신형경수로1400 첨단 제어실 설계 및 평가

신영철 · 송태영 · 이동훈
한국수력원자력(주) 신형원전개발센터 I&C 그룹

설계 접근 방법

1. 전산화된 첨단 제어실 도입

미국 원자력규제위원회는 TMI-II 사고 결과에 따른 조치 계획으로 운전원의 작업 부하 및 인적 오류를 최소화하기 위해, 사업자는 제어실에 설계 검토 수행과 발전소 안전 변수 표시 장치를 제어반에 추가하도록 요구하였다.

그러나 이러한 조치 계획을 기존 제어실에 적용하기에는 재설계 및 재건설에 따른 과도한 비용 문제로 한계가 있었다. 왜냐하면 아날로그(analog) 방식의 계기와 스위치로 구성된 기존 제어실은 운전 정보를 처리하거나 운전 기능을 통합할 수 있는 유연성이나 능력이 부족하기 때문이다.

비록 기존 제어실에도 컴퓨터를 통해 그래픽화된 추이(trending)와 데이터 계산과 같은 정보 지원 기능을 제공하지만, 제어반(control panel)과 연계된 부적합한 통합 기능은 이러한 운전 지원 기능 사용을 어렵게 한다.

따라서 운전원은 컴퓨터를 통한 정보 기능 사용이 신체적 및 정신적 작업 부하로 인해 어려움이 있다고 판단하는 경우 쉽게 포기하게 된다.

이러한 배경에서 신형경수로 1400(advanced power reactor 1400) 첨단 제어실에는 각 운전원에게 워크스테이션(workstation) 기반의 전산화된 시각 표시 장치(visual display unit)를 제공하여 발전소 감시 및 제어 정보를 통합 제시함으로써, 최소화된 육체적 및 정신적 작업 부하로 운전을 수행할 수 있는 환경을 제공하게 되었다.

2. 자동화 설계

신형경수로1400 첨단 제어실의 인간 기계 연계(man-machine interface: MMI) 시스템은 다음과 같은 자동화 설계를 통해 안전성을 확보하였다.

가. 필수 안전 기능 감시

비상 운전 절차서 수행시 필수 안전 기능이 자동적으로 평가되고, 불만족되면 운전원에게 경보가 제공된다. 이 때 운전원은 비상 운전 절차서 수행을 중단하고 필수 안전 기능 회복 절차서(functional recovery procedure)를 수행하게 된다.

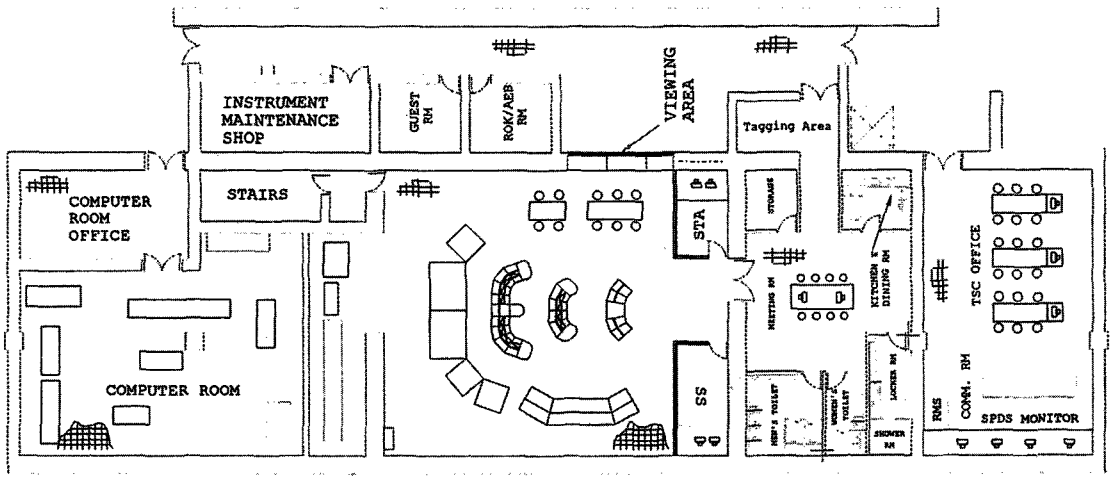
나. 절차서 수행 조건 감시

절차서는 정해진 단계에 따라 순차적으로 수행되지만 발전소 상태에 따라 수행 순서에 변화가 있을 수 있다. 대표적으로 절차서 진입 조건, 계속 수행 단계는 항시 감시되어야 하며, 이를 운전원이 직접 수행하는 경우 정신적 부담으로 오류의 확률이 높았다.

