

SMART MMIS를 위한 소프트웨어 개발

이철권, 장귀숙, 서용석, 박희윤, 구인수

한국원자력연구소

요 약

SMART 제어반 구현에 필수기기인 소프트웨어를 기존 제어입력장치 설계에 적용된 규제요건이나 설계지침을 만족하도록 개발한다. 그러나 이를 위해서는 현재 원자력 분야 MMIS 개발의 현안인 디지털 계측제어기술 적용과 인간공학적 설계절차 반영, 그리고 공통의 운전원 연계기기 사용에 따른 기기의 신뢰성확보와 기기의 단일고장 대처방안 마련 등이 해결하여야 할 핵심사항이다. 따라서 본 연구에서는 이러한 주요 현안을 검토, 분석하여 SMART 제어반의 소프트웨어의 개발개념을 설정하고 설계요건과 구조를 개발하였다.

1. 배경

MMIS 설계에 컴퓨터, 정보통신망 등과 같은 디지털기술의 사용이 일반화되고, 인간공학적인 설계요소를 고려한 운전원 연계기능의 강화가 필요한 시점에서, 앞으로의 운전원 제어반은 입석식의 대규모 형태가 아닌 소형의 착석식 제어반으로의 설계가 이루어지는 추세이다.¹⁾ 제어실의 운전원 제어반은 크게 운전정보 표시기와 플랜트 보호 및 운전을 위한 운전원 모듈과 각종 제어기기로 구성된다. 지금까지 입석식 대규모 제어반은 주로 정보표시 또는 제어기기를 아날로그 기기나 이를 모사한 디지털 기기를 사용하여 이들을 나열하여 운전원 연계를 절차서와 더불어 해결하였으나, 소형의 착석식 제어반은 디지털기기에 의한 집적된 정보로부터 제한된 공간에서 운전원 연계사항을 해결하여야 하는 어려움이 있다. 그간 전자기술의 발전으로 정보표시기 분야에서는 SMART(System-integrated Modular Advanced Reactor) MMIS 요건을 충족하기에 큰 어려움이 없을 정도로 다양한 기기의 개발이 있었지만, 제어기기 분야에서는 기술의 진척이 미진하였다. 비록 소형의 스위치류나 평판표시기를 이용한 제어기기가 산업계에 널리 사용되고는 있지만 이들은 재래식 제어기의 기본적인 설계개념에서 크게 벗어나지 못한 단순한 제어기기 교체수

준의 기술에 불과한 것으로 소형의 착석식 제어반설계에는 그 적용성이 의문시된다. 따라서 원자로와 같은 대규모 시설에서는 운전원의 작업능력을 벗어나는 수준의 다량의 제어변수가 존재함을 고려할 때 소형의 착석식 제어반설계를 위해서는 새로운 개념으로 설계된 제어기의 개발이 필수적이라 하겠다.

본 연구에서 개발되는 소프트웨어(Soft-controller)는 운전원의 제어행위를 컴퓨터 및 Non-hardwired 기기를 사용하여 소프트웨어적으로 수행하는 제어기를 의미하는 것으로, SMART를 안전하고 경제적으로 유지하기 위하여 모든 운전모드에 대하여 각종 기기나 공정을 정상상태로 운전할 수 있도록 제어스위치, 공정제어기, 운전원모듈, 보수 및 시험반의 제어수단을 제공한다.

2. 개발개념

SMART MMIS의 소프트웨어기는 제어반설계에 결정적인 요소로서 SMART에서 추구하는 정상운전시 1인 운전 목표를 달성하고 소형의 제어반 설계를 가능케한다. 디지털기술은 그간 일반 산업계와는 달리 원자력산업에서는 신뢰성 및 안전성에 따른 인허가 문제로 인하여 도입이 늦어지고 있었으나 디지털기술의 확대보급으로 이제는 보편화되고 있다. 그러나 디지털기술의 도입은 하드웨어 뿐만아니라 소프트웨어의 검증이 큰 문제점으로 대두되어 현재 이를 해결하기 위한 많은 노력이 규제기관과 연구기관에서 세계적으로 진행되고 있으며, 본 연구에서도 방안을 마련 중에 있다.²⁾ SMART 소프트웨어기는 현재 상용화된 디지털기술을 사용하되, 관련 인허가 사항을 만족하도록 신뢰성과 안전성, 운전성이 향상된 제어기로 개발하며, 추후 디지털기술 관련 인허가 사항의 확립이나 진보된 기술이 개발되면 이를 수용하여 설계변경할 것이다. 현재 설정한 소프트웨어기의 주요 개발개념은 다음과 같다.

