KAERI/TR-3030/2005

기술보고서

수출전략형 연구로 디지털 소프트웨어 분류 및 설계요건 분석

Investigation of Classification and Design Requirements for Digital Software for Advanced Research Reactors

한 국 원 자 력 연 구 소

Korea Atomic Energy Research Institute

제 출 문

한국원자력연구소장 귀하

본 보고서를 2005 년도 “수출전략형 연구로 계통설계해석” 과제의 기술보고서로 제출합니다.

2005. 6. 30

주저자: 박 기 용
공저자: 정 환 성
류 정 수
박 철

요 약 문

컴퓨터를 기반으로 하는 디지털 기술이 혁신적으로 발달함에 따라 전 산업체에 걸쳐서 계측제어 시스템에 디지털 시스템이 광범위하게 적용되고 있다. 원자력 분야에서도 상업용 신규 원자력발전소에는 디지털 계측제어 시스템이 기존 아날로그 시스템을 대체하여 설치되어 운전하는 추세에 있다. 연구로인 하나로의 경우 안전에 중요한 계통 및 핵심 제어계통은 아날로그 시스템으로 구축되어 운영되어 왔다. 그러나 수출용 연구로의 경우에는 세계적인 추세에 맞추어 보호 및 제어 계통 모두 디지털 시스템으로 구축하는 것이 바람직하다.

컴퓨터 기반 디지털 시스템은 기존 아날로그 시스템이 가질 수 없는 우수한 성능과 구현 및 변경 작업에 있어서 뛰어난 유연성을 가지고 있다. 또한 새로이 개발되는 디지털 제품을 아날로그 시스템에 비하면 별 어려움 없이 기존 제품에 교체 설치하여 시스템 개선을 이룰 수 있는 장점이 있다. 디지털 기술의 발전은 디지털 하드웨어 고 직접화를 구현할 수 있게 하였고 이러한 고 직접화는 전자회로의 부품을 크게 줄이고 아울러 점차 고성능의 연산처리기에 있어서 구동 소프트웨어의 역할을 크게 증대 시켰다. 따라서 디지털 시스템의 전자회로가 단순화 됨에 따라 하드웨어 상의 물리적인 고장은 크게 감소하였으나 소프트웨어의 오류로 인한 시스템 고장 가능성은 상대적으로 크게 증대되었다. 따라서 수출형 연구로에서 디지털 계측제어에 쓰이는 소프트웨어의 안전이 심도있게 고려해야 하는 중요한 고려사항이다. 본 보고서는 이러한 사항에 입각하여 디지털 계측제어 계통에 쓰이는 소프트웨어의 분류와 관련하여 국내외 현황을 파악하였으며 또한 소프트웨어 개발 특히 안전에 중요한 계측제어 시스템에 쓰이는 소프트웨어의 설계요건에 대하여 국제적으로 표준화된 지침을 조사하여 분석한 결과를 기술하였다.

Summary

As the digital technology is being developed drastically, it is being applied to various industrial instrumentation and control (I&C) fields. In the nuclear power plants, I&C systems are also being installed by digital systems replacing their corresponding analog systems installed previously. There had been I&C systems constructed by analog technology especially for the reactor protection system in the research reactor HANNARO. Parallel to the pace of the current trend for digital technology, it is desirable that all I&C systems including the safety critical and non-safety systems in an advanced research reactor is to be installed based on the computer based system.

There are many attractable features in using digital systems against existing analog systems in that the digital system has a superior performance for a function and it is more flexible than the analog system. And any fruit gained from the newly developed digital technology can be easily incorporated into the existing digital system and hence, the performance improvement of a computer based system can be implemented conveniently and promptly. Moreover, the capability of high integrity in electronic circuits reduces the electronic components needed to construct the processing device and makes the electronic board simple, and this fact reveals that the hardware failure itself are unlikely to occur in the electronic device other than some electric problems. Balanced the fact mentioned above are the roles and related issues of the software loaded on the digital integrated hardware. Some defects in the course of software development might induce a severe damage on the computer system and plant systems and therefore it is obvious that comprehensive and deep considerations are to be placed on the development of the software in the design of I&C system for use in an advanced research reactor. The work investigates the domestic and international standards on the classifications of digital software for use in I&C systems in nuclear power plants and describes the requirements for software development recommended by international standard.

목 차

표 목차

그림 목차

1. 서 론

한국원자력연구소에 있는 하나로를 포함한 기존의 연구로나 상용 원자력발전소에서는 계측제어계통은 특히 원자로 보호계통과 같은 안전에 중요한 계통은 아날로그 시스템으로 구축되어 있다. 그러나 아날로그 시스템의 노후화와 기술의 낙후성으로 인해 운전 및 유지보수 비용이 증가하고 안전성까지 위협 받고 있다. 반면에 디지털 기술은 급속도로 발전하여 그 성능의 우수성을 인정 받고 여러 산업 분야에서 활용되고 있다. 원자력 산업에서도 이러한 추세와 보조를 같이하여 비안전에 해당하는 계측제어계통이 디지털화 되었으며, 디지털 기술의 급격한 발전으로 인해 점차 안전계통에도 디지털 기술을 적용하고 있는 추세이다.

디지털 기술은 고 집적화 고밀화 기술이 발달함에 따라 디지털 시스템을 구성하는 전자회로 보드들이 점차로 단순화(compact)되어서 장착되는 부품이 현저하게 줄어드는 추세이다. 반면 집적화된 부품은 고도의 복잡한 기능을 수행할 환경을 제공하게 되고 이러한 기능의 정교한 구현은 소프트웨어 상에서 이루어지게 되었다. 따라서 전자 회로상에서 하드웨어적인 고장 발생 율은 줄어드는 반면 소프트웨어는 역할이 증대됨에 따라 소프트웨어 상의 결함이 중대한 고장을 유발할 가능성은 더 커지게 되었다.

따라서 원자력발전소에 디지털 시스템이 계측제어 계통에 활용화 되는 경우 이러한 소프트웨어의 결함이 없는 고 신뢰도의 소프트웨어를 구축하는 것은 매우 중요한 현안이다. 계측제어 계통에 적용되는 소프트웨어를 개발할 때에는 모든 소프트웨어에 대하여 동일한 수준의 품질과 기술 수준을 적용하는 것은 매우 어렵고 방대한 일이다. 계측제어 계통이 원전 안전과 관련하여 등급을 부여하여 등급 별로 적합한 품질 보증과 기술 수준을 적용하듯이 소프트웨어에서도 이러한 기법을 적용하는 것이 바람직한 일일 것이다.

따라서 본 보고서는 국내외 적으로 원전에 적용하는 소프트웨어를 어떠한 방식으로 등급을 정하였는지 파악하여 그 결과를 기술하였으며 이렇게 분류된 소프트웨어를 어떠한 절차와 수준으로 설계하는 지 파악하였다. 전반적으로 소프트웨어 분류는 디지털 계측제어 계통의 하드웨어 분류 방식에 따라 같이 분류되었으며, 안전에 매우 중요한 기능을 수행하는 기기에 적용되는 소프트웨어는 가장 엄격한 수준의 품질 및 기술을 적용하였다. 따라서 본 보고서는 소프트웨어 설계시 필요한 사항을 기술함에서 가장 수준이 높은 안전-필수 혹은 안전 소프트웨어에 대한 설계 요건에 대하여 국제적으로 표준화된 자료를 기반으로 기술하였다. 계통 기술에 있어서도 안전에 중요한 계통에 대하여 주로 기술하였다.

2. 디지털 소프트웨어 안전 등급 분류

디지털 계측제어 계통 내에서 사용되는 소프트웨어는 일반적으로 디지털 계측제어 계통의 안전 등급 분류에 따라 나누어 지며, 이러한 등급에 따라서 여러 품질 및 안전 요건의 수준이 나누어 진다. 본 장에서는 국외 여러 나라에서 원자력발전소의 계측제어 계통의 안전 등급 분류에 대하여 기술하며 특히 국제적인 표준 기능을 포함하고 있는 국제 원자력 에너지 기구(IAEA)에서 분류한 등급과 국제 전기기기 표준(IEC)에서 분류한 등급에 대하여 등급 분류를 위한 배경 및 원리와 이를 기반으로 분류된 등급에 대해서 자세하게 기술하고 마지막으로 국내에서 계측제어 계통에 대한 안전 등급 분류에 대하여 기술한다.

2.1 국제 원자력 에너지 기구(IAEA)의 안전 등급 분류

국제 원자력 에너지 기구에서는 원자력 발전소 계측제어 안전 등급 분류를 위한 지침으로서 IAEA 안전 지침서 No. NS-G-1.3 (2002): Instrumentation and Control Systems Important to Safety in Nuclear Power Plants를 발간하였다[2-1-1]. 이 안전 지침서는 계측제어 계통의 안전 등급 분류를 위한 배경 및 방법에 대하여 기술하고 이러한 방법에 의한 분류된 등급 및 해당 계통에 대하여 기술되어 있다. 또한 본 지침서는 이렇게 분류된 등급을 기준으로 계측제어 계통의 여러 주요 고려 인자에 대한 기술적, 품질상의 설계 요건에 대해서도 기술하고 있으나 본 보고서에서는 설계 요건에 대한 내용은 기술하지 않고 안전 등급을 분류한 원리 및 분류된 등급에 대해서 기술한다. 본 지침서에 사용된 용어는 2.1.4절에 정리하였으며 인용된 참고문서는 2.1.5절에 있다.

2.1.1 안전 등급 분류 개요

안전에 중요한 계측제어 계통은 안전 그룹에 일부분인 계측제어 계통과 오 동작이나 고장이 현장 작업자나 대중 사람들의 방사선 노출로 전개되는 계측제어 계통을 말한다. 그러한 계측제어 계통으로는 일반적으로 다음과 같다.

- 원자로 보호 계통 (Reactor Protection Systems)
- 원자로 제어 계통 (Reactor Control Systems)
- 정상 원자로 냉각을 감시하고 제어하는 계통
- 비상 전원 공급을 감시하고 제어하는 계통
- 격납용기 격리 계통 (Containment Isolation Systems)

안전에 중요한 품목인 모든 계측제어 계통과 계측제어에 필요한 소프트웨어 및 기기들은 먼저 설계 요구사항에서 파악되어야 하고 그들의 기능과 안전에 대한 중요도에 따라서 분류가 되어야 한다. 안전에 중요한 계측제어 계통은 필요한 계측제어 안전 기능과 그 기능을 수행하는 계통의 정의를 통해서 파악된다.

2.1.2 안전에 중요한 발전소 기능

원자력 발전소를 안전하고 효율적으로 운전하기 위하여 계측제어 계통을 포함하는 중요한 발전소의 기능들이 있다[2-1-2]. 주요 발전소의 안전 기능으로는 다음과 같다.

- 반응도 제어
- 노심으로부터 열 제거
- 방사성 물질의 구속 및 운전상의 방출 제어

가상개시사건 후의 이들 안전 기능을 충족시키는 계통, 구조물, 기기들은 체계적인 방법을 통하여 파악되어야 한다. 이들 주요 기능은 세부적으로 파악하기 위하여 보다 확장되고 구체화된다. 이들 기능의 확장은 사고 조건을 방지하고 사고 조건의 결과를 완화시키는데 필요한 기능들을 포함한다. 이러한 기능들은 정상 운전, 예상 운전 과도사건이 사고 조건으로 전개되는 것을 방지하거나 사고 조건 후의 결과를 완화시키는데 필요한 구조물, 계통 및 기기들에 의하여 이루어 진다.

반응도 제어를 위한 안전 기능으로는 다음과 같다.

- 안전 제한치 내 정상 반응도 제어
- 허용할 수 없는 반응도 과도상태 방지
- 예상운전 과도사건이 설계기준사고 상태로 전개되는 것을 방지하기 위한 원자로 정지
- 사고 상태결과를 완화하기 위한 원자로 정지
- 모든 정지 동작 후 안전한 정지 상태에 있기 위한 원자로 유지.

노심으로부터 열 제거를 위한 안전 기능으로는 다음과 같다.

- 출력 운전 동안 노심으로부터 열 제거
- 적절한 운전 상태에서나 원자로 냉각수 경계가 건전한 설계기준사고 상태에서의 잔열 제거
- 정상운전 상태나 어는 가상개시사건 후의 노심 냉각을 위한 충분한 냉각수 유지
- 원자로 냉각수 압력 경계의 고장 시 핵연료 손상을 방지하기 위한 노심

열 제거
- 노심 열 제거에 사용된 중간 단계의 열침원(heat sink)에서 최종 열침원으로 열 전달.

방사능 물질의 구속 및 운전 방출의 통제에 대한 안전 기능으로는 다음과 같다.
- 노심 핵연료 보호막 건전성 유지
- 원자로 냉각수 압력 경계의 건전성 유지
- 방사성 물질 누출 제한 및 방사선 피폭 최소화

상기한 안전에 중요한 기능들은 계측제어 계통을 포함하는 공학적 설비에 의해 수행되어야 한다. 안전에 중요한 계측제어 계통의 주요 기능으로는 다음과 같다.
- 보호 기능
- 제어 기능
- 감시 및 표시 기능
- 시험 기능

상기한 주요 기능 이외에도 이들 기능을 보조하는 기능들이 있다. 계측제어 계통의 주요기능에 대한 항목 별 특징으로는 다음과 같다.

(1) 보호 기능

보호 기능은 발전소 다른 계통에서 고장 발생시 대처하는 기능을 제공하며 안전 기능들 중 가장 중요한 것들 중의 하나로 원자력 안전과 직접적으로 관련이 있다.

(2) 제어 기능

제어 기능은 발전소가 정상 및 비 정상 조건에서 운전 영역 내에서 제어되고 유지될 수 있도록 하는 기능을 말한다. 제어 기능은 발전소 과도상태나 가상 개시사건의 영향을 완화시켜 보호 기능의 동작을 최소화 함으로써 원자력 발전소 안전에 기여할 수 있다.

(3) 감시 및 표시 기능

감시 및 표시 기능은 발전소와 운전 및 유지 보수 요원과의 연계를 제공한다. 이러한 기능들은 발전소 운전자가 변동 상황을 감지하여 발전소를 안전 운전 영역 내로 유지하는 기능을 제공한다는 점에서 안전에 중요하다.

(4) 시험 기능

시험 기능은 안전에 중요한 다른 기능이 사용 가능하며 효과적이라는 것을 보증하거나 안전에 중요한 다른 기능이 저하되지 않았다는 것을 확신하는 기능을 제공한다.

반응도 제어와 관련이 있는 기능을 수행하는 계측제어 계통에 대한 일례로써는 다음과 같다.

- 원자로 정지를 개시하기 위한 계통
- 운전 변수를 감시하고 다음과 같은 제한치 내에서 유지하기 위한 계통
  - ☞ 안전에 중요한 운전 제한치 (냉각수 온도 제어 계통)
  - ☞ 안전 해석에서 초기 조건으로 설정한 제한치 (원자로 출력 제한치를 위한 제어 계통)
- 계통의 오 동작이나 고장이 반응도 제어 계통과 같은 보호 기능을 수행하는 계통의 동작을 야기하는 계통
- 안전정지 상태를 유지하는데 중요한 기능을 수행하는 계통, 예를 들면, 임계치에 대한 여유도 계산을 제공하는 계통
- 예상운전 과도 상태나 설계기준 사고 상태를 방지, 종결, 또는 완화시키는데 중요한 기능을 수행하는 계통 (원자로 출력 감발 계통)
- 예상 과도상태 시 원자로 정지 없이 변동을 완화하는 계통이나 발생 가능한 설계 오차를 고려한 계통과 같은 보호기능을 제공하는 계통의 다양한 백업을 제공하는 계통.

노심 열 제거와 관련된 기능을 수행하는 계측제어 계통에 대한 예는 다음과 같다.

- 원자로 보호 계통 및 공학적 안전 설비의 구동 계통과 같이 예상운전 과도상태의 결과로써 명시된 설계 제한치를 초과하지 않도록 하기 위하여, 설계기준사고 상태를 감지하고 사고 결과를 완화하기 위하여, 또는 제어 계통의 불안전한 동작을 보상하기 위한 계통 운전을 자동적으로 개시하는 계통
- 안전에 중요한 발전소 장비들의 적절한 기능 수행을 위하여 필요한 발전소 환경 조건을 감시하고 제어하는 계통.

방사성 물질의 구속 및 운전상 방출의 통제 기능과 사고 누출 제한 기능을 수행하는 계측제어 계통에 대한 예는 다음과 같다.

- 방사선 폐기물 관리나 사용후 핵연료 냉각을 제어하는 계통과 같은 오 동작이나 고장이 방사성 물질의 외부 누출을 야기시키지만 별도의 안전 기능이 구비되지 않은 계통
- 원자로 냉각수 계통으로부터 누수를 감지하고 측정하기 위한 계통

- 지진 감시계와 같은 안전에 악영향을 미치는 자연현상이나 운전 요원에 의한 현상을 감시하고 제어하기 위한 계통
- 사고를 감시하고 평가하기 위한 계통.

안전에 중요한 기타 다른 기능을 보조하는데 사용될 수 있는 계측제어 계통으로는 다음과 같다.

- 안전에 중요한 여러 계측제어 계통에 대하여 보조기능을 제공하는 계통. 즉, 계통간 또는 계통 내 기기들 간에 신호를 전송하는 디지털 데이터 통신계통
- 안전계통의 상태를 감시하는 계통. 즉, 안전 채널의 고장을 감시하거나 안전계통 내에 있는 파이프, 밸브, 또는 펌프의 결함을 감시하는 계통
- 보호계통 시험과 같은 안전계통 운용에 활용될 수 있는 계통
- 통신, 화재 감지, 접근 통제와 같은 안전에 중요한 특수한 계측제어 적용분야에 활용되는 계통.

2.1.3 계측제어 계통 분류

상기한 계측제어 계통들에 대하여 본 IAEA 안전 지침서는 안전에 대한 중요도에 따라 등급 분류를 설정하였다. 구조물, 계통, 및 기기들에 대한 안전 중요도의 분류는 결정론적 방법에 주된 기반으로 하여 분류하되 확률론적인 방법과 공학적 판단이 필요 시 적용될 사항에 보완적으로 활용될 수 있다. 계측제어 계통 분류 시 보호 설계 요구사항을 기반으로 고려하여야 할 사항은 다음과 같다.

- 수행되어야 할 안전 기능
- 계측제어 계통의 고장에 따른 결과
- 계측제어 계통이 안전 기능을 수행하도록 요구될 확률
- 가상개시사건 이후에 계측제어 계통이 동작하도록 요구하는 시간과 주기

상기한 고려 사항 이외에도 다음과 같은 사항도 고려되어야 하며, 이러한 고려사항에 대하여 분류되어야 할 계측제어 계통이 안전에 대한 상대적인 중요도를 정량적 또는 정성적으로 나타날 수 있는 기준을 선택하여야 한다. 아래의 고려사항의 각 항목 별로 기준 예시를 항목과 같이 기술하였다.

- 계측제어 계통이 고장일 경우 가상개시 사건이 발생할 확률과 그 사건의 잠재적 심각도 (예: 방사능 누출 사건의 발생 확률: 높음, 중간, 낮음; 사건 심각도: 높음, 중간, 낮음)
- 계측제어 계통 그 자체가 하나의 가상개시 사건을 유발할 가능성 (즉, 그 계측

제어 계통의 고장 모드), 그러한 가상개시 사건에 대응하기 위하여 안전 계통이나 본 안전 지침서에서 기술한 다른 계측제어 계통의 구비 (계측제어 계통 고장을 감지하는 기능 구비) 및 그러한 가상개시 사건의 발생 확률 및 결과의 조합 (고장 빈도 및 방사능 누출 결과)

- 안전 기능이 개시되면 그 계측제어 계통이 요구되는 시간 길이 (즉, 12시간 까지, 또는, 12시간 이상)
- 다른 대체 동작이 취해지는 것과 관련해서 적절성 및 신뢰도 (중간/낮은 신뢰도, 30분/고신뢰도 이상)
- 계측제어 계통에서 한 고장이 감지되고 보수되는 것에 대한 적절성 (즉, 12시간 까지, 또는, 12시간 이상) 및 신뢰도.

모든 계측제어 계통 각각에 대해 상기 사항들이 고려되면, 계측제어 계통을 분류하여야 한다. 계측제어 계통은 그림 2-1-1에 나타난 바와 같이 크게 다음과 같은 두 가지 부류로 나눌 수 있다.

- 안전에 중요한 계측제어 계통: 이 계측제어 계통은 발전소 안전기능 수행에 참여하는 계통을 말한다.
- 안전에 중요하지 않은 계측제어 계통: 안전에 중요한 계측제어 계통 이외의 계통을 말한다.

안전에 중요한 계측제어 계통은 다음과 같이 두 개로 더 분류할 수 있다.

(1) 안전 계측제어 계통

안전 계측제어 계통은 다음과 같은 중요한 안전기능을 수행하는 안전에 중요한 계측제어 계통이다.

- 원자로의 안전 정지
- 노심으로부터 잔열 제거
- 예상운전 과도사건과 설계기준사고의 파급 효과 제한

(2) 안전 관련 계측제어 계통

안전 관련 계측제어 계통은 안전 계측제어 계통이 수행하지 않는 안전에 중요한 다른 기능들을 수행하는 안전에 중요한 계측제어 계통이다.

안전 계측제어 계통은 보호 기능을 수행하는 계통을 포함하며, 이러한 보호 기능에 해당하는 계측제어 계통으로는 원자로 보호 계통과 특별한 안전 계통들의 하부로 사용되는 계측제어 계통이 있다. 안전 계통의 하부로 사용되는 계측제어 계통

으로는 원자로 정지 계통, 긴급 노심 냉각 계통, 및 격납용기 격리 계통을 들 수 있다. 아울러 안전 계측제어 계통은 사고 후 감시 기능과 관련 보조 기능(예, 보호 계통이나 특별한 안전 계통을 위한 중요 데이터 통신 계통)을 수행할 필요가 있다.

안전 관련 계측제어 계통으로는 제어 계통, 감시 및 표시 계통, 그리고 안전 계측제어 계통으로 분류되지 않은 다른 계통(제어봉 인출 금지나 원자로 출력 감발과 같은 제한 계통, 또는 긴급 급수 계통 구동과 같은 위험 감소 계통)들이 있다. 각 계측제어 계통을 보조하는 계통(전기, 공압/유압 동력 공급, 윤활 계통)은 보조하는 대상 안전 기능의 분류에 따라 분류되어야 한다.

계통간 연계가 필요한 경우 모든 계측제어 계통은 낮은 등급의 계측제어 계통에서 발생한 고장이 상위 등급의 계측제어 계통으로 파급되지 않도록 적절하게 설계된 계통 간 연계를 가져야 한다. 고장 파급을 방지하는 장비들은 계통들의 등급이 다른 경우 상위 등급을 적용한다.

모든 계측제어 계통과 장비는 계통의 명세, 확인 및 검증, 품질 보증, 품질 통제 및 신뢰도가 그 계통이 해당하는 등급에 상응하는 절차에 따라서 설계, 제작, 유지되어야 한다.

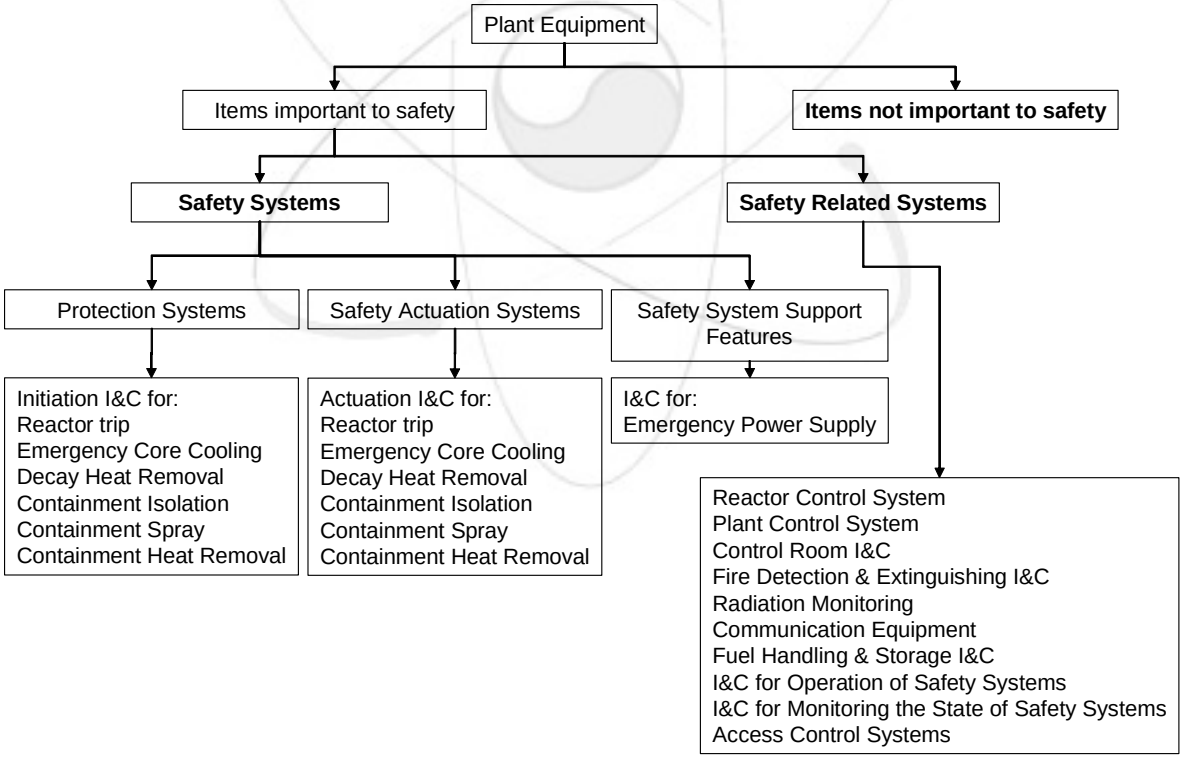


그림 2-1-1. 안전에 중요한 계측제어 계통 분류 및 예제

2.1.4 용어 정의

- **사고 상태 (Accident Conditions)**
  예상 운전 과도 사건 보다는 심각한 정상운전으로부터의 일탈. 설계 기준 사고와 중대사고를 포함함.
- **구동 장비 (Actuated Equipment)**
  하나 또는 그 이상의 안전 업무를 달성하는데 사용된 발동기나 구동 기기의 집합체.
- **구동 장치 (Actuated Device)**
  구동 장비에 대하여 구동력을 직업 제어하는 기기. 구동 장치의 예로 회로 단락기와 릴레이 및 파일럿 밸브 등을 들 수 있다.
- **예상 운전 과도 사건 (Anticipated Operational Occurrences)**
  안전에 중요한 품목에 심각한 손상을 야기하지 않거나 사고 조건으로 전개되지 않는 운전 공정을 말하며 발전 설비의 운영 기간 중 적어도 한번은 발생할 수 있는 정상 운전으로부터의 일탈된 운전 공정.
- **가용도 (Availability)**
  한 계통이 원하는 목적을 수행할 수 있는 시간 분율.
- **우회 (Bypass)**
  어느 한 회로나 계통의 기능을 의도적으로 그러나 임시적으로 정지하는 장치.
- **보수 우회 (Maintenance Bypass)**
  안전 계통 장비를 보수, 시험, 및 수리하는 동안 우회시키는 것.
- **운전 우회 (Operational Bypass)**
  발전소 운전 중 특정 모드에서 어떤 보호 동작이 필요하지 않을 때 그 동작을 우회시키는 것.
- **채널 (Channel)**
  하나의 단일 출력을 개시하는 한 계통 내에서 상호 연결된 기기들의 정렬. 한 채널의 단일 출력 신호가 다은 채널에서의 출력신호와 결합하는 지점에서는 그 채널의 존재는 상실된다.
- **동시성 (Coincidence)**
  보호 계통의 한 특징으로서 여러 채널로부터 두 개 이상의 중첩된 또는 동시 출력신호를 활용하여 논리에 의한 보호 동작 신호를 생성하는 것.
- **공통 원인 고장 (Common Cause Failure)**
  어느 단일 특정 사건이나 원인에 의한 두 개 혹은 그 이상의 구조물, 계통 또는 기기들의 고장.
- **기기 (Component)**
  한 계통의 구별된 한 요소.
- **신뢰성 (Dependability)**

한 계통에 대해서 전반적으로 신뢰할 수 있는 것을 기술하는 일반적인 용어. 즉, 적합한 신뢰가 이 계통에 할당된 정도를 말한다. 신뢰도, 가용도, 및 안전성은 확실성에 대한 특성들이다.

- **설계 기준 사고 (Design Basis Accident)**
  구축된 설계 기준에 따라 설계된 원자력 발전소에 대한 사고 조건을 말하며 핵연료 손상이나 방사성 물질의 누출이 인가된 제한치 내에 있는 사고 조건.
- **다양성(Diversity)**
  정의된 기능을 수행하는 데에 두 개 또는 그 이상의 중복된 계통이나 기기의 존재를 말함. 다른 계통이나 기기는 공통원인고장의 가능성을 감소하기 위하여 다른 특성을 가지고 있다.
- **구동된 장비(Driven Equipment)**
  발동기에 의해 구동되는 펌프나 밸브와 같은 장비를 말함.
- **기능적 격리(Functional Isolation)**
  어느 회로나 계통 또는 다른 것의 운전 모드나 고장에 영향을 미치는 것을 방지하는 것.
- **안전에 중요한 품목(Item Important to Safety)**
  안전 그룹의 부분인 품목이거나 그 고장이나 오 동작이 발전소 요원이나 대중에 방사능 누출을 야기하는 품목.
- **정상 운전(Normal Operation)**
  명시된 운전 제한치나 운전 조건 내에서의 운전.
- **원자력 안전(Nuclear Safety)**
  돌이킬 수 없는 방사능 위험으로부터 작업자, 대중, 및 환경을 보호하는 적절한 운전 조건의 달성, 사고 예방이나 사고 결과의 완화를 말함.
- **운전 상태(Operational States)**
  정상 운전 및 예상운전 과도사건 하에서 정의된 상태.
- **물리적 격리(Physical Isolation)**
  거리나 방향과 같은 배치나 적절한 방벽, 또는 두 가지 상호 결합된 격리.
- **가상 개시 사건 (Postulated Initiating Event)**
  설계 동안 예상 운전 과도 사건이나 사고 조건으로 전개할 수 있는 파악된 사건.
- **발동기 (Prime Mover)**
  모터나 솔레노이드 구동기 또는 공압 구동기와 같이 구동 장치에 의해서 명령되었을 때 에너지를 동작으로 변환하는 장비.
- **보호 계통 (Protection System)**
  원자로의 운전을 감시하고 비정상 조건을 감지한 경우 위험한 조건이나 잠재적으로 위험한 조건을 방지하기 위하여 자동적으로 동작을 수행하는 계통.
- **보호 동작 (Protective Action)**

어느 특정한 보호 구동 장치의 작동을 요구하는 보호 계통의 동작.

- **보호 업무 (Protective Task)**
  주어진 가상 개시 사건에 의해 요구된 안전 업무가 달성되도록 하는 데에 필요한 최소한의 보호 동작의 생성을 말함.
- **품질 보증 (Quality Assurance)**
  어느 품목, 공정, 또는 서비스가 인허가에 명시된 것과 같은 품질 요구사항을 만족하는 것에 대한 적절한 신뢰도를 제공하는데 필요한 계획되고 체계적인 활동.
- **품질 통제 (Quality Control)**
  구조물, 계통, 및 기기들이 기 정해진 요구사항에 상응하는 것을 검증하고자 하는 품질 보증의 일부분.
- **다중성 (Redundancy)**
  대체 구조나 계통 또는 기기를 구비하여 운전 상태나 어느 다른 고장에도 불구하고 요구된 기능을 수행할 수 있도록 하는 것을 말함.
- **신뢰도 (Reliability)**
  어느 계통이 해당하는 기능을 수행하도록 요구 받았을 때에 그 기능에 대한 최소 성능 요건을 만족할 확률.
- **응답 시간 (Response Time)**
  한 기기가 어느 출력 상태에 있을 것을 요구하는 입력 신호를 받은 시간부터 명세된 출력 상태로 도달하기까지의 시간 주기.
- **안전 동작 (Safety Action)**
  안전 구동 계통에 의해 행해지는 단일 동작.
- **안전 구동 계통 (Safety Actuation System)**
  보호 계통에 의해 개시되었을 때에 필요한 안전 동작을 수행하는 데에 필요한 장비의 집합.
- **안전 기능 (Safety Function)**
  안전을 위하여 수행되어야만 하는 특별한 목적을 말함.
- **안전 그룹 (Safety Group)**
  어느 특정한 가상 개시 사건에 대하여 예상운전 과도상태 및 설계기준 사고 시에 설계 기준에 명세된 제한치가 초과되지 않도록 요구되는 모든 동작을 수행하도록 고안된 장비의 집합.
- **안전 제한치 (Safety Limits)**
  인가된 설비가 안전 상태인 것을 보였던 범위 내에서의 운전 매개변수의 제한치.
- **안전 관련 계측 제어 계통 (Safety Related I&C System)**
  안전 계통은 아니지만 안전에 중요한 계측제어 계통.
- **안전 계통 (Safety System)**
  안전에 중요한 계통으로 원자로를 안전하게 정지하거나 노심으로부터 잔열 제거

를 하거나, 예상 운전 과도 상태나 설계 기준 사고 발생시 사고의 결과를 제한하는 기능을 제공하는 계통.