신형경수로1400 MMI 설계에는 이러한 감시 기능을 자동화시켜 인적 오류 발생 가능성을 최소화하였다.

다. 운전 행위 감시

절차서 수행시 운전원이 특정 단계에 대한 수행 완료를 결정할 경우에는 발전소 상태를 정확히 읽고 수



〈그림 1〉 신형경수로1400 첨단 제어실 배치

행하여야 한다.

비록 절차서 수행의 모든 권한은 운전원에게 부여되어 있지만 신형경수로1400 MMI 설계에는 컴퓨터를 통해 운전원 판단에 대한 오류 유무를 내부적으로 점검하여 적절히 알려준다.

이 경우 운전원은 수행하였던 행위를 재판단, 컴퓨터에 의한 운전 행위 감시 결과의 수용 여부를 최종 결정한다.

3. 신호 검증

가. 공정 대표값 계산

기존 주제어실의 경우 센서(sensor)의 종류에 따라 유사하거나 동일한 공정값에 대해 수많은 표시기가 있었다(예를 들어 가압기 압력을 표시하기 위해 16개의 표시기가 있음). 이들 센서는 최적 작동 영역이 달라 운전원이 정확히 값을 읽고 타당한 공정값을 유추하기 어려웠다.

그러나 첨단 제어실의 신호 검증 알고리듬은 센서를 통한 다양한 값들을 통계적인 기법이나 모델에 기초한 계산을 수행, 정확한 공정 대표값(process representation value)을 산출하여 제시한다.

나. 사고 후 감시 변수 검증

Reg. Guide 1.97 Category 1 변수는 사고 상황 후에도 감시될 변수이며 신뢰성이 매우 높다. 따라서 공정 대표값을 계산할 때 이 변수에 기준을 두고 계산하면 신뢰성 있는 결과를 얻을 수 있다. 운전원에게 제시되는 변수들은 사고 후 감시 변수(post accident monitoring indicator: PAMI)에 대비하여 검증된 값이다.

다. 제어 신호 검증

대부분 비정상적 원자로 정지는 운전원이 센서 고장을 감지, 진단하고 적절한 조치를 수행하는 데 충분한 시간을 가지지 못하기 때문에 발생한다. 따라서 신형경수로1400에는 제어 신호 검증을 자동화하여, 어느 센서가 정상인지 확인하고 정상인 신호가 원자로 개시 회로에 사용되도록 설계하였다.

4. 고장 허용 설계

신형경수로1400 제어실에 설치된 컴퓨터는 운전원별 워크스테이션 제공 및 각 워크스테이션별 여러 대의 컴퓨터 제공, 모든 워크스테이션 고장에 대비한 안전 제어반(safety console) 제공 등을 통해 신뢰성을 향상시켰다. 또한 다양한 자기 진단 기능과 Watch Dog 기능은 조기에

오류를 찾아내고 경보 기능과 형상 재배치 기능을 제공하였다.

운전원 제어 오류는 제어 행위시 재확인 단계를 넣어 예방하였다. 절차서 수행중 운전원 판단 오류는 전산화 절차서(computerized procedure system)의 자동 판단 기능에 따라 예방되고 필수 안전 기능은 CFM/SPM으로 확인된다.

또한 대형 정보 표시반은 운전원에게 공통되고 전반적인 발전소 상태를 보여 줌으로써 감시 다중성을 제공하였고, 여러 워크스테이션을 운전원들이 제한 없이 접근하여 조기에 발전소 이상 상태를 발견할 수 있도록 설계하였다.

