책

원자력발전소의 안전계통들은 그 기능요건들을 신뢰성 있게 만족해야 한다. 이 같은 목적을 달성하기 위해서 안전계통들은 1개의 기기 또는 채널에서 고장이 발생하더라도 요구되는 안전기능(예: 원자로정지, 공학적안전설비자동 등)이 수행되어야 한다는 단일고장기준을 만족하도록 설계되어야 한다. 이런 설계목적을 달성하기 위해서 대개의 경우 다양한 형태의 다중성이 적용되고 있다.

다중성 방식에는 크게 두 가지, 즉 능동적(active) 다중성과 예비적(standby) 다중성이 있다. 능동적 다중성은 여러 개의 동일한 기기 출력들을 서로 비교해서 어떤 출력을 실제로 사용할 것인지를 선정하게 된다. 만약 각 개별 기기들이 매우 신뢰할 만하고 고장이 독립적으로 발생한다면 어떤 선정된 출력은 매우 높은 신뢰도를 갖게 된다. 그렇지만, 기기의 다중성도 공통원인 혹은 공통모드 고장들에 의해서 파괴될 수가 있다. 공통원인고장은 동일한 원인에 의해서 여러 기기들이 고장난 것을 의미하고 공통모드 고장은 여러 기기들이 같은 고장방식으로 고장난 것을 의미한다. 공통원인 및 공통모드 고장들은 기기의 고장이 독립적으로 일어난다는 가정이 무너질 때 발생하고 공통된 외적 또는 내적 영향 때문에 생길 수 있다. 외적 원인으로는 운전 요인, 환경 요인, 또는 인적 요인 등이 있으며, 공통된 원인은 또한 독립된 기기들의 내부 설계오류일 수도 있다.

공통된 설계오류를 방지하기 위해서는 동일한 기능을 수행하지만 서로 다른 내부 설계를 갖는 기기들을 사용하는 것으로서, 이러한 방식을 "설계 다양성"이라고 부른다. 동일한 요건명세서로부터 작성된 여러 버전의 소프트웨어들을 사용하는 것이 설계 다양성의 일례이다. 예를 들면, 서로 다른 알고리즘을 사용해서 동일한 정현함수를 계산하는 두 종류의 소프트웨어들을 말한다.

표 1 소프트웨어 수명주기 활동

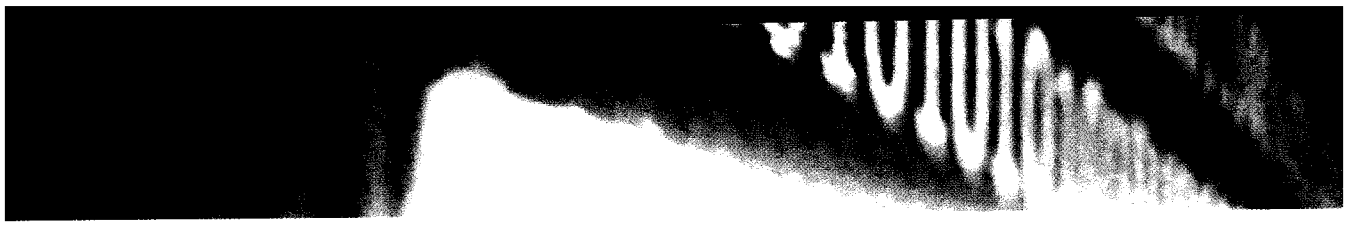
수명주기활동	공정계획, 공정이행 및 설계결과물	비 고
계획활동	SW관리/개발/QA계획, 통합/설치/보수/훈련/운전계획, SW안전성계획, SW V&V 계획, SW CM계획	- V&V: 확인 및 검증 - CM: 형상관리 - 명시된 각 주제에 대해 개별적인 문서를 작성할 필요는 없으나, 프로젝트 문서 내에는 모든 주제가 포함되어야 한다.
요건활동	요건명세서, 요건안전성분석보고서, 요건분석 V&V보고서, 요건 CM보고서	
설계활동	설계명세서, HW 및 SW구조설명서, 설계안전성분석보고서, 설계분석 V&V보고서, 설계CM보고서	
구현활동	코드목록, 코드안전성분석보고서, 구현분석/시험V&V보고서, 구현CM보고서	
통합활동	통합문서, 통합안전성분석보고서, 통합분석/시험V&V보고서, 통합CM보고서	
검증활동	검증안전성분석보고서, 검증분석/시험V&V보고서, 검증CM보고서	
설치활동	운전 메뉴얼, 설치 구성표, 보수 메뉴얼, 훈련 메뉴얼, 설치안전성분석보고서, 설치분석/시험V&V보고서, 설치CM보고서	
운전 및 보수활동	변경안전성분석보고서, 변경V&V보고서, 변경CM보고서	