- **안전 계통 보조 설비 (Safety System Support Features)**
  보호 계통 및 안전 구동 계통에 의해 요구되는 냉각, 윤활, 에너지 공급과 같은 보조 기능을 제공하는 장비의 집합.
- **안전 업무 (Safety Task)**
  어느 특정한 가상 개시 사건을 나타내는 하나 또는 그 이상의 변수들을 감지하고, 신호처리를 수행하고, 설계 기준에서 명시된 제한치를 초과하지 않도록 안전 동작을 개시하고 완료하며 안전 계통 보조 설비로부터 어떤 보조기능을 개시하고 완료하는 것.
- **단일 고장 (Single Failure)**
  어느 한 기기가 의도된 안전 기능을 수행하는 능력을 상실하고 이로부터 결정적인 고장을 유발하는 고장.
- **계통 생명 주기 (System Life-Cycle)**
  한 계통이 개념부터 최종 처분까지 거쳐야 하는 모든 단계를 말함.

2.1.5 참고 문서

[2-1-1] International Atomic Energy Agency, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide Series No.NS-G-1.3, IAEA, Vienna, 2002.

[2-1-2] International Atomic Energy Agency, Safety of Nuclear Power Plants: Design, Safety Standards Series No.NS-R-1, IAEA, Vienna, 2000.

2.2 국제 전기기술 위원회(IEC)의 안전 등급 분류

국제 전기기술관련 표준을 제정하는 국제 전기기술 위원회(IEC: International Electrotechnical Commission)에서 국제 원자력 에너지 기구 (IAEA)에서 요청한 안전 중요도에 따라 계측제어 계통을 분류하는 국제 표준을 정하기 위하여 국제표준(IEC 61226)을 발간[2-2-1] 하였다. 본 절에서는 1993년도에 발간한 참고문서 [2-2-1]의 IEC 61226: Nuclear Power Plants - Instrumentation and Control Systems Important for Safety – Classification 및 진행 중인 개정판을 참조하여 이들 기술표준에 명시된 등급 분류에 대하여 기술한다. 본 표준에서도 IAEA의 권고에 따라 계측제어 계통을 분류하는 방법을 주로 결정론적 안전 해석을 기반으로 하였으며, 필요한 경우 확률론적 방법을 이용하여 보완하도록 요구하고 있다.

본 표준은 원자력 발전소에 대한 정보 및 명령 기능, 그 기능을 수행하는 계측제어 계통 및 장비에 대하여 그 기능의 안전에 대한 중요도를 나타내는 분류 등급에 따라 분류하는 방법에 대하여 기술한다. 설계 기준은 이렇게 분류된 등급에 따라 수준이 정해진다. 본 표준에서 기능, 계통, 및 장비는 자동화된 보호, 폐/개회로 제어, 운전자 필요 정보를 제공하는 것을 말한다. 본 표준은 참고문서 [2-2-2]의 IAEA 안전 코드 NS-R-1과 참고문서 [2-2-3]의 안전 지침 NS-G-1.3에 명시된 원리를 준수하며 이러한 코드 및 지침서에 포함된 지침을 원자력 발전소 안전에 중요한 기능을 수행하는 계측제어 계통에 적용하기 위한 구조화된 방법을 정의한다. 본 표준을 기술함에 있어서 사용된 용어는 2.2.6절에 정의되어 있으며 관련 참고문서는 2.2.7절에 기술되어 있다.

2.2.1 안전 등급 분류

계측제어 계통이 수행해야 하는 기능들은 그 기능들의 안전에 대한 중요도에 따라 분류된 등급에 지정되어야 한다. 어느 기능의 안전에 대한 중요도는 그 기능이 수행되어야 할 때 고장에 의한 결과와 예측하지 못한 동작을 할 경우의 결과에 의해 파악되어야 한다. 계측제어 계통 및 장비에 대한 설계와 품질 요건은 이러한 등급에 따라 결정된다.

본 표준의 등급 분류 원칙은 IAEA에서 제시한 다음과 같은 원칙을 따라서 분류하는 작업을 수행하였다. 안전에 중요한 모든 구조물, 계통 및 기기, 그리고 계측제어 계통에 사용된 모든 소프트웨어는 먼저 파악되어야 하고 그리고 나서 안전에 대한 그들의 기능과 중요도에 따라서 분류되어야 한다.

본 표준은 IAEA 안전 지침서 NS-G-1.3 [2-2-3]에서 명시된 분류 전략을 확장하여 안전에 관련된 등급을 세 부류(등급 A, B, C)로 나누고 이러한 등급으로 계측제어 기능들을 분류하기 위한 기준과 방법들을 기술한다. 또한 안전에 직접적으로 역할

을 담당하고 있지 않은 계측제어 기능은 미 분류 등급으로 분류하였다. 안전 계통의 경계에 해당하는 계측제어 기능은 일반적으로 등급 A나 B에 할당하고, 안전 관련으로 정의된 계측제어 기능은 일반적으로 등급 B 또는 C에 할당한다.

2.2.2 안전 등급 개요

원자력 발전소에서 계측제어 계통들은 안전에 대한 중요도가 각기 다른 수준인 기능들을 수행한다. 각 계측제어 계통의 안전에 대한 중요도는 안전에 도달하고 유지하는 것, 그 기능이 구동되어야 할 때 고장이 발생하여 이로 인한 발생 가능한 결과, 및 이러한 결과가 발생할 확률에 따라 결정된다. 따라서 계측제어 기능들을 분류하기 전에 원자력 발전소의 초기 안전 해석이 완료되어야 한다. 계측제어 기능의 가상 고장 시에 발생 가능한 결과의 심각성에 따라서 그 기능을 수행하는 계통이나 장비의 여러 특성(기능성, 성능, 신뢰도)에 대한 확신 수준이 결정된다. 설계, 평가, 인허가 과정을 위하여, 안전 등급 A, B, C는 안전 중요 계측제어 계통 및 장비의 설계/구현 시 적용될 계측제어 계통의 특성에 대한 기술적 및 품질 요건들을 이용하여 정의 되어야 한다.

(1) 안전등급 A (Category A)

안전등급 A는 설계 기준 사건이 발생한 경우 이 사건이 허용 불가 결과로 전개되는 것을 방지하도록 하여 원자력 발전소 안전을 달성하고 유지하는데 주된 역할을 수행하는 기능들을 포함한다. 이러한 역할은 다른 대안 동작이 취해질 수 없는 발전소 과도현상 초기에, 역할을 수행하는 기능 및 계통에 내부 고장이 있더라도, 매우 중요하다. 안전등급 A는 또한 어느 기능의 고장이 안전등급 A에 있는 다른 기능에 의해 완화될 수 없는 경우 허용 불가 결과를 야기하는 사고 상태로 바로 전개되는 기능도 포함한다. 안전등급 A 기능은 고 신뢰도 요건을 가진다. 따라서 안전등급 A에 해당하는 계통이나 기기들은 기능성 및 복잡성에 있어서 제한을 가진다.

(2) 안전등급 B (Category B)

안전등급 B는 원자력 발전소 안전을 달성하고 유지하는데 안전등급 A의 기능을 보조하는 역할을 수행하는 기능을 포함한다. 안전등급 B의 기능들은 특히 발전소 과도 상태에서 통제된 상태로 된 이후에 기 발생한 설계 기준 사건이 허용 불가 결과로 전개되는 것을 방지하거나 설계 기준 사건을 완화시키는 역할을 수행한다. 안전등급 B 기능의 운전이 안전등급 A 기능의 개시 필요성을 덜어줄 수도 있다. 안전등급 B의 기능이 설계 기준 사건을 완화시키는 데에 안전등급 A의 기능을 보완하거나 더 향상시켜 발전소나 장비 손상 또는 방사능 누출

을 방지하거나 최소화 시킬 수 있다.

안전등급 B에 해당하는 기능에 고장이 발생할 경우 가상개시 사건과 같은 심각한 사고를 유발할 수도 있다. 그러나 이러한 사건이 발생하더라도 안전등급 A가 이러한 사건이 심각한 결과로 전개되는 것을 방지하기 때문에 안전등급 B 기능의 안전 요건은 안전등급 A의 안전 요건만큼 높을 필요는 없다. 따라서 안전등급 B의 기능들은 안전등급 A의 기능들 보다 높은 기능성을 가질 수가 있다.

(3) 안전등급 C (Category C)

안전등급 C는 원자력 발전소 안전을 달성하고 유지하는데 부수적이고도 간접적인 역할을 수행하는 기능들을 포함한다. 안전등급 C는 어느 정도 안전 중요도는 있지만 안전등급 A나 B에 분류되지 않은 기능들을 포함한다. 이 등급의 기능들은 설계 기준 사고에 대한 종합 대책에 일부분일 수는 있으나 이러한 사고의 물리적인 결과를 완화시키는 데에나 설계 기준 사고 이상의 경우에 필요한 기능들에 대해서는 직접적으로 관여하지 않는다.

2.2.3 안전등급 분류 기준

안전등급을 분류하는 기준은 아래와 같으며 이러한 기능에 만족하지 않은 계측제어 기능들은 미 분류 등급(NC)으로 분류한다. 여러 등급에 해당되는 기능이 존재하면 그 기능에 대한 등급은 최 상위 등급이 된다.

(1) 안전등급 A

한 계측제어 기능이 다음과 같은 기준들 중 어느 하나를 만족하면 안전등급 A로 분류된다.

a) 발전소를 통제 상태로 만드는데 필요한 기능, 설계기준 사건이 허용 불가 결과로 전개되는 것을 방지하는데 필요한 기능, 또는 설계기준 사건의 결과를 완화시키는데 필요한 기능
b) 고장이나 오 동작이 허용 불가 결과로 전개되고 안전등급 A의 다른 기능들이 그러한 결과를 완화 시킬 수 없는 기능
c) 운전자가 수동으로 발전소를 통제 상태에 이르게 하는 데에 필요한 정보와 제어 기능을 제공하는 데에 필요한 기능.

(2) 안전등급 B

안전등급 A에 분류되지 않고 아래의 기준들 중 어느 하나를 만족하면 안전등급 B로 분류된다.

a) 설계기준 사건이 통제 상태에 도달되고 난 후 사건이 허용불가 결과로

진행하는 것을 방지하거나 그 사건의 결과를 완화시키는데 필요한 기능

b) 통제 상태에 도달한 후 설계 기준 사건이 허용불가 결과로 진행하는 것을 방지하거나 그 사건 결과를 완화시키기 위하여 수동 작업을 수행할 때 필요한 정보 및 제어 기능을 제공하는 기능

c) 정상 운전 동안 발생한 고장이 어느 사고 방지를 위한 안전등급 A 기능 동작을 유발하는 기능.

d) 안전 해석을 통하여 명시된 어느 한 설계기준 사고의 발생 빈도를 현저하게 감소하는 기능.

e) 주요 공정 변수들이 안전 해석에서 가정한 제한치 내에서 유지되도록 하는 발전소 공정제어 기능들로써 그러한 기능 고장 시 안전등급 A 기능의 동작을 직접 유발하는 기능.

(3) 안전등급 C

다음과 같은 기준들 중 어느 하나를 만족하고 안전등급 A나 안전등급 B에 분류되지 않는 기능들은 안전등급 C로 분류한다.

a) 주요 공정 변수들이 안전 해석에서 가정한 제한치 내에서 유지되도록 하는 발전소 공정제어 기능들로써 그러한 기능 고장 시 안전등급 A 기능의 동작을 직접 유발하지 않는 기능

b) 원자력 발전소 설계기준 내에서 심각도가 적은 방사성 누출 또는 핵연료 감쇠를 방지하거나 완화시키는 데에 사용되는 기능

c) 안전등급 A 또는 B의 기능들을 수행하는 계통의 고장을 운전자에게 알려주거나 연속적으로 그 계통의 가용도를 감시하는 기능

d) 어느 설계기준 사건의 발생 빈도 저감을 포함하는 확률론적 안전 목적을 달성하는 데에 필요한 기능

e) 안전 해석을 통하여 명시된 바와 같이 안전등급 A 기능 요구를 저감시키는 기능

f) 안전등급 A 및 B의 기능을 수행하는 계통 중 특히 계통 내 고장이 가상 개시 사건을 야기하는 계통의 신뢰도를 확인하기 위한 시험을 수행하고 계통 상태를 기록하는 기능

g) 원자력 발전소 설계기준 범위 내의 내부 위험(화재, 침수)이 발생한 경우 이를 감시하고 완화시키는 동작을 수행하는 기능

h) 원자력 발전소에서 방사성 누출이나 방사선 피폭과 같은 사건이 발생한 경우 이를 운전자에게 알리고 운전자의 안전을 확인하기 위한 기능

i) 자연 발생 사건 (지진, 강풍) 발생 시 이를 감시하고 완화시키는 동작을 수행하는 기능

j) 설계기준 사고 이상의 사건에 대해 사고 관리 전략(Accident Management

Strategy)을 위하여 안전한 상태를 달성하고 유지하기 위한 기능

k) 심각한 사고의 결과를 최소화하기 위하여 구비된 기능

l) 원자력 발전소 접근 통제를 제공하는 기능

2.2.4 등급 분류 절차

등급분류를 수행하는 절차와 관련된 전반적인 개요는 그림 2-2-1에 나타나 있다.

2.2.4.1 설계 기준 파악

기능의 분류 절차에 있어서 주요 입력 내용으로는 원자력 발전소의 성격과 노형(PWR, BWR, 또는 기타 다른 원자로), 관련 가상개시 사건, 그리고 기계/전기적인 계통 및 기기의 다중성에 대한 주요 설계기준이 있다. 다른 주요 입력으로는 각각의 가상개시 사건에 대하여 중요한 사고를 완화하는 기능과 이를 보조하는 기능을 파악하는 것이다. 가상 개시 사건의 발생 빈도나 결과를 평가함으로써 발전소의 설계 기준을 나타내는 설계 기준 사건으로 진행할 수 있다. 발전소의 설계 특성의 입장에서 운전 상태와 사고 상태의 명시된 범위와 정의된 방사선 제한치가 이 단계에서 반영되어야 한다.

통합된 종합 안전 방책을 이루는 개개 별 안전 원리는 원자력 발전소의 안전을 확신할 수 있어야 하며 이러한 원리는, 파악된 설계기준 사건과 방사선 피폭이 제한치에 있게 하기 위한 성공적인 물리적 방호를 고려함을 통해서, 설계에 반영된다.

발전소의 설계 기준 사건 과 주요 설계 기준(다중성, 격리, 등), 그리고 보호 및 완화 기능과 이 기능을 보조하는 기능은 분류 절차에 중요 입력이 된다. 각각의 계측제어 기능의 안전에 대한 중요도는 원자력 발전소 안전을 달성하고 유지하는 역할과 그 기능 고장의 파급 효과에 따라 결정된다. 따라서 어느 특정 원자력 발전소의 초기 안전 해석은 계측제어 기능을 분류하기 전에 완료되어야 한다.

2.2.4.2 기능 파악 및 분류

안전 관련 기능들은 원자력 발전소 설계 초기에 파악되어야 한다. 이들 기능을 파악하고 이들 기능을 계측제어 기능에 할당하거나 운전자의 작업으로 지정하는 절차는 국제 표준 IEC 60964 [2-2-4]에 따라서 수행되어야 한다. 이러한 초기 기능 파악을 수행한 후, 각각의 기능의 등급 분류는 본 표준에 따라서 수행되어야 한다. 기능의 안전 중요도를 분류하는 방법은 결정론적인 안전 해석을 기반으로 수행되며 필요시 확률론적 방법과 공학적 판단에 의해 보완할 수 있다. 이 때 고려되어야 하는 요인들은 다음과 같다.

- 수행되어야 하는 안전 기능
- 가상개시 사건을 방지하거나 완화하는 데에 그 기능의 역할

- 모든 운전 모드(기동, 정상운전, 재장전, 등) 동안 기능의 역할
- 자연 사건(지진, 홍수, 강풍, 번개) 및 내부 위험(화재, 침수, 미사일, 딴 곳에서 방사능이나 화학품 누출)과 같은 가상개시 사건 발생 시 기능 역할
- 계측제어 기능의 고장 결과
- 계측제어 기능의 오 동작 파급 효과
- 안전 중요 기능을 수행하도록 요구될 확률
- 설계 기준 사건 발생 시 동작하도록 요구될 빈도
- 유지, 보수, 그리고 시험 전략.

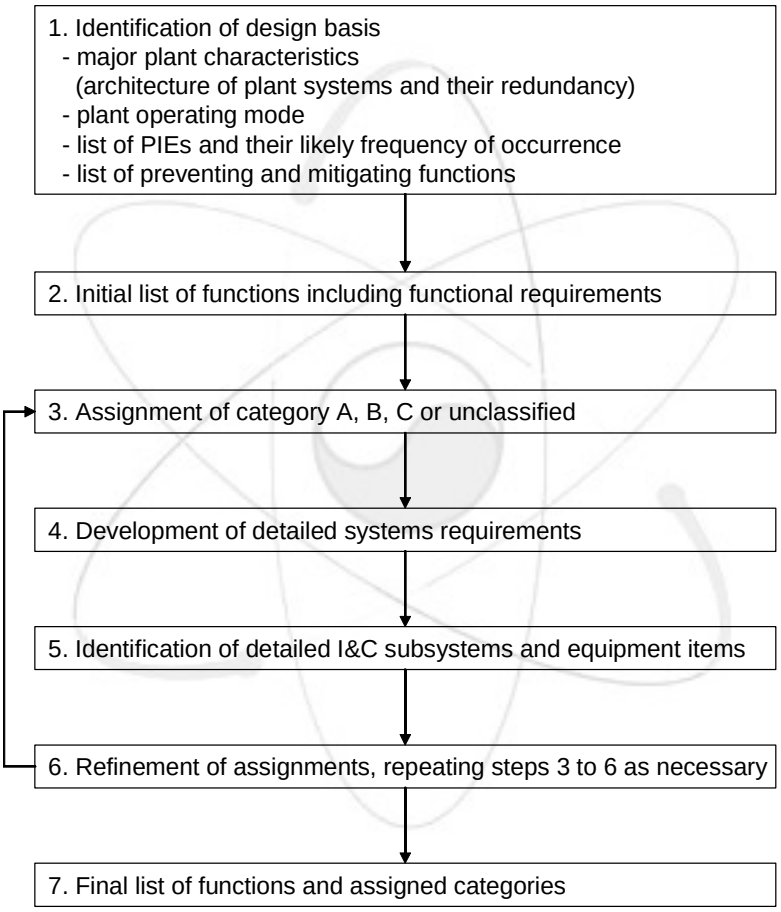


그림 2-2-1. 등급 분류 방법

설계 초기부터 모든 기능을 상세하게 파악하는 것은 불가능하다. 따라서 기능을 파악하고 분류하는 절차는 설계 단계가 진행함에 따라 반복적으로 계속해서 수행하여야 한다. 기능의 등급 초기 분류가 확실하지 않은 경우 그러한 사항을 나타내는 설명 등을 등급에 첨가하여야 한다. 각각의 기능들이 요구사항 명세의 여러 단계의 구현에서 활용될 수 있으므로 그러한 기능들이 여러 등급에 분류될 수 있다. 그러

한 경우에는 최상위 등급을 해당 기능에 할당하여야 한다.

기능에 대한 다중성, 다양성, 및 다른 기술 요건들이 상세하게 결정됨에 따라 분류 목록은 정제되고 개정되어서 최종적인 목록을 도출하여야 한다. 이러한 목록은 문서화 되어야 하고 형상 통제하에 유지되어야 한다.

2.2.5 등급 분류 예제

상기한 등급 분류 절차를 통하여 일반적인 원자력 발전소를 대상으로 하여 분류한 계측제어 기능 혹은 계통에 대한 예제가 다음과 같다.

2.2.5.1 안전등급 A

(1) 전형적인 기능
- 원자로 정지 및 미임계 유지
- 격납용기 격리
- 수동운전 작업에 필수적인 정보 제공.

(2) 전형적인 계측제어 계통
- 원자로 보호 계통
- 안전 구동 계통 및 안전 계통 보조 설비
- 원자력 발전소 운전 지침에 정의된 단기간에 발전소 안전을 확신하는데 필요한 미리 계획된 운전 작업을 가능하게 하는 주요 계측 및 표시기.

2.2.5.2 안전등급 B

(1) 전형적인 기능
- 사용후핵연료 저장조 냉각 계통
- 주 냉각계통 격리
- 사고후 감시 계통
- 1차 및 2차 계통에서 변수들을 안전 해석에서 가정한 제한치 내로 유지하고 또한 사건이 사고로 신속하게 확장되는 것을 방지하는 자동제어
- 고장 발생 시 심각하지 않은 방사선 누출을 야기하는 핵연료 취급 감시 및 제어.

(2) 전형적인 계측제어 계통
- 원자력발전소 자동제어 계통 또는 예방 보호 계통

- 단기간에 필요하지 않지만 잔열(residual heat)을 최종 열침원(heat sink)으로 전송하는 기능을 수행하는 부분
- 원자로 정지 시 핵연료 취급 계통의 안전 회로 및 연동 장치
- 설계기준 사건에 대한 운전 절차에 필요한 계측.

2.2.5.3 안전등급 C

(1) 전형적인 기능
- 사고 후 단계에서 문제 발생의 조기 경보를 획득하고 방사선 누출을 합리적으로 도달 가능한 낮은 수준으로 유지하기 위한 개개의 계통과 장비 품목의 성능 감시 및 제어
- 내부 위험의 결과를 제한
- 작업자의 실수가 심각하지 않은 방사선 누출로 전개하거나 발전소 운전자에게 방사선 위험을 야기할 수 있는 기능
- 내부나 외부 위험(화재, 홍수, 폭발, 지진 등)을 경보 하는데 필요한 기능
- 접근 통제 계통.

(2) 전형적인 계측제어 계통
- 경보 계통
- 방사성 폐기물 흐름 감시 및 연동 장치, 구역 방사선 감시
- 접근 통제 계통
- 긴급 통신 계통
- 제어실 데이터 처리 계통
- 화재 방호 계통.

2.2.6 용어 정의

▪ **예상 과도운전 사건 (AOO: Anticipated Operational Occurrence)**
발전소 운전 기간 동안 한번 또는 몇 번 발생할 수 있는 정상 운전으로부터의 이탈로써, 이러한 이탈이 적절한 설계 작업에서는 안전 중요 품목에 심각한 손상을 유발하거나 사고상태로 진행하지 않는 모든 운전절차를 말한다.

▪ **공통 원인 고장 (CCF: Common Cause Failure)**
하나의 단일 사건 또는 원인에 기인한 두 개 또는 그 이상의 구조물, 계통, 또는 기기들의 고장을 말한다.

▪ **설계 기준 사고 (DBA: Design Basis Accident)**
원자력 발전소가 확립된 설계 기준에 따라 설계된 상태를 벗어나는 사고로 발생

하더라도 핵연료 손상이나 방사성 물질 누출이 허가된 제한치 내에 유지되는 사고 상태를 말한다.

- **설계 기준 사건 (DBE: Design Basis Event)**

  설계 기준 사고 및 예상 과도운전 사건을 통틀어 일컫는 용어.

- **다양성 (Diversity)**

  어느 특정한 목적을 달성하기 위한 둘 이상의 다른 방법이나 수단의 존재를 말한다. 다양성은 특히 공통 원인 고장에 대한 대책으로서 강구되는 방법이다. 다양성은 각각 물리적으로 서로 다른 계통을 구축함으로써 달성될 수 있고 또는, 유사한 계통이지만 다른 방법으로 그 목적을 달성하는 기능적 다양성에 의해 충족될 수 있다.

- **장비 (Equipment)**

  한 계통의 하나 이상의 부품을 말함. 장비 품목은 한 계통에서 단일(single) 정의를 내릴 수 있는 (그리고 제거가 가능한) 요소 또는 부품을 말한다.

- **기능 (Function)**

  수행되어야 하는 특수한 목적이나 목표로써 그러한 목표를 달성하는 물리적 수단을 언급하지 않더라도 분명하게 명시 혹은 기술이 가능한 것을 말함.

- **기능성 (Functionality)**

  입력 정보로 출력 정보를 내는 운전 또는 동작을 정의하는 어느 한 기능의 특성.

- **안전 중요 계측제어 계통 (I&C Systems Important to Safety)**

  계통의 오 동작이나 고장이 현장 종사자나 일반인들에게 치명적인 방사선 피폭을 야기할 수 있는 계측제어 계통과 예상 과도운전 사건이 허용할 수 없는 결과로 전개되는 것을 방지하는 계측제어 계통.

- **발전소 상태 (Plant State)**

<table>
<tr><td colspan="3">운전 상태
(Operational States)</td><td colspan="3">사고 상태
(Accident Conditions)</td></tr>
<tr><td rowspan="3">정상 운전 (Normal Operation)</td><td colspan="2">설계 기준 사건 (DBE)</td><td colspan="3">설계 기준 사고 이상
(Beyond DBAs)</td></tr>
<tr><td rowspan="2">예상 과도운전 사건
(AOO)</td><td rowspan="2">a)</td><td rowspan="2">설계 기준 사고
(DBA)</td><td>b)</td><td>중대 사고</td></tr>
<tr><td colspan="2">사고 관리
(Accident Management)</td></tr>
<tr><td colspan="6">a) Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them
b) Beyond design basis accidents without significant core degradation.</td></tr>
</table>

- **성능 (Performance)**

  의도된 기능이 수행하는데 대한 효과.

- **가상 개시 사건 (PIE: Postulated Initiating Events)**

  예상 운전과도 사건 또는 사고 상태로 전개될 수 있는 설계 단계에서 파악한 사건들.

- **다중성 (Redundancy)**

  동일하거나 다른 형태의 구조물, 계통, 또는 기기를 구비함으로써, 하나가 손실

될 경우 모든 기능이 손실되지 않도록 하는 대비를 말함.

- **안전 그룹 (Safety Group)**
  어느 한 가상 개시 사건이 발생한 경우, 이러한 사건으로 인하여 설계 기준 사건에 대하여 설계 기준이 명시한 제한치가 초과되지 않도록 하는, 모든 동작을 수행하는 장비들의 집합.
- **안전 계통 (Safety Systems)**
  안전 중요 계통으로 원자로 안전 정지, 노심 잔열 제거, 또는 예상 운전과도 사건 및 설계 기준 사고 결과 제한을 확실하게 수행하는 계통.
- **안전 관련 계측제어 계통 (Safety Related I&C Systems)**
  안전 계통은 아니지만 안전에 중요한 계측제어 계통을 말한다.
- **단일 고장 (Single Failure)**
  어느 한 기기가 요구된 안전 기능을 수행할 능력을 상실하게 되는 고장 및 그로 인하여 수반되는 어느 고장들을 말함.
- **계통 (System)**
  설계에 따라 반응하는 기기들의 집합으로써, 한 계통의 어느 요소가 다른 계통이 될 수 있으며 이 경우 하부 계통이라고 한다.
- **허용 불가 결과 (Unacceptable Consequences)**
  운전 상태 혹은 가상 개시 사건의 결과로써, 대상 발전소 상태에 대하여, 현장 및 주변 방사선 누출의 관점에서, 명시된 제한치를 초과한 결과를 말한다.

2.2.7 참고 문서

[2-2-1] International Electrotechnical Commission, Instrumentation and Control Systems Important to Safety - Classification, Standard No.61226, IEC, Geneva, 2004.

[2-2-2] International Atomic Energy Agency, Safety of Nuclear Power Plants: Design, Safety Standard Series No.NS-R-1, IAEA, Vienna, 2000.

[2-2-3] International Atomic Energy Agency, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide Series No.NS-G-1.3, IAEA, Vienna, 2002.

[2-2-4] International Electrotechnical Commission, Design for Control Rooms of Nuclear Power Plants, Standard No.60964, IEC, Geneva.

2.3 국내 안전등급 분류

2.3.1 배 경

국내 규제요건이나 산업기술 기준은 원자력 안전에 중요한 구조물, 계통 및 기기는 수행해야 할 안전 중요도에 상응한 품질보증 요건과 기술기준을 적용 받아야 함을 규정하고 있으나, 원자력발전소 계측제어 계통의 경우 이러한 요건이나 기준을 어떻게 적용할 것인가에 대한 입장이 아직까지 확립되어 있지 못한 부분이 있다. 이것은 계측제어 계통의 안전 중요도를 평가할 수 있는 정량적 척도가 없고, 계측제어 계통이 심층방어(Defense-in-Depth) 관점에서 안전에 미치는 중요도와는 상관없이 원자로 보호계통 또는 안전계통의 일부인가 아닌가에 따라 단순히 안전 등급 1E 또는 비안전등급으로 분류한 사유 때문인 것으로 사료된다.

그러나 디지털 계측제어 계통을 단순히 안전등급 1E 또는 비안전등급으로 분류하기에는 문제가 있다. 공통유형고장(Common Mode Failure)에 대비한 계측제어 계통의 심층방어 계층들은 제어계통, 원자로정지계통, 공학적 안전설비 작동계통, 그리고 감시 및 표시계통으로 구성된다. 이 계통들 중에서 어느 한 계통 이상이 공통유형 고장으로 인해 상실되면 나머지 계통들이 발전소 안전운전에 관여 하게 된다. 그런데 아날로그 계측제어 계통에서는 제어계통의 잘못된 기능이 원자로 보호계통에서 충분히 감당할 것으로 확신할 수 있지만, 디지털 원자로 보호계통의 경우에는 공통유형 고장에 취약하므로, 이러한 역할이 수행될 것인지 의문이 발생한다. 그러므로 이전에 비안전등급으로 분류되는 제어계통의 역할은 실질적으로 경시 되어서는 안되며, 경우에 따라 제어계통이 원자로 보호계통의 기능을 상당히 보완해 줄 수 있는 것으로 평가된다.

이러한 점을 고려할 때, 계측제어계통의 고유한 특성에 맞는 안전등급 분류와 체계가 필요하다. 이러한 사항을 고려하여 현실에 적합한 국내 계측제어 분류를 위하여 한국원자력안전기술원(KINS)에서 분류관련 보고서를 발행한 바 있다[2-3-1]. 따라서 본 절의 국내 계측제어 계통 등급분류는 한국원자력안전기술원의 규제 지침을 기술한 참고문서 [2-3-1]의 보고서를 참조하여 분류 현황을 기술한다.

2.3.2 국내 계측제어 계통 안전등급 분류

원자력발전소 계측제어계통의 안전등급 분류기준은 그림 2-3-1과 같이 발전소 설계 기준에 근거한다. 원자로 보호계통과 안전관련 정보 연동계통 등은 발전소 설계기준사건 (DBE: Design Basis Event)에 대비하여 설계되며, 다양성 보호계통은 원자로 정지불능 과도사건 (ATWS: Anticipated Transient Without Scram) 혹은 원자로 보호계통의 공통유형 고장과 같은 특정 사건에 대비하여 구축된다. 발전소 제어

계통은 발전소 정상운전을 위해 필요한 공정설비들을 계측 및 제어하는 계통들을 포함한다. 그림 2-3-1에 나타난 바와 같이 발전소 설계기준에 근거한 계측제어 계통의 안전등급은 다음과 같이 크게 두 부류로 분류된다.

- 안전에 중요한 계측제어 계통 (I&C Systems Important to Safety):
  여기서 이 분류에 속하는 계측제어 계통을 안전성 계측제어 계통이라 칭한다.
- 안전에 중요하지 않는 계측제어계통 (I&C Systems not Important to Safety):
  안전성 계측제어 계통에 속하지 않은 계측제어 계통으로 여기서는 비안전성 계측제어 계통으로 칭한다.