주제어실 및 인간-기계 연계 설계

신형경수로1400에서 가장 현저한 설계 변화는 기존 발전소의 주제어실과 계측 제어 계통을 최신의 기술을 적용한 MMI로 교체한 것이다.

신형경수로1400 MMI는 지금까지 입증된 한국 표준형 원전(Korean Standard Nuclear Plant: KSNP)의 설계 특징을 유지하면서 모든 계측 제어 계통의 디지털화와 데이터 통신을 적용하고, 인간 공학 설계 원리를 적용한 그래픽화된 화면 기반을 제어실에 제공하였다.

신형경수로 1400 주제어실 배치는 <그림 1>과 같으며, 설계 특징은 다음과 같다.

1. 대형 정보 표시반

대형 정보 표시반은 안전 변수 감시 계통(safety parameter display system: SPDS)과 우회 및 운전 불능 상태 지시 계통(bypassed & inoperable status indication: BISI)을 포함한 발전소 개요 정보 표시 장치이다.

대형 정보 표시반은 고정 영역(fixed display section)과 변동 영역(variable display section) 등 두 개 부분으로 구분할 수 있으며, 고정 영역에는 주요 경보, 기기 및 계통상태 정보, 변수 정보 등을 지속적으로 제공한다.

이것은 발전소 정보를 공간적으로 고정된 영역에 그래픽 화면으로 제공함으로써 소형 제어반의 화면 이동을 통한 정보 접근의 단점을 보완한다.

변동 영역에는 운전원들이 필요로 하는 정보를 선택적(또는 가변적)으로 제공하여 운전원간 의사 소통을 지원한다.

2. 소형 제어반

소형 제어반은 각 운전원이 발전소 안전 운전과 출력 운전에 관련된 모든 감시 운전 및 제어 운전을 위해서 요구되는 정보와 제어 기기를 제공한다.

소형 제어반은 안전 계통과 비안전 계통을 모두 포함하며, 다음과 같은 설계 요소로 구성되었다.

- 평판 화면 표시 장치(flat panel display: FPD) ; 마우스(mouse)를 이용하여 공정계통 감시, 공정 및 기기 제어 또는 전산화 절차서를 지원하는 4대의 FPD
- 고정형 푸시 버튼(dedicated push buttons) ; 원자로 정지와 공학적 안전 설비 계통을 수동으로 동작시킬 수 있는 버튼
- 작업 영역(writing space area) ; 운전 기록, 도면 열람 및 종이 절차서 등을 이용하기 위한 운전 보조 영역 채널 확인 스위치(channel confirm switches) ; 안전 등급 기기 제어를 위한 4개의 채널 확인 스위치
- 경보 확인 버튼(alarm acknowledge button) ; 대형 정보 표시반에서의 경보 발생시 경보 확인을 수행하는 2개의 확인 버튼
- 키보드(keyboard) ; 운전 일지 작성, 꼬리표(tagging) 작업 또는 전산화 절차서 운영을 지원하기 위한 키보드

3. 안전 제어반

첨단 주제어실에는 소형 제어반과는 독립적으로 모든 안전 관련 기기들을 제어하기 위한 안전 제어반을 포함한다. 안전 제어반에서는 정상 운전시에는 정기 점검을 수행하고, 원자로 정지 후에는 전기 운전원(electrical operator)에 의해 비상 운전을 지원한다.

안전 제어반은 설계 기준 사고시 사고 완화와 소형 제어반의 공통 모드 고장(common mode failure: CMF)시 안전 정지 운전을 위해 요구되는 모든 기능을 제공한다.

4. 소형 제어반의 정보 표시기

주제어실 소형 제어반은 4대의 정보 표시기(information FPD)를 이용하여 발전소 정보에 접근할 수 있다.

소형 제어반에서는 기존 발전소의 제어반을 대신한 계층적인 계통 기능 정보, SPDS의 중요 부분인 필수 안전 기능 정보, 전산화 절차서에 의해서 제공되는 계층적 직무 지원 정보 등이 제공된다. 여기에서 모든 정보는 구체적인 운전 기능을 지원하도록 설계되었다.