- 특정 제어변수 전용의 제어기사용 및 Hardwired 형태의 스위치 사용은 제어반의 제한된 공간을 고려했을 때 최대한 배제되어야 하므로 제어기기의 형태에 구애받지 않는 제어기설계가 가능한 소프트웨어 구동 디지털기기를 사용한다.

- 소프트웨어기는 기기별 제어가 아닌 계통, 기능 단위의 제어기를 제공하여 소형 제어반 설계를 가능케한다. (그림 1)

- 보호 및 안전기기 제어기는 단일고장기준을 만족하도록 4-채널, 2-트레인 개념을 적용하여 중복성 및 독립성요건을 만족한다.^{3,4)}

- SMART 디지털기기 개발방법론에 입각한 설계를 수행하며, 원자력 산업에서 요구되는 기기 (하드웨어 및 소프트웨어) 검증요건을 만족한다.⁵⁾

- 제어기설계에 인간공학적 설계절차를 따르며, 인간공학 요소를 반영한다.⁶⁾

3. 설계요건

소프트제어기는 MMI 관점과 제어 및 보호시스템의 설계관점에서 동시에 고려되어 개발되어야 한다. 즉, 기능적인 측면에서 운전원의 운전성이 확보되어야 하며 동시에 제어 및 보호시스템에서 요구하는 안전성 및 성능 확보가 보장되어야만 한다. 본 연구에서는 앞서 언급한 개발개념과 일반 산업체에서의 소프트웨어 사용경험 분석, 제어기 설계지침, SMART MMIS의 제어 및 보호 시스템 요건을 근거로 아래와 같이 주요 설계요건을 정립하였다.

- 1) 안전성 확보 및 기능적인 측면에서의 요건으로는,
 - 단일고장에 의한 제어기능 상실이 발생하지 않도록 중복개념을 적용한다.
 - 독립성 요건(채널간 격리요건)을 만족하도록 R.G. 1.75의 규제요건을 따른다.
 - 인체 및 기기보호와 같은 자동제어기능 수행에 방해되지 않도록 한다. 즉, 주요 안전기능을 진행중인 자동제어기능을 침해하지 않도록 하며, 이에 관한 정보를 운전원에게 제공한다.
 - 제어기에서 수동모드 선택시 수동제어 허용조건에 따른 허용연동을 가지도록 한다.
 - 원자로의 운전모드에 따라 자동적으로 제어기의 제어모드가 전환되도록 한다.
- 2) 성능 및 신뢰성 확보를 위하여,
 - 안전시스템 설계요건을 만족하는 기기를 선정 또는 설계한다.
 - 하드웨어 요건 : 내환경 및 내진요건, 전자파장애 요건을 만족한다.
 - 소프트웨어 요건 : 안전등급 소프트웨어 기준을 만족할 수 있도록 설계 및 검증한다.
 - 공통모드고장에 대비한 소프트웨어 설계를 수행하며, 특히 공통의 연계 제어기기 사용에 따른 공통모드고장에 대비하여 기기의 신뢰성확보는 물론 다양성을 고려한 설계를 한다.
- 3) 제어정보 및 화면 구성은,
 - 기기/변수 단위의 제어기가 아닌 기능/직무분석 결과를 근거로 계통이나 기능 위주의 집 단화된 제어기를 제공하여 운전성을 개선한다.
 - 사용되는 제어기들의 종류를 최소화하며, 이들은 종류별로 쉽게 구별될 수 있게 한다.
 - 제어기에 표시되는 운전정보 만으로도 최소한의 제어수행이 가능하게 한다.
 - 제어기는 현재 수행중인 제어변수를 연속적으로 제공하며, 이에따른 시간지연이 발생치 않도록 한다.
 - 제어변수로의 접근을 용이하도록 설계하여 시간지연을 초래하지 않도록 한다.
 - 오조작에 의한 제어수행이 발생치 않도록 각종 버튼들의 설계에 인간공학적인 측면을 고려한다.
 - 제어기 화면은 다양한 형태로 표시되지만 제어실 내에서 일관성을 유지한다.