안전성 계측제어 계통은 다시 안전관련 계측제어 계통(Safety-Related I&C Systems)과 비 안전관련 계측제어 계통(Non-Safety-Related I&C Systems)으로 분류되며, 이러한 계층 구조가 그림 2-3-2에 나타나 있다. 안전관련 계측제어 계통은 다시 안전등급 IC-1, IC-2 및 IC-3으로 분류되고, 비 안전관련 계측제어 계통은 Non-IC로 분류된다. 안전등급 IC-1과 IC-2는 발전소 설계기준 사건에 대비하여 안전관련 기능을 수행하고, 안전등급 IC-3은 특정사건(예, ATWS)에 대비하여 안전관련 기능을 수행하는 계측제어 계통이다. 비 안전등급(Non-IC)은 발전소 정상운전 중에 사용되는 설비이며, 예상운전과도사건(AOO: Anticipated Operational Occurrences) 또는 사고 후에 안전기능을 직접적으로 수행하지는 않지만, 그것의 잘못된 기능 또는 고장이 발전소 안전에 심각한 영향을 주는 발전소 공정설비를 제어하는 계측제어계통이다.

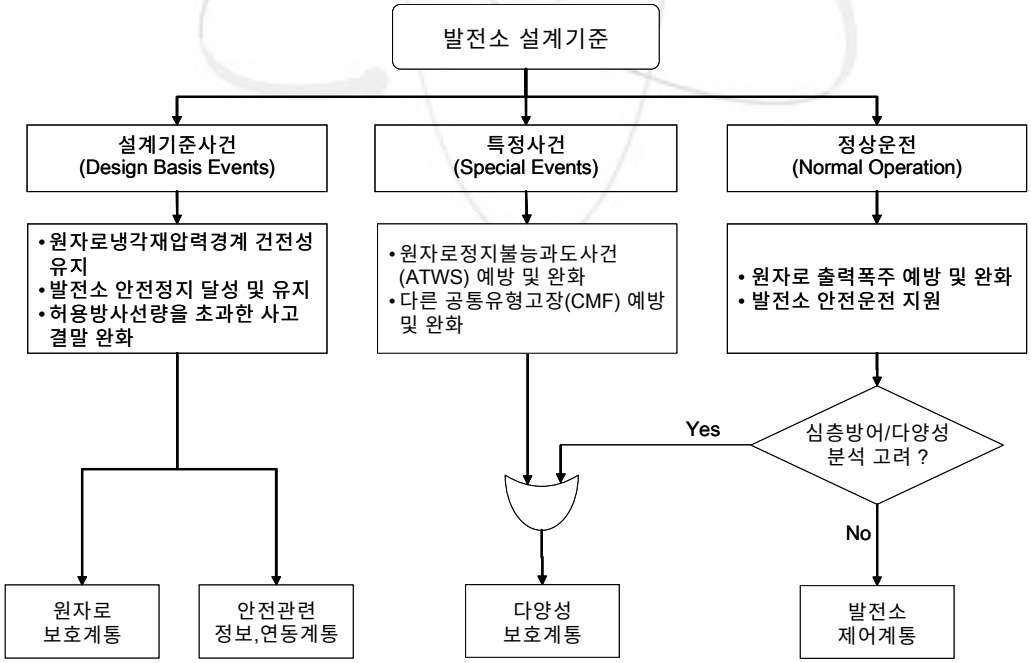


그림 2-3-1. 발전소 설계기준 및 계측제어계통의 안전등급 블록

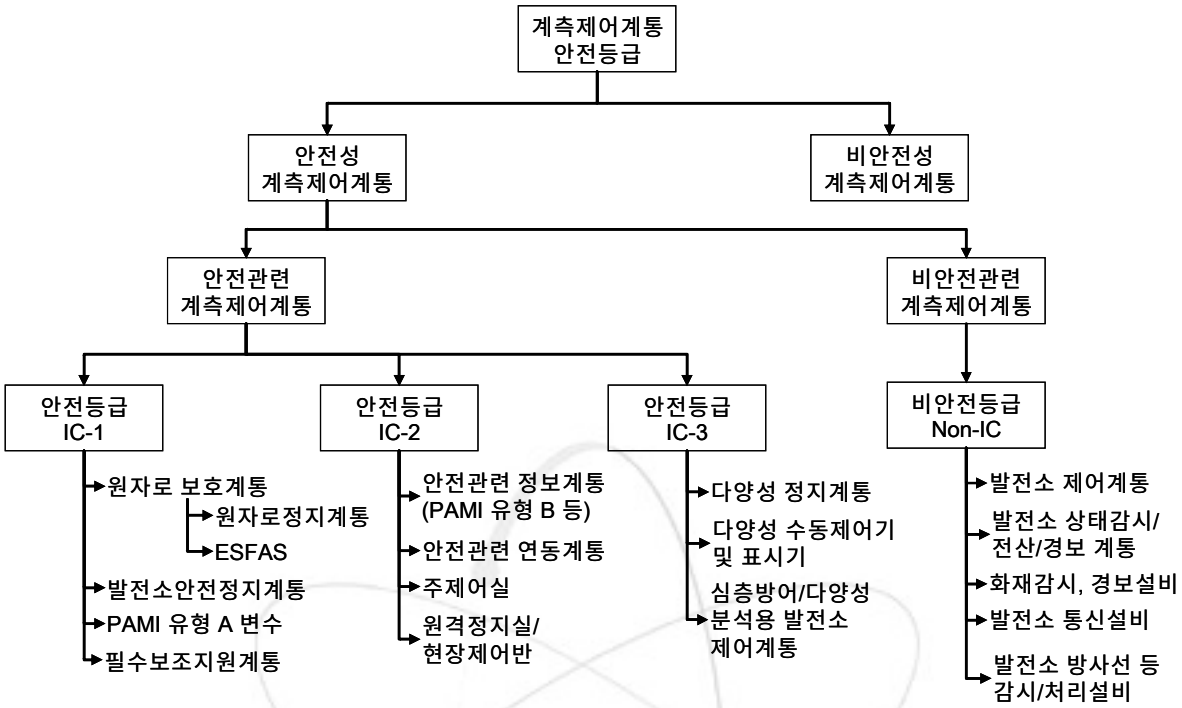


그림 2-3-2. 계측제어계통의 안전등급체계 및 하부계통

2.3.3 계측제어 계통의 안전등급 분류

2.3.3.1 안전등급 IC-1 계측제어 계통

안전등급 IC-1은 원자력발전소의 설계기준사건에 대비하여 안전관련 기능들을 수행하는 원자로 보호계통, 즉 원자로 정지계통(RTS) 및 공학적 안전설비 작동계통(ESFAS)과 발전소 안전정지 및 냉각기능을 수행하는 계측제어 설비, 사고후 감시(PAM) 유형 A 변수 계측 설비, 그리고 필수보조 지원계통을 포함한다. 원자로 보호계통은 원자로 정지기능과 공학적 안전설비 작동기능을 위해 사용되는 공정계측 및 핵계측 신호들을 발생하는 감지, 명령 및 실행 설비 들을 포함한다. 안전정지 계측제어 설비는 노심을 미임계 상태로 진입하게 하고, 그리고 발전소 고온 및 저온 정지 상태를 달성 및 유지하기 위하여 적절한 노심 냉각기능을 수행하는 안전관련 설비들을 포함한다. 자동화된 안전기능이 없는 경우 운전자가 수동 조치를 취하는데 필요한 주요 정보를 제공하고, 설계기준사고 시에는 안전기능을 달성하기 위해서 안전계통에서 반드시 요구되는 사고후 감시 유형 A 변수와 안전등급 IC-1 계측 설비가 안전기능을 수행할 수 있도록 지원하는 필수보조 지원설비, 즉 공기조화 (HVAC), 필수 전력 및 공기, 그리고 필수냉각 설비들이 포함된다.

2.3.3.2 안전등급 IC-2 계측제어계통

안전등급 IC-2는 안전관련 정보계통(PAMI 유형 B, C, D 포함), 안전관련 연동계통, 주제어실, 원격 제어실 및 현장 제어반을 포함한다. 안전관련 정보계통은 발전소 정상운전, 예상운전과도사건, 그리고 사고 시에 안전한 운전을 위해 필요한 정보를 제공하며, 또한 안전계통의 수동 개시 및 제어를 위한 정보를 제공한다. 발전소 정상운전 동안에는 안전계통의 정상상태에 관한 정보뿐만 아니라 우회 및 작동불능 상태에 관한 정보를 제공한다. 안전관련 연동계통은 특정사건의 발생 가능성을 줄이거나 또는 사고 시에 안전계통을 가용한 상태로 유지하는 설비들을 포함한다. 안전관련 연동계통은 그 안전 조치가 사고 이전 또는 사고 예방을 위해 취해진다는 점에서 원자로 보호계통과는 다르다.

2.3.3.3 안전등급 IC-3 계측제어계통

안전등급 IC-3은 다양성 보호계통, 그리고 심층방어 및 다양성 분석용 발전소 제어계통을 포함한다. 다양성 보호계통은 발전소 특정사건, 즉 원자로정지불능사건 완화 또는 원자로 보호계통의 공통유형고장에 대비하여 원자로 보호계통과는 다른 방법으로써 안전기능을 수행하는 설비를 의미한다. 그리고 심층방어 및 다양성 분석용 발전소 제어계통은 디지털-기반 원자로 보호계통의 심층방어 및 다양성 분석에서 고려된 높은 품질의 발전소 제어계통을 포함한다.

2.3.3.4 비 안전등급 Non-IC 계측제어계통

비 안전등급 Non-IC는 발전소 제어계통, 발전소 상태감시 및 진단설비, 전산설비 및 경보계통, 화재감시 및 경보설비, 통신설비, 방사성 폐기물 처리설비, 그리고 사용후 핵연료처리 등의 계측제어 설비를 포함한다. 발전소 제어계통은 예상운전과도사건 또는 사고 후에 안전기능을 직접적으로 수행하지 않지만, 그것의 잘못된 기능 또는 고장이 발전소 안전에 심각한 영향을 주는 발전소 공정설비를 제어하는 계측제어 계통을 포함한다.

2.3.4 디지털 소프트웨어의 안전등급 분류

소프트웨어는 계측제어 계통의 구성 요소이므로, 안전성 계측제어계통에 사용된 소프트웨어 안전등급은 수행되어야 할 기능의 안전 중요도에 따라 3개 등급, 즉 안전성-필수 소프트웨어, 안전성-관련 소프트웨어 그리고 비안전성 소프트웨어로 분류된다.

2.3.4.1 안전성-필수 소프트웨어(Safety-Critical Software)

안전성-필수 소프트웨어는 안전등급 IC-1 계측제어계통에 사용된 소프트웨어로서 가장 엄격한 소프트웨어 품질보증요건과 기술기준을 적용하며, 심층방어 및

다양성 분석결과에 따라 필요하다면 다양성 백업설비가 요구될 수 있다. 원자로 보호계통 소프트웨어 개발에 따른 안전성 분석에서는 소프트웨어 구성요소가 원자로 보호계통에 미치는 위험요소 또는 위험도 분석들을 수행하여 공통유형고장 발생 가능성을 최소화하여야 한다. 소프트웨어 확인 및 검증 활동들은 개발 조직과는 기술, 조직, 책임, 권한 및 재정적으로 독립된 확인 및 검증조직에 의해 수행 되어야 한다.

2.3.4.2 안전성-관련 소프트웨어(Safety-Related Software)

안전성-관련 소프트웨어는 안전등급 IC-2와 IC-3 계측제어 계통에 사용되는 소프트웨어로서 안전성-필수 소프트웨어보다도 완화된 품질보증요건과 기술기준을 적용 받게 된다. 안전성-관련 소프트웨어에 대한 안전성 분석은 요구되지 않지만, 그 소프트웨어가 안전성-필수 소프트웨어에 영향을 미칠 수 있는 위험요소가 있다면 찾아서 시정하여야 하며, 확인 및 검증 활동들은 설계 팀과는 적절하게 독립된 확인 및 검증 조직에 의해 수행되어야 한다.

2.3.4.3 비안전성 소프트웨어(Non-Safety Software)

비안전성 소프트웨어는 비안전등급 Non-IC 계측제어 계통에 사용된 소프트웨어이며, 발전소 안전운전에 적합한 수준의 품질보증 요건과 기술기준에 맞게 개발되어야 한다. 만약 비안전성 소프트웨어가 안전성-필수 또는 안전성-관련 소프트웨어와 함께 동일한 컴퓨터에 탑재(loading)되어 실행된다면, 그 소프트웨어가 다른 상위의 소프트웨어에 미칠 수 있는 위험요소를 분석하고 필요하다면 적절한 보완(예, 격리)을 하여야 한다.

2.3.5 안전성 계측제어계통에 대한 적용 규제지침

표 2-3-1은 원자력발전소 안전성 계측제어계통의 안전등급에 따른 적용지침을 나타내고 있다. 계통 안전등급 분류에 따른 소프트웨어 분류 및 적용도 표 2-3-1에 나타나 있다.

표 2-3-1. 안전성 계측제어계통의 안전등급에 따른 적용지침

안전등급	안전관련 계측제어계통			비안전관련 계측제어계통
	IC-1	IC-2	IC-3	Non-IC
품질 보증	품질등급 1	품질등급 1 준용	품질등급 2	품질등급 3
단일고장기준	적 용	적용/미적용	미적용	미적용

환경 검증(*)	적 용	적 용	적 용	적 용
내진 검증	내진범주 1	내진범주 2	미적용	미적용
전기 등급	안전등급 1E	안전등급 1E/ 비안전등급	비안전등급	비안전등급
심층방어 및 다양성분석	적 용	미적용	미적용	미적용
소프트웨어	안전성-필수 소프트웨어	안전성-관련 소프트웨어	안전성-관련 소프트웨어	비안전성 소프트웨어

(*) 안전성 계측제어 계통이 대처해야 할 특정사건 발생 시 또는 그 이후의 환경조건에 맞게 검증되어야 한다.

2.3.5.1 품질 보증

① 안전등급 IC-1 계측제어계통은 원자로 시설 등의 기술기준에 관한 규칙 [2-3-2], 제2장 “원자로시설의 기술기준,” 제4절 “원자로시설의 건설 및 운영에 관한 품질보증” 또는 품질등급 1에 대한 품질요건[2-3-3]을 만족하여야 한다.

② 안전등급 IC-2 계측제어계통은 원자로 시설등의 기술기준에 관한 규칙 [2-3-2], 제2장 “원자로시설의 기술기준,” 제4절 “원자로시설의 건설 및 운영에 관한 품질보증” 또는 품질등급 1에 준한 품질요건을 만족하여야 한다.

③ 안전등급 IC-3 계측제어계통은 품질등급 2의 품질기준 또는 다양성 계측제어계통에 관한 품질지침을 만족하여야 한다.

④ 비안전등급 Non-IC 계측제어계통은 품질등급 3, 즉 산업기준 또는 규격을 만족하여야 한다.

2.3.5.2 단일고장기준의 적용

① 안전등급 IC-1 계측제어계통은 단일고장기준을 만족하여야 한다. 안전정지 계측제어 설비는 계통-수준의 단일고장기준과 소내 외 전력계통의 운전성을 고려하여야 한다. 단일 고장기준의 적용과 관련해서는 안전성 디지털-기반 계측제어계통에 관한 규제지침 [2-3-1] (이하 규제지침) 5, “단일고장분석”을 참조한다.

② 안전등급 IC-2 계측제어계통은 동 계통이 지원하는 안전계통 또는 안전관련 설비(예, 공학적 안전설비)의 설계기준에 따라 단일고장기준을 적용할 수도 있고, 그렇지 않을 수도 있다. 안전관련 정보계통은 규제지침 14 [2-3-1], “안전관련 정보계통”을 준수해야 한다. 특히, 범주 1 사고감시 계측설비(PAMI)는 다중성, 독립성 및 단일고장기준을 만족하여야 한다. 안전관련 연동계통은 동 계통이 지원하는 안전관련설비의 설계기준을 만족하여야 한다.

③ 안전등급 IC-3의 계측제어 계통은 단일고장기준을 만족할 필요가 없다. 그러나

동 계통의 가용도(availability) 향상을 위해서는 다중성 설계기준을 적용할 수 있다.

④ 비안전등급 Non-IC 계측제어 계통은 단일고장기준을 만족할 필요가 없다. 그러나 동 계통의 가용도 향상을 위해서는 다중성 설계기준을 적용할 수 있다.

2.3.5.3 환경 검증

① 안전등급 IC-1 계측제어계통은 규제지침 8 [2-3-1], “기계 및 전기 기기의 기기 환경검증”과 규제지침 9, “전자파 환경검증”을 준수하여야 한다.

② 안전등급 IC-2 계측제어계통은 동 계통이 대처해야 하는 특정사건 발생 또는 그 이후의 환경조건에 맞게 규제지침 8, “기계 및 전기 기기의 기기 환경검증”과 규제지침 9, “전자파 환경검증”에 따라 적절히 검증되어야 한다. 표시계통 및 기록장치에 대해서는 원자로 보호계통으로부터 분리되는 격리장치만을 환경검증에 포함한다.

③ 안전등급 IC-3 계측제어계통은 동 계통이 대처해야 하는 특정사건 발생 또는 그 이후의 환경조건에 맞게 규제지침 8, “기계 및 전기 기기의 기기 환경검증”과 규제지침 9, “전자파 환경검증”에 따라 적절히 검증되어야 한다.

④ 비안전등급 Non-IC 계측제어계통은 원칙적으로 환경검증을 받지 않아도 되나, 가상된 사고조건에서 그것의 고장이 상위 안전등급 계측제어계통의 안전기능 수행에 나쁜 영향을 주는 기기는 상위 안전등급의 계측제어계통과 동등한 수준의 환경검증을 받아야 한다.

2.3.5.4 내진 검증

① 안전등급 IC-1 계측제어계통은 내진범주 1의 규제요건과 기술기준에 맞게 검증되어야 한다.

② 안전등급 IC-2 계측제어계통은 지진이 진행하는 동안 또는 이후에 소정의 안전기능을 수행해야 한 경우는 그에 상응한 지진조건에서, 즉 내진범주 2의 요건과 기술기준에 맞게 검증되어야 한다.

③ 안전등급 IC-3 계측제어계통은 내진 검증을 고려할 필요가 없다.

④ 비안전등급 Non-IC 계측제어계통은 발전소 특정 사건과 동시에 지진 발생을 가정하지 않으므로 내진 검증을 고려할 필요가 없다.

2.3.5.5 전기 등급

① 안전등급 IC-1 계측제어계통은 안전등급 1E 요건과 기술기준을 만족하여야 한다.

② 안전등급 IC-2 계측제어계통은 동 계통이 지원하는 안전계통 또는 안전관련 설비의 설계기준에 따라 안전등급 1E 요건을 적용할 수 있고, 그렇지 않을

수도 있다.

③ 안전등급 IC-3 계측제어계통은 안전등급 1E 요건을 만족할 필요가 없다.

④ 비안전등급 Non-IC 계측제어계통은 안전등급 1E 요건을 만족할 필요가 없다.

2.3.5.6 심층 방어 및 다양성 분석

① 원자로 보호계통에 대해서는 심층방어 및 다양성 분석이 수행되어야 한다. 그 분석은 규제지침 12 [2-3-1], “디지털-기반 계측제어계통의 심층방어 및 다양성 분석”을 참조한다.

② 안전등급 IC-2 계측제어 계통은 심층 방어 및 다양성 분석을 수행할 필요가 없다.

③ 안전등급 IC-3 계측제어 계통은 심층 방어 및 다양성 분석을 수행할 필요가 없다.

④ 비안전등급 Non-IC 계측제어 계통은 심층 방어 및 다양성 분석을 수행할 필요가 없다.

2.3.5.7 소프트웨어 안전등급

① 소프트웨어 등급별 적용지침은 규제지침 6 [2-3-1], “소프트웨어 품질보증 및 개발공정”을 적용한다.

② 소프트웨어 등급별 확인 및 검증 활동들은 규제지침 6, “소프트웨어 품질보증 및 개발공정”에서 상세히 다루고 있다.

2.3.6 규제영향 분석

2.3.1절의 배경에서 언급한 바와 같이 현행 규제요건 및 산업기술 기준에서는 원전 사업자(또는 설계자)가 원전의 설계, 건설, 및 운영에 있어서 안전에 중요한 구조물, 계통 및 기기를 일관되고 체계적인 분류기준에 따라 안전 등급을 부여하고, 이에 상응한 등급별의 품질보증 요건과 기술기준을 적용하도록 융통성을 부여하고 있다. 그러나 지금까지 계측제어 계통에 관한 안전 중요도를 평가할 수 있는 정량적인 척도가 없고 중요도에 따른 등급별 환경검증 및 품질보증 요건이 수립되어 있지 않으며 안전 중요도별 계측제어 장비를 분류하고 관리하기가 매우 복잡하고 그로 인한 간접비 부담이 크다는 이유로 계측제어 계통을 단순히 등급 1E 및 Non-1E로만 분류하여 왔다. 이와 같은 기존의 분류방식은 공통원인 고장에 취약한 디지털 계측제어 계통에 적용하기에는 많은 문제점이 있는 것으로 지적되고 있다. 본 절의 분류는 이러한 사항을 고려하여 현행 국내 안전등급 분류방식을 일부 보완하여 분류기준과 체계를 제시하고 있다.

2.3.7 용어 정의

- **가용도 (Availability)**
  어떤 시스템이나 기기가 임의의 시점에서 요구될 때 운전 중일 확률이다.
- **내진등급 I (Seismic Classification I)**
  안전정지지진(SSE) 발생시 또는 이후에 소정의 기능을 수행할 수 있도록 설계되어야 할 구조물, 계통, 그리고 기기에 대한 안전등급이다.
- **안전등급 1E(Class 1E)**
  원자로 정지, 비상노심 냉각, 격납용기 격리, 그리고 격납용기 및 노심 잔열 제거에 필수적이거나, 또는 심각한 량의 방사성 물질의 환경 방출을 방지하는 데에 필수적인 전기 기기 및 계통에 대한 안전등급이다.
- **안전성-필수 소프트웨어(Safety-Critical Software)**
  동 소프트웨어의 실패 또는 상실이 발전소 안전에 치명적인 영향을 줄 수 있거나 또는 막대한 재정적 또는 사회적 손실을 초래할 수 있는 소프트웨어이다.
- **유형 A 변수**
  유형 A 변수는 운전자가 자동화된 기능이 마련되어 있지 않는 특정한 수동 제어조치를 취하는데 필요한 일차적인 정보이며, 설계기준사고 시에 안전기능을 달성하기 위해 안전계통에서 필요로 하는 감시변수이다. 여기서 일차적인 정보라 함은 안전기능을 직접 달성하기 위하여 필수적인 정보를 의미하며, 비정상 또는 비상 절차서 수행 기간에 가끔 사용되는 부수적인 동작이나 내용은 포함되지 않는다.
- **유형 B 변수**
  유형 B 변수는 발전소 안전기능이 달성되고 있는지를 나타내는 정보를 제공하는 감시변수이다. 발전소 안전기능들은 반응도 제어, 노심 냉각, 원자로냉각재계통 건전성과 격납용기 건전성 유지기능(방사능 유출 제어 기능)을 포함한다.
- **유형 C 변수**
  유형 C 변수는 방사능 방벽(barrier)의 파손으로 핵분열생성물이 방출되는 것을 고려하여 방벽의 파손 가능성 또는 방벽의 실제 파손을 나타내는 정보를 제공하는 감시변수이다. 원전의 설계에 반영되는 방벽은 핵연료 피복재, 일차냉각재 압력경계와 격납용기이다.
- **유형 D 변수**
  유형 D 변수는 각 안전계통과 안전관련계통의 동작 또는 운전 상태를 나타내는 정보를 제공하는 감시변수들이다. 이 변수들은 운전자가 사고 결과를 완화함에

있어서 안전에 중요한 각 계통을 적절하게 사용할 수 있도록 지원한다.

- **유형 E 변수**

  유형 E 변수는 방사능/성 물질의 방출량을 결정하고 그와 같은 방출을 지속적으로 평가하기 위해 필요한 감시변수이다.

- **확인 및 검증(Verification and Validation)**

  시스템 또는 기기에 대한 요건이 완전하고 정확한지, 각 개발단계의 제품이 바로 직전 단계에서 부여된 요건 또는 조건을 충족시키는지, 그리고 최종 시스템 또는 구성요소가 규정된 요건을 준수하는지를 결정하는 공정이다. 디지털 시스템에 대한 확인 및 검증 활동들은 원자력 안전관련 분야에 사용된 다른 유형의 장비에 대한 설계 확인과 수락 시험에서 종전부터 수행해 왔던 활동들과 같은 것이다.

2.3.8 참고 문서

[2-3-1] 한국원자력안전기술원, 디지털 계측제어계통에 대한 안전 규제 일반원칙 및 규제지침 (안), 2001.

[2-3-2] 원자력법시행규칙, 과학기술부령 제 16호, 원자로 시설 등의 기술기준에 관한 규칙, 2000년 4월 18일.

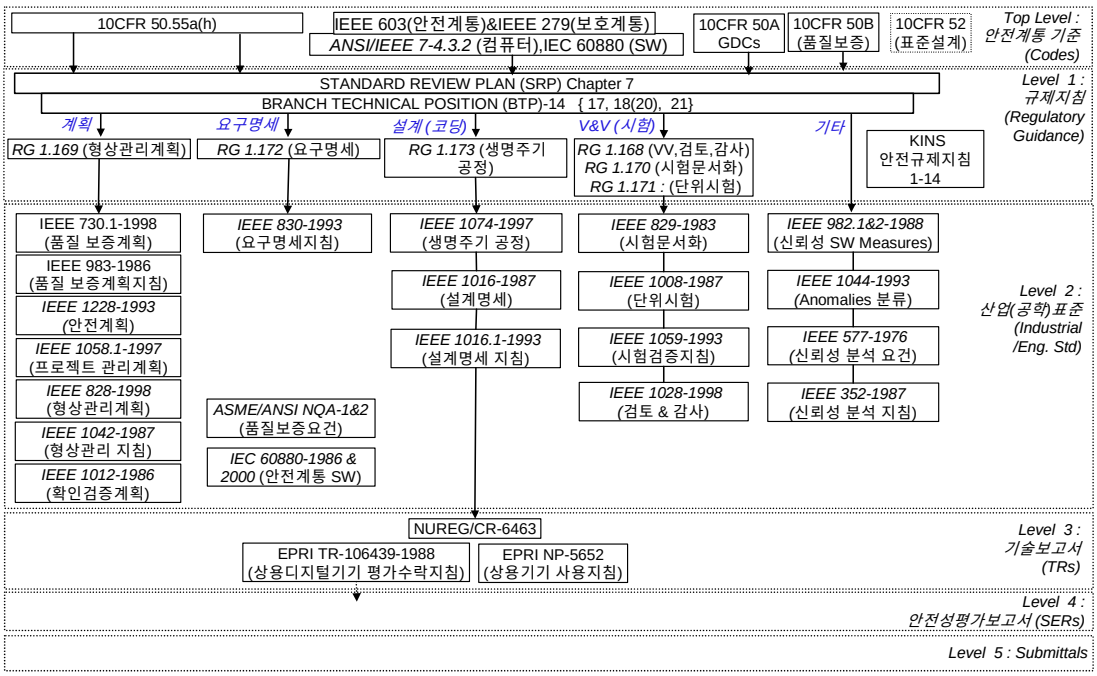
[2-3-3] KINS-G-002(개정 1판), 원자로 시설의 품질보증계획 일반지침, 1997년 10월, 한국원자력안전기술원.

3. 디지털 소프트웨어 규제요건 분석

3.1 개요

안전 기능을 수행하는 계측제어 계통에 탑재되어 구동되는 소프트웨어는 등급별로 개발 시 엄격한 품질 보증과 기술 기준을 적용하여 개발되며 아울러 디지털 소프트웨어는 상기한 기준에 반영되거나 별도로 적용되는 규제 요건을 충실히 준수하여야 한다. 본 장에서는 국·내외적으로 일반적으로 적용되는 안전 기능에 활용되는 소프트웨어 규제요건을 기술한다. 이 장에서는 국내 분류 기준(2.3절)을 따라서 분류된 안전성 소프트웨어의 등급에 대하여 적용되는 요건에 대하여 기술한다[3-1]. 본 장에서의 분류 및 적용 요건은 국제적인 기준과도 크게 다르지 않으며 해외 다른 기준에 대하여 적용할 때에는 본 장에서 인용한 요건을 국제적 혹은 특정 국가의 요건에 대하여 대응시키는 절차에 의하여 적용해 나가면서 크게 상이하거나 본 장에서 미비한 요건은 별도로 국제적 혹은 특정 국가의 요건에 맞는 기준을 적용하면서 분석을 수행해 나가면 좋을 것으로 사려된다.

상기한 바와 같이 안전성 소프트웨어(안전성-필수 및 안전성-관련 소프트웨어)는 기본적으로 원자로 안전 계통의 계통요건을 만족하는 범주에서 소프트웨어 품질과 개발공정 전체에 엄격한 규제 요건이 적용되어야 한다. 그림 3-1은 안전성 소프트웨어 개발을 위한 규제요건의 계층적 구조를 나타낸다.



디지털 안전계통 개발을 위해서는 10 CFR 50 & 52, NUREG-0800 SRP(Standard Review Plan) Chapter 7 [3-2], Branch technical Position(BTP)-14, IEEE Std 603-1991 [3-3], IEEE Std 7-4.3.2-1993 [3-4]의 소프트웨어-관련 규제요건과, 이들 규제요건을 설계 개발에 적용하기 위한 산업계의 기술기준 및 기술 보고서를 안전성 소프트웨어 개발을 위한 규제요건 분석의 범위로 한다. 그리고, 공급자 (Supplier)의 디지털 안전계통 소프트웨어 개발에 따른 규제기관의 안전성 소프트웨어에 대한 최근의 규제동향과 입장을 파악하여 원자로 안전계통의 효율적인 소프트웨어 개발과 인허가에 따른 문제점(인허가 현안)에 대한 대책을 설계 초기단계부터 마련하는데 목적을 둔다.

3.2 규제요건 분석

3.2.1 안전요건 분석

10 CFR 50, SRP Chapter 7, BTP-14, IEEE Std 603-1998, IEEE Std 7-4.3.2-1993의 안전관련 요건은 디지털 안전계통 설계의 안전기준으로도 사용된다. 디지털 계통 안전규제 항목은 표 3-1과 같이 요약된다. 표 3-1의 음영표시 항목은 인허가를 위한 디지털 안전계통 소프트웨어의 필수적인 검토 항목이다. 그러므로, 안전성 소프트웨어의 인허가를 위해서는 표 3-1의 안전심사 항목 중 설계 지침의 적합성, 소프트웨어 수명주기(SWLC: Software Life Cycle) 공정, 심층방어 및 다양성, 확인검증, 형상관리, 소프트웨어 개발과 하드웨어/소프트웨어 통합, 기성 소프트웨어, 소프트웨어 도구(Tools)에 대한 기준과 대책마련이 요구된다.

디지털 계측제어계통의 소프트웨어는 공통모드고장의 발생가능성 때문에 안전현안으로 쟁점화되어 왔으며, 소프트웨어에 의한 공통모드고장 문제를 해결하기 위해 심층방어 (Defense-in-Depth) 및 다양성(Diversity) 설계를 적용한다.

안전계통 소프트웨어의 신뢰도분석에 IEEE Std 352-1987[3-5] 을 적용하기 위해서는 척도의 표준화가 더 필요하며, NUREG/CR-5930, “고-건전성(High Integrity) 소프트웨어에 대한 표준지침”은 기존 지침서들의 문제점을 분석하여 표준화 지침서가 가져야 할 기준을 제시 하고 있다. 그리고 소프트웨어의 안전성을 보장하는 방법으로 소프트웨어 위험도 분석 (Software Risk Analysis)을 요구하며, 그 기준도 함께 제시된다. IEC 60880-2000, Part 2[3-6]는 공통원인고장(Common Cause Failures) 대책, 소프트웨어 도구, 그리고 기성(pre-developed) 소프트웨어의 사용에 따른 안전요건을 규정한다.

미국 원자력규제위원회는 ITAAC(Inspection, Tests, Analyses and Acceptance Criteria) 항목들이 소프트웨어 구조 및 품질과 같은 설계현안(Design Issues)을 반영함으로써 안전규제 요건을 만족하도록 요구한다. 1종 정보는 계측제어계통 장비의 설계, 시험,

그리고 설치에 사용되는 (1) 소프트웨어에 대한 개발공정, (2) 설계공정, 설계준수사항, 설계준수사항의 반영여부에 대한 확인 (검사, 시험, 분석), (3) 적절한 설계가 이루어졌는지의 판단기준(허용기준)을 포함해야 한다. 소프트웨어에 대한 ITAAC은 계획 작성, 설계 정의, 소프트웨어 설계, 소프트웨어 코딩, 통합, 검증, 변경 관리와 같은 설계 단계를 확인해야 하며, 소프트웨어 개발 요소 중 1종 정보는 다음과 같다.