또한 원하는 정보 화면에 대한 접근성을 보장하기 위해 메뉴를 통한 화면 이동, Format Chaining을 이용한 직접적인 화면 이동, 고정 버튼을 이용한 화면 이동과 같은 다양한 방법이 제공된다.

5. 소프트 제어기

신형경수로1400에는 효과적인 제어 수행을 위한 주요 수단으로 소프트 제어기를 설계하였다. 소프트 제어기는 기존 발전소에서 스위치 형태(hard-wired switch)로 제공된 물리적 기기를 대신하는 소프트웨어 기반의 제어 기기로, 설계의 유연성 및 변경성을 보장한다.

또한 하나의 소형 제어반에서 운전원이 모든 제어기를 제어할 수 있으며 채널 확인 스위치를 이용하여, 안전 기기와 비안전 기기 제어가 동일한 소형 제어반에서 제어됨으로써 발생할 수 있는 제어의 독립성을 유지하였다.

6. 경보 시스템

신형경수로1400 첨단 제어실에서의 경보 시스템은 다음과 같은 기준을 고려하여 설계하였다.

- 운전원이 대응해야 할 경보 수를 줄여 중요 경보를 구분하여 인지할 수 있도록 한다.
- 실제 공정 변수가 정상 범위를 벗어난 것과 센서 고장을 구분하여 정보를 제공하도록 한다.
- 논리 설계를 통하여 불필요한 경보, 즉 실제로 운전원이 대응할 필요가 없는 경보를 최소화한다.
- 중요도에 따라 경보를 우선 순위화하여 운전원이 가장 중요한 경보에 집중할 수 있도록 한다.
- 발전소 출력 운전에 영향을 미칠 수 있는 경보를 결정하고, 이를 낮은 수준의 시스템 경보와 구분할 수 있도록 한다.

필수 안전 기능과 같은 우선 순위 1(first priority) 경보는 대형 정보 표시반의 고정 영역에서 제시된다. 또한 모든 경보를 소형 제어반 정보 화면에서 다양한 종류의 경보 목록 형태로 제공하며, 시스템 감시 화면에서는 각 경보를 관련 기기와 변수에 그룹핑한 경보 정보를 제공함으로써 시스템이나 발전소의 전반적인 운전 상태를 신속하게 파악할 수 있도록 설계하였다.

7. 전산화 절차서

전산화 절차서는 독창적인 제어 행위가 불가능하도록 수동적인 설계로 구현되어 있다. 절차서 화면의 가운데 부분은 모든 절차서 단계들이 스크롤이 가능한 플로우챠드 형태의 절차서 개요 화면으로 설계되었다.

전산화 절차서는 절차서 각각의 단계 수행을 원자로 운전원(reactor operator)이나 터빈 운전원(turbine operator)과 같은 특정 운전원에게 할당한다.

상세 단계 지시창(action details window)에는 운전원이 수행해야 하는 행위에 대해 일반적인 문구로서 제공된다.

전산화 절차서 운영중에는 의사결정을 지원하기 위해 실시간 발전소 정보나 Format Chaining을 적절한 화면으로 제공하며 소프트 제어기의 직접적인 접근도 가능하다.

또한 강제 지시 기능(forcing function)은 운전원들로 하여금 절차서 수행에 있어 맹목적으로 컴퓨터를 따르는 것을 방지한다.

이러한 전산화 절차서 설계에 따른 주요 장점으로는 컴퓨터를 이용

한 계속 수행 단계(continuously applicable procedure)의 진보된 감시 기능, 절차서 수행 중 정보와 제어에 대한 직접 접근 기능, 절차서 통합, 그리고 오류 가능성과 응답 다양성의 감소 등이 있다.

검 증

1. 목적 및 접근 방법

신형경수로1400 MMI 설계에 대한 인간 공학적 확인 및 검증의 목적은 본 시스템이 주제어실 운전원이 직무를 수행하는 데 있어 예상되는 결함 사항이 없음을 증명하고, 평가를 통해 도출된 결과를 지속적으로 축적하여 설계의 안전성을 확보하는 데 있다. 이를 위해 반복 확인 및 검증 수행을 원칙으로 설계 개념 및 표준 설계 특성에 대한 검증을 수행하였다.