또 다른 다양성은 "기능 다양성"으로서 기기-수준에서 완전히 서로 다른 기능들을 수행하는 기기들을 의미한다. 즉, 기능 다양성은 동일한 또는 서로 다른 시스템-수준의 요건들을 만족시키기 위해 서로 다른 동작원리 또는 물리적 원리를 이용하는 것이다. 이 경우에 있어서의 핵심은 기기의 요건들을 서로 다르게 작성하는 것으로써 기능 다양성의 일례는 제어봉을 이용하여 원자로를 정지시키기 위해 원자로 고출력정지변수를 사용하는 것과 보론 농도를 이용해서 원자로를 정지시키기 위해 냉각재 고온도정지변수를 이용하는 경우 등이다. 소프트웨어의 경우 기능 다양성은 소프트웨어의 거동요건들을 서로 다르게 하는 것이다. 예를 들면, 한 프로그램은 두 개의 수치가 같은 것인지를 점검하고, 기능적으로 다양한 다른 프로그램은 2개 숫자 중 더 큰 수를 선정하는 것이다.

소프트웨어 공통모드고장은 다중성을 갖고 있는 안전계통의 기능들을 상실시킬 가능성을 갖고 있기 때문에 소프트웨어 공통모드고장에 대한 대비책으로서 심층방어 및 다양성 설계가 요구되고 있으며, 이 같은 내용을 중요하게 평가하고있다.

디지털 기기 검증

일반적으로 기존 원자력발전소의 아날로그계통 설계의 경우에도 안전관련 계통 또는 설비는 사전에 엄격한 기기검증 시험이 수행되어져 왔다. 원전에서 사용되고 있는 기기에 대한 성능검증시험은 지진발생으로 인한 진동조건하에서 설비의 건전성을 보장하기 위한 내진검증시험과 원전 사고로 인한 극한 환경조건하에서 설비의 건전성을 보장하기 위한 내환경 검증시험으로 분류된다. 따라서 이러한 기기검증 시험요건은 디지털설비의 경우에도 동일하게 적용되고 있다. 그러나 응답속도가 빠른 디지털 논리회로를 이용한 시스템들은 일반적으로 전자기/라디오주파수장해(EMI/ RFI) 영향에 민감한 것으로 밝혀졌으며, 거짓 신호가 합리적인 논리신호로 잘못 해석될 수도 있다. 따라서 디지털설비의 경우에는 특히 낮은 전압레벨에서 운전되고 있어서 전자기파와 같은 주위의 환경인자에 민감하게 영향을 받을 수 있기 때문에 기존의 아날로그설비에서 크게 고려



하지 않았던 전자기파 장해(EMI) 영향에 대한 대응능력(EMC)을 갖출 것을 요구하고 있다. 그 외에도 써지저항능력(SWC)의 확인에서는 디지털시스템이 원자력발전소의 환경적인 과도현상에 견딜 수 있는지와 정전기방전(ESD)도 디지털기기의 동작을 불가능하게 할 수 있기 때문에 정전기방전에 대비한 검증이 요구되고 있다.

실시간 성능

실시간(real time) 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 몇 가지 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 엄격하게 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.

데이터 통신계통 독립성

데이터통신계통은 일반적으로 특수한 하드웨어와 내장 소프트웨어, 그리고 모(mother) 계통과 상호 연결된 컴퓨터에서 운영되는 통신프로토콜 소프트웨어로 이루어진다. 원자력발전소의 안전계통에 사용되는 데이터통신계통에 대한 규제기술현안으로는 데이터통신계통의 독립성설계, 통신프로토콜, 그리고 통신 매체 등이 있다.