- 4) 제어기 운전 및 기타 고려사항으로는,
- 제어기의 조작절차는 표준화하여 운전원의 혼란을 최소화한다.
 - 동일변수 제어기에 대하여 중복제어 수행이 발생치 않도록 한다.

4. 소프트웨어 구조

SMART는 가능한 많은 수준의 제어자동화를 이루고 있으나 자동화에서 제외된 기기제어와 자동제어의 보조수단인 운전원에 의한 수동제어 수단으로서 제어반 상에 제어기를 설치한다. 그러나 원자로정지 등 안전기능 수행을 위한 시스템 수준의 제어스위치나 원격제어반으로의 제어절환스위치 등을 제외한 모든 기기제어 및 공정제어 기능을 모두 소프트웨어로 수행하게 된다. SMART MMIS 설계에서 제어기는 제어스위치나 공정제어기 기능상실시 또는 보호계통과 ESFAS 계통 및 관련기기 시험에 사용되는 안전등급의 운전원모듈, 개폐제어 방식으로 안전관련 기기의 제어 및 보호를 담당하는 안전등급의 제어스위치와 그 외 비안전관련 기기 및 공정제어를 담당하는 공정제어기로 이루어진다. 일반적으로 비안전등급의 제어기설계는 일반 플랜트에서 사용되는 제어기설계와 큰 차이는 없으나, 안전등급의 제어기설계는 원자력산업에서 적용되는 엄격한 안전등급의 기기에 관한 설계기준을 따라야 하므로 소프트웨어의 개발은 기본적으로 기존의 아날로그 제어기설계에서 요구되는 설계요건과 소프트웨어의 사용으로 추가로 요구되는 설계요건을 동시에 따라야 한다. 따라서 이러한 요건에 근거하여 SMART 소프트웨어 구조를 설정하였다. (그림 2, 3)

- 제어기는 정보표시계통과는 분리, 설계하여 상호간에 기기고장으로 인한 영향을 없애며,
- 단일고장에 대처하기 위하여 안전계통의 채널별로 제어기를 설치하여 중복개념을 유지하며,
- 안전채널 간 또는 안전채널과 비안전채널들 간에는 격리기사용 및 이격거리 유지로 채널의 독립성요건을 만족하며,
- 또한 소프트웨어를 사용에 따른 공통모드고장에 대비하여 개발중인 소프트웨어 개발방법 및 절차를 준수함으로써 기기의 안전성을 확보하고
- 공통연계 기기 사용에 따른 공통모드고장에 대비하여 이중화시스템의 도입으로 신뢰성을 제고하며, 이 결과를 고장모드영향분석이나 고장수목분석 등을 통하여 확인한다.

5. 결론

SMART MMIS 설계에서 소프트웨어기는 제어반 형상을 결정짓는 중요한 요소이다. 그러나 이를 개발하기 위해서는 체계적인 개발방법이 우선 정립되어야 하며, 제어기 설계시의 고려사항을 분석한 후 이들에 대한 해결방안이 마련되어야 한다. 분석결과 소프트웨어 개발을 위해서는

디지털기기의 사용에 따른 제어기의 안전성 및 신뢰성 확보가 우선 해결해야 할 현안으로 밝혀졌다. 그러나 현재 이들에 대한 규제요건을 충분히 만족시킬 수 있는 기술적인 방법이 마련되어 있지 못한 점을 고려하여 본 연구는 이들의 해결방안 마련에 역점을 두면서 개념을 개발하고, 이를 근거로 설계요건 및 구조를 개발하였다. 또한 원자력분야에서 사용경험이 없는 소프트웨어 개발을 위한 기술 및 규제요건 측면의 해결방법을 제시하였다.