표 3-1. 디지털 안전계통 소프트웨어의 안전심사 항목

<table>
<tr><th colspan="2">안전심사지침
부록7.0-1
디지털계통 검토절차</th><th colspan="2">안전심사지침 7.1
II. 허용기준
디지털 컴퓨터-기반
안전계통에 관한
추가 지침</th><th>IEEE Std
603-1991</th><th>IEEE Std 7-4.3.2-1993</th><th>관련 문서</th></tr>
<tr><td rowspan="11">III.3.1
설계기준
&지침의
적합성

III.3.2
계통
중요도에
따른
검토수준
선택</td><td>III.3.3
심층방어
&다양성
검토</td><td colspan="2">공통모드고장의
방어 대비책
(심층방어&다양성)</td><td></td><td>부록 B</td><td>SECY-93-087
부록 7-16
(심층방어&다양성)</td></tr>
<tr><td rowspan="4">III.3.4, 6,7
SWLC
공정계획,
이행,
결과물에
대한
검토</td><td rowspan="4">컴퓨터
시스템
품질</td><td>SW개발과
HW/SW
통합</td><td rowspan="4">§5.3
품질</td><td>§5.3 품질
§5.3.1 SW 개발</td><td>부록 7-13 (검토지침)</td></tr>
<tr><td>기성 SW</td><td>§5.3.2 기성 SW,
부록 D</td><td>부록 7-15(PLC),
EPRI-TR-106439</td></tr>
<tr><td>SW 도구</td><td>§5.3.3 SW Tools</td><td>EPRI-TR-106439</td></tr>
<tr><td>확인&검증</td><td>§5.3.4 확인 및 검증,
부록 E</td><td>부록 7-13</td></tr>
<tr><td rowspan="5">III.3.5
개별
시스템의
기능
요건
검토</td><td>형상 관리</td><td>§5.3.5 형상관리</td><td>부록 7-13</td></tr>
<tr><td>기기
검증</td><td>기기
검증 (EQ)</td><td rowspan="2">기기검증</td><td rowspan="2">§5.4 기기검증,
부록 C</td><td>IEEE 323, 344</td></tr>
<tr><td>전자파
적합성</td><td>전자파검증
(EMI/EMC)</td><td>EPRI TR-102323</td></tr>
<tr><td colspan="2" rowspan="2">시스템 건전성</td><td rowspan="2">§5.5
계통 건전성</td><td>§5.5.1 컴퓨터 건전성</td><td>부록 7-17
(실시간 성능)</td></tr>
<tr><td>§5.5.2 시험 및 교정</td><td>부록 7-14
(자기시험)</td></tr>
<tr><td colspan="2">통신독립성
(안전-비안전 격리)</td><td>§5.6
독립성</td><td>§5.6 독립성, 부록 G</td><td>7.9절</td></tr>
<tr><td></td><td colspan="2">신뢰도</td><td>§5.15
신뢰도</td><td>§5.15 신뢰도 ,부록 H
R.G 1.152에서 부록
A-H와 정량적인
신뢰도 평가에만
의존하는 것을 승인하지
음</td><td>부록 7-13
(SW 검토지침)</td></tr>
<tr><td></td><td colspan="2">New SW 개발방법론
(정형적 방법,
비절차성 언어)</td><td colspan="3">- SRP 7.1 II 허용기준 중 상기 7가지를 대체 불가
- 관련기술의 미완성단계</td></tr>
</table>

(a) 소프트웨어 품질보증 계획서 (SQAP: Software Quality Assurance Plan): 관리되고 수행되어야 할 소프트웨어의 활동을 기술. SQAP는 다른 소프트웨어 개발계획서의 작성기준 수립.

(b) 소프트웨어 관리 계획서 (Software Management Plan): 설계조직과 권한체계, 절차, 주요 활동간 상호관계 수립.
(c) 소프트웨어 형상관리계획서 (Software Configuration Management Plan): 소프트웨어 제품들을 파악하고, 변경 사항을 관리하고 이행; 변경이행 상태를 기록하고 보고하는 방법의 제시.
(d) 소프트웨어 개발 계획서 (Software Development Plan): 소프트웨어 수명주기에 따른 개발공정, 도구문서, 제품의 기술.
(e) 소프트웨어 확인 및 검증 계획서 (Software Verification & Validation Plan): 설계공정에서 수명주기 각 단계의 요구사항이 그 다음 단계에서 완전하고 정확하게 구현되었는지에 대한 보장 방법을 기술. 안전관련 소프트웨어 모듈은 그 소프트웨어 모듈을 개발한 조직과 독립된 조직이 확인 및 검증을 수행한다.
(f) 소프트웨어 안전 계획서 (Software Safety Plan): 안전성 및 위험요소에 대한 분석 사항을 기술.
(g) 소프트웨어 운영 및 유지보수 계획서 (Software Operation & Management Plan): 소프트웨어가 정확하게 운영되고 소프트웨어의 품질이 유지되는지를 보장하는데 필요한 절차의 기술.

상기한 1종 정보들은 소프트웨어 관리 계획서, 형상관리 계획서, 그리고 확인 및 검증 계획서 속에 통합될 수도 있는데, 이는 표준설계인증을 위한 표준설계기술서(1종 정보)가 위의 정보들을 기술해야 함을 시사한다. 예를 들면, System 80+ 설계관리 문서 작성에서는 보호계통, 공학적 안전설비-기기제어계통, 이산 지시 및 경보계통(DIAS), 데이터처리계통(DPS), 출력제어계통 및 공정-기기제어 계통(P-CCS)으로 구분하여 소프트웨어 개발 요소의 1종 정보를 적절히 기재하고 있다. 원자력안전기술원(KINS)은 ITAAC 문서작성에 대한 지침서를 작성하였다[3-7].

원자력안전기술원은 10 CFR 50, 부록 A [3-8]와 부록 B [3-9], IEEE Std. 603-1991, IEEE Std.-1971, 279, SRP, 그리고 IAEA 안전지침 등이 규정하는 안전기준을 준용하여 국내 규제실정에 맞도록 작성 중에 있다[3-10]. 또한 안전요건의 적용에 있어 기술적으로 타당한 방법, 설계 보완, 또는 대체 방법에 대한 규제 입장을 규제지침에 반영하였다. 안전성 계측제어계통에 관한 안전요건 중 소프트웨어와 관련된 요건은 다음과 같다.

(a) 안전등급 분류 (Safety Categorization)**:** 안전등급 IC-1 계통의 소프트웨어는 안전성-필수 (Safety-Critical), 안전등급 IC-2 및 IC-3 계통의 소프트웨어는 안전성-관련 (Safety-Related)으로 구분. 비안전관련 계측제어계통 (Non-IC)의 소프트웨어는 비안전 소프트웨어로 분류.
(b) 신뢰도**:** 디지털-기반 안전계통에 대한 정성적 또는 정량적인 신뢰도 목표를 설

정한 경우 그 설계분석에는 소프트웨어도 고려하여야 함. 정량적인 신뢰도 목표치 달성뿐 아니라 소프트웨어 개발공정에 따른 철저한 품질활동도 고려함.

(c) 인적요소 고려: 디지털-기반 안전계통의 소프트웨어 개발과 같은 안전 중요도가 높은 계통의 개발에 참여하는 사람은 응용 전문가뿐 아니라 컴퓨터 소프트웨어(및 하드웨어 전문가)를 포함하여야 한다.

(d) 품질: 안전계통의 부품 및 모듈은 최소 보수요건과 낮은 고장율을 갖는 품질을 가져야 한다. 디지털-기반 안전계통의 개발공정은 컴퓨터 하드웨어와 소프트웨어 개발을 모두 포함함. 소프트웨어 개발공정은 소프트웨어 자체개발, 기성 상용 소프트웨어 사용, 소프트웨어 도구사용, 확인 및 검증과 형상관리에서 품질기준을 만족하여야 함.

(e) 독립성: 안전계통과 그 보다 낮은 등급의 계통간의 통신은 단방향 경로를 통해 통신격리기능(예, 소프트웨어 격리)을 확보하여야 함. 양방향 통신은 시험 및 교정 시에만 국한하여 제한적으로 사용함.

(f) 심층방어 및 다양성 (Defense-in-Depth & Diversity): 디지털-기반 원자로 보호계통 설계는 소프트웨어 설계오류를 포함한 공통유형고장의 취약성을 적절히 고려하였는지를 입증하는 심층방어 및 다양성 분석을 수행. 필요하다면 적절한 형태의 백업기능을 마련.

(g) 안전성 위험분석 (Safety Hazards Analysis): 디지털-기반 안전계통과 그 소프트웨어 개발 생명주기 각 단계에서 잘 계획되고 문서화된 안전성 위험분석을 수행. 이 분석에서는 계통의 안전요건이 정확하게 반영되었는지, 새로운 위험요소가 생기지 않았는지, 안전성에 영향을 미칠 수 있는 소프트웨어의 요구사항, 설계 및 코드가 있었는지, 모든 소프트웨어 요구사항, 설계 및 코드가 안전성에 악영향을 미치지 않을 것인지, 그리고 확인된 안전현안과 해결방안 등이 적절한 것인지를 확증.

(h) 접근통제 (Control of Access): 디지털-기반 안전계통 바이러스 등으로부터 보호될 수 있도록 구획화 또는 방호 설계.

3.2.2 개발공정 및 품질 요건분석

IEEE Std 7-4.3.2-1993의 5절은 안전계통 디지털 컴퓨터의 소프트웨어 개발, 상용 소프트웨어의 품질보증, 소프트웨어 도구, 확인 및 검증, 소프트웨어 형상관리에 대한 기준을 규정하고 있다. 또한 신뢰도 목표 달성의 증명에는 사용된 소프트웨어도 포함하도록 규정하고 있다. 한편, 국제 전기기술 위원회(IEC: International Electro-Technical Commission)가 표준으로 채택한 IEC 60880(1986, 2000)에서도 안전계통의 컴퓨터 소프트웨어에 대한 기준을 제시하고 있다. IEC 60880-1986은 안전계통의 소프트웨어 개발에 대한 일반 및 품질보증, 요구명세, 설계 및 코딩, 검증, 하드웨어/소

프트웨어 통합, 컴퓨터시스템 확인, 유지보수 변경, 그리고 운영에 대한 요건을 규정한다. 소프트웨어 품질 및 개발공정에 대한 주요 요건은 다음과 같다.

3.2.2.1 소프트웨어 생명주기 공정 (SLCP: Software Life Cycle Process)

(1) 규제: NRC는 Reg. Guide 1.173[3-11]을 규제기준으로 소프트웨어 생명주기 전체 단계에 대한 감사와 검토를 수행하고 필요한 문서의 종류를 명시하였다. 원자력 안전기술원은 디지털-기반 안전계통의 개발공정에 컴퓨터 하드웨어뿐 만 아니라 소프트웨어 개발을 모두 포함하고, 컴퓨터 하드웨어 및 소프트웨어 통합과 컴퓨터를 안전계통에 통합하는 활동들은 개발공정의 일환으로 수행하도록 요구한다. 소프트웨어 개발공정은 소프트웨어 개발, 기성 상용 소프트웨어 검증, 소프트웨어 도구, 확인 및 검증, 그리고 형상관리 등의 품질기준을 만족하도록 요구한다.

(2) 기술기준: IEEE Std 1074[3-12]는 소프트웨어 생명주기 공정 개발의 활동, SLCP 구성요소, 맵핑(mapping)(활동 순서를 소프트웨어 생명주기 관리(SLCM)에 연결), 그리고 입출력 정보에 대한 기술기준을 규정한다.

3.2.2.2 계획

(1) 규제: NRC는 소프트웨어 생명주기 전체단계에 대하여 감사와 검토를 수행하고 필요한 문서의 종류를 명시하도록 하고 있다. 아울러 IEEE Std 7-4.3.2-1993, Reg. Guide 1.169[3-13]에 의거하여 계획단계에 적용되는 기술기준을 참조하여 규제하고 있다.

(2) 기술기준: IEEE Std 1058.1[3-14]에 의한 프로젝트 관리계획(PMP), IEEE Std 730.1[3-15]에 의한 소프트웨어 품질보증계획(SQAP), IEEE Std 1228-1993[3-16]에 의한 소프트웨어 안전계획 (SSP), IEEE Std 828-1998[3-17]에 의한 소프트웨어 형상 관리계획(SCMP), IEEE Std 1012-1986[3-18]에 의한 소프트웨어 확인검증계획(SVVP) 이 수립되어야 한다.

(3) 문제점: 세부 기술 기준과 한계에서 구체적이고 명확한 규정이 미약한 실정. (애매 모호성을 갖는 예: 프로젝트 관리 계획에서 개발팀과 확인 및 검증 팀의 독립성에 대한 정의; 소프트웨어 안전 계획에서 소프트웨어에 대한 정량적인 신뢰도 명시 및 문서의 세부적인 기술사항.)

3.2.2.3 요구사항 분석

소프트웨어 요구사항 명세(SRS: Software Requirements Specifications)를 작성하고 분석을 수행하는 단계로써, 요구사항 명세는 자연어나 정형언어에 의해 작성되고 요구사항 분석은 수학적으로 증명이 가능한 정형기법(Formal Method)이 권장되며, 특히 안전계통 소프트웨어 개발 시에는 필수적인 방법으로 간주된다. 정형화된 요구사항 명세는 자동화 도구에 의해 개발 시스템의 동작을 모의함으로써 결함을 조

기에 발견할 수 있으며, 그리고 시험 케이스(test case)도 자동 생성할 수가 있다.

(1) 규제: NRC는 Reg. Guide 1.172[3-19]를 규제기준으로 한다.

(2) 기술기준: 요구사항 명세작성의 지침으로 IEEE Std 830-1993[3-20]이 사용될 수 있다.

(3) 문제점: 수학적 형식론(Formalism)은 자연어에 의한 의사전달보다 자연스럽지 못하다.

3.2.2.4 설계

(1) 기술기준: IEEE Std 1016-1987[3-20]은 소프트웨어 설계명세(SDD: Software Design Description) 생산과 SDD 정보내용 및 구조(organization)를 규정한다. SDD 정보내용은 설계 항목(design entity)과 설계항목속성(design entity attribute)로써 기술된다. 항목(entity)은 계통, 하부계통(subsystem), 데이터저장소(data stores), 모듈, 프로그램, 프로세스로 존재할 수 있으며, 각각의 설계항목은 이름, 목적, 기능(function)을 갖는다. 설계의 복잡도, 설계기법, 프로그래밍 환경과 같은 많은 요인에 따라 설계를 몇 개의 항목, 어떤 형태(type)의 항목(entity)으로 나눌(partition) 것인가가 결정된다. SDD 구조는 소프트웨어 프로젝트 활동에 적합한 설계항목속성 정보의 부분집합으로 설계 관점에 의해 기술된다. 그리고, 설계 관점으로써 분할(decomposition) 기술, 독립성(dependency) 기술, 연계 기술, 상세(detail) 기술에 대하여 각각의 범위(scope), 사용(use), 표현(presentation)으로 나누어 기술한다. 부록에는 IEEE/EIA 12207.1-1997과의 준수 지침이 첨부되었다. IEEE Std 1016-1987의 적용과 그 응용범위는 제한적이지 않으며, 특정한 설계, 형상관리, 품질보증 방법론에 국한되지 않는다. 그러므로 문서화(paper documents), 자동화 데이터베이스(automated databases), 설계 명세 언어(design description language), 및 다른 명세수단에 응용될 수 있다.

(2) 문제점: 요구분석에 수학적 정형이론의 응용이 시도되고 있으며, 구조적 설계방법(Structured Design Method)에서 객체지향 설계방법(Object-Oriented Design Method)으로 바뀌고 있다. 이러한 객체지향 설계 및 분석방법이 적용될지라도 안전성 향상에는 직접적인 관계가 없으나, 재사용성이 높기 때문에 소프트웨어 신뢰도를 높이고 확인 및 검증 비용을 감소시킬 수 있다.

3.2.2.5 구현

(1) 규제: 소스코드(source code)를 요구할 수 있다.

(2) 기술기준: NUREG/CR-6463[3-22]은 미국 원자력규제위원회가 원자력발전소의 고-건전성 소프트웨어(high-integrity software)의 검토지침으로 사용된다. NUREG/CR-6463은 안전성에 직접적인 영향을 미치지 않는 객체지향분석 및 설계, 코드 재사용(code reuse), 그리고 자원요구(resource requirements)를 최소화하거나 반응시간(response time)을 최적화 하는 효율성은 언급하지 않는다. 안전계통을 위한 고급언어(Ada83,

C/C++, PLC Ladder Logic, IEC Std 1131-3 Sequential Function Charts, Pascal, PL/M, Ada95, IEC Standard 1131-3 Structured Text, IEC 1131-3 Function Block Diagrams)로 씌어진 소프트웨어의 프로그래밍과 감사를 위한 각 언어별 지침으로 활용될 수 있다. 안전에 직접적으로 관련되는 소프트웨어의 품질에 대하여 3 레벨 계층으로 구성되며, 최상위 수준에는 신뢰성(Reliability), 견고성 또는 강인성 (Robustness), 추적성(Traceability), 유지보수성 (Maintainability)의 4개 속성이 정의된다. NUREG/CR-6463은 주로 구현(즉, 프로그래밍)에 목적을 두고 작성되었기 때문에, 설계, 요건(requirements), 확인검증(V&V), 그리고 개발공정과 관련된 이슈는 다른 산업표준이나 IEEE 7-4.3.2-1993, IEC 60880, NUREG/CR-5930, NUREG/CR-6263, NUREG/CR-6293 등을 참조하면 된다. 프랑스 N4에서는 Ada 언어가 사용되었으며, 소프트웨어에 의한 공통모드고장을 최소화하기 위해 다양성을 프로그래밍 언어(컴파일러)에서부터 적용하고 있다. 한편, 고장허용 소프트웨어는 생명주기 전반에 걸쳐 다양성을 고려하는 N-Version Programming과 Recovery Block 기법이 사용되고 있다.

(3) 문제점: (a)소프트웨어 자격심사(Qualification): 운영체제, 컴파일러, CASE 도구 및 시험도구, 에디터 등의 표준화 (b)N-Version Programming과 Recovery Block 기법: 소프트웨어 복잡도 증가에 따른 안전성 위해 요소에 대한 문제제기.

3.2.2.6 통합, 확인, 검증시험

(1) 규제: NRC는 Reg. Guide 1.168[3-23], Reg. Guide 1.170[3-24], Reg. Guide 1.171[3-25]을 규제기준으로 작성하였다. 한편, KINS에서는 참고문서 [3-10]의 규제지침 7을 적용하고 있다. 규제자 입장에서의 시험에 대한 관점은 “소프트웨어 확인 및 검증 활동들의 핵심이 소프트웨어 단위시험을 포함한 소프트웨어 시험이며, 소프트웨어 시험은 소프트웨어 품질을 확보하고 결함을 확인하기 위한 소프트웨어 검증 활동의 일환”으로 취급한다. 한편, 복잡한 소프트웨어나 패키지의 품질을 보장하기 위하여 단위-수준의 시험, 통합-수준의 시험, 그리고 시스템-수준의 시험(시스템 검증 및 수락시험)을 사용한다. 규제지침 7은 소프트웨어 생명주기, 소프트웨어 시험단계, 소프트웨어시험 생명주기, 소프트웨어 시험 프로그램 및 문서, 소프트웨어 확인의 독립성, 그리고 소프트웨어 시험전략에 대한 규제입장을 제시한다. 상용 소프트웨어에 대한 규제는 NUREG/CR-6421[3-26]의 안전관련 분야에 사용되는 상용(Commercial Off-The-Shelf, COTS) 소프트웨어를 포함한 기성 소프트웨어에 대한 시험전략을 따른다. 안전성-필수 또는 안전성-관련 소프트웨어의 시험전략으로도 적용될 수 있다. 그리고 참고문서 [3-10]의 규제지침 6, 부록에서는 확인 및 검증을 안전등급별로 차등화하여 적용하도록 권장하고 있다.

(2) 기술기준: IEEE Std 1008-1987[3-27]은 소프트웨어 확인 및 검증 계획뿐 만 아니라, 소프트웨어 단위시험의 계획, 준비, 이행 및 평가하는 방법에 따라 확인 및 검증 계획, 그리고 보다 상위수준의 소프트웨어 시험계획에서 수립된 계획정보를

준수하도록 규정한다. IEEE Std 829-1983[3-28]는 안전계통의 소프트웨어 시험에 관한 문서화 기준으로 시험계획 요건, 시험설계 명세, 시험사례(Test-case) 명세, 시험-절차 명세, 시험-항목 전달보고서, 시험기록, 시험 사고보고, 시험 종합보고 요건에 대한 내용을 기술한다. IEEE Std 1028-1994[3-29]은 소프트웨어 검토 및 감사에 대한 기술 기준을 기술한다. IEEE Std 1074-1997[3-12]는 소프트웨어 시험활동을 반영한 생명주기 공정과 고-건전성 안전계통의 소프트웨어 개발에 관례적 적용으로 사용되어 왔으며, EPRI TR-106439-1988[3-30]는 특별시험 및 검사, 기성 소프트웨어에 대한 조사활동, 소스확인, 그리고 기성 소프트웨어의 성능기록의 4가지 검증방법을 제시한다. 확인 및 검증 독립성, 자체시험, 확인 및 검증 정도 등이 관심의 대상이며, 고-신뢰도 소프트웨어 개발을 위해서는 더 엄격하고 명확한 객관적인 기준이 필요하다.

(3) 문제점: (a)소프트웨어의 완벽한 시험은 근본적으로 불가능. (b)신뢰도 목표가 높을수록 (고-신뢰도) 시험비용이 증가.

3.2.2.7 설치 및 운영, 유지보수

(1) 규제: 설치 문서, 운전 및 유지보수 지침서, 훈련 지침서 등 설치, 운영, 유지보수에 필요한 문서들이 마련되어야 하고, 개발과정에서 발견되지 않은 결함을 보완하기 위해 보수 계획, 회귀 분석 시험 계획과 이에 따른 형상관리 변경, 확인검증 부적합사항 보고서(anomaly report), 안전성분석 변경 등이 수행되어야 한다.

(2) 문제점: (a)디지털 계측제어계통의 소프트웨어 유지보수성: 시험가능성 여부.

3.2.2.8 상용기기

(1) 규제: NRC는 EPRI NP-5652[3-31]의 검토로 몇 가지 추가할 것을 지적 사항으로 권고(GL 89-02, GL 91-05, GL 95-02)하여 미국 원자력산업계에서 지침서로서 활용할 수 있도록 승인하였다. 상용 디지털기기의 평가 및 수락지침으로 EPRI TR-106439-1988[3-30]이 사용된다. KINS는 이들 규제기준을 수용한다.

(2) 기술기준: EPRI를 중심으로 디지털 기기 평가 및 승인 지침서(EPRI NP-5652)를 통해 10년 전부터 상용기기 문제를 해결하기 위해 각 전력회사 자사의 실정에 맞게 수정하고 보완(USNRC의 권고사항)하여 지침서로서 활용하고 있다. EPRI NP-5652[3-31]는 하드웨어 상용기기 부분만을 언급하였으나 EPRI NP-106439[3-30]에서부터 소프트웨어, ASIC 펌웨어(firmware)에 대한 인증도 고려하였다.

3.3 인허가 및 규제동향 분석

3.3.1 한국 원자력안전기술원 입장

한국 원자력안전기술원은 디지털 계측제어 계통에 대한 규제지침[3-10]으로

“원자로 시설의 계측 제어계통에 관한 기준(안)”을 과학기술부 고시로 공표할 준비를 하고 있다. 이에 따르면 전체 요건 중에서 안전등급, 신뢰도, 인적요소 고려, 품질, 독립성(소프트웨어 격리), 심층방어 및 다양성, 안전성 위험분석, 그리고 접근통제 항목이 직접 또는 간접적으로 소프트웨어 안전규제에 해당된다. 그리고 안전요건의 적용에 있어 기술적으로 타당한 방법, 설계 보완, 또는 대체 방법을 규제자 입장을 나타내는 규제지침을 통하여 소프트웨어 품질과 개발공정에 대한 규제를 강화하고 있다. 규제지침에는 안전등급별로 규제 및 기술기준을 차등화 적용하는 소프트웨어 생명주기를 안전성분석, 확인 및 검증, 형상관리, 그리고 품질보증에 적용하도록 권장하고 있다. 이러한 소프트웨어 규제는 안전심사지침의 디지털계통 안전심사 항목 중 설계지침의 적합성, 소프트웨어 수명주기 공정, 심층방어 및 다양성, 확인검증, 형상관리, 소프트웨어 개발과 하드웨어/소프트웨어 통합, 기성 소프트웨어, 소프트웨어 도구에 잘 나타난다. 한편, 표준설계의 인허가를 위해 ITAAC 문서작성에 대한 지침서도 작성하였다. 그러므로, 소프트웨어 개발 요소의 1종 정보를 보호계통과 공학적 안전설비로 각각 구분한 작성도 예측된다.

3.3.2 미국 원자력 규제위원회 입장

미국 원자력 규제위원회는 최근에 디지털 장비의 신뢰도 평가 및 공통모드 고장우려 등에 대한 다양한 접근방안을 개발하여 SRP인 NUREG-0800-1997 (Rev.4)를 전면 수정하였다. 그리고, 디지털 계측제어계통의 고-신뢰도 소프트웨어의 개발방법론, 확인 및 검증 기술개발에 주력하고, 계측제어 및 인간공학위원회 (Control, Instrumentation, and Human Factors Branch)가 주관이 되어 Oak Ridge National Laboratory(ORNL), Laurence Livermore National Laboratory (LLNL), 버지니아대학 등과 공동으로 디지털 계측제어 규제관련 연구개발을 수행하고 있다.

미국 원자력 규제위원회는 Nuplex 80+의 설계에 대하여 양면 검토 접근법을 사용한다. 즉, 블록도 수준에서의 상세한 기능적 검토와 기능적 요건에 대한 디지털 보호계통의 적정성을 단계별 ITAAC에 의한 문서검토가 이에 해당한다. NRC 입장은 시스템적인 기능검토를 위한 Design Acceptance Criteria(DAC)-관련 자료의 Level of Detail 문제를 제기하였으며, 단계별 ITAAC에 의한 문서검토를 실시한다는 것이다.

특히, 소프트웨어 ITAAC과 시스템 ITAAC의 차이를 분명히 하고 있다. 그리고, 소프트웨어를 사용하는 마이크로 프로세서-기반 시스템(Microprocessor-Based System)의 독자적인 공통모드고장 대응가능성, 하드와이어 다중(Hard-wired redundant) 시스템의 필요성 즉, 다양성(Diversity)에 대하여 NRC와 웨스팅하우스 사이의 입장 차이를 나타내었다.

3.3.3 공급자의 인허가 접근동향

미국은 계측제어 계통 개선(upgrade)에 10년 장기 계획으로 산학연 공동과제를 추진하고 있다. 이러한 개선 계획은 크게 7가지 기술분야로 나누어 집중적으로 해결책을 모색하고 있으며, 이들 중 소프트웨어의 확인 및 검증 기술 연구와 지침서 및 표준화 관련 연구가 포함된다. 이 두 분야에서 15개의 연구 프로젝트가 추진되고 있으며, 사용자(utility) 협의체가 규제기관을 선도하고 있는 실정이다.

미국 웨스팅하우스(WH-CENP)에서는 Eagle 21과 영국 Sizewell B 발전소의 Digital Protection System 개발 경험을 활용하여, W-ISCO 개발에 CASE 도구(Teamwork)를 Customizing하여 사용하였다. Nuplex 80+ 디지털 계측제어계통의 품질보장을 위한 표준으로 IEEE-7-4.3.2-1982를 사용하였으며, 프로세스-기반 보호계통의 공통모드 고장을 극복하기 위해 소프트웨어 품질과 다양성에 중점을 두고 있다. 다양성과 심층방어에 대한 NRC의 입장이 표명되고 이에 대한 검토가 진행되어 왔다. 그리고, 안전성 관련 요건으로 고-신뢰도 소프트웨어를 지향한다. Nuplex 80+가 현재 수립된 기능적 요구사항에 따라 개발되기 위해서는 단계별 소프트웨어 ITAAC의 각 공정이 충실히 수행되어야 한다. 소프트웨어 관련 쟁점사항 중 소프트웨어 공통모드고장, 소프트웨어의 정량적 신뢰도 측정, 공통유형 고장분석, 통신망 프로토콜(protocol)과 성능에 대한 시험방법론에 대한 문제 제기나 제시에 대하여 웨스팅하우스의 소프트웨어 관련 응답은 “Nuplex 80+ Software Program Manual”과 “Nuplex 80+ Software Safety Plan Description”이다.

프랑스 프라마톰 N4 시리즈 보호계통 개발에서는 소프트웨어 개발을 지원하기 위해 Merlin-Gerin에서 개발한 SAGA와 OST CASE를 CASE (Computer-Aided Software Engineering)도구로 사용하였다. SAGA는 설계 명세를 코드(code)로 번역하는데 사용되고 OST는 실시간 코드를 수행하는 다중 마이크로프로세서를 모의하는데 사용된다. CASE 도구를 사용함으로써 계측제어계통 소프트웨어를 체계적으로 개발하고, 확인 및 검증 방법론 개발에 많은 노력을 기울이고 있다.

캐나다 AECL은 통합기법(IA: Integrated Approach) 공학기술 및 통합 환경에 의한 고-신뢰도 소프트웨어 개발을 통해 소프트웨어 다양성을 전제로 하는 Rational Design Process (RDP) 방법론이 거의 완성 단계에 있다. AECL 설계 방법은 엄격한 문서화와 표준적용이 미흡하여 인허가에 문제점이 발생하였다. AECL은 국제표준 IEC-60880-1986을 사용하였으며, 15가지로 세분된 소프트웨어 생명주기 재설계와 갱신을 하고 있다. 한편, CANDU-3 개발부터 철저하게 소프트웨어 공학기법을 적용하였다.

독일의 Siemens AG KWU는 마이크로프로세서-기반 보호계통(Teleperm XS)의 소프트웨어 개발에 CASE 도구인 SPACE를 사용하였으며, OPAL 121에 연결하여 프로그램 코드를 자동 생산하고 있다.

국내에서는 차세대원자로(최근, APR1400로 명명)의 컴퓨터-기반 보호계통 개발에

소프트웨어-하드웨어 통합, 통합 개발공정, 소프트웨어 개발, 상업용 컴퓨터 검증, 소프트웨어 개발 툴, 확인 및 검증, 형상관리 등에 관한 요건들을 엄격하게 적용하고 있다. 그리고 한국전력기술(주)이 울진 5호기 및 6호기 디지털 보호계통 설계를 수행하고 있다.

3.4 용어정의 및 참고문서

3.4.1 용어 정의

- **정확도 (Accuracy)**
  센서 및 운전원 입력, 또는 구동기 출력에 오류가 없는 정도. 지시 값이 공인된 표준 값 또는 참 값과의 일치하는 정도.
- **활동 (Activity)**
  관련된 작업들의 집단.
- **예상운전과도사건 (Anticipated Operational Occurrences)**
  예상운전과도사건은 안전성 설비에 심각한 손상을 야기하지 않고 사고상태로 전개되지 않는 조건을 말하며, 발전소 운전 수명기간 동안 수 차례 발생이 예상되는 정상운전으로부터 이탈되는 모든 운전 과정을 의미한다.
- **가용도 (Availability)**
  어떤 시스템이나 기기가 임의의 시점에서 요구될 때 운전 중일 확률이다.
- **안전등급 1E (Class 1E)**
  원자로 정지, 비상노심 냉각, 격납건물 격리, 그리고 격납건물 및 노심 잔열제거에 필수적이거나, 또는 심각한 량의 방사성 물질의 환경 방출을 방지하는 데에 필수적인 전기 기기 및 계통에 대한 안전등급이다.
- **공통유형고장 (Common Mode Failures)**
  다중 기기 또는 개별 기기의 인과관계로 인한 고장으로서 심각한 환경, 설계 오류, 교정 및 보수 오류, 그리고 종속고장을 포함한다. 이 고장은 다중성을 위협하거나 또는 다중성 계통에 고장을 유발한다.
- **형상관리 (Configuration Management)**
  형상 항목의 기능적, 물리적 특성을 식별하거나, 변경을 파악하고, 변경을 제어하며, 변경이 적절하게 구현되었음을 확인하기 위한 기술적 또는 행정적 활동.
- **심층방어 (Defense-in-Depth)**
  어떤 주어진 기능을 달성하기 위해 대체 또는 백업 수단을 둔다든지 또는 동일한 목표를 달성하기 위해 다른 기능을 마련하거나 조치를 강구해서 소정의 기능을 달성하게 하는 설계원칙이다. 이러한 대체 또는 백업 수단은 수동

방식일 수 있거나 안전성 또는 비안전성 관련 설비를 사용할 수 있다.