데이터통신계통의 구조는 일반적으로 동일한 채널의 컴퓨터들간 데이터통신, 다른 채널들간 데이터통신, 또는 안전등급이 서로 다른 컴퓨터들간 데이터통신 등으로 설계될 수 있다. 또한 안전계통의 컴퓨터시스템은 단일 안전채널내의 컴퓨터들간, 안전채널들간, 그리고 안전급 컴퓨터와 비안전급 컴퓨터간에 수준 높은 데이터 통신을 하게 된다. 이런 통신능력을 부적합하게 사용하면 소정의 많은 기능들을 수행해야 하는 컴퓨터가 그 기능을 상실하게 되고, 그로 인해서 안전계통이 그 기능을 수행할 수 없게 된다. 이와 같은 통신구조가 부적합하게 설계되면 모 계통(예: 원자로보호계통 등)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.

상업제품 인증

원자력산업계는 일반적으로 원자력관련 법규[6,9]의 "원자력 등급" 기준을 적용 받는 판매자로부터 기기들을 구매하여 설치 및 사용하고 있다. 그러나 원자력산업은 시장 규모가 작고 지난 수년간 세계적으로 원자력산업이 쇠퇴하였기 때문에 몇몇 기기 판매업자들은 기존의 원자력 등급 생산라인을 폐쇄하고 있는 추세이 있다. 또한 납품업체수의 감소로 인해서 원자력 등급 장비/기기의 값이 크게 증가하고 있다. 따라서, 일반산업계에서 널리 쓰이고 있는 저비용의 풍부한 운전이력을 갖는 상업용 장비/기기들이 원자력 등급과 동등한 품질요건을 만족할 수만 있다면 이 같은 장비/기기의 사용을 고려할 필요가 있다. 결과적으로 상업용 장비/기기를 구매해서 그것을 안전계통에 사용하기 위해 특수한 검증절차, 즉 "인증절차"라고 불리우는 절차에 따라 그 적격성을 확인해서 사용하자는 것이 원전 소유주 또는 업

체의 공통된 의견이다. 여기서 인증절차(dedication)라 함은 원자력관련법규[6,9]의 공식적인 품질보증절차에 따라 개발 및 생산된 기기들과 동등한 수준의 품질을 보증하는 절차이다. 일반적으로 통용되고 있는 인증절차는 상업제품에 대한 필수적인 물리 및 성능 특성들을 정해 놓고 그 제품이 그러한 특성들을 가지고 있는지를 입증함으로써 그 제품의 사용을 인정해 주는 것이다.

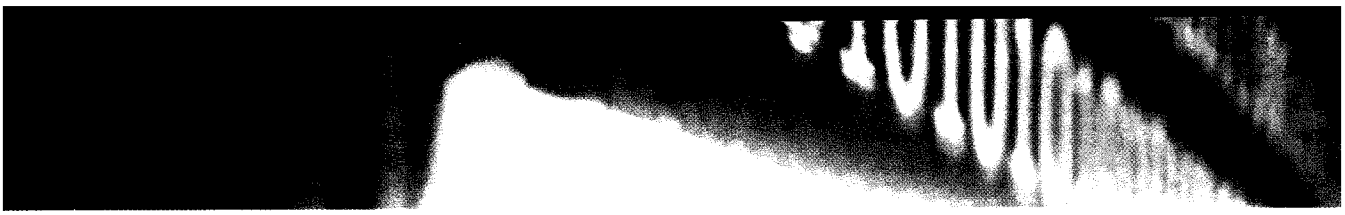
사업 착수단계에서부터 원자력 등급으로 개발된 디지털 계측제어 장비 및 소프트웨어에 대해서는 소프트웨어 설계 및 개발공정을 관리하고 감시하며 정상적인 확인 및 검증을 통해서 요구된 품질을 보증하게 된다. 그러나 상업제품에 대해서는 그러한 절차들이 일반적으로 지켜지지 않았고 품질을 확인할 수 있는 자료가 문서화되지 않았기 때문에 품질을 확인할 수 있는 절차들을 역으로 추적하고 시험 등을 재수행하는 것이 쉽지가 않다. 즉, 디지털 계측제어시스템을 인정해 준다는 것은 소프트웨어의 정확성을 보증해야 하고 소프트웨어 개발공정에 관한 제한된 정보만을 가지고 고장모드들을 확인 및 평가해야 한다는 점에서 매우 어려운 일이다. 일반적으로 원자력발전소의 비안전성 분야에는 소유주의 성능표준을 만족한 상업제품이 사용될 수 있다. 여기서 표준을 만족한다는 것은 일반 용도에서 널리 사용 및 실증되었고 유사한 분야에서 수용 가능한 성능기록을 보유하고 있으면 만족한 것으로 평가한다. 그러나 그 성능이 원자력 안전성과 발전소 인허가 기준에 영향을 줄 수 있는 분야에 대해서는 수준 높은 표준들을 만족해야 하고 이들 제품의 성능과 품질이 인허가 조건을 만족한다는 것을 규제기관에서 승인을 받아야 한다. 그러한 분야에 대해서는 그 제품을 소정의 용도에 맞게 사용하기 위해 관련내용을 평가하고 검증하기 위한 합의된 방법이 필요하다.