【참고문헌】

1. EPRI URD Vol. III, Ch.10, "Man-Machine Interface Systems", 1990
2. SMART MMIS 설계개발, KAERI/RR-1706/96, Jul., 1997
3. IEEE-279, "Criteria for Protection Systems for NPGS"
4. IEEE-603, "Criteria for Safety Systems for NPGS"
5. IEEE-7.4.3.2, "Criteria for Digital Computers in Safety Systems of NPGS"
6. NUREG 0700, "Human-System Interface Design Review Guideline", Rev. 1, 1995 (Draft)

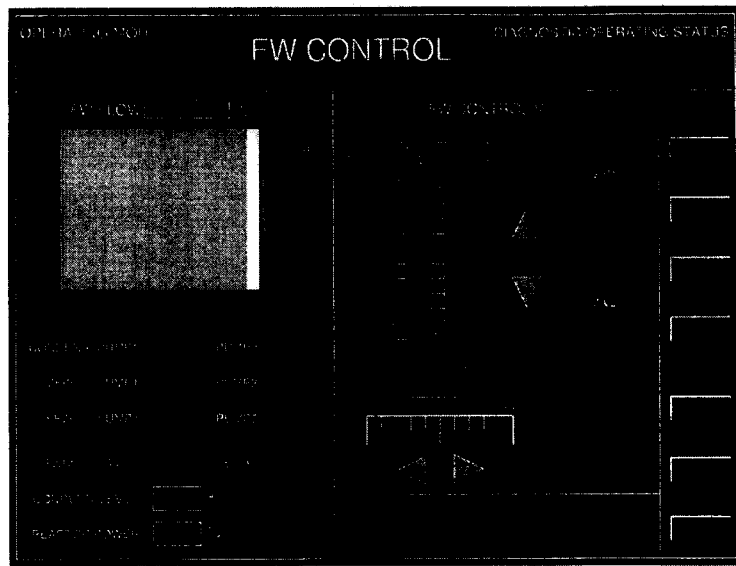


그림 1 소프트웨어기

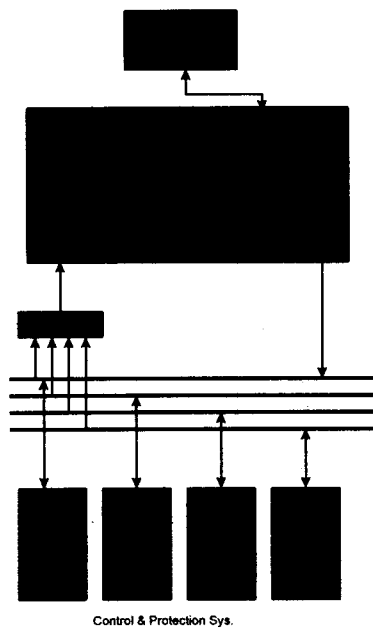


그림 2 안전등급(CH-A) 제어기구조

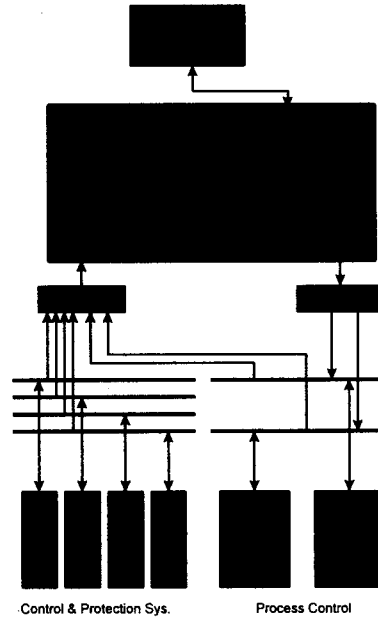


그림 3 공정제어용 제어기구조