- **설계 수락 요건 (DAC: Design Acceptance Criteria)**
  규제기관이 설계 인증을 최종 결정할 때 근거로 삼는 제한치, 파라미터, 절차, 특성들의 집합.
- **설계기준사고 (DBA: Design Basis Accidents)**
  설계기준사고는 적절한 설비에 의해 방사성 물질의 유출을 허용 제한치 이내로 유지시켜야 하는 사고상태로서 중대사고를 포함하지는 않는다.
- **설계기준사건 (DBE: Design Basis Event)**
  구조물, 계통 및 기기에 대한 허용 가능한 성능요건을 수립하기 위해 설계에서 사용되는 가상사건을 의미한다.
- **설계인증문서 (DCD: Design Certification Document)**
  설계인증에 필요한 정보를 담고 있는 최상위 문서.
- **다양성 (Diversity)**
  동일한 기능을 달성하기 위해 적어도 서로 다른 두 가지의 설계원칙들을 사용하는 것을 의미한다. 즉 기능 다양성(예, 서로 다른 알고리즘, 감지 변수, 물리적 원리) 또는 그 기능을 달성하는데 사용된 장비(하드웨어 및/또는 소프트웨어) 다양성 등이 있다.
- **공학적 안전설비 (Engineered Safety Features)**
  설계기준사건 발생시 또는 그 이후에 소외방사선량에 대한 법적 제한치에 상응한 또는 초과하는 설계기준사건 결말을 예방 또는 완화하는 구조물, 계통 또는 기기이다.
- **필수 보조 지원 계통 (Essential Auxiliary Supporting Systems)**
  안전에 중요한 계측제어계통이 그 기능을 수행할 수 있도록 해 주는 계통.
- **사건 (Event)**
  보호 또는 안전 관점에서 무시할 수 없는 운전 오류, 기기 고장, 또는 연이어 발생하는 고장을 포함하는 모든 의도하지 않은 사건.
- **결함 (Faults)**
  컴퓨터시스템의 거동이 그 명세서에서 규정한 거동과는 다른 편차(deviation) 를 나타낸 것이다. 하드웨어 결함은 컴퓨터시스템의 거동을 바람직하지 못한 방향으로 이르게 하는 하드웨어 자체의 물리적 변화이다. 소프트웨어 결함은 코드 안에서의 실수(또는 버그)이다. 사용자 결함은 어떤 절차를 수행하면서 발생한 인간의 실수이다. 환경 결함은 컴퓨터시스템 외부에서 예상된 거동과는 다른 편차를 의미한다.
- **고장 또는 실패 (Failures)**
  오류를 표면화한 것이다. 즉 고장은 오류에 따른 외적 영향이며, 사용자나 다른 프로그램이 인식한다.

▪ **펌웨어 (Firmware)**
ROM에 저장되어 있는 소프트웨어이다.

▪ **정형적 방법 (Formal Methods)**
수학적 어의(semantics)로 정의된 명세서와 그 명세서에 규정된 수학적 분석 기법을 사용하는 것을 의미한다.

▪ **기능성 (Functionality)**
소프트웨어에 의해 수행되어야만 하는 동작들.

▪ **위험도 분석 (Hazards Analysis)**
어떤 시스템에서 수락 불가한 위험요소를 가진 부분들을 찾아내는 분석방법이며, 그 목적은 위험요소를 줄이거나 없앨 수 있는 설계 변경 사항을 장려하고, 또는 시스템의 취약한 부분에 대해 신뢰성을 높일 수 있는 특별한 분석 또는 시험을 수행하는데 있다.

▪ **비 안전계통 (Non-Safety Systems)**
안전성 설비 중에서 안전계통이나 준-안전계통을 제외한 계통이며 발전소 정상운전 또는 특수한 조건에서 사용되지만, 그 계통의 고장이 원자로 정지 혹은 안전관련계통의 작동을 유발한다.

▪ **기성 소프트웨어 (Pre-Developed Software)**
이미 존재하거나, 상업적 또는 자산적 제품이거나, 컴퓨터 기반 기능에 사용을 고려하고 있는 소프트웨어.

▪ **자원 (Resources)**
계획 문서에 정의된 작업을 수행하는데 필요한 자료.

▪ **안전 정지 계통 (Safe Shutdown Systems)**
발전소의 안전 정지 조건을 획득하거나 유지하기 위해 작동하는 제반 계통.

▪ **안전성-필수 소프트웨어 (Safety-Critical Software)**
동 소프트웨어의 실패 또는 상실이 발전소 안전성에 치명적인 영향을 줄 수 있거나 또는 막대한 재정적, 사회적 손실을 초래할 수 있는 소프트웨어이다.

▪ **안전계통 (Safety Systems)**
설계기준사건 발생 또는 그 이후에 안전기능을 수행한 계통이다.

▪ **보안성 (Security)**
통제되지 않거나, 예상되지 않은 안전에 위협이 되는 침입을 방지하는 능력.

▪ **소프트웨어 개발공정 특성(Software Development Process Characteristic)**
설계공정의 구현에 의한 소프트웨어 개발공정 설계 결과물의 특성.

▪ **소프트웨어 생명주기 (Software Life Cycle)**
소프트웨어 개발 프로젝트에 특정한 시간 순서의 일련의 활동.

▪ **특정 사건 (Special Events)**
발전소 설계기준(plant design basis)의 일부 사건이며, 설계기준사건(DBE)으로

분류되지 않지만, 대체적으로 공통원인 또는 공통모드 고장으로 인해 발생하는 원자로정지불능사건(ATWS), 화재, 또는 소내정전사건(station blackout) 등이다.

- **시험성 (Testability)**
  시험 요건이 만족하는가를 결정하기 위하여 시험 요건 및 성능을 확립하기 위해 요건이 서술되는 정도.
- **추적 가능성 (Traceability)**
  생명주기 결과물의 각 요소가 이전 또는 다음 단계의 결과물에 반영되어 있는가를 추적할 수 있는 정도.
- **확인 및 검증(Verification and Validation)**
  시스템 또는 구성요소(component)에 대한 요건이 완전하고 정확한지, 각 개발단계의 제품이 바로 직전 단계에서 부여된 요건 또는 조건을 충족시키는지, 그리고 최종 시스템 또는 구성요소가 규정된 요건을 준수하는지를 결정하는 공정이다.

3.4.2 참고 문서

[3-1] 권기춘 외 9인, 디지털 계측제어계통 규제요건 분석, 기술보고서 KAERI/TR-1942, 한국원자력연구소, 2001.

[3-2] USNRC, NUREG-0800, Standard Review Plan, Chapter 7, July 1997.

[3-3] IEEE Std 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 1991.

[3-4] IEEE Std 7-4.3.2, IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 1993.

[3-5] IEEE Std 352, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems, 1987.

[3-6] IEC Std 60880, Supplement 2 Draft, Software for Computers Important to Safety for Nuclear Power Plants - Part 2: Software Aspects of Defense against Common Cause Failures, Use of Software Tools and of Pre-Developed Software.

[3-7] 원자력안전기술원, 차세대원자로 안전규제기술개발 (표준설계 인허가제도 요건 및 표준설계기술서 (설계 시공 성능 검증계획) 작성지침 개발 (III-2)), KINS/GR-217, 2001년 2월.

[3-8] 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants”; GDC 20, “Protection System Functions”.

[3-9] 10 CFR 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”.

[3-10] 한국원자력안전기술원, 디지털 계측제어계통에 대한 안전규제 일반원칙 및

규제지침(안), 2001.
[3-11] Regulatory Guide 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission. 1997.
[3-12] IEEE Std 1074, IEEE Standard for Developing Software Life Cycle Processes, 1995.
[3-13] Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.
[3-14] IEEE Std 1058.1, Standard for Software Project Management Plans, 1987.
[3-15] IEEE Std 730.1, Standard for Software Quality Assurance Plans, 1989.
[3-16] IEEE Std 1228, Standard for Software Safety Plans, 1993.
[3-17] IEEE Std 828, Standard for Software Configuration Management Plans, 1983.
[3-18] IEEE Std 1012, Standard for Software Verification and Validation Plans, 1992.
[3-19] Regulatory Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.
[3-20] IEEE Std 830, Guide for Software Requirements Specifications, 1984.
[3-21] IEEE Std 1016, Recommended Practice for Software Design Descriptions, 1987.
[3-22] NUREG/CR-6463, Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems.
[3-23] Regulatory Guide 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.
[3-24] Regulatory Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.
[3-25] Regulatory Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.
[3-26] USNRC/CR-6421, A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications, US Nuclear Regulatory Commission.
[3-27] IEEE Std 1008, Standard for Software Unit Testing, 1987.
[3-28] IEEE Std 829, Standard for Software Test Documentation, 1983.
[3-29] IEEE Std 1028, Standard for Software Reviews and Audits, 1988.
[3-30] EPRI Topical Report TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, Electric Power

Research Institute, October 1996.

[3-31] NP 5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications, Final Report, Electric Power Research Institute, June 1988.

4. 디지털 소프트웨어 개발 절차 및 요건

디지털 기술의 급격한 발전과 디지털 기술이 가지고 있는 뛰어난 성능 및 장점으로 인하여 원자력 발전소 계측제어에 있어서도 기타 산업체의 적용 활동에 발 맞추어 디지털 기술을 적용하고 있는 추세이다. 그러나 디지털 기술에서 제어 및 구동 결정에 핵심이 되는 부분은 소프트웨어가 담당하고 있으며 소프트웨어를 구현하는 데에 있어서 소프트웨어 그 자체에 대해서 달성할 수 있는 안전성이나 신뢰도는 기존 하드웨어와는 많은 차이가 존재한다.

현재의 기술로는 디지털 시스템에 구현된 소프트웨어가 충분히 안전한지 그리고 신뢰성이 있는 지에 대한 전반적으로 합의된 정량적으로 규격화된 절차나 정확한 통일된 기법은 없는 실정이다. 소프트웨어에 대한 신뢰성(dependability)을 보장할 수 있는 방법은 오직 체계적이고 완벽하게 문서화되고 검토 가능한 공학적인 절차를 통해서 어느 정도 달성할 수 있는 것이 유일한 방법이다.

본 장에서는 IAEA의 안전 지침서인 IAEA Safety Guide Series No.NS-G-1.1[4-1]을 기반으로 안전-필수 (또는 안전) 디지털 시스템에 대한 소프트웨어를 구현하는 데에 있어서 소프트웨어의 안전성이나 신뢰성을 유지하기 위하여 필요한 절차나 요건에 대하여 기술한다. 소프트웨어 개발은 그 소프트웨어가 적용될 시스템의 안전 등급에 따라 분류된 품질이나 기술 기준에 따른 개념을 소프트웨어에도 적용하여 개발되는 것이 바람직하다. 안전 및 비안전에 대한 소프트웨어들에 대하여 차이나 분류화된 사항들이 3장에 기술한 바와 같이 존재하나 본 장에서는 원자로 보호계통 등 안전에 필수적인 계통에 적용되는 소프트웨어 개발에 대하여 기술한다. 그 외 등급에 적용되는 소프트웨어 개발에 대한 절차나 요건은 참고문서 [4-2]에 나타나 있다. 아울러 본 문서는 IAEA 안전 지침서 NS-G-1.1의 내용을 기반으로 기술하되 NS-G-1.1에서 참조하는 내용 및 문건에 대해서는 해당 문건이 본 내용에서도 기술되면 참고문서에 기술하되 해당 문건에 있는 자세한 내용을 기술하지 않는다.

4.1 디지털 시스템의 기술적 고찰

4.1.1 디지털 시스템 특징

기존 아날로그 시스템에 비하여 디지털 시스템은 프로그램이 가능한 것과 이산 디지털 논리에 의해 구동된다는 것이 큰 차이점이다. 기존의 아날로그 하드웨어는 마모나 환경 요인에 의해서 주로 고장이 발생하는데 비하여 디지털 시스템은 마모나 경년(aging)에 의한 고장은 거의 없지만 운영 환경에 의해 영향을 받으며 디지털 시스템에 장착되는 소프트웨어는 요구사항 명세에서 불 분명한 사항이나 오류로 인하여 또한 소프트웨어 구현 시 (즉, 코드 작업 시) 유발된 오류로 인하여 고장이 발

생할 수 있다. 따라서 소프트웨어 상의 고장은 하드웨어 상의 고장 유형처럼 임의의 시점에서 발생하는 것이 아니라 절차상에서 발생하는 것이라고 할 수 있다.

디지털 시스템은 기존 아날로그 시스템에 비해서 발전소 공정 감시나 운전원 연계, 자기 진단 및 교정 등에 있어서 뛰어난 성능을 보이고 있으나 이러한 기능을 구현하기 위해서는 소프트웨어가 복잡하게 구성되어야 하고 이러한 것이 오류에 취약한 면을 지니고 있다. 또한 기존 하드웨어에 비하여 소프트웨어는 그 기능이 온전한지 다른 결함을 지니고 있지 않은지 이러한 문제점에 대하여 완벽하게 시험하는 것이 매우 어렵다.

4.1.2 개발 공정

안전 중요 계통의 개발은 순서화되고 분리된 단계로 나누고 단계별 순서대로 수행하여야 한다. 각 단계에서는 전 단계에서 개발된 정보를 활용하며 또한 다음 단계에 입력 정보를 제공한다. 개발 순서는 또한 반복적이라서 개발이 진행 됨에 따라 전 단계에서 생각지 못한 부분이 도출되면 다시 단계를 반복하여 빠진 내용이나 부분을 해당 단계에서 보완해 나간다. 이러한 절차의 중요한 특징은 각 개발 단계에서의 산출이 전 단계에서 도출한 요구사항을 반영하였는지 검증하는 것에 있다.

디지털 시스템 개발 공정에 대한 전형적인 절차가 그림 4-1에 나타나 있다. 그림 4-2는 요구사항에 대한 확인 및 검증의 일반적인 관계를 나타내고 있다.

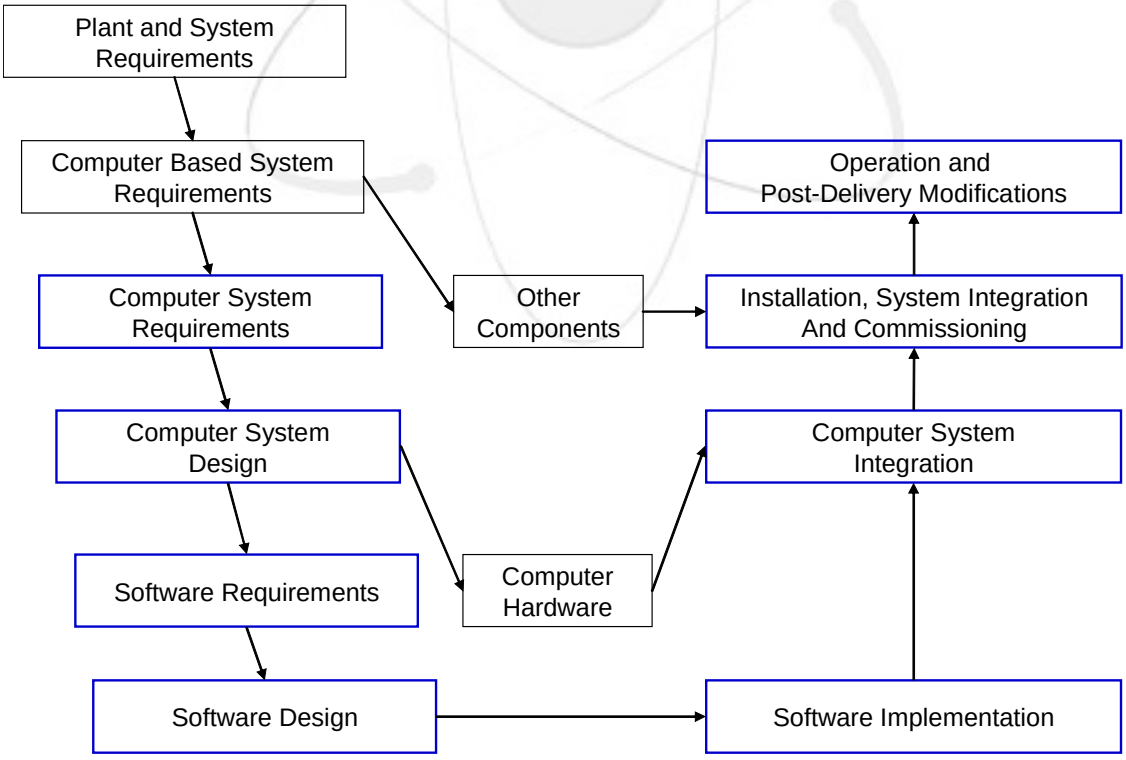


그림 4-1. 안전 중요 디지털 시스템에 대한 소프트웨어 개발

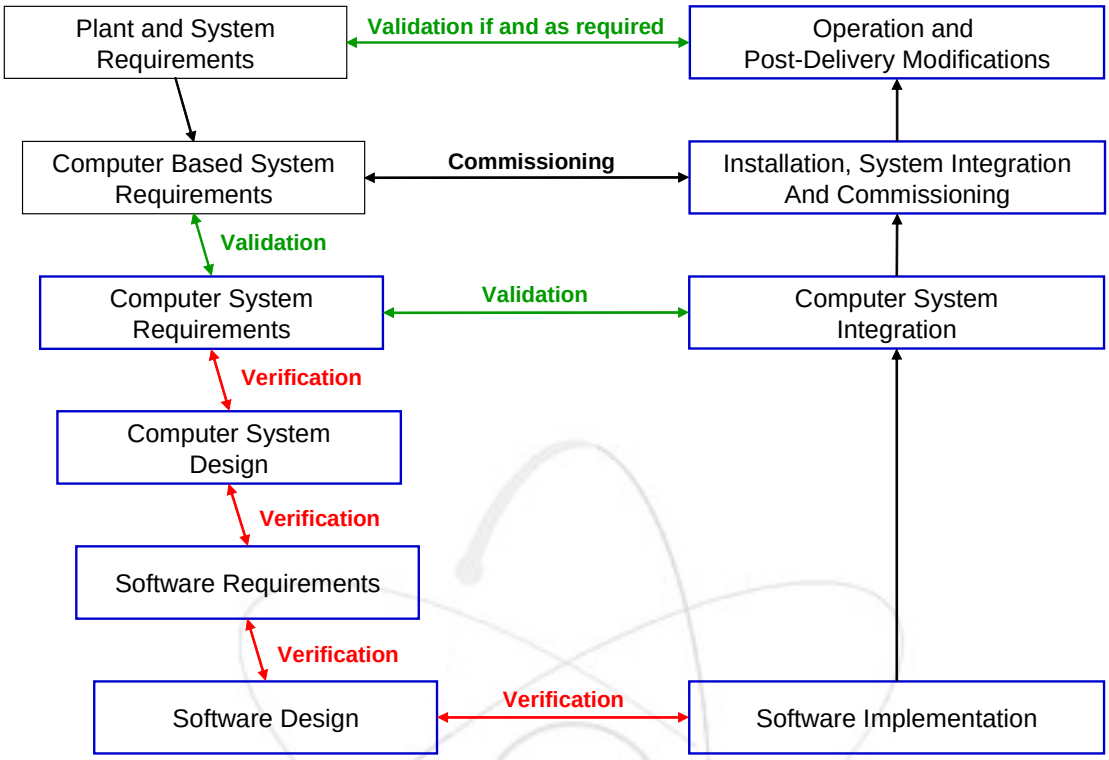


그림 4-2. 확인, 검증, 및 시험운전 관계

디지털 시스템의 개발은 안전 전문가와 소프트웨어 전문가를 포함한 전문적인 공학자에 의한 원자력발전소 및 계통 요구사항을 분석하는 것에서 시작한다. 이런 분석의 결과를 토대로 디지털 시스템에 대한 요건이 도출된다. 디지털 시스템에 대한 요구사항이 도출되면 이러한 요구사항을 컴퓨터 시스템과 기타 다른 전기/전자 장치에 기능에 적합하도록 할당한다.

컴퓨터 시스템 요구사항은 또한 소프트웨어 요구사항과 컴퓨터 하드웨어로 분류되어 할당된다. 소프트웨어는 이러한 요구사항에 따라 컴퓨터에서 구동될 코드 형태의 모듈들로 구성된다. 이러한 모듈들이 구현되면 소프트웨어는 하드웨어와 통합하여 컴퓨터 시스템을 구축하게 된다. 컴퓨터 시스템은 발전소에 설치되어 시험운전을 거친 후 운전을 수행하게 된다.

4.1.3 안전 및 신뢰도 현안

컴퓨터 시스템에서는 기존에 활용하였던 정량적인 신뢰도 분석 방법이 소프트웨어에 대해서는 적용하기가 곤란하다. 그러한 이유는 소프트웨어 상에서 발생하는 고장은 하드웨어에서 발생하는 마모나 노화에 의한 무작위 형태의 고장과는 달리 체계적 형태로 고장이 유입되고 발생하기 때문이다. 또한 소프트웨어를 이용한 디지털 시스템의 가장 큰 신뢰도 현안은 공통원인 고장의 발생 가능성이다. 디지털

시스템을 다중으로 구현한다고 하더라도 그 시스템에 상주하는 소프트웨어들이 동일한 제품을 설치할 경우 소프트웨어의 결함에 의한 고장은 다중으로 구현된 하드웨어의 목적을 파괴할 수 있다. 따라서 소프트웨어 설계자는 이러한 소프트웨어의 결함/고장 유형과 공통고장 가능성을 인지하여 소프트웨어 설계 시 개개 별에 대한 독립성과 다양성을 기하여야 하고 포괄적이고 체계적인 품질 전략을 확보하여야 한다.

4.2 디지털 시스템에 안전관리 요구사항 적용

디지털 시스템의 안전관리 요구사항은 기존의 요구사항을 적용할 수 있으나, 약간의 다른 내용이 존재한다. 디지털 시스템의 설계 및 제작에 적합한 안전관리 요구사항에 대하여 간략히 기술하면 다음과 같다.

4.2.1 안전관리에 대한 요구사항

4.2.1.1 설계 단순화 (Simplicity in Design)

안전에 중요한 계통은 그 안전 기능을 수행하기 위한 설계 및 구현이 불필요하게 복잡한 구조를 가지는 것을 회피하여야 한다. 이러한 요구사항은 컴퓨터 시스템에 정확하게 일치시키는 것은 매우 어렵다. 따라서 구조화된 설계와 프로그램을 수행하는 절차 및 코딩 절차의 준수를 확증하는 증거물은 컴퓨터 시스템에서는 이러한 요구사항을 증명하는 일부분이 된다. 디지털 시스템에 대해서는 하향식 분리, 각 수준 별로 추상화 및 모듈화하는 것은 그 시스템에 할당된 기능을 수행하는데 발생하는 복잡성을 줄이는 중요한 방법이다. 또한 모듈에서도 모듈 별 할당된 기능에 대한 알고리즘은 여러 종류가 있는 경우 가장 단순하면서도 그 기능을 충분히 수행할 수 있는 알고리즘을 선택하여야 한다. 컴퓨터 시스템 모듈화나 연계도 가능한 한 단순하여야 하며 컴퓨터 하드웨어 구조는 소프트웨어를 복잡하게 하지 않는 구조로 구성되어야 한다.

4.2.1.2 안전 문화 (Safety Culture)

안전에 매우 중요한 기능을 수행하는 컴퓨터 시스템을 설계하고 구현할 때에는 안전 요구사항을 충족하기 위하여 컴퓨터 전문가 뿐만 아니라 안전해석 전문가나 계통분석 전문가가 같이 참여를 하여 컴퓨터 시스템의 기능과 이에 따른 안전 요구사항이 잘 만족되도록 한다.

4.2.1.3 안전분류 (Safety Classification Scheme)

안전 분류는 계통개발 절차에 사용될 계측제어 시스템의 안전 중요도를 정의 한

다. 이에 따라 각 계측제어 시스템의 개발에 따른 자원 집중이 결정된다.

4.2.1.4 위험요소 감소와 개발노력 사이의 균형

기능을 잘 수행하기 위한 설계 노력과 개발된 시스템의 위험인자를 감소하기 위한 노력은 상충되는 조건을 유발할 수 있다. 이러한 상충되는 조건을 상호 보완하는 업무가 계통 설계 단계에서 정밀하게 분석되어야 한다. 이러한 분석을 수행하는 데에 안전등급 분류 정보를 활용하여 분류화된 설계나 품질 요구사항을 도출하여 안전에 매우 중요한 컴퓨터 시스템은 그 안전등급 기준을 만족하도록 해야 한다.

4.2.1.5 심층 방어 (Defense in Depth)

원자력발전소의 설계에 적용된 심층 방어 개념[4-3,4-4]이 디지털 시스템 및 관련 소프트웨어에도 적용되어야 한다. 소프트웨어가 주요 안전 특징을 구성하는 경우, 다른 이차의 보호 시스템과 같은 심증 방어는 반드시 구비되어야 한다.

4.2.1.6 다중성 (Redundancy)

아날로그 시스템에 적용되는 다중 계측 채널 및 보팅(voting) 구현은 컴퓨터 하드웨어에 대해서는 분명한 장점이 있으나 컴퓨터 시스템 하드웨어나 소프트웨어에 존재하는 공통원인 고장에 대해서는 완벽한 방어를 제공하지는 않는다.

4.2.1.7 단일 고장 기준 (Single Failure Criterion)

하드웨어에 대한 단일고장 기준은 하나의 고장이 그 시스템이 수행하여야 하는 안전 기능을 저해하지 않음을 분명하게 증명할 수 있으나 디지털 소프트웨어에서는 어느 한 소프트웨어의 결함이 다른 계통에 복사되어 있는 경우에는 같은 결함이 존재하기 때문에 이러한 사항을 만족하기가 어렵다.

4.2.1.8 다양성 (Diversity)

다양성은 소프트웨어 공통원인 고장에 대한 디지털 시스템의 신뢰도를 향상시킬 수 있다. 이를 위해서 설계 여러 단계에서 다양한 기능들과 다양한 시스템 구성기기들의 사용은 고려하여야 하고 방법상, 언어, 도구, 및 작업자에 있어서 다양성은 소프트웨어 설계 시 고려하여야 한다.

4.2.1.9 고장-안전 설계, 감독, 및 고장허용

시스템 고장-안전 특징, 감독, 고장 허용 기법이 소프트웨어에 포함되어야 하며 이러한 추가가 안전 증진을 저해할 정도로 복잡하지 않아야 한다.

4.2.1.10 보안 (Security)

디지털 시스템이 운전 기간 동안 물리적인 공격, 의도하거나 의도하지 않은 침투, 부정수단, 또는 바이러스에 대하여 보호될 수 있어야 한다. 보호 계통은 안전하다고 입증되지 않는 한 외부 통신망과는 연결될 수 없다.

4.2.1.11 유지성 (Maintainability)

디지털 시스템은 고장을 검출하고, 위치를 파악하고, 진단하는 기능을 구비하도록 하여 고장 발생 시 시스템을 효율적으로 수리하거나 교체할 수 있도록 하여야 한다. 이를 위해서 디지털 시스템은 모듈 구조로 구성하는 것이 설계 분석이나 수리에 매우 유리하다. 또한 추후 기능 수정 시 이러한 변경 사항을 용이하게 수용하도록 디지털 시스템 설계 시 반영하도록 하고 이러한 변경이 소프트웨어의 작은 부분에서 이루어 지도록 해야 한다.

4.2.1.12 운전 모드 (Operating Modes)

안전에 중요한 시스템에 활용되는 소프트웨어의 요구사항이나 설계는 모든 운전 모드에 대한 입력과 출력간의 관계를 분명하게 명시하여야 한다. 소프트웨어 설계는 모든 운전 모드를 나타내는 입력의 조합들을 충분히 고려할 수 있을 만큼 단순한 구조로 설계되어야 한다.

4.2.1.13 인간-기계 연계 및 운전자 한계조건 예측

운전자 연계 설계는 안전에 지대한 영향을 끼친다. 운전자 연계장치들은 운전자에게 충분하고도 구조화된 그러나 지나치게 많지 않은 정보를 제공하여야 하고 아울러 운전자 판단에 필요한 충분한 시간을 제공하여야 한다. 모든 운전자 입력은 운전 실수에 의한 손상 방어 차원에서 그 유효성이 점검되어야 한다. 이러한 확인 점검을 운전자가 파괴할 가능성에 대해서도 신중하게 검토하여야 한다.

4.2.1.14 증명 가능한 신뢰성 (Demonstrable Dependability)

계통이 신뢰성이 있어야 할 뿐만 아니라 그러한 신뢰성을 규제 기관에게 보일 수 있어야 한다.

4.2.1.15 시험성 (Testability)

각 요구사항과 설계 특징은 이러한 특성이 잘 구현되었는지 판단할 수 있는 시험이 행해질 수 있도록 하여야 한다. 시험은 기능(functional) 및 비기능(non-functional) 요구사항 모두를 포함한다.

4.2.2 설계 및 개발 활동

4.2.2.1 단계 별 공정 (Process Controlled Step by Step)

설계 및 개발 공정은 단계 별로 통제되어야 한다. 이러한 개발 공정은 그 절차의 수립 그 자체 만으로도 정확성에 대한 증거를 제공할 수 있다. 이러한 사항은 검증 절차를 간편하게 하고 오류를 설계 초기 단계에서 파악할 수 있게 한다.

4.2.2.2 검토성 (Reviewability)

정확하고도 손쉽게 검토할 수 있는 문서들이 개발 공정 모든 단계에 대하여 생성되어야 한다.

4.2.2.3 포괄적 시험 (Comprehensive Testing)

시험은 확인 및 검증에서 매우 중요한 부분이기 때문에 포괄적인 시험이 적용되어야 한다.

4.2.2.4 자동화된 도구 사용

모든 사용되는 도구들은 상호 호환가능 하여야 한다. 도구들은 소프트웨어 개발이나 안전 증명에 있어서 그들의 기능 또는 역할에 상응하는 수준으로 품질을 갖추어야 한다.

4.2.2.5 추적성 (Traceability)

요구사항은 설계로 추적가능 하여야 하고 설계는 코드로 추적가능 하여야 하며 설계와 코드는 시험으로 추적가능 하여야 한다. 추적성은 변경이 발생한 경우에도 추적가능 하여야 한다. 이 모든 것이 역 방향으로도 추적가능 하여 의도하지 않은 기능이 생성되었는지 파악할 수 있어야 한다.

4.2.2.6 표준 준수 (Compliance with Standards)

안전관리 요구사항, 안전 요구사항 및 기술 표준은 개발 시 언급되고 파악되어야 한다. 디지털 시스템 명세와 구현 시에 사용된 주요 핵심 표준[4-5]을 준수하였는지 준수 분석을 수행하여야 한다.

4.2.3 관리 및 품질 보증

4.2.3.1 작업자의 명확히 정의된 기능 및 자격

발전소 관리는 작업자의 수준이 적절한지 증명하여야 한다. 관리는 소프트웨어 설계, 생산 및 유지 프로그램에 참여한 작업자의 기능과 자격요건을 확립하여야 하며 오직 자격과 경험이 있는 작업자가 그들의 기능을 수행한 것을 확증하여야 한다. 작업자의 자격요건은 품질보증 프로그램을 수행하는 것을 포함하여 소프트웨어 개

발과 유지 내에서 각각의 업무에 대하여 수립되어야 한다.

4.2.3.2 허용 가능한 실행 (Acceptable Practices)

소프트웨어 개발 시에는 잘 정립된 방법이나 언어, 및 도구를 활용하여야 한다. 현재 연구 단계인 방법이나 언어, 도구의 사용은 금한다.

4.2.3.3 품질보증 프로그램

조직상의 품질 보증 프로그램은 소프트웨어 개발 공정에도 확장되어야 하며 소프트웨어가 개발되어 전수된 후에도 형상 관리 (configuration management) 및 변경 통제 (change control)를 포함하여야 한다. 최소한 안전 계통에 대해서는 독립적인 확인, 검증 및 시험, 그리고 감사가 이루어져야 한다. 소프트웨어에 대한 품질 요구사항은 소프트웨어 품질 보증 계획에 기술되어야 한다.

4.2.3.4 책임 할당

설계 조직에서 내부 간 또는 설계 조직과 다른 조직간의 연계가 확립되어야 한다. 설계 연계와 관련된 통제가 구축되어야 하고 이러한 통제는 책임 할당과 조직간 문서의 발간을 포함하여야 한다.

4.2.4 문서화 (Documentation)

소프트웨어 개발품의 신뢰성을 확신하기 위하여 개발 공정상의 건전함을 증명할 수 있어야 하며 이러한 건전함을 보이는 데에 문서화는 투명하고도 추적 가능한 중요한 역할을 수행한다. 문서들은 설계 결정의 추적을 보장할 수 있어야 하며[4-6, Q3] 개발 공정 각 단계에서 적절한 문서가 생성되어야 한다. 문서화는 시험운전 및 추후 관리 공정을 포함한 개발 반복을 통하여 갱신되어야 한다. 요구사항, 설계, 및 코드에 대한 문서화는 명확하고 분명하여 설계자나, 프로그램 작업자, 그리고 독립적인 검토자가 개발 각 단계 별로 충분히 이해할 수 있어야 하며 정확성과 완전성을 검증하는데 아무런 문제가 없어야 한다.