인간 공학 확인 및 검증은 적합성 검증(suitability verification)과 시스템 통합 검증(integrated system validation) 등 두 가지 활동을 통해 수행되었다.

적합성 검증에서는 전문가적 지식 기반과 경험 기반을 바탕으로 수행한 하향식 접근 방식(top-down approach)과 인간 공학적 지침에 근거한 상향식 접근 방식(bottom-up approach)을 이용하여 MMI 설계가 운전원 작업 수행에 적합함을 확인하였다.

시스템 통합 검증은 MMI 설계가 주제어실이라는 통합적 환경에서 운전 수행에 적합함을 확인하는 것이다.

이 평가는 신형경수로 1400 기술개발 과정에서 총5회 실시되었으며, 이를 통해 새롭게 설계된 다양한 MMI 구성 요소가 시스템 통합 측면에서 운전원 직무 수행에 효과적으로 지원됨을 확인하였다.

2. 검증 결과

인간 공학 확인 및 검증 평가 결과 신형경수로1400 MMI는 정상 및 비상 운전뿐만 아니라 미비한 비정상 발생시 발전소 감시(monitoring), 탐지(detection), 상황 판단(situation assessment) 등의 직무를 수행하는 데 적합함을 확인하였다.

특히 대형 정보 표시반에 국한된 평가 결과 운전원은 초기 발전소 상태에 관한 지식, 다른 운전원의 협조, 기타 MMI 설계 요소의 도움이 없더라도 대형 정보 표시반만을 이용하여 발전소 상황을 파악하였다.

대형 정보 표시반과 연계 사용되는 경보 시스템 또한 운전원이 미미한 이상을 나타내는 신호 감지 후 발전소 상태를 관찰하는 데 유용하였다.

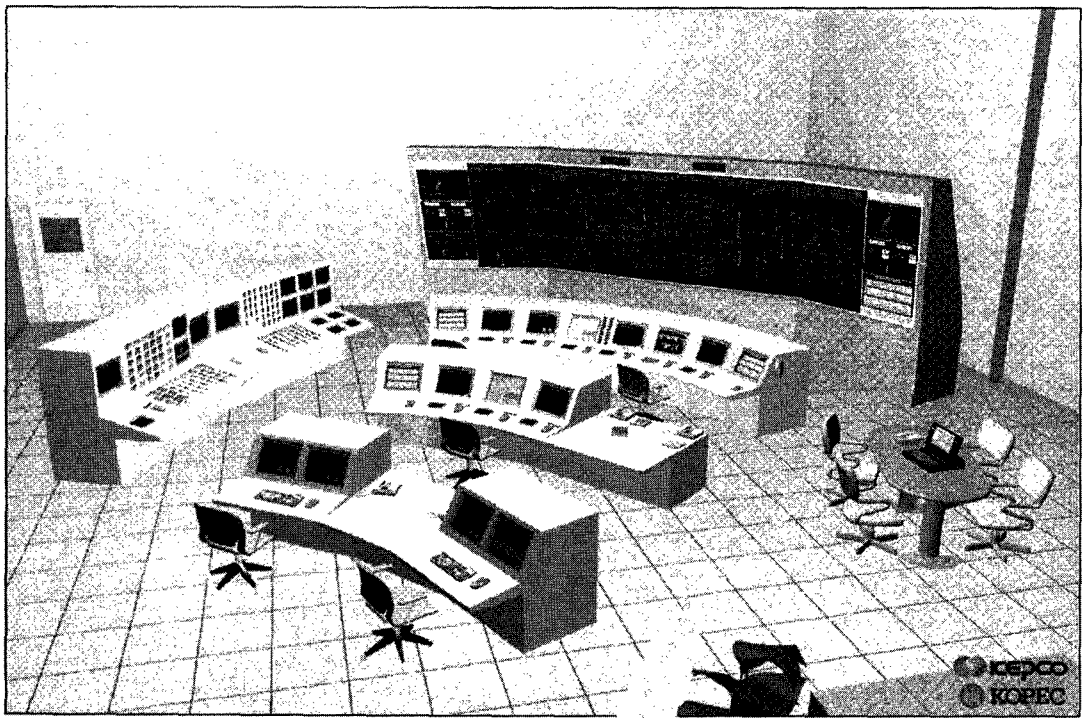
평가에 참여한 대부분의 운전원들은 특히 Alarm Message Lists는 시간 순서에 따라 발생된 이상 상태(abnormal conditions)가 무엇이며 어떠한 경로로 전개되었는지를 쉽게 알 수 있는 유용한 정보를 제공함을 지적하였다.