현재까지는 상업용 디지털 계측제어시스템을 사안별로 평가해서 인정해 주고 있는 실정이다. 그러나 보다 잘 정의되고 안정적인 접근방식이 필요하며, 중요한 것은 상업제품의 고장 모드 및 영향, 특히 소프트웨어 혹은 하드웨어 고장으로 인한 무의도된 또는 예상치 못한 결과들을 어떻게 평가할 것인가 하는 문제이다. 이것은 안전성에 영향을 줄 수 있는 고장모드들을 찾아내고, 그러한 고장모드들이 주기 시험 등에서 운전원에게 알려지고, 그리고 발전소 시스템과 운전원 절차 및 훈련에서 그러한 고장들을 대처할 수 있음을 보증해야 한다. 따라서, 이 현안에 대한 규제기술은 기존 상업용 컴퓨터가 안전계통에 사용될 만큼 충분히 높은 품질과 신뢰도를 갖고 있는지를 확인하고 평가하는 것이다. 이 현안에서 다루게 될 상업제품에는 프로그램논리제어기(PLC) 사용을 비롯한 각종 디지털 하드웨어와 기성 소프트웨어 및 툴, 그리고 펌웨어 등이 포함된다.

결 론

원자력발전소의 계측제어분야는 컴퓨터기반 소프트웨어, 통신네트워크 및 인간-기계 연계기술들을 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 보완되고 발전될 것으로 예상된다. 이와 같은 측면에서 소프트웨어 신뢰도 및 품질보증, 소프트웨어 확인 및 검증 방법, 심층방어 및 다양성분석, 전자기파 장해를 포함한 기기검증, 실시간 성능, 데이터통신계통 독립성 및 상용제품인증 문제 등이 지속적으로 연구되고 확립되어야 할 주요 규제기술 현안사항들이다.

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 디지털 소프트웨



어 설계과정 중의 철저한 품질보증과 심층방어 및 다양성설계기법을 들 수 있다. 즉, 설계과정 중의 철저한 확인 및 검증활동을 통한 품질보증은 설계 및 운전과정에서 인적실수로 인한 공통모드고장의 발생가능성을 최소화할 수 있으며, 각 설비 및 전체 계측제어계통(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] NUREG-1709, "Selection of Sample Rate and Computer Wordlength in Digital Instrumentation and Control Systems," U.S. NRC, August, 1999.

[3] NUREG/CR-5501, "Advanced Instrumentation and Maintenance Technologies for Nuclear Power Plants," U.S. NRC, August 1998.

[4] Technical Reports No. 367, "Software Important to Safety in Nuclear Power Plants," International Atomic Energy Agency, Vienna, 1994.

[5] 00-68000-SWP-002, "Procedure for the Specification of Software Requirements for Safety Critical Systems," Software Work Practices, AECL, September, 1991.

[6] "원자력관계법령집(원자로시설 등의 기술기준에 관한 규칙)", KINS, 2001

[7] 10 CFR 50, App. A, "General Design Criteria for Nuclear Power Plants", January 1997

[8] KINS/G-001(개정 2) "경수로형 원자력발전소 안전심사지침서", KINS, 1999

[9] 10 CFR 50, App. B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants", January 1997