문서들은 이해성(comprehensibility), 정교성(preciseness), 추적성(traceability), 완전성(completeness), 일관성(consistency), 검증성(verifiability), 수정가능성(modifiability)와 같은 속성을 가져야 한다.

4.3 사업 계획 (Project Planning)

개발 공정은 신중하게 계획되어야 하고 개발 공정 진행 시 안전에 중요한 계통에 대한 인허가 사항이 구현되었다는 것을 증명하여야 한다. 사업 계획은 디지털

시스템에 대한 포괄적이고도 세세한 안전 계획에서 문서화 되어야 하며 개개의 계획들을 취합하였을 경우 사업의 모든 면을 다루어야 한다. 개발 계획은 개발 활동과 각각의 활동에 대한 중요 특징을 정의하여야 한다.

4.3.1 개발 계획 (Development Plan)

개발 계획은 어느 결정된 사업에 대한 개발 공정을 파악하고 정의하여야 한다.

4.3.1.1 개발 단계 (Phases)

개발 공정의 모든 단계들은 파악되어야 한다. 각 단계는 명세와 설계 그리고 구현으로 구성된다. 한 단계에서 설계 활동은 다음 단계에서 요구사항을 결정하며 어느 단계에서 요구사항을 명세화 하는 것은 전 단계에서의 설계활동이 된다. 구현은 예를 들면 기존 코드를 선택하거나 부가적인 필요 코드를 생성하는 과정이다. 검증은 개발 각 단계를 통하여 수행되어야 하며 다음 단계로 넘어가기 전에 수행되어야 한다.

4.3.1.2 방법

개발에 사용된 방법들은 파악되어야 하며 이러한 방법 선택은 표준이나 절차에서 확립된 품질보증 프로그램 기술과 관련 되어야 한다.

4.3.1.3 도구

사용하고 하는 도구는 개발 계획에서 파악되어야 하며 적용한 표준이나 절차 또는 방법들을 적합하게 구현할 수 있는 도구를 선택하여야 한다. 전 사업에 대해 미리 계획함으로써 개발에 적절한 통합 도구를 선택할 수 있다. 도구의 사용은 작업자의 수동 작업에 의한 프로그램 작업이나 검증 등 오류에 취약한 업무를 수월하게 수행할 수 있도록 해 주기 때문에 개발 시 적용되어야 한다.

4.3.1.4 문서

각 단계에서 생산되는 문서들은 파악되어야 하고 그들의 내용은 명세화 되어야 한다. 모든 요구사항에 대하여 품질 속성과 성능 특성을 발견할 수 있어야 하고 모든 사업에 대하여 어떠한 허용기준이 적용되었는지 명시되어야 한다. 문서는 사업이 개발계획을 잘 준수하고 있다는 것을 보여야 한다.

4.3.1.5 일정 및 이정표

문서에 대한 일정표가 수립되어야 하고 사업 감사에 대한 주기도 파악되어야 한다.

4.3.1.6 참여자

개발 활동에 참여하는 일원으로 관련 표준, 절차 및 방법 적용에 있어서, 설계, 프로그램 작업, 분석 도구나 방법을 사용하는 데 있어서, 형상 관리와 변경 통제 업무를 수행하는데 있어서 적임자가 선정될 수 있도록 계획이 준비되어야 한다.

4.3.2 품질보증

품질보증 프로그램 기술이 준비되고 구현되어야 하며 이러한 프로그램 기술이 사업 시작하기 전에 규제 검토에 활용될 수 있어야 한다. 소프트웨어 품질보증 계획은 사업의 사업시작 단계에서 생산되어야 한다. 이 계획은 다음을 포함하여야 한다.

(1) 품질보증 프로그램이 적용되는 하드웨어 및 소프트웨어 품목 파악 및 적용 표준, 절차 및 도구 파악
(2) 각각의 문서에 대하여, 공식 발간을 위한 검토와 승인을 누가 할 것인지에 대하여 품질보증 프로그램에 명시
(3) 품질보증 감사의 독립을 보증하는 사업 조직 구조의 기술
(4) 사업에 참여하는 참여원의 자격 및 훈련에 대한 기술
(5) 표준 및 절차의 비 준수에 따른 지적, 보고, 및 수정 절차
(6) 모든 필요한 계획 파악
(7) 계통의 안전등급에 따른 품질보증 감사의 횟수 및 범위 명시
(8) 도구에 품질을 부여하기 위한 절차
(9) 외부 공급자로부터 공급되는 기기들의 품질을 점검하기 위한 절차.

4.3.3 확인 및 검증 계획

계통의 정확성이나 안전성을 증명하기 위해서는 다양한 확인 및 검증 활동을 요한다. 자세한 내용은 참고문서 [4-7]에 나타나 있다. 그림 4-2에 나타난 바와 같이 검증은 전 단계의 출력에 대한 현 단계의 산출물을 점검하는 것이고 확인은 상위 요구사항이나 목적에 대한 산출물의 점검을 말한다.

확인은 컴퓨터 시스템이 그것의 전반적인 안전 및 기능 요건을 만족하는지 파악하여야 한다. 이를 위해서 첫 번째로 컴퓨터 시스템의 요구사항을 발전소 및 계통 요구사항에 대하여 적합한지 확인하는 것이고 두 번째로 컴퓨터 시스템 구현이 컴퓨터 시스템 요구사항을 잘 만족하는지 확인하는 것이다.

검증은 다음과 같은 개발 단계에서의 산출물에 대하여 수행되어야 한다.

(1) 컴퓨터 시스템 설계

(2) 소프트웨어 요구사항
(3) 소프트웨어 설계
(4) 소프트웨어 구현

소프트웨어를 검증하기 위한 기법은 확인 및 검증 계획에 기술되어야 하며 이러한 기법을 활용하기 위한 절차도 기술되어 있어야 한다. 확인 및 검증 결과에 대한 기록도 계통의 생명기간 동안 유지되어야 하며 확인 및 검증을 수행하기 위한 팀이나 조직도 확인 및 검증 계획에 명시되어야 한다. 독립적인 확인 및 검증의 정도나 형태는 시스템의 안전 등급에 따라 명시되어야 한다. 독립성은 기술적 독립, 관리적 독립, 재정적 독립이 있으며 안전에 필수적인 소프트웨어의 경우 앞의 세 유형의 독립이 유지되어야 한다.

4.3.4 형상 관리 계획

형상 관리는 개발계획과 품질보증 프로그램의 연장으로써 별도로 분리되어 계획되고 관리될 만큼 소프트웨어 개발에서는 중요하다. 형상 관리에는 산출물의 버전(version)관리와 변경 통제가 있다.

4.3.5 설치 및 시험운전 계획

시스템이 구축되고 시스템 상에서 모든 확인이 수행된 후, 이 시스템은 발전소 시스템과 통합되어야 하고 실제 운전 환경하에서 시험되어야 한다. 이러한 설치 및 시험운전에 대한 절차는 신중하게 계획되어서 개발에서 사용으로 전환이 적절하게 이루어져야 하며 또한 개발자와 검증자로부터 사용자나 유지보수원으로 업무인수가 잘 이루어지도록 계획되어야 한다.

4.4 컴퓨터 시스템 요구사항

컴퓨터 시스템 요구사항은 최소로써, 상위 수준에서 결정된 발전소의 안전 요구사항을 만족할 수 있는 필요하고 충분한 컴퓨터 시스템의 기능 및 비기능적인 특성을 정의하는 것이다. 컴퓨터 시스템 요구사항 명세는 컴퓨터 시스템의 요구되는 행위를 나타내는 데에 있다. 운전자나 외부 계통과의 연계에 대한 정확한 정의도 이 요구사항의 출력의 일부분이며 연계의 정의는 연계의 기능적 및 비기능적 특성에 제한된다. 컴퓨터 시스템 요구사항의 정교성은 상위 수준의 발전소 설계 결과물에 의존한다. 사고 해석, 과도 해석, 또는 발전소 안전 해석과 같은 안전 해석은 컴퓨터 시스템 설계에 매우 필수적인 것이며 이러한 사고 분석의 정확한 결과가 컴퓨터 시스템 요구사항을 정확하게 도출하는데 도움이 된다. 컴퓨터 시스템의 요구사항의

정확한 도출은 매우 중요하며 이 단계에서 유발하는 오류나 결함은 공통원인 고장으로 전개될 수 있으며 이러한 것을 개발 시에 감지하지 못하는 경우 확인 절차에 큰 어려움을 유발할 수 있다.

4.4.1 권고 사항

4.4.1.1 일반

컴퓨터 시스템 요구사항은 구현과는 독립적이어야 하며 명세를 수행할 때에 확립된 어문(syntax)과 어의(semantics)를 가진 정형화가 그러한 작업의 결과를 나타내는 데 적용되어야 한다. 정형 명세는 요구사항의 완전성이나 일관성을 자동 검증할 수 있는 도구를 적용할 수 있는 이점이 있다. 이러한 요구사항은 정확하고 명쾌하게 기술되어야 하며 이러한 기술은 모든 규제원, 공학자, 및 전문가들이 이해 가능하여야 한다.

컴퓨터 시스템의 요구사항 기술은 활용하기가 용이하여야 한다. 이를 통하여 컴퓨터 시스템과 소프트웨어의 검증이 이루어 지며 시스템을 확인하기 위한 시험에 대한 명세를 정의하기 때문에 쉽게 사용될 수 있어야 한다. 요구사항 기술은 시스템 및 발전소 주변과의 연계에 대한 정확한 모델을 기반으로 하여야 한다. 제어 변수와 감시 변수에 대한 모델에 대한 자세한 내용은 참고문서 [4-8]에 나타나 있다.

4.4.1.2 확인

시스템 요구사항은 확인되어야 한다. 즉, 그것의 건전성, 일관성, 및 완전성은 발전소 안전 해석으로부터 도출된 명세와 연관되어 수립되어야 한다. 컴퓨터 시스템의 일관성과 완전성을 분석하기 위한 도구들은 각각의 수준에 상응하여 확인되어야 한다.

4.4.1.3 시스템 연계

컴퓨터 시스템은 수동 백업이나 간섭 또는 원자로 정지 후 수동 리셋과 같은 보호 활동에 있어서 운전자의 참여를 보장할 수 있도록 설계되어야 한다. 입력 데이터 및 운전자 명령은 운전자로부터 재화인 되어야 하며 처리되기 전에 시스템 상에서 확인하여야 한다. 운전자 연계에 화면 표시 장치가 사용되는 경우, 적절한 응답 시간, 검색 및 도움말 기능에 설계시 주의를 기울여야 한다. 모든 연계는 일관성이 있고 동일하고 유일한 이름과 식별자(identifier)를 가져야 한다. 직무 분석이 수동 안전 장비 및 관련된 정보 표시에 대한 적합성에 대하여 수행되어야 한다.

시스템 연계는 또한 비정상적인 보호 활동을 유발하지 않고 가동 중 검사를 수행할 수 있도록 설계되어야 한다. 발전소 통신망과 같은 시스템 연계는 외부 시스템에 의해 수행되는 다은 보호 기능을 저해하지 않도록 설계되어야 한다. 외부 시

스템이나 보조 시스템에 의한 오동작이나 고장이 발생하더라도 시스템이 안전한 상태에 유지되도록 하여야 한다.

컴퓨터 시스템과 발전소 사이의 연계와 같은 계통 경계가 정교하게 정의되어야 한다. 특히, 센서와 구동기, 운전자, 유지보수원, 및 다른 외부 계통과 시스템과의 연계는 명세화 되어야 한다. 입력, 출력 및 표시 데이터에 대한 형태 그리고 경보 구조는 주의 깊게 명세되어야 한다. 데이터 값을 표시하는 데에 있어서 시스템에 의한 기본 값의 자동 생성은 경고 없이 생성되지 않도록 하여야 한다. 발전소 내 기존 계통과의 호환성 및 비안전 계통의 고장 전파에 대한 예방에 대해서는 언급되어야 한다.

4.4.1.4 기능적 안전 요구사항 (Functional Safety Requirements)

안전 계통에 대하여, 발전소에 대한 안전 요구사항을 만족하는데 필요하고 아울러 충분하게 만족할 수 있는 시스템 기능은 명세화 되어야 한다. 이러한 기능적 안전 요구사항은, 시스템에 의한 발전소 매개 변수의 제한치내에 유지와 같은, 부가적인 제한 사항이나 발전소에 대한 시스템의 영향 효과를 통하여 표현되어야 한다.

안전 관련 계통에 대한 기능적 안전 요구사항을 도출하기 위하여 안전 분석이 수행되어야 한다.

4.4.1.5 비기능적 요구사항 (Non-Functional Requirements)

비기능적 요구사항은 다음과 같은 사항들을 명세한다.

- 시스템 거동 특성
- 신뢰도, 가용도, 보안과 같은 시스템 행위에 필요한 신뢰성 속성
- 강인성. 즉, 디지털 시스템이 발전소와의 연계에서 센서 고장이나 범위를 벗어난 입력이 존재하는 경우에 어떻게 대응할 것인가에 대한 사항
- 물리적 격리가 필요한가에 대해서 필요하다면 어디에 구축할 것인지에 대한 사항
- 필요한 경우 시스템 설계 시 도입되어야 할 다양성에 대한 형태
- 시스템의 어는 부분을 교체하고자 하는 경우 교체 하는 방법.

4.4.1.6 분석

안전 계통에 대해서는 안전의 기능적 및 비 기능적 요구사항은 발전소 안전 분석과 그에 따른 결과로써 도출된 것임을 보일 수 있어야 한다. 계통 안전 증명의 일부분으로 컴퓨터 시스템 요구사항은 고장 분석의 주제로 활용되어야 한다. 잠재적인 시스템 부정확 결과가 파악되어야 하고 이에 따른 발전소와 주변에 대한 영향이 평가되어야 하고 이에 대한 심층 방어가 적절한지 확인되어야 한다. 공통원인 고장에 대한 잠재적인 요소에 대해서도 파악되어야 한다.

4.4.2 문서화 작업

이 단계에서 생성되는 문서들은 다음과 같은 항목을 다루어야 한다.

- 기능적 요구사항에 대한 명세
- 비기능적 요구사항에 대한 명세
- 운전자, 유지보수요원, 및 외부 계통에 대한 연계에 대한 명세
- 사고 후 분석을 위하여 공문 기록과 데이터에 대한 필요한 사항
- 검증 시험과 시험 도달범위(coverage)에 대한 명세
- 컴퓨터 시스템 요구사항에 대한 검증 보고서.

4.5 컴퓨터 시스템 설계

컴퓨터 시스템 설계의 초기 버전은 컴퓨터 시스템이 수용해야 하는 계통 요구사항을 다음과 같은 구성품을 가진 컴퓨터 시스템에 대응시키는 것에서 생성된다.

- 기존 또는 기 개발된 소프트웨어 또는 펌웨어(firmware) (예: 운영체제)
- 하드웨어 또는 응용 직접회로
- 개발되는 소프트웨어 또는 기 개발된 소프트웨어를 구성하여 생성된 소프트웨어.

4.5.1 권고 사항

컴퓨터 시스템 설계 시 요구사항 단계에서 명시한 시스템 연계와 컴퓨터 시스템의 성능 및 신뢰도와 같은 비기능적 요구사항을 만족하도록 한다. 컴퓨터 시스템 설계 명세는 초기에는 완벽하게 명세를 작성할 수 없으므로 추후 하위 수준에서 설계할 때에 상위 수준에서 반영할 사항이 발생하면 이를 반영할 수 있는 여지를 남겨두어야 한다. 컴퓨터 시스템 설계 초기 명세가 작성된 후 변경이나 추가 가능한 항목으로는 다음과 같다.

- 컴퓨터 시스템 설계나 소프트웨어 설계와 관련하여 하위 수준의 결정이나 선정으로부터 유발되는 요구사항
- 컴퓨터 시스템에 영향을 미치는 외부 계통 부분들에 대한 하위 수준의 결정으로 인한 요구사항.

이러한 요구사항이 시스템 요구사항 명세에서 변경되든지 아니면 하위 수준 명세 문서에서 변경이 반영되는지 간에 이러한 추가 요구사항에 대하여 형상 통제를 유지하여 이러한 변경 사항에 대하여 확인이 필요한지에 대한 평가가 이루어 질 수 있도록 한다.

4.5.1.1 안전 측면과 비안전 측면의 격리

안전 계통은 맡은 바 안전 기능을 충실히 수행할 수 있는 환경이 되어야 한다. 안전 계통으로 비안전 기능이 추가되는 경우 전체 시스템이 안전 시스템으로 분류될 수 있는지 평가를 수행하여야 하며 이러한 추가된 비안전 기능으로 인하여 안전 계통의 안전 기능이 저해된다든지 하는 저해요인이 발생하지 않아야 한다.

안전 기능을 가지는 시스템은 가능한 한 단순성을 유지하여야 하고 비안전 기능은 비교적 복잡한 기능을 가져도 좋으므로 이러한 두 기능은 별도의 컴퓨터에 장착한다든지 해서 격리를 하는 것이 적합하다. 격리가 이루어진 후에는 비안전 계통에 대한 제한 조건을 완화하여 다양한 자원을 활용하여도 무방하나 안전 기능에는 영향을 미치지 않도록 확실한 격리가 이루어져야 함. 안전과 비안전 기능들이 공유하는 자료들은 자료 접근 시 발생한 오류로 인하여 안전 기능을 수행할 수 없는 상황이 발생하지 않도록 해야 하며 이러한 공유 접근 방식은 회피하여야 함.

4.5.1.2 다중성, 다채널, 및 보팅(voting) 논리

다중성은 시스템의 신뢰성을 향상시키는 것과 온라인 시험하는 것에 유용하기 때문에 다중성은 확보되어야 한다. 그러나 다중성은 임의적으로 발생하는 하드웨어 고장에는 유용하지만 소프트웨어의 공통원인 고장에는 완벽한 방어를 주는 것은 아니다. 다중 기기들 간에 상호 간섭 현상을 제거하기 위하여 다중 기기들은 물리적으로 전기적으로 격리되어야 한다. 이러한 다중 기기들을 통한 결과들은 보팅 논리를 통하여 최종 출력으로 전송되도록 한다. 보팅 논리를 수행 시 격리된 기기들로부터 동일하게 신호를 접수하기 때문에 이를 방지하기 위한 버퍼 장치를 구비하여야 한다.

4.5.1.3 다양성(Diversity)

공통원인 고장을 감소하기 위하여 다양성이 전체 컴퓨터 시스템의 안전성과 신뢰도 요구사항을 만족시키도록 컴퓨터 시스템 구조에 반영되어야 한다. 장비 다양성은 다중 기능을 수행하는 데에 다른 기종의 장비를 이용하여 구축하는 것을 말한다. 기능 다양성은 어느 특정한 기능을 수행하는데 다른 기법이나 방법을 사용하는 것을 말한다. 소프트웨어의 다양성은 동일한 소프트웨어를 사용하는 것보다 공통원인 고장의 가능성을 줄일 수 있으나 공통원인 고장을 완벽하게 제거하였다는 기준은 아직까지는 없는 실정이다. 단지 실험을 통하여 다양성을 가진 소프트웨어는 동일한 소프트웨어를 사용하였을 때에 존재하는 소프트웨어의 결함에 대하여 10%에서 100%사이에서 결함을 줄이는 효과가 있다는 것이 보고되었다[4-9]. 이러한 사항을 고려하여 소프트웨어와 하드웨어 사이에 기능이 적절하게 할당되도록 해야 하며, 또한 보팅 논리는 하드웨어와는 달리 소프트웨어 상에서는 기능 구현 시 훨씬 복잡한 형태가 된다는 것을 고려하여야 한다.

4.5.1.4 결함 감지 및 고장-안전 기능

컴퓨터 시스템은 내부 혹은 외부 시스템에서 발생한 고장이 컴퓨터 시스템의 안전 기능 수행에 저해 요인이 되는 경우 이러한 고장을 감지할 수 있는 기능을 가져야 한다. 이러한 고장이 발생하거나 혹은 컴퓨터 시스템이나 구동 장치에 전원이 상실되더라도 컴퓨터 시스템은 기본적으로 안전한 상태가 되어야 한다. 어떠한 고장이나 결함이 컴퓨터 시스템을 고장-안전 상태를 유발할 정도로 심각하지 않더라도 그러한 고장이 발생한 경우 운전자에게 즉시 알리도록 하여 그러한 고장으로 인하여 혹시 모를 다중 고장이 발생하기 전에 수리할 수 있도록 해야한다.

4.5.1.5 고장 허용 (Fault Tolerance)

컴퓨터 시스템의 하드웨어 및 소프트웨어의 구조는 제한된 하드웨어 및 소프트웨어 고장 발생 후에도 시스템이 미리 정한 안전한 방식으로 운영되도록 해야 한다. 이를 위해서 대안의 데이터 소스(source) 및 다중 구조를 고려하여야 하고 이러한 기법의 제한 사항이나 운영 절차상의 주의할 점은 컴퓨터 시스템 설계 시 고려되어야 하고 운영 절차서에 기술되어야 한다.

4.5.1.6 계통 및 장비 감시

컴퓨터 시스템은 컴퓨터 시스템 자체 기기의 구동상황 뿐만 아니라 발전소 계통 공정과 발전소 기기들에 대한 감시도 수행하도록 설계하여야 한다.

4.5.1.7 운전 중 시험

컴퓨터 시스템이 안전 중요 계통에 설치된 경우, 발전소 운전 중에 주기적으로 시험 가능하여야 한다. 이를 통하여 컴퓨터 시스템의 계속 운전과 신뢰도를 파악하도록 한다. 주기 시험의 빈도는 안전 해석을 통한 결과를 기반으로 결정한다. 주기 시험에 대한 범위(scope) 및 시험 도달범위(coverage)에 대한 사항은 컴퓨터 시스템 설계 시 기술되어야 한다.

4.5.1.8 정밀도 및 응답시간

소프트웨어, 하드웨어 및 기타 부품으로 이루어진 컴퓨터 시스템은 요구된 정밀도와 응답시간을 만족하도록 설계하여야 한다. 이를 위하여 정밀도와 타이밍(timing)이 신호 왜곡이나 지연 등 모든 요인에 대하여 분석되어야 한다. 시스템 응답에 대한 파악 및 분석을 용이하도록 통신 프로토콜과 컴퓨터 자원에 대한 스케쥴링 기법은 결정론적인 방법을 활용하여야만 한다. 이러한 분석은 발전소의 최악의 환경(즉, 중대 사고가 발생하여 많은 입력 신호에 변동을 유발하고 많은 출력 구동 신호를 요하는 환경)을 반영하여 수행하여야 한다.

4.5.1.9 비기능 요구사항 (Non-Functional Requirements)

컴퓨터 시스템 요구사항에서 명세된 비기능적 사항들이 컴퓨터 시스템 설계 시에 적절하게 반영되어야 한다. 비기능적 요건에 포함되는 사항들은 내부 과온도, 방사선 피폭, 정전기, 고주파(radiofrequency) 간섭, 전자기파(electromagnetic) 간섭들이 있다. 고주파 간섭과 전자기파 간섭에 대한 차단은 시스템이 설치된 후에 증명 가능한 사항들이다. 컴퓨터 시스템 설계 시에는 향후 내부 부품 교체에 관련된 사항들도 고려가 되어야 한다.

4.5.2 문서화 작업

컴퓨터 시스템 설계에 관련된 문서들은 선택한 컴퓨터 시스템 구조(architecture)에 대한 명확한 기술이 포함되어야 한다. 또한 컴퓨터 시스템이 요구된 시스템 신뢰성 측면과 이러한 구조가 모든 기능 요건들을 구현할 수 있다는 측면에서 정당화될 수 있는 사항들을 포함하여야 한다. 설계한 구조는 개념상에서 단순성을 유지하며 성능 요건을 만족할 수 있는 능력이 있음을 보여야 한다. 컴퓨터 설계의 정당성은 부분적으로 모델 및 분석, 정형 기법이나 본보기(prototyping)을 활용할 수 있다. 그러한 분석 결과들은 컴퓨터 시스템 설계 문서들에 반영되어야 한다.

컴퓨터 시스템 요구사항에서 명세된 기능 및 성능 요구사항을 반영하는 것 이외에도 다음과 같은 항목들로부터 도출되는 부가적인 요구사항들도 설계에 반영되어야 한다.

4.5.2.1 가동 중 시험

가동 중 검사가 어떠한 방식으로 수행할 것인지 (예를 들면, 온라인으로 수행할 것인지 오프라인으로 수행할 것인지, 자동인지 수동인지) 그리고 어떠한 방식으로 유지성이 만족될 것인지에 대한 결정은 소프트웨어의 기능성에 대한 요구사항뿐 만 아니라 부가적인 하드웨어 연계에 대한 요구사항을 필요로 한다. 소프트웨어 논리를 저장하는 매체의 설정은 컴퓨터 시스템의 건전성을 지속적으로 파악하기 위하여 온라인으로 검사할지 오프라인으로 검사할지에 대한 방식에 영향을 미친다.

4.5.2.2 운전자 연계

인간 요인 공학자는 경보 방식과 이러한 경보를 제공하기 위한 장비들을 운전자에 적합하도록 선정하여야 한다. 또한 운전자에게 작업이나 의사 결정에 필요한 정보를 어떠한 방식으로 제공하는 것이 최적의 방법인 가를 결정하여야 한다. 이러한 결정은 부수적인 하드웨어 연계와 소프트웨어의 기능을 필요로 한다.

4.5.2.3 하드웨어와 소프트웨어 연계 분석

드라이버나 통신 프로토콜 같은 내부 연계에 대한 분석이 수행되어야 하고 문서화 되어 모든 연계 특성이 명세화 된 것을 증명할 수 있어야 한다. 확보해야 하는 안전 특성(회선 쟁탈의 해결 및 교착(deadlock) 제거)에 대하여 기술이 되어야 하고 연계 특성에 대한 분석에 의하여 만족되고 있음을 확인할 수 있어야 한다.

4.5.2.4 입출력 신호 처리 및 데이터 취급 및 저장

신호 처리 기능은 발전소 공정 데이터가 컴퓨터 시스템에서 활용될 수 있도록 컴퓨터 하드웨어나 소프트웨어 또는 외부 장비 상에서 구현될 수 있어야 한다. 이와 관련된 설계 결정이나 물리적이고 논리적인 수단의 특성 및 데이터 접근에 대한 것이 컴퓨터 시스템의 설계 상에서 기술되어야 한다.

4.5.2.5 컴퓨터 시스템의 위험도 분석

위험도 분석이 컴퓨터 시스템의 구조나 기능에 대하여 수행되어야 하며 이를 통하여 안전 기능을 저해할 수 있는 어떤 위험 요소를 파악하고 이를 기반으로 구조 변경이나 부가적인 기능의 추가를 제시하여야 한다. 그러한 분석은 안전 증명에 포함되어야 한다.

4.5.2.6 컴퓨터 시스템의 안전 구조물

컴퓨터 시스템, 와치독 타이머(watchdog timer)와 같은 특성, 프로그램 순서 점검, 변수들의 재 초기화, 및 다른 고장 검출 기구에 대한 위험도 분석을 통하여 파악된 어떤 위험 요소에 대응하여 추가된 위험 완화 기능을 보완하는 기능은 좋은 방안이라고 할 수 있다. 그러나 시스템의 단순성이 유지되어야 하므로 이러한 특성을 반영하는 것이 소프트웨어를 불 필요하게 복잡하게 해서는 안 된다.

4.5.2.7 보안성

컴퓨터 시스템 설계는 컴퓨터 시스템 기능성에 대한 의도적인 또는 부주의한 위법이 어떠한 방식으로 방지될 것인가를 결정하여야 한다. 이러한 결정 사항은 시스템에 대한 변경이 어떠한 방식으로 이루어 지고 검증될 것인지 아울러 무단 변경이 어떠한 방식으로 방지될 것인지에 대한 절차나 통제에 대하여 자세히 기술하여야 한다. 또한 이러한 보안에 대한 존재할 수 있는 위협에 대하여 분석이 있어야 하며 구현된 보안 수준의 정당성에 대한 분석도 제시되어야 한다.

4.5.2.8 고장-안전 기구의 도달범위

컴퓨터 시스템 설계에 대한 문서화 작업은 비기능적 컴퓨터 시스템 요구사항을 만족하도록 명세된 고장-안전 기구에 의한 도달범위를 명세하여야 한다. 또한 신뢰

도와 관련된 제한 사항에 대하여도 언급하여야 한다.

4.5.2.9 시스템 통합 요건

컴퓨터 시스템 설계에 관한 문서화는 다음과 같은 계통 통합 요구사항을 포함하여야 한다.

- 기존 소프트웨어 및 펌웨어 (예: 운영체제)
- 하드웨어 및 응용 직접 회로
- 개발될 소프트웨어 및 기 개발된 소프트웨어를 재구성한 소프트웨어.

이러한 시스템 통합 요구사항은 하드웨어와 소프트웨어에 대한 연계 분석으로부터 도출되고 소프트웨어와 하드웨어 사이의 연계 및 관련 예외처리를 포함하여야 한다. 이러한 정보는 통합 시스템의 검증을 위한 완벽한 시험 명세 생성에 필요하다.

4.5.3 문서 양식(Style)

컴퓨터 시스템 설계 문서는 시스템 요구사항에서 산출한 문서와 연속적인 흐름을 가져야 하며 컴퓨터 시스템에 해당하는 요구사항은 설계 문서에 그대로 반영되어 있어야 한다. 컴퓨터 시스템 설계 문서 내에 전반적이고도 구성 요소까지 세세하게 기술된 요건은 명확하고도 완전하여야 하며 이러한 요구사항에 대한 근거나 요인까지 추적 가능하여야 한다.

4.6 소프트웨어 요구사항

소프트웨어 요구사항은 궁극적으로 컴퓨터 프로그램으로 구현해야 할 컴퓨터 시스템 요구사항의 부분이다. 소프트웨어 요구사항은 어느 특정한 컴퓨터 시스템 설계의 선정에 따른 요구사항들을 반영한다. 상위 수준 요구사항에 대한 소프트웨어 요구사항의 검증은 인허가 과정에서 매우 중요한 단계이다. 따라서 개발자이거나 요구사항 개발에 참여하지 않은 사람이라도 소프트웨어 요구사항의 근본을 파악할 수 있어야 하며 검증할 수 있어야 한다.

4.6.1 권고 사항

4.6.1.1 일반사항

소프트웨어 요구사항은 소프트웨어에 할당된 시스템 요구사항을 포함하여야 하고 이러한 반영을 수행할 때에는 안전 요구사항 및 잠재적 고장 조건, 각 운전 모드에 대한 기능 및 운전 요구사항, 타이밍 및 제한조건, 고장 진단, 자아 감독, 안전 감시 요구사항 및 보안 요구사항에 대하여 주의를 기울여야 한다. 소프트웨어 요구

사항은 적절하게 문서화 되고 이해하기가 쉬어서 소프트웨어 설계자, 컴퓨터 시스템 공학자, 규제자 등 관련 작업자가 쉽게 사용할 수 있어야 한다. 또한 관련 문서는 특정한 설계나 구현과는 무관하게 독립적인 형태로 작성되어야 한다.

소프트웨어 요구사항은 모호성, 불일치성, 및 미정의 조건에 대하여 분석되어야 하며 결함이 존재하는 경우 이러한 결함이 발견되고, 해결되고, 수정되어야 한다. 소프트웨어 요구사항은 검증가능하고 일관성이 있어야 한다. 또한 최소 정밀도 및 정확도, 타이밍 거동, 구동 스레드들(threads)의 독립성 및 고장-안전 거동과 같은 비기능적 소프트웨어 요구사항도 명시적으로 기술되어야 하며 필요한 경우 정량적인 항으로 기술되어야 한다.

4.6.1.2 수행 기능

소프트웨어는 디지털 시스템의 기능 요구사항을 구현하는데 있어서 중축적인 역학을 수행한다. 소프트웨어 요구사항은 이들의 기능 요구사항들을 디지털 입력의 디지털 출력으로 변환하는 데로 전이 되어야 한다. 요구되는 변환은 논리 식이나 수학 함수 및 관계 또는 알고리즘의 형태가 될 수 있다. 보다 나은 추적성과 이해성을 위하여 입력변수, 출력변수, 및 내부변수들은 시스템 환경에서 의미가 있는 이름이나 코드 명을 가져야 한다.

4.6.1.3 안전성

시스템의 안전에 중요한 기능들은 소프트웨어 요구사항 문서에 명확하게 명시되어야 한다. 각각의 출력에 대하여 감지할 수 있으나 복구할 수 없는 고장 발생의 경우 안전한 상태에 대하여 명시되어야 한다. 컴퓨터 시스템에서 부수적으로 명시한 안전과 관련한 입출력 관계 사항은 부가적인 안전 요구사항으로 기술되어야 한다.