그러나 짧은 시간 중 다량의 경보가 발생하는 비상 사고 초기에는 연속적으로 새로운 경보가 발생함에 따라 Alarm Message List상의 정보를 읽을 시간적 여유가 없어 발전소 상태를 파악하는 데 어려움이 있었다.

이에 따라 현재의 경보 체계를 정상 운전과 비상 운전시 다르게 운영하는 것을 해결안으로 제시되었으며, 이와 관련된 평가 및 최종 결정은 건설 단계에서 수행될 예정이다.

전산화 절차서는 운전원이 발전소 상황을 이해하고 판단하는 데 유용하였다. 전산화 절차서 도입으로 비상 운전에 필요한 모든 정보가 개별적인 운전원 제어반에 제시, 공유하게 되어 기존 가동 중 원전 주제어실 운전원에 비해 충분히 여유를 가지고 상황 조치를 위한 직무 수행이 가능하였다.

또한 전산화 절차서 도입과 함께 제기되었던 운전간 대화 감소는 전술한 운전원간 정보 공유에 따른 대화의 불필요성에 기인한 것으로 - 즉 기존 가동중 원전의 경우 정보공유를 위해 필연적으로 요구되었던 대화가 감소한 것으로 - 평가 결과 운전 수행도에 직접적인 영향을 끼치지 않는 것으로 확인되었다.



APR1400 주제어실 구성

그러나 향후 건설 단계에서는 전산화 절차서 사용으로 기존과 달라진 운전원 역할 및 직무의 원활한 수행을 위해 멀티미디어(multimedia) 언어 전문가를 통한 절차서 문구(언어) 설계를 통한 정형화된 의사 소통 체계가 마련될 예정이다.

그래픽화된 정보를 제공하는 운전 제어반 정보 FPD는 제시된 정보를 이용한 운전원의 진단 직무와 제어를 위한 계획 수립에 적합하였다.

운전 제어반의 정보 FPD는 단시간(short-term)에 요구되는 제어기기 탐색 및 조작뿐만 아니라, 장시간(long-term) 동안 요구되는 중요 변수의 상태 감시 등에 대한 직무를 적절하게 지원하였다.

특히 정보 FPD에 제공되는 다양한 Trend Display는 비상 운전시 발전소 상태를 지속적으로 감시하는데, System Mimic Display는 특정 시스템 및 기기에 대한 상세한 정보를 파악하는 데 유용한 것으로 평가되었다.

또한 정보 FPD의 화면 구성 체계(hierarchy)는 화면 순항을 최소화한 설계 구현으로 운전원이 원하는 정보와 제어에 필요한 기기를 빠른 시간 내 찾을 수 있도록 체계적으로 구성되었음을 확인하였다.

이상과 같은 신형경수로1400 MMI의 인간 공학적 확인 및 검증은 현재 진행중인 건설 단계에서도 지속적으로 수행될 예정이다.

특히 건설 단계에서는 신형경수로 1400 계통 설계를 반영한 Full-scope Simulator 개발하여, 신형경수로 고유 절차서를 적용하고 운전원이 참여하는 확인 및 검증 수행하게 된다.

이러한 과정은 신형경수로1400 MMI 사용에 의한 운전 수행도를 향상시키고, 결국 전체 발전소의 안전성을 보장하는 데 크게 기여할 것이다.