4.6.1.4 신뢰도 및 가용도

컴퓨터 시스템 요구사항에서 기술한 신뢰도 및 가용도에 대한 사항은 소프트웨어 및 하드웨어 상에서 그러한 사항을 만족하는 내용을 기술하여야 한다. 소프트웨어의 요구사항은 하드웨어의 요구사항에서 명시한 신뢰도와 결합하였을 때 전체 컴퓨터 시스템에서 요구하는 신뢰도의 목표를 달성하여야 한다. 소프트웨어의 전반적인 신뢰도 목표치는 기술되거나 제시할 수 있지만 이러한 목표치를 달성함을 증명하는 완벽한 방법은 없다. 따라서 이러한 목표치 달성에 대한 어떠한 모델을 사용한 경우 규제 기관에서 동의한 인허가 및 인증 계획서에 그 타당성이 나타나 있어야 한다.

4.6.1.5 연계

소프트웨어와 운전자, 계측기, 하드웨어, 및 기타 다른 소프트웨어 사이의 연계 관련한 내용이 기술되어 소프트웨어의 경계(boundary)를 정의하여야 한다.

4.6.1.6 설계 제한

소프트웨어 요구사항을 작성하는 것과 병행하여 소프트웨어 설계나 구현을 제한하는 설정이 수행될 것이다. 이러한 작업은 문서화 되고 소프트웨어 요구사항에서 필요 시에 참조되어야 한다. 그러한 설계 제한 사항은 정당화 되어야 하고 추적 가능하여야 한다.

4.6.1.7 모델

소프트웨어 요구사항은 구현될 시스템의 모델에 기반할 수도 있다. 이러한 경우 모델과 모델의 적용에 관하여 잘 정의되어야 하고 요구사항 명세와 같이 잘 문서화 되어야 한다. 일례로, 제어 소프트웨어는 유한상태 기계(Finite State Machine) 모델에 의해 기술될 수 있다. 이러한 경우 유한상태 기계모델의 사용을 기술하여 상태 천이(transition)와 어느 상태에서의 함수가 잘 이해될 수 있도록 해야 한다.

4.6.1.8 타이밍 성능

소프트웨어에 의해 수행되는 변환에 요구되는 시간 제약이 기술되어야 한다. 이러한 제약 사항은 입력과 출력 사이 또는 연속적이고 관련된 출력들 사이의 최소 및 최대 시간을 포함할 수 있다. 또한 이러한 제약 사항은 예측한 타이밍 특성이나 소프트웨어가 취급할 입력에 대한 샘플링 율을 포함할 수도 있다.

4.6.1.9 연산 정확도

소프트웨어에서 처리할 수치 정보에 대한 연산 정확도가 명시되어야 한다. 연산은 제한적인 길이를 가진 디지털 컴퓨터에서 수행됨으로 연산 정밀도에서 오차가 발생할 수가 있다. 따라서 허용 가능한 부정확 수준에 대하여 명시적으로 기술하여 소프트웨어 설계자가 수치 데이터를 표시하는 소프트웨어 선택 시 이를 반영하도록 한다.

4.6.1.10 보안

컴퓨터 시스템에 적용된 어느 보안 사항은 소프트웨어의 요구사항에 그대로 반영될 수 있다. 예로 입력의 유효범위 점검, 저장된 데이터나 프로그램의 유효성 점검 등이 있다.

4.6.2 문서화 작업

4.6.2.1 내용

소프트웨어 요구사항 관련 문서들의 주 목적은 소프트웨어 개발과 인허가에 기반을 제공하는데 있다. 따라서 이러한 문서들은 소프트웨어 설계나 인허가, 및 어느 요구사항에 대한 기본 배경을 제공하는 다른 사항들과 연관된 측면을 포함할 수도 있다.

4.6.2.2 문서 양식

소프트웨어 요구사항 관련 문서들을 작성할 때는 정형화된 표준에 따라 작성되어야 한다. 이들 문서는 검증 가능하고 유지성을 확보하여야 한다. 정형 명세 언어의 사용은 소프트웨어의 일관성과 완전성을 확보하는데 도움이 될 것이다. 소프트웨어 요구사항의 문서화에 대한 양식이나 자세한 지침은 참고문서 [4-5]에 나타나 있다.

4.7 소프트웨어 설계

소프트웨어 설계는 소프트웨어를 여러 개의 상호작용하는 모듈들로 나누고 이러한 모듈들에 자세한 기술을 수행하는 것이다. 설계는 소프트웨어의 모든 요구사항을 포함하여야 하며 위험한 항목을 포함하지 않아야 한다. 설계는 일반적으로 소프트웨어의 구조와 그 구조 내 상세 설계에 대하여 언급한다.

4.7.1 권고 사항

소프트웨어 구조 및 구조에 대한 상세 설계와 같은 최소한 두 수준의 설계가 권고된다.

4.7.1.1 복잡성 회피

안전 중요 계통에서는 불필요한 복잡성은 모든 설계 단계에 있어서 회피되어야 한다.

4.7.1.2 안전성

소프트웨어 설계 단계에서는 전 단계에서 파악된 위험 요소에 대하여 언급하여야 하고 안전에 중요한 것으로 파악된 요구사항에 대해서도 언급하여야 한다. 이러한 요구사항은 구동 시 발생할 수 있는 하드웨어 고장을 감지하기 위한 자기 감독 기능을 포함하여야 한다. 소프트웨어는 또한 자기 자신의 제어 흐름과 데이터 흐름을 감시하여야 한다. 소프트웨어와 하드웨어로 이루어진 모듈의 생존을 파악하기 위하여 와치독 기법과 같은 고장 감지 기구를 구비할 수도 있다. 고장이 감지되면,

적절한 행동이 수행되어야 하며 이러한 행동에는 정지 과정, 복구, 오류 메시지가 포함될 수 있다. 오류 메시지는 계속적인 것이 건 일시적인 것이 건 기록되어야 한다. 코드나 데이터 접근에 대한 감독과 건전성은 하드웨어에서 수행할 수 없는 경우 소프트웨어 상에서 수행하여야 한다.

4.7.1.3 이해 가능성 및 수정 가능 구조

검토를 용이하게 하기 위하여, 소프트웨어 구조 조직은 계층적으로 이루어 져야 하며 수준 별 압축을 제공해야 한다. 정보 은닉(Information Hiding)은 단편적인 검토와 검증이 가능하기 위해서 사용되어야 한다. 그래픽 기법 사용은 이해에 도움을 주기 때문에 사용하기를 권한다. 설계는 잘 정의된 어의(semantics)와 어문(syntax)을 가진 정형 기법[4-8]으로 수행되고 자연어로 충분히 설명을 두는 것을 권한다.

연계는 단순하여야 하며 예상되는 변경은 단일 모듈이나 몇 개의 모듈 내에서 가능하도록 하여야 한다.

4.7.1.4 추적성

요구사항의 추적을 용이하기 위하여, 각 모듈이나, 프로시져(procedure), 서브루틴(subroutine), 또는 파일과 같은 설계 요소들은 유일한 식별자(identifier)를 가져야 한다.

4.7.1.5 예측성

설정한 구조는 결정론적(deterministic)이어야 한다. 설계에서는 소프트웨어가 입력에 대한 응답이나 응답 시간과 같은 관점에서 볼 때 예측 가능한 방향으로 구동하도록 설정하여야 한다. 통신 프로토콜(protocol)도 결정론적이어야 하며 외부 시스템의 정확한 작동과 관련하여 의존적이지 말아야 한다.

4.7.1.6 일관성 및 완전성

설계에서는 불일치나 모호함이 없어야 한다. 모듈간 연계는 완전하게 기술되어야 한다. 연계에서 양 측면은 서로 보합(match)하여야 하고 모듈 입출력 사이에 일관성있는 순서와 변수명을 사용하여야 한다.

4.7.1.7 검증 가능성 및 시험 가능성

설계와 설계 설명서는 모든 소프트웨어 요구사항이 만족되었으며 상세 설계에 대하여 구현은 정확하였다는 것을 검증하기에 부족함이 없어야 한다.

4.7.2 문서화 작업

소프트웨어 설계와 관련된 문서화 작업은 소프트웨어 전반적인 구조와 모든 소프트웨어 모듈에 대한 상세 설계 상의 기술적(technical)인 정보를 제공하여야 한다. 문서는 이전 단계에서 파악된 위험요소와 안전에 중요한 요구사항을 소프트웨어 설계는 언급하고 있음을 잘 나타내도록 작성하여야 한다.

4.7.2.1 소프트웨어 구조

모듈로 전체 사항을 분해하고 이러한 분해된 사항을 전체 요구사항으로 사상(mapping)시키는 것이 적합한 근거자료와 함께 기술되어야 한다. 구조는 시스템 운전 기간동안 필수불가결하게 발생하는 변경사항에 대한 고려가 이루어질 수 있도록 하여 유지와 갱신 작업이 용이하게 수행할 수 있도록 해야한다.

소프트웨어 모듈 간 및 소프트웨어와 외부 환경 간에 존재하는 연계는 파악되어야 하고 문서에 명시되어야 한다. 만약 시스템이 다중 처리기(multiple processor)를 사용하여 소프트웨어를 거기에다 분산시키는 경우라면 어느 소프트웨어가 어느 처리기에서 구동하는지 파일과 화면 표시는 어디에 위치하는지에 대하여 명세 되어야 한다. 구조는 모듈들의 제한사항이나 다양성 사용 결정에 따라 파생하는 연계 제한사항들을 고려하여야 한다.

4.7.2.2 구현 제한사항

설계 단계에서 선택한 기술적 특징들은 구현상에 제한사항을 유발한다. 따라서 다양성을 보증하는 조건은 프로그램 언어, 컴파일러(compiler), 서브루틴 라이브러리(subroutine library), 및 기타 지원 도구에 제한 사항을 부과한다. 이러한 정보는 소프트웨어 문서화 작업에서 명시되어야 한다. 구현 제한 사항은 증명되어야 하고 상위 수준의 요구사항이나 제한 사항으로 추적이 가능하여야 한다. 문서화된 증명은 고장발생 검출 시 복구나 프로시져(procedure) 정지, 및 오류 메시지를 통한 작업이 시스템을 안전한 상태로 유지하는 것을 갖추어야 한다.

4.7.2.3 상세 설계

소프트웨어 구조 상의 각각의 소프트웨어 모듈은 상세 설계에서 기술되어야 한다. 일반적으로 모듈에 대한 기술은 모듈 간 연계와 그 모듈의 기능 및 전체 소프트웨어 속에서 그것의 역할이나 기능에 대하여 완벽하게 정의하여야 한다.

4.7.2.4 문서 양식

일반적인 문서 양식의 요건은 4.2.4절을 따른다. 다이아그램(diagram)이나 흐름챠트(flow chart) 등을 사용하여야 한다.

4.8 소프트웨어 구현

이 단계에서 입력으로는 내부 설계와 소프트웨어 모듈 간 연계에 대한 명세로 이루어지고 출력은 소스 코드(source code)와 실행 코드 및 단위 시험(unit tests)과 연계 시험의 결과들이다. 코드는 기존 요구사항 및 설계에 개발 공정에 따라 생성되는 방법과 상위 수준 언어로 적용 방향의 시스템 기술을 입력으로 받아서 자동으로 코드를 생성하는 방법에 의해 생성된다.

4.8.1 권고 사항

4.8.1.1 검증 가능성 및 검토 가능성

소프트웨어 사양을 정확하게 실현하는 코드의 생성은 매우 중요한 사항이다. 코드는 설계 사양에 대하여 검증가능 하여야 한다. 코드를 사람이 검사하는 경우에는 코드가 읽기 쉬워야 하며 적당한 주석을 달아야 하며 이해 가능하여야 한다. 확인된 도구가 코드 검증 과정에서 사용되어야 한다.

4.8.1.2 변경 및 버전 통제

코드는 초기에 모든 사항을 구현할 수 없다. 따라서 구현 시 변경이나 수정은 주의 깊게 통제되어야 하며 연속 버전 사이의 일관성은 유지되어야 한다.

4.8.1.3 프로그램 언어

안전 계통에 쓰이는 소프트웨어에 대한 프로그램 언어는 엄격하게 정의되고 문서화된 어의와 어문을 가져야 한다. 또한 프로그램 언어는 적절한 표현 능력을 가져야 한다. 기계 지향의 언어보다는 응용 지향의 언어를 응용 소프트웨어로 사용하여야 하며 어셈블러 사용은 특별한 경우를 제외하고는 지양하여야 한다. 프로그램 언어와 그 번역기는 오류 제한 생성자, 번역 시간 유형 점검, 구동 시간 유형 및 배열 제한 점검의 사용을 막지 않도록 해야 한다.

4.8.1.4 도구 사용

적절한 도구들이 구현을 위하여 선택되어야 한다. 이들 도구는 번역기, 코드 생성기, 디버거, 링커, 그리고 시험 및 검증 도구들을 포함한다. 이러한 도구들은 개발 다른 단계에서 활용한 다른 도구들과 호환 가능하여야 한다.

4.8.1.5 다양성

소프트웨어 다양성은 두 개 이상의 기능적으로 동일한 프로그램 버전이 동일한 상양으로부터 다른 프로그래머나 프로그램 팀에 의해 개발되도록 하는 개발 기법에 의해 달성된다. 비록 소프트웨어의 다양성 구현은 공통원인 고장의 발생 가능성을

낮출 수 있지만 모든 고장에 대한 치료책으로 보지 않도록 해야 한다. 기능적 다양성은 소프트웨어에 있는 잠재적인 오류를 상당히 줄일 수 있으므로 사용되어야 한다. 기능적인 다양성과 함께 동일한 안전 목적을 달성하는 다른 수단도 제시될 수 있다.

소프트웨어 다양성은 다른 기법, 회복 블록 및 N-변환 기법에 의해 달성될 수 있다. 소프트웨어 다양성은 소프트웨어 구현과 시험의 다른 측면으로 적용될 수 있다. 여러 기법의 선택과 정당성은 적절하게 문서화 되어야 한다.

보팅 논리는 복잡도를 증가시킬 수 있으므로 이러한 사항이 고려되어야 한다. 다중 시스템의 경우에는 보팅은 각 하부 시스템의 다양성을 극대화하기 위하여 가능한 한 각 독립적인 하부 시스템의 결정 사슬에서 상당히 멀리 떨어진 공정까지 진행 한 후에 수행되어야 한다.

온라인으로 오류를 검출하는 능력은 소프트웨어 다양성에 긍정적으로 작용한다. 다양한 변환자는 시험하지 않은 입력 벡터(vectors)나 예기치 않은 환경 변화에 대해 다른 출력을 생성할 것이며 이러한 것은 오류 거동이 보다 잘 검출되도록 한다.

어느 유형의 다양성은 어느 정도의 독립성을 의미한다. 만약 장비나 소프트웨어나 기능적으로나 다양성이 사용된 경우에는 요구되는 수준의 독립성을 증명하여야 한다.

4.8.1.6 모듈 프로그램 작업

모듈의 프로그램 작업이 시작하기 전에 모듈의 설계와 연계에 관한 사양이 완전하고 활용 가능해야 하는 것은 필수적이다.

4.8.1.7 코드 단순화

어느 모듈에서 각 프로그램의 코드는 단순함을 유지하여야 하며 그것의 전반적인 구조와 또한 상세한 구조에서 쉽게 이해 가능하여야 한다.

4.8.1.8 일관적인 데이터 구조

데이터 구조 및 명칭은 전 시스템을 통하여 단일한 방식으로 수행되어야 한다. 각각의 데이터 구조 식별자(identifier)는 일관성 있게 그 유형(배열, 변수, 상수 등)과 범위 그리고 종류(입력, 출력, 내부 변수 등)을 반영하여야 한다.

4.8.1.9 위험한 언어 회피

어떠한 언어에서 어떤 언어 특징을 제거한다든지 또는 부수적인 정적-어의 규칙을 부과함으로써 존재하는 위험성을 제거하지 못할 때에는 그 언어의 사용을 지양하여야 하거나 파악해서 철저하게 검증하여야 한다.

4.8.1.10 코딩 규칙 (Coding Rules)

권고한 프로그래밍 기법은 승인된 상세 코딩 규칙 문서에 기술되어야 하며 이러한 규칙으로부터 이탈을 소프트웨어 모듈 검증 시에 파악되어야 한다. 코딩 규칙에 과한 지침서는 참고 문서 [4-5]를 참조 바람.

4.8.1.11 자아 감독 및 자아 점검

소프트웨어 설계는 구동 시 발생할 수 있는 하드웨어 고장을 검출하기 위하여 필요한 자아 감독 기능을 가져야 한다. 소프트웨어는 또한 소프트웨어 상의 제어 및 데이터 흐름에 대한 감독을 수행하여야 한다.

4.8.1.12 운영 시스템 (Operating Systems)

오직 철저하고도 만족스럽게 시험 검증된 운영 시스템이 사용되어야 한다. 운영 시스템의 사용은 본 안전 지침서의 권고사항을 준행할 수 있는 시스템만 사용해야 하며 사용범위도 필수 불가결한 기능에만 국한하여야 한다. 이러한 기능은 파악되어야 하고 잘 정의된 연계를 가져야 한다. 각각의 특별한 함수는 항상 같은 방식으로 호출되어야 한다. 안전 기능과 비안전 기능의 격리가 공통의 운영 시스템의 사용으로 인하여 위협받지 않아야 한다.

4.8.1.13 시험 가능성

여러 시험 기법에 의한 시험에 대해 모든 실행 가능한 코드로 접근할 수 있어야 한다.

4.8.2 문서화 작업

어느 모듈에 대한 각 프로그램의 코드는 문서의 특정 위치에 사양에 대한 이 프로그램의 정확성을 검증하는 데에 필요한 문맥상(contextual) 정보와 같이 표기되어야 한다. 문맥상 정보는 모듈의 프로그램을 다른 프로그램이나 모듈과는 별도로 이해하고 시험하는 데에 충분하여야 한다. 또한 이러한 정보는 소프트웨어 설계 사양서의 관련이 있는 부분이나 모듈 내 모든 프로그램에 의해 만족해야만 하는 논리 주장, 선행 및 후행 조건에 대한 복제된 내용을 기술되어야 한다. 또한 문맥상 정보는 호출하고 호출되는 프로그램이나 모듈, 입출력 변수 및 유효 범위에 대해서도 기술되어야 하고 이해력을 돕기 위하여 이러한 내용이 한 두 페이지 내에서 기술되어야 한다.

프로그램 언어 선택에 대한 정당성이 제공되어야 하고 문서화 되어야 한다. 언어 어의나 어문에 대한 기술은 완전하고 사용 가능하여야 한다. 모든 도구의 선택은 근거가 제시되어야 하고 문서화 되어야 한다. 도구를 확인 검증한 절차도 문서

화되어야 한다.

4.9 검증 및 분석

검증은 각 개발 단계에서 생산한 산출물이 전 단계에서의 요구사항을 만족하는지 확증하는 공정이다. 분석은 각 개발 단계에서의 산출물이 내부적으로 일관성이 있고 선택한 기법을 적절하게 적용하였는지 점검하는 공정이다. 검증 팀(team)의 목적은 요구된 신뢰도를 만족하면서 전체적이고 엄격한(searching) 조사를 제공하는 것이다.

4.9.1 권고 사항

4.9.1.1 일반 사항

검증과 확인을 위한 다양한 기법이 활용될 수 있으며 이에 대한 사항은 참고문서 [4-8]과 [4-10]을 참조한다. 각각의 기법은 생산 품질을 보증하나 단일 기법이 완전한 보증을 제공하는 것은 아니다. 따라서 다양한 보조 수단이 활용되어야 한다. 육안 검사와 검토가 모든 문서들에 대하여 수행될 수 있다. 그러나 다은 형태의 검증 및 분석도 바람직하며 보증을 달성하는데 필수적일 수가 있다. 예로, 정적 코드 분석은 비용이 드는 시험 프로그램의 반복을 제거할 수 있다 그러나 이러한 방법이 시험의 대체 방법으로 생각해서는 안 된다. 모든 형태의 정적 분석은 프로그램 거동의 모델에 기반하고 있으나 시험은 이러한 모델이 파악할 수 없는 프로그램 동적 거동 조사에 필수적이다.

확인 및 분석에 적용한 각 기법의 범위와 심도는 충분하게 타당성이 있어야 한다. 부적합 사항에 대한 빈도 및 유형이 유지되어야 한다. 이들 기록은 어느 교훈이 얻어지건 않건 간에 검토되어야 하고 적절한 공정 개선이 이루어져야 한다. 공정과 기법을 기술하는 문서는 형상 관리하에 있어야 하며 여기서의 형상관리는 컴퓨터 시스템 문서에 대한 형상 관리와 구분되어야 한다.

검토나 워크스루(walkthrough), 검사 및 감사와 같은 수동 기법은 모든 생명 주기 단계에서 검증 활동에 적용될 수 있으며 이러한 기법이 때로는 소스 코드 생성의 전 단계에서는 유일한 적용 방법일 수가 있다. 이러한 수동 검증은 검토목록(checklist)을 기반으로 수행하며 수행한 결과는 반드시 기록되어야 한다. 검증자가 그의 검토 결과를 기록하는 수단에 대해서는 검증 계획에 선택한 방법의 근거제시와 함께 기술되어야 한다.

소프트웨어 설계와 구현에 관한 문서 작업의 검사는 소프트웨어 시험 케이스(test cases)를 설계하기 전에 수행하여야 한다. 시험 케이스 사양은 충분하게 문서화되고 검토되어야 한다. 시험 도달범위(coverage)는 타당성이 입증되어야 한다. 검토

는 설계와 코드의 제한 사항이 소프트웨어 산출물에서 발견되는 가를 점검하여야 만 한다.

4.9.1.2 정적 분석 (Static Analysis)

정적 분석을 위하여 다음과 같은 기법들이 소스 코드의 정확성을 확증하기 위하여 활용될 수 있다.

- 설계, 규제 및 표준 요건 준수에 대한 검증
- 제어 흐름 분석
- 데이터 사용 및 정보 흐름 분석
- 기호 실행 (Symbolic Execution)
- 정형 코드 검증

소프트웨어 요구사항이 정명 명세화 된 경우에는 정형 코드 검증이 가능하다. 정적 분석은 소프트웨어 최종 버전에 대하여 수행하여야 한다.

4.9.1.2 시험 전략 및 도달범위

시험은 목적 코드의 실행을 포함한 소프트웨어의 분석이다. 검사 시 소프트웨어에 대한 조사는 적절한 시험 케이스를 설계함으로써 구축될 수 있다. 시험 전략은 전체 소프트웨어에 대하여 점진적으로 증대하는 방향으로 설계되어야 한다. 전형적인 시험 프로그램은 소프트웨어 계층에서 최 하위 수준의 모듈 프로그램을 시험하는 것으로 시작하여 점진적으로 상위 수준의 모듈 프로그램들을 시험하는 것으로 진행한다. 이런 방식으로 이미 시험한 하위 수준 프로그램은 시험 환경에 통합될 수 있고 바로 상위 수준의 모듈 프로그램 시험에 활용될 수 있다.

시험의 전체 기능적 도달 범위를 증명할 수 있는 수단은 검증 계획서에 정의되어야 한다. 각각의 시험 케이스는 추적성 매트릭스(matrix)에 의해 추적할 수 있어야 한다. 소프트웨어에 구현된 모든 비기능적 요구사항도 시험하여야 한다. 성능 시험은 결함을 발견하고 복구하는데 걸리는 시간과 모든 명세된 입력 율을 수용하는 능력에 대해 다루어야 한다. 시험의 구조적 도달범위 메트릭스(metrics), 즉, 100% 실행문(statement) 도달 및 분기(branch) 도달, 의 목표치가 기술되어야 하고 검증 계획서에 타당성을 기술하여야 한다. 계획서에 있는 목표치에 대한 이탈은 근거가 제시되어야 하고 문서화되어야 한다.

시험 프로그램은 연계 시험에 특별히 주의를 기울여야 한다. 모든 데이터 전송 기능과 연계 프로토콜은 만족하게 동작함을 보여야 한다. 예외 조건(0으로 나눔, 범위 이탈)에 대한 시험을 수행하기 위한 수단을 고려하여야 한다. 이러한 수단은 특별한 시험 도구를 요구할 수 있다.

모든 입력 변수의 범위에 대하여 시험을 수해하여야 한다. 이러한 시험을 용이하게 수행하기 위하여 등가치 분할(equivalent class partitioning)과 경계값 분석

(boundary value analysis)과 같은 기법을 활용하여야 한다. 모든 시스템 운전 모드가 시험 케이스 설계 시 고려되어야 한다.

4.9.1.3 시험 준비 및 실행

시험에 대한 전 도달범위를 증명할 수 있는 방법은 검증 계획서에 정의되어야 한다. 계획서에 있는 목표치와의 이탈은 타당성을 제시하여야 하고 문서화되어야 한다. 시험 계획은 회귀 시험이 용이하도록 설계한다. 즉, 시험이 반복적이고 이러한 시험 수행 시 작업자의 간섭을 최소화하는 시험이 되도록 한다.

시험을 계획하고 수행하는 작업자는 도구나 절차나 기법에 대하여 숙련된 사람이어야 하고 개발팀의 일원이 아니어야 한다. 시험 장비는 추적 가능한 표준을 기준으로 교정되어야 하고 시험을 실행하는 장비는 시험 절차서에 유일하게 식별되고 기록되어야 한다.

시험 시 시스템으로부터의 모든 출력은 감시되어야 한다. 예측 결과와 다른 경우 분석하여 그 분석 결과를 문서화해야 한다. 시험 기록은 유지되어야 한다. 시험 수행 시 발생한 부적합 사항은 검토되어야 하고 시험 절차에 수정이 필요하다는 것으로 판단될 때에는 적절한 변경 통제 절차가 적용되어야 한다.

만약 하드웨어나 소프트웨어에 오류가 존재하는 것으로 결정나면, 필요한 변경은 승인된 수정 절차의 통제하에 변경하여야 한다. 오류 원인에 대해 분석을 수행하여야 하고 개발 공정에서 조기 감지의 미진한 부분은 조사되어야 하며 적절한 회귀(regression) 시험이 수행되어야 한다.

4.9.1.4 위험도 분석

발전소 계통 수준의 위험 요소에 디지털 시스템이 영향을 미치는 경우 그러한 영향이 컴퓨터 시스템 설계에 기인한 것인지 소프트웨어 설계나 코드에 기인한 것인지 추적해야 한다. 또한 요구사항에 대해서도 이러한 영향에 대해 추적하여 발전소 안전 분석에 포함시켜야 한다.

추후 발전소 안전 기준이 소프트웨어 설계 단계에 만족이 되는지 소프트웨어 구현 단계는 안전에 영향을 미치는지 아니면 새로운 위험 요소를 도입하였는지에 대하여 검증을 수행하여야 한다. 이러한 검증과 설계에 대한 변경이나 부가적인 특징 추가의 형태로 충격 파악은 매우 어렵기 때문에 그러한 작업은 구현이 끝난 다음에 하는 것 보다는 설계가 진행됨에 따라 수행하는 것이 바람직하다.

4.9.1.5 도구 평가

소프트웨어를 생성하는데 사용된 도구는 다음과 같은 유형으로 나뉠 수 있다.

- 소프트웨어 개발 도구. 출력이 프로그램 구현의 일부분이 되며 오류를 유발할 수 있음.

- 소프트웨어 검증 도구. 오류를 유발하지 않으나 오류를 감지하지 못할 수는 있음. 정적 분석이나 시험 도달범위 감시관련 도구들.

상기 어느 도구가 사용되건, 도구의 기능성에 대한 정교한 정의가 있어야 한다. 소프트웨어 개발 도구에 대해서는 적용 범위가 정확하게 파악되어야 하고 소프트웨어 검증 도구에 대해서는 그 도구가 수행하는 분석이나 점검이 잘 정의되어야 한다.

모든 경우에 있어서 도구는 그것이 최종 산출물의 안전을 위해 하지 않는다는 것을 확증하는 충분한 안전 신뢰성을 가져야 한다. 소프트웨어 개발 도구에서 그 출력물이 더 이상의 검토없이 사용되는 경우 신뢰성은 가장 높은 수준의 신뢰성을 가져야 한다. 출력물을 검증하는 경우에는 도구의 신뢰성은 완화될 수 있다. 소프트웨어 검증 도구의 요건은 그 출력물이 자세히 검토된다는 일반적인 상황을 감안하여 다소 완화될 수 있다.

4.9.1.6 역 공학 (Reverse Engineering)

소스 코드와 기계어 코드를 공통 정형 언어로 변환하여 기계의 도움으로 두 개의 정형 언어들을 비교하여 검증하는 것은 적용 가능성이 매우 높으므로 고려되어야 한다.

4.9.1.7 운전 이력 평가

소프트웨어의 가동 중 검사 결과의 활용은 그 소프트웨어가 원하는 기능을 수행하는지 또한 다은 검증을 수행하는데 확증을 제공할 수 있다. 그러한 정보가 활용된다면 과거 사용의 연관성 분석, 특히 적용하려고 하는 새로운 환경과의 호환성 및 새로운 적용과의 연관성은 제공되어야 한다.

4.9.2 문서화 작업

검증 및 분석은 문서화하여야 한다. 문서들은 개발의 생산품이 완전하고 정학하며 일관성이 있는지에 대한 증거들의 일관적인 자료들을 제공하여야 한다. 확인 및 검증 계획은 사업 초기 단계에 구축되어야 하며 이 계획은 사용될 검증과 분석 기법들을 정의하여야 하고 이러한 기법이 충분한 근거자료를 제시할 것이라는 것을 제공하여야 하며 특별히 준비하여야 할 기록, 보고서 및 문서들을 정의하여야 한다. 또한 확인 및 검증 계획서는 누가 각 공정을 수행하고 이러한 공정이 어떠한 방식으로 다른 공정과 개발 공정과 조합될 것인지에 대한 관리적인 사항들을 다루어야 한다.

검증은 한 단계의 결과물을 이전 단계의 결과물과 비교하는 것이므로 전 단계가 완료되면 검증 준비는 바로 시작될 수 있다. 그러한 준비 사항은 검증 결과의 첫 부분으로써 문서화 되어야 한다. 이들 문서는 다음과 같은 사항들을 포함하여야 한

다.

- 체크 리스트 및 원하는 응답
- 증명에 대한 준행
- 시험 케이스 및 예상 결과
- 시험 도달범위 목표치 및 타당성
- 도구 평가 기준

검증 공정 시에는 검증자는 공정에 대한 충분한 정보를 기록하여 반복될 경우 동일한 결과를 획득할 수 있어야 한다. 만약 어떤 검증 도구가 사용된 경우 그 도구는 완전하게 버전이나 형상이 파악되어야 하고 사용된 입력이나 설정 변수들은 기록되어야 한다.

검증 결과는 모든 예비된 측면이 도달되었다는 것을 보이기 위해서 기록되어야 한다. 다양한 검증 및 분석 활동에서 발견된 부적합 사항은 기록되어야 하고 조사되어야 한다. 그러한 부적합 사항 기록은 유지되어야 하고 또한 부적합 사항 해결 결과도 유지되어야 한다. 변경이 문서나 소스 코드에 행해져야 한다고 판단되면 수립된 변경 절차가 적용되어야 한다.

시험 계획은 포괄적이고 실제 적용하기에 완전하여야 한다. 시험에 관한 시험 계획이나 절차나 예상 결과 및 기록물들은 유지되어야 하고 품질 보증 감사와 제 3 자 평가에 활용가능 하여야 한다. 시험 절차는 각 시험 케이스에 대한 타당성을 제시하여야 하고 시험 케이스의 관련 소스 문서들에 대한 추적을 제공하여야 한다. 예상 결과가 실제 시험을 수행하기 전 시험 문서에 기술되어야 한다. 위험도 분석의 결과는 기록되어야 하고 그 범위의 완전성이 평가되어야 한다.

4.10 컴퓨터 시스템 통합

컴퓨터 시스템 통합관련 활동은 다음 세 가지와 같다.

- 모든 소프트웨어를 하드웨어 시스템에 로딩(loading)
- 소프트웨어-하드웨어 연계 요건이 만족되는지 시험
- 모든 소프트웨어가 소프트웨어-하드웨어 통합 환경에서 작동하는 지 시험.

시스템 통합 검증은 설계자의 시스템 통합과 시험이 끝난 후 수행한다. 이 단계에서의 목적은 시스템 통합이 적절하게 통제되었는지를 증명하는 것이어야 한다.

4.10.1 권고 사항

하드웨어 통합 활동은 컴퓨터 시스템 통합 단계 이전에 수행하여야 한다. 시스템 통합 계획은 컴퓨터 시스템 설계의 문서화 작업의 일부분인 시스템 통합 요구사항으로부터 유래하여야 한다. 문서화된 추적성 분석은 검증활동의 일부분으로써 수

행되어 시스템 통합 요구사항이 컴퓨터 시스템 설계 사양에 대하여 완전한지 보일 수 있어야 한다.

오직 검증된 하드웨어나 소프트웨어 모듈들이 시스템 통합 단계에 사용되어야 한다. 이것은 다음을 포함하는 통합 시스템의 엄격한 형상 통제의 필요성을 의미한다.

- 모든 하드웨어 모듈들의 통제된 구축 목록
- 소프트웨어 라이브러리로부터 정확한 모듈 버전 확보

시스템 통합 단계에 사용된 소프트웨어 및 하드웨어 버전은 현재 검증된 버전이어야 한다. 시스템 통합 검증은 모든 통합 연계가 다 조사되었는지 점검하도록 설계되어야 한다. 시스템 통합 검증 시험을 수행하는 팀은 설계자나 개발자와는 독립적인 사람들로 구성되어야 한다. 시험 팀과 설계자 사이의 의견 교화관련 업무는 기록되어야 한다. 승인된 시험 절차에 대한 모든 변경은 기록되어야 하고 재 승인을 받아야 한다.

시험 케이스를 구축할 때에는 다음 사항을 고려하여야 한다.

- 모든 통합 요구사항들의 도달범위
- 모든 하드웨어-소프트웨어 연계
- 전 범위(연계 신호의 범위 이탈을 포함하여)의 도달
- 예외 처리
- 등가치 분할 및 경계 조건
- 타이밍 관련 요구사항(응답시간, 입력신호 접수, 동기화 등)
- 정확도.

4.10.2 문서화 작업

이 단계에서 생성하여야 하는 문서는 다음과 같다.

- 시스템 통합 검증관련 계획서
- 추적성 분석 결과
- 시스템 통합 검증에 사용된 방법의 타당성
- 시스템 정상 운전에서 시험 시 거동을 파악하기 위한 개입 또는 조정(intervention) 수준의 타당성.

시스템 통합 검증관련 보고서는 다음과 같은 사항들을 다루어야 한다.

- 시험 도달범위 검토
- 모듈 통합 및 시험 검토
- 하드웨어-소프트웨어 통합 시험 결과 검토
- 내부 타이밍 성능 평가
- 추적성 검토.

4.11 컴퓨터 시스템의 확인

확인은 컴퓨터 시스템이 기능적 및 비기능적 요구사항에서 정의된 의도된 기능을 수행하는지 보이는 공정이다. 안전 증명에 있어서 이러한 공정은 현재 분석 기법으로는 시스템의 정확도를 완벽하게 증명하는 것이 불가능하기 때문에 필수적인 작업이다. 컴퓨터 기반 시스템의 고유 특성 상 요구사항 준수를 증명하기 위한 시험 횟수를 판단하기 위하여 기존 하드웨어에서 쓰이는 내삽(interpolation)이나 외삽(extrapolation)의 유용성이 이 시스템에서는 큰 도움이 되지 못하기 때문에 확인자가 요구된 시스템 신뢰도와 연관하여 시험의 수량을 도출하여야 한다.

등가치 분할 방식이나 경계 조건이 고려될 수 있다. 아울러 시험 운전 시에는 발전소와 컴퓨터 기반 시스템과 연계한 운전 모드나 상호 작용을 충분히 만족스럽게 시험하지 못하는 문제가 있다. 어쨌든 입력은 허용 가능한 증명을 위하여 적절한 입력 신호 모사 수준을 확보하여야 한다.

4.11.1 권고 사항

확인 시험은 철저하고 순서화된 방식으로 품질보증 프로그램 상의 기술이나 절차에 따라 실행되어야 한다[4-5]. 확인 시험을 수행하는 팀은 설계자나 개발자와는 독립적인 사람들로 구성되어야 한다. 시험 팀과 설계자 사이의 의견교환은 기록되어야 한다. 승인된 시험 절차에 대한 모든 변경은 기록되고 재승인 받아야 한다.

이 단계에서 시험은 컴퓨터 시스템 요구사항을 기반으로 블랙박스(blackbox) 시험을 수행한다. 그러나 여러 설계 단계에서 추가한 특성들이 시스템 수준에서 시험하기에 적합한 것이라면 특성을 파악하기 위하여 분석을 수행하여야 한다. 이러한 것으로 입력 신호가 범위를 벗어나거나 품질이 현저히 저하된 경우 고장-안전 동작이 정확한지 확인하는 것이 있다. 시험 케이스를 구축하는 데는 다음과 같은 사항을 고려하여야 한다.

- 모든, 강인성 시험과 보안 특성을 포함한, 요구사항의 시험 적용
- 전체, 입력신호의 범위이탈을 포함하는, 범위의 시험 적용
- 등가치 분할 및 경계조건
- 타이밍 관련 요구사항 (응답 시간, 입력신호 취득, 동기화 등)
- 정확도
- 시스템 통합 상의 하드웨어-소프트웨어 연계 및 확인 중 외부 연계와 같은 모든 연계
- 응력(stress) 및 부하(load) 시험
- 컴퓨터 시스템의 모든, 모드 사이 전환 및 전원 상실 후 복구를 포함하여, 운전 모드

추적성 분석이 확인 요구사항(시험 및 평가)이 검퓨터 시스템 요구사항에 대하

여 완전한지 증명하기 위하여 수행되어야 한다. 확인 시험에 사용되는 시스템 하드웨어는 현장 설치용 디지털 시스템의 최종 형상을 충분히 나타내어야 하며 시스템 소프트웨어는 동일한 것을 사용해야 한다. 시스템은 광범위의 정적 및 동적 입력 신호를 이용한 시험을 거쳐야 한다. 시스템의 모든 부분은 실제 상황 하에서 시험하여야 하나 실제 사고를 유발할 수 없으므로 사고 상황을 모사하는 모사기를 이용하여 시험을 수행하여야 한다. 시험 장비는 이러한 결과를 기록하여야 한다.

동적 시험은 가상 개시 사건에 의한 발전소 과도상태 분석을 기반으로 수행되어야 한다. 시험 내용은 컴퓨터 시스템 동작을 요하는 예상 발전소 매개변수의 변동을 충분히 나타내야 한다. 시험 수행 횟수는 시스템의 신뢰성에 대한 확신을 제공할 만큼 충분하여야 한다. 컴퓨터 시스템 신뢰도를 확인하는 다른 방법으로 통계적으로 유효한 시험을 연속적으로 시행하는 것이 있으며 이러한 방법도 고려하여야 한다. 이러한 시험에 대한 내용은 참고문서 [4-8]에 기술되어 있다. 입력을 임의적으로 변동하여 시험하는 임의(random) 시험도 고려할 수 있다.

동적 시험과 통계적 시험은 시험 횟수는 컴퓨터 시스템에 대한 신뢰도 요구사항과 연관이 있어야 한다. 오류 검출이 적절하였는지 증명하는 증거도 제시되어야 한다. 시험은 설정치 정확도 및 히스테리시스(hysteresis)가 정확히 동작하는지 확인하는 작업도 수행하여야 한다. 시스템 운전 및 유지 설명서도 이 단계에서 확인되어야 한다.

4.11.2 문서화 작업

확인 단계의 문서는 다음을 포함하여야 한다.

- 확인 계획의 수정 가능성
- 여러 설계 단계에 추가한 특징 분석
- 시험 및 평가에 대한 확인 요구사항이 컴퓨터 시스템 요구사항에 대하여 완전한지 증명하는 추적성 분석
- 확인 결과
- 통계적 시험, 일정 및 결과에 대한 계획
- 통계 시험용 가상 개시 사건에 의한 발전소 과도 상태 분석
- 임의(random) 시험, 일정 및 결과에 대한 계획

4.12 설치 및 시험운전

현장에 인수한 후, 컴퓨터 시스템은 발전소에 설치되어야 한다. 설치는 각 위치에 할당된 장비의 여러 항목들의 안전점검, 전원 연결, 및 컴퓨터 시스템이 수송과 설치 도중에 손상을 입지 않았다는 것을 보이기 위한 제작 공장에서 수행한 시험의

반복을 포함하는 점진적인 공정이다. 이러한 작업이 끝나면 통신 및 발전소 신호 케이블을 포함하는 발전소 케이블을 컴퓨터 시스템에 연결한다.

시험운전은 원자력발전소 기기나 시스템이 구축된 후에 운전 상에 있도록 하여 설계 가정에 부합하는지 성능 기준을 만족하는 지 검증하는 공정이다. 이 단계에서는 컴퓨터 기반 시스템은 점진적으로 다른 기기나 발전소 품목과 통합되어 나간다. 발전소 환경 조건 상에서의 시험은 컴퓨터 기반 시스템의 시험운전에서 중요한 부분 중의 하나이다. 특히, 운전 모드나 발전소와의 직접 연계는 확인 단계에서 쉽게 시험할 수 없는 것으로써 시험운전 단계에서 반드시 시험되어야 한다.

발전소 안전 요건에 대한 컴퓨터 기반 시스템의 확인은 확인 및 검증 공정에 있어서 마지막 단계이다.

4.12.1 권고 사항

컴퓨터 시스템 통합 및 확인 단계가 완료되기 전까지는 전 시스템이 발전소에 설치되어서는 안 된다. 그러한 것이 불가능한 경우에는 설치 후 시험 적합성에 대한 타당성이 구비되어야 한다. 설치한 시스템의 안전 증명은 제작 공장에서 수행했던 것과 동일한 수준으로 수행하여야 한다. 소프트웨어의 건전성을 확인하기 위하여 앞의 여러 절에서 기술한 모든 수행 시험과정이 고려되어야 한다. 특히 외부 시스템 연계 시험 및 연계 기기의 정확한 성능 확인에 대하여 주의를 기울여야 한다. 시험운전 단계에서 수행된 시험은 연계 상에서 정상 및 예외적 대응의 정확성에 대한 이전시험의 결과를 확증하여야 한다.

컴퓨터 기반 시스템은 비교적 긴 기간 동안 현장 수습 기간을 가져서 이 기간 동안의 운전이나 시험 및 유지가 가능한 한 운전 중 조건과 비슷하여야 한다. 가능하다면 새로운 시스템은 이 수습 기간 동안 기존 장비와 병렬로 운전하여서 이 새 시스템이 적절한지를 확증하여야 한다. 운전 및 유지보수 설명서의 확인이 이 단계에서 완료되어야 한다. 이 기간 동안 시스템은 정기적인 시험 및 유지보수 활동이 행해져야 한다. 발견한 결함과 보수 활동은 기록되어야 한다.

컴퓨터 시스템이 점진적으로 통합되어 감에 따라 이 컴퓨터 시스템이 안전 기능을 충분히 수행하는 수준까지 도달하여야 한다. 지속적인 시험운전 및 실제 운전을 수행하는데 필요한 모든 실행 가능한 시험은 이러한 수준이 도달되기 전에 모두 완료되어야 한다. 아울러 유지보수 하는데 필요한 모든 소프트웨어 및 하드웨어는 이 시스템이 안전 기능을 수행하기 전에 구비되어야 한다.

시험 운전을 수행하는 작업자는 개발자와는 별도의 사람들이어야 하고 이러한 작업자는 적합한 자격요건을 갖추어야 한다. 엄격한 컴퓨터 시스템의 형상 통제가 시험 운전 프로그램 동안 유지되어야 한다.

4.12.2 문서화 작업

디지털 안전 시스템을 만족하기에 시험 운전 프로그램이 적합하였다는 것을 포괄적으로 증명하기 위하여 충분한 문서화 작업은 이루어 져야 한다. 시험 도달범위의 적합성 및 소스(source) 요구사항(안전 계통 요구사항)에 대한 시험의 추적성을 증명하는 문서들은 시험운전 팀에서 준비하여야 한다. 시험운전 적합성을 확증하는 문서는 발전소 운전자가 보관하여야 하며 제 삼자 평가에 활용 가능하여야 한다. 이 단계에서 생산되는 문서들은 다음 항목과 같은 타당성을 포함하여야 한다.

- 어느 시스템 통합 및 설치 후 수행한 확인 시험의 적합성
- 이 단계에서 수행되는 설치 전 시험의 반복 횟수
- 소스 요구사항(컴퓨터 시스템 요구사항)에 대한 시험 추적을 포함한 시험운전 시험 도달범위, 모든 시험운전 기록 및 완성된 보고서, 부적합 사항 및 시험 실패 기록 및 이러한 비정상 시 해결책의 설명
- 컴퓨터 시스템이 시험운전 모든 단계에서 적절한 안전기능을 수행할 능력.

4.13 운전

디지털 시스템의 운전은 설치 후 시험운전을 거치고 규제기관에서 사용 승인을 취득한 후 수행한다. 이 시스템은 발전소의 일부가 되고 발전소 운영자에 의해 운영된다. 어느 시스템의 운전 단계는 그 시스템이 제거되거나 교체될 때까지 지속된다. 디지털 시스템의 운전은 그 시스템을 좋은 상태로 유지하고 고장난 기기를 수리하는 유지보수 활동을 포함할 것이다.

4.13.1 권고 사항

4.13.1.1 수습 기간 (Probationary Period)

개선작업을 수행한 경우 운전의 수습기간을 두어서 이 기간 동안 디지털 시스템의 운전 중 시험의 빈도를 높여서 시험을 수행하여야 한다.

4.13.1.2 보수 활동

하드웨어 기기가 고장난 경우 하드웨어 보수작업은 각각의 고장난 하드웨어를 하나씩 수리하고 관련 소프트웨어 모듈을 하드웨어에 실은 후 다른 고장난 하드웨어 기기를 수리하는 식으로 하여야 하고 이 때 하드웨어를 개선하거나 수정하여 서는 안 된다.

4.13.1.3 보안

디지털 시스템에서는 암호 관리 등 적절한 보안 절차가 구현되어 있어야 한다. 보안 사항을 저장하는 장치와 절차 통제는 오직 인가된 소프트웨어의 버전이 발전소 기기에 로드(load)될 수 있도록 해야 한다.

4.13.1.4 교정 데이터 (Calibration Data)

교정 데이터는 디지털 시스템 신뢰도를 저해하지 않도록 정밀도가 충분히 높아야 한다. 안전 계통에 대해서는 이러한 데이터가 디지털 시스템과 같은 표준에 따라 개발된 시스템에 의해 자동으로 생성되어야 하며 만약 그러한 경우가 아니라면 생성된 교정 데이터는 독립 그룹에 의해 수행된 다양한 방법에 의해 점검되어야 한다. 운전자는 시스템에 입력된 데이터를 반드시 확인하여야 하고 모든 입력 데이터는 기록되고 독립 그룹에 의해 안전 계통이 복귀하기 전에 점검되어야 한다.

4.13.2 문서화 작업

충분하고 정확한 시스템 운전 기록이 운영자에 의해 보관되어야 하고 제 삼자 평가에 활용할 수 있어야 한다. 이들 기록은 모든 유지보수 활동(예방 및 보수 활동을 포함), 운전 중 시험, 및 시스템 운전 중 발생한 부적합 사항을 포함하여야 한다.

디지털 시스템 관련 사건 및 부적합 사항은 이러한 목적으로 준비된 절차에 따라 기록되어야 한다. 발생 사건 조사 및 보수 활동 수행의 결과는 기술되어야 한다. 소프트웨어 수정과 관련된 보수 활동은 다음 절에서 기술하는 것과 같은 엄격한 변경 통제하에서 수행하여야 한다.

안전 계통에 대하여 교정 데이터 생성 시스템이 디지털 시스템의 표준과 동일한 표준에 따라 개발되지 않은 경우 교정 데이터 생성 절차가 기술되어야 하고 다양성을 증명하여야 한다.

4.14 인수 후 수정

운전 중 수정작업을 위하여 발전소 안전 현안을 다루는 적절한 변경 통제 절차가 구비되어야 한다. 수정 후 안전 영향에 대해 훈련 받은 요원에 의해 분석되어야 한다.

4.14.1 권고 사항

발전소 설계자나 운전자는 적절한 변경 통제 절차를 구비하여야 하며 이러한 통제 절차는 적합한 절차 및 수정의 안전 현안의 검토 및 승인을 위한 조직 구성을 포함하여야 한다. 이러한 절차는 사업 시작 단계에서 준비되어야 한다. 모든 수정 사항은 고려되어야 하고 안전 중요도에 따라 분류되어야 한다. 안전에 매우 중요한

수정 사항은 규제 기관에 제출되어야 한다.

절차가 구비되고 설계자나 개발자와는 독립적인 전문가가 제안한 수정이나 변경 구현의 적합성을 평가하여야 한다. 변경 절차에 의한 변경은 소프트웨어 변경, 하드웨어 변경 및 도구 변경을 포함한다. 변경 절차는 각 안전 증명이 각각의 수정에 대해 준비되어 있음을 확증하여야 한다.

운전 중 특히 컴퓨터 시스템 소프트웨어의 수정은 자세한 타당성에 의해 보완되고 이러한 작업에 별도의 기기가 구비되지 않은 경우에만 허락하여야 한다. 발전소 운전 동안 변동을 초래하는 매개변수 수정은 이러한 목적을 위하여 준비된 공학적 설비를 활용하여 수행되어야 한다. 공학적 설비에 의해 제공되는 변동의 정도는 발전소 안전 분석에서 증명된 한계 내에 있어야 한다.

엄격한 형상 통제가 변경 과정 동안 유지되어야 한다. 완전한 변경 절차를 거친 항목만이 발전소 기기에 설치되어야 한다. 변경 절차는 문제 해결이나 시험이 컴퓨터 시스템이 구동하지 않을 경우 임시적인 변경을 요하는 경우에 대해서도 다루어야 한다. 다양성의 하부 시스템에서 어느 다중 하부 시스템으로 수정된 소프트웨어를 설치하는 것은 계획되어 있어야 하고 일시적인 시스템 저하의 영향을 줄이는 방향으로 구성하여야 한다. 수정한 소프트웨어를 안전 계통으로 설치할 때에는 공통원인 고장을 줄이기 위하여 단계 별(한번에 하나의 하부 시스템 수정) 설치하여야 한다.

4.14.2 문서화 작업

다음과 같은 정보는 제안한 변경의 각각에 대하여 반영되어야 한다.

- 수정 이유
- 수정의 기능 기술
- 발전소 안전이 변경에 의해 악 영향을 받지 않는다는 것을 증명하는 수정의 안전 평가
- 설계 수정의 자세한 기술. 설계 수정에 따른 영향 받은 모든 발전소 품목 및 제안된 변경의 전체에 걸친 충격 분석
- 확인 및 검증 그리고 제 삼자 평가, 그들의 범위와 회귀 분석의 타당성을 포함하는, 보고서
- 제안된 설치 방법의 타당성
- 현장에서 수행한 시험 보고서

모든 변경관련 문서는 소프트웨어 변경 통제의 항목 상에 날짜, 문서번호 및 파일을 기입하여야 한다. 시간 상의 연대기 적인 기록들이 구축되어야 하고 보관되어야 한다. 변경 관련 문서는 규제 요원에게 활용 가능하여야 한다,

4.15 용어정의 및 참고문서

4.15.1 용어 정의

- **안전 중요 디지털 시스템 (Computer Based System Important to Safety)**
  안전에 중요한 발전소 시스템으로 그 시스템의 안전 기능은 내장용(embedded) 컴퓨터 시스템을 통하여 달성된다.
- **컴퓨터 시스템 구조 (Computer System Architecture)**
  컴퓨터 시스템 하드웨어 기기 (프로세서, 메모리, 입출력 장치), 기기의 연결, 통신 시스템 및 이들 기기의 소프트웨어 기능의 매핑(mapping).
- **컴퓨터 시스템 통합 (Computer System Integration)**
  소프트웨어와 하드웨어를 통합하여 컴퓨터 시스템을 만드는 과정
- **컴퓨터 시스템 요구사항 (Computer System Requirements)**
  컴퓨터 시스템이 상위 설계 수준에서 정의한 발전소 안전 요구사항을 필요충분적으로 만족하는 기능적 및 비 기능적 특성.
- **신뢰성 (Dependability)**
  인수한 품목에 대한 신뢰를 타당하게 부여할 수 있다는 믿음. 신뢰도, 가용도, 및 안전성은 신뢰성의 특성이다.
- **펌웨어 (Firmware)**
  메모리 같은 종류에 로드(load)되는 컴퓨터 프로그램과 데이터로써 구동 중 컴퓨터에 의해 쉽게 수정할 수 없는 것.
- **기능적 안전 요구사항 (Functional Safety Requirements)**
  인수되어야 할 안전 품목 및 안전 기능.
- **구현 (Implementation)**
  설계를 하드웨어 기기나 소프트웨어 구성품으로 변환하는 과정 및 이러한 과정의 결과.
- **비 기능적 요구사항 (Non-Functional Requirements)**
  보증되어야 할 특성이나 성능.
- **기 개발 또는 기성 소프트웨어 (Pre-Developed or Pre-Existing Software)**
  디지털 시스템에 사용되는 소프트웨어로써 시스템 개발 통제하에서 개발되지 않은 소프트웨어. 상용 소프트웨어(Off-the-shelf Software)는 기성 소프트웨어의 하나의 유형이다.
- **다중성 (Redundancy)**
  대체 구조, 시스템, 또는 기기를 구비하는 것으로 다른 하나가 고장이나 운전 상태와는 상관없이 어느 하나만으로 필요한 기능을 수행할 수 있는 것.
- **역 공학 (Reverse Engineering)**

수행 완료한 설계에서 요구사항을 생성하는 것. 이러한 요구사항을 원래 요구사항과 상호 양립하는 것을 보이기 위하여 두 요구사항을 비교함.

- **검토성 또는 검토 가능성 (Reviewability)**
  소프트웨어 요소나 쉽게 파악가능한 사업 진행상황을 평가하는데 계획한 결과에 대한 차이를 허용하는 품질.
- **안전 관련 시스템 (Safety Related System)**
  안전 시스템은 아니지만 안전에 중요한 시스템.
- **안전 시스템 (Safety System)**
  안전에 중요한 시스템으로써 원자로 안전정지나 노심 잔열 제거, 또는 가상개시사건 및 설계기준 사고의 결과를 제한하는데 활용되는 시스템.
- **소프트웨어 요구사항 (Software Requirements)**
  소프트웨어 구성요소가 수행해야 하는 것을 기술한 것으로써 이러한 구성요소가 선택된 컴퓨터와 주변장치에 대해서 구동하는 경우 계통 요구사항을 만족시키기 위한 소프트웨어 상의 필요사항.
- **안전에 중요한 시스템 (System Important to Safety)**
  어느 시스템이 안전 그룹의 부분이거나 그 시스템의 고장이 현장 작업자나 일반 대중의 방사선 피폭을 유발하는 시스템.
- **시스템 통합 (System Integration)**
  컴퓨터 시스템을 발전소 다른 기기들과 통합하는 과정.
- **시스템 생명 주기 (System Life Cycle)**
  시스템 개념부터 폐기처분까지 포함하는 모든 단계.
- **타이밍 (Timing)**
  소프트웨어에 수행되는 변환에 대한 시간 제한치.
- **추적성 (Traceability)**
  개발 공정에서 두 생산물간에 구축된 상호 관계 특히 서로 간에 선행자(predecessor)와 후행자(successor)로써 관계를 갖는 정도.
- **확인 (Validation)**
  통합 컴퓨터 시스템이 기능, 성능, 및 연계 요구사항을 준수하는지 확증하는 시험 및 평가 공정.
- **검증 (Verification)**
  시스템 생명 주기상의 어느 단계가 그 이전 단계에서 부과한 요구사항을 만족하고 있는지 확증하는 공정.
- **보팅 (Voting)**
  출력 신호들을, 3개 출력 신호에서 2개만을 선택하는 방식으로, 선택(vote)하여 시스템의 비정상 활동 가능성을 줄이고자 하는 전략.

4.15.2 참고 문서

[4-1] International Atomic Energy Agency, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standard Series No.NS-G-1.1, IAEA, Vienna, 2000.

[4-2] International Electrotechnical Commission, Instrumentation and Control for Systems Important to Safety: Software for Computer-Based I&C Systems Supporting Category B or C Functions, Standard No.62138. IEC, Geneva, 2003.

[4-3] International Atomic Energy Agency, Safety of Nuclear Power Plants: Design, Safety Standard Series No.NS-R-1, IAEA, Vienna, 2000.

[4-4] International Nuclear Safety Advisory Group, Basic Safety Principles for Nuclear Power Plants, Safety Series No.75-INSAG-3 Rev.1, INSAG-12, IAEA, Vienna, 1999.

[4-5] International Electrotechnical Commission, Software for Computers in Safety Systems of Nuclear Power Plants, Standard No.60880, IEC, Geneva, 2003.

[4-6] International Atomic Energy Agency, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Facilities, Code and Safety Guide Q1~Q14, Safety Series No.50-C/ SG-Q, IAEA, Vienna, 1996.

[4-7] International Atomic Energy Agency, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, Technical Reports Series No.60384, IAEA, Vienna, 1999.

[4-8] International Atomic Energy Agency, Software Important to Safety in Nuclear Power Plants, Technical Reports Series No.60367, IAEA, Vienna, 1994.

[4-9] U. Voges, “Software Diversity”, Proc. 9th Annual Conf. on Software Safety, Lexembourg, 1992, Center for Software Reliability, City Univ., London, 1992.

[4-10] International Atomic Energy Agency, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, Technical Reports Series No.384, IAEA, Vienna, 1999.

5. 결 론

본 보고서는 “수출전략형 연구로 계통설계해석”과제의 일환으로 연구로 설계 시 계측제어 분야에서의 설계 방향중의 하나이다. 향 후 연구로의 계측제어 분야는 상용 원자력발전소와 같이 컴퓨터 기반 디지털 시스템을 기본으로 하여 설계, 구현되는 것이 바람직하여 또한 이러한 방향은 세계적인 추세이다. 디지털 시스템에서 연구로나 발전소의 안전 및 비안전 기능을 수행하는 것은 대부분 소프트웨어 상에서 이루어 진다. 따라서 디지털 계측제어 시스템의 안전성은 소프트웨어의 건전성 및 안전성에 지대한 영향을 받는다. 본 보고서는 디지털 계측제어 계통에서 소프트웨어의 분류와 규제요건 및 소프트웨어 개발 시 수행되어야 하는 절차 및 필요 사항에 대하여 기술한다.

본 보고서의 제 2 장에서는 디지털 소프트웨어의 등급 분류 원리와 내용에 대하여 기술되어 있다. 지금 과제로 수행하는 연구로 과제는 해외 수출을 위한 목적으로 연구되고 있는 것이기 때문에 소프트웨어 분류에서 국내 분류 지침뿐만 아니라 국제적 등급 분류 표준에 대하여도 자료를 조사하여 내용을 기술하였다. 제 3 장에서는 디지털 소프트웨어에 대한 규제요건에 대한 분석 내용을 안전 요건과 개발공정 및 품질 요건의 관점에서 기술하였다. 실제 이러한 규제요건을 고려하여 소프트웨어를 개발하는 공정과 필요 사항에 대하여 제 4 장에서 기술하였다. 소프트웨어 개발 공정 및 공정 내 업무에 대해서는 각 나라 별로 지침서가 있으나 본 장에서는 국제 원자력 에너지 기구에서 발간한 안전 지침서를 기반으로 디지털 소프트웨어 개발 절차를 기술하였다.

서 지 정 보 양 식

수행기관보고서 번호	위탁기관보고서 번호	표준보고서 번호	INIS 주제코드
KAERI/TR-3030/2005			

제목/부제	수출전략형 연구로 디지털 소프트웨어 분류 및 설계요건 분석
연구책임자/부서명	박기용 / 기계공학연구부
연구자 / 부서명	정환성, 류정수, 박 철 / 하나로운영부

출 판 지	대전	발행기관	한국원자력연구소	발행일	2004. 6.
페 이 지	102 p.	도 표	있음(V), 없음( )	크 기	21x29.7 Cm

참고사항			
비밀여부	공개(V), 대외비( ), (__)급 비밀	보고서종류	기술보고서
연구위탁기관			

초록 (15-20 줄 내외)

컴퓨터를 기반으로 하는 디지털 기술이 혁신적으로 발달함에 따라 전 산업체에 걸쳐서 계측제어 시스템에 디지털 시스템이 광범위하게 적용되고 있다. 원자력 분야에서도 상업용 신규 원자력발전소에는 디지털 계측제어 시스템이 기존 아날로그 시스템을 대체하여 설치되어 운전하는 추세에 있다. 연구로인 하나로의 경우 안전에 중요한 계통 및 핵심 제어계통은 아날로그 시스템으로 구축되어 운영되어 왔다. 그러나 수출용 연구로의 경우에는 세계적인 추세에 맞추어 보호 및 제어 계통 모두 디지털 시스템으로 구축하는 것이 바람직하다.

컴퓨터 기반 디지털 시스템은 기존 아날로그 시스템이 가질 수 없는 우수한 성능과 구현 및 변경 작업에 있어서 뛰어난 유연성을 가지고 있다. 또한 새로이 개발되는 디지털 제품을 아날로그 시스템에 비하면 별 어려움 없이 기존 제품에 교체 설치하여 시스템 개선을 이룰 수 있는 장점이 있다. 디지털 기술의 발전은 디지털 하드웨어 고 직접화를 구현할 수 있게 하였고 이러한 고 직접화는 전자회로의 부품을 크게 줄이고 아울러 점차 고성능의 연산처리기에 있어서 구동 소프트웨어의 역할을 크게 증대 시켰다. 따라서 디지털 시스템의 전자회로가 단순화 됨에 따라 하드웨어 상의 물리적인 고장은 크게 감소하였으나 소프트웨어의 오류로 인한 시스템 고장 가능성은 상대적으로 크게 증대되었다. 따라서 수출형 연구로에서 디지털 계측제어에 쓰이는 소프트웨어의 안전이 심도있게 고려해야 하는 중요한 고려사항이다. 본 보고서는 이러한 사항에 입각하여 디지털 계측제어 계통에 쓰이는 소프트웨어의 분류와 관련하여 국내외 현황을 파악하였으며 또한 소프트웨어 개발 특히 안전에 중요한 계측제어 시스템에 쓰이는 소프트웨어의 설계요건에 대하여 국제적으로 표준화된 지침을 조사하여 분석한 결과를 기술하였다.

주제명키워드 (10 단어 내외)	디지털 계측제어, 디지털 소프트웨어, 등급분류, 개발절차, 설계요건

BIBLIOGRAPHIC INFORMATION SHEET

Performing Org. Report No.	Sponsoring Org. Report No.	Standard Report No.	INIS Subject Code
KAERI/TR-3030/2005			

Title/Subtitle	Investigation of Classification and Design Requirements for Digital Software for Advanced Research Reactors
Project Manager and Department	Gee Yong Park / Advanced Reactor Technology Development
Researcher and Department	H. S. Jung, J. S. Ryu, and C. Park / HANARO Management Div.

Publication Place	Daejeon	Publisher	KAERI	Publication Date	June, 2005
Page	102 p.	Fig. & Tab.	Yes(V), No( )	Size	21x29.7 Cm

Note			
Classified	Open (V), Restricted ( ), __ Class Document	Report Type	Technical Report
Sponsoring Org.		Contract No.	

Abstract (15-20 Lines)

As the digital technology is being developed drastically, it is being applied to various industrial instrumentation and control (I&C) fields. In the nuclear power plants, I&C systems are also being installed by digital systems replacing their corresponding analog systems installed previously. There had been I&C systems constructed by analog technology especially for the reactor protection system in the research reactor HANNARO. Parallel to the pace of the current trend for digital technology, it is desirable that all I&C systems including the safety critical and non-safety systems in an advanced research reactor is to be installed based on the computer based system.

There are many attractable features in using digital systems against existing analog systems in that the digital system has a superior performance for a function and it is more flexible than the analog system. And any fruit gained from the newly developed digital technology can be easily incorporated into the existing digital system and hence, the performance improvement of a computer based system can be implemented conveniently and promptly. Moreover, the capability of high integrity in electronic circuits reduces the electronic components needed to construct the processing device and makes the electronic board simple, and this fact reveals that the hardware failure itself are unlikely to occur in the electronic device other than some electric problems. Balanced the fact mentioned above are the roles and related issues of the software loaded on the digital integrated hardware. Some defects in the course of software development might induce a severe damage on the computer system and plant systems and therefore it is obvious that comprehensive and deep considerations are to be placed on the development of the software in the design of I&C system for use in an advanced research reactor. The work investigates the domestic and international standards on the classifications of digital software for use in I&C systems in nuclear power plants and describes the requirements for software development recommended by international standard.

Subject Keywords (About 10 words)	Digital I&C, Digital Software, Classification, Development Process, Design Requirements