'97 추계학술발표회 논문집
한국원자력학회

차세대원전 Safety Console 개념 설계

박현신, 이광대, 정학영
전력연구원
대전광역시 유성구 문지동 103-16

요 약

현재 개발이 진행중인 차세대원전의 MMIS 설계는 기존 원자력발전소와 달리 Compact Workstation 개념을 적용하고 있다. 그리고 차세대 원전 Compact Workstation의 설계 개념에 따르면, 안전 계통과 비안전 계통 모두를 동일한 제어기 (Soft Controller)로 제어하는 방식을 고려하고 있다. 따라서 Compact Workstation 고장시에 발전소를 안전하게 정지시키고 그 상태를 유지하기 위해서 Safety Console이 필요하며, 본 연구에서는 차세대원전의 MMIS 설계 개발의 일부로서 주제어실에 설치될 Safety Console을 설계하기 위하여, 우선적으로 Safety Console의 기능을 정의하고 안전 기기 제어 능력 그리고 디지탈 기기를 사용하는 데에 따른 공통모드고장 대처 방안을 평가하였다. 그 평가 결과로서 Safety Console에 대한 설계 기준 및 초기 설계 방향을 제안한다.

1. 서론

현재 개발이 진행중인 차세대원자로의 MMIS 설계는 기존 원자력발전소와 달리 Compact Workstation 개념을 적용하고 있다. 그리고 차세대 원전에서는 Compact Workstation을 적용하면서 안전 계통과 비안전 계통 모두를 동일한 제어기로 제어하는 방식을 고려하고 있으며 운전원의 운전 부담을 감소시킬 수 있도록 발전소 정보 및 경보계통을 개발하고 있다. 이러한 Compact Workstation으로의 설계/개발은 Compact Workstation 고장 시에 발전소를 안전하게 정지시키고 그 상태를 유지하기 위한 Backup 기능을 포함한 운전원 패널을 필요로 하고 있다. 본 연구에서는 새로운 운전원 패널의 필요성을 충족시키기 위한 방안으로 Safety Console을 제시한다. 본 논문에서는 차세대원전의 MMIS 설계 개발의 일부로서 주제어실에 설치될 Safety Console을 설계하기 위하여, 우선적으로 Safety Console의 기능을 정의하고 Safety Console이 가져야 할 안전 기기 제어 능력 그리고 디지탈 기기를 사용하는 데에 따른 공통모드고장 대처 방안을 평가하였다. 그리고 평가 결과로서 Safety Console에 대한 설계 기준 및 초기 설계 방향을 제안한다.

2. 본론

본 연구에서는 차세대원자로의 MMIS 설계 개발의 일부로서 주제어실에 설치될 Safety

Console 을 설계하기 위하여, 우선적으로 Safety Console의 기능을 정의하고 안전 기기 제어 능력 그리고 디지탈 기기를 사용하는 데에 따른 공통모드고장 대처 방안을 평가하였다. 그 평가 결과로서 Safety Console 에 대한 설계 기준 및 설계 방향을 제안한다.

2.1 Safety Console 기능 정의

Safety Console 은 IEEE Std.-603[1]에서 정의한 Class 1E 요건을 만족한다. 그리고 정상운전 중에 사용되는 Softcontrol의 고장을 포함한 설계기준사건 발생시 발전소를 안전하게 정지시키고 그 상태를 유지하는데 필요한 기기를 운전원이 제어할 수 있도록 기능을 제공한다. 이 기능과 관련하여 필요한 Fixed Position Controls, 경보 및 표시 기능을 제공한다. 그리고 Safety Console 은 평상시 사용되지 않는 Backup 패널이 되지 않고, 필요시 운전원이 쉽게 조작할 수 있도록 하기 위하여 발전소 정상 운전동안 주제어실에서 제어되는 모든 안전기기에 대한 주기적인 시험 및 보수유지에 필요한 경보, 표시기 및 제어 기능이 제공된다. Safety Console 은 EPRI URD Chapter 10[5]의 요건에 따라 발전소에 사건 발생시 세 번째 운전원을 수용한다. 그리고 정상상태에서 운전원이 사용하는 Workstation에 대해서 발전소의 안전성 및 이용률을 향상시킬 수 있도록 다양한 (Diverse) Workstation을 제공한다.

2.2 안전 기기를 위해 필요한 제어 능력

차세대원전 주제어실에 설치되어 정상 운전시에 주로 사용될 Workstation은 Class 1E 제어기를 포함하지 않는다. 따라서 설계기준사건시에 발전소를 안전하게 정지시키기 위해서는 필요한 Class 1E 기기를 제어할 수 있도록 주제어실내에 Class 1E 제어기가 제공되어야 한다. 이 제어기는 IEEE Std.-603의 Class 1E 요건을 만족하여야 한다.

Safety Console은 다음과 같은 사건시에 모든 안전 기능을 수행하는데 필요한 경보, 표시 및 제어 기능을 제공한다.

(1) 안전계통의 단일 고장을 포함한 N+1 사고시에 설계기준사건의 결과를 완화시킨다. 여기에서 N+1 사고는 설계 단계에서 고려되지 않은 사건을 의미한다. 예를 들어, Three Mile Island 사고는 안전해석에서 가정하지 않았던 사고였다. 발전소는 "N"개의 알고있는 사건, 즉 안전해석에서 정의된 사건에 대처할 수 있도록 설계된다. 그리고 이 경우에도 발전소 설계는 가정된 사건 외의 사건에 대처할 수 있도록 설계된다.

(2) 모든 비상운전절차 (Emergency Operating Guideline) 사건시에 필요한 기능을 제공한다. 비상운전절차는 원자로 트립 이후에 발전소 사건을 완화시키기 위한 모든 기능 및 직무를 정의하고, 운전원으로 하여금 설계기준사건에 대처할 수 있도록 지침을 제공한다. Safety Console은 EOG 에서 사용되거나 또는 EOG에는 정의되어 있지는 않지만 EOG 직무를 완결하는데 필요한 모든 Class 1E 제어기 및 품질보증된 (Qualified) 경보 및 표시기가 제공되어야 한다.

Safety Console은 "Fixed Position" 되어야 할 경보, 표시, 및 제어에 대한 Minimum Inventory를 제공한다. Minimum Inventory에 대한 요건은 새로운 개념을 가지는 발전소 설계, 즉, Nuplex 80+, ABWR, 및 AP600에 대해서 미국 NRC가 요구하는 사항으로, 차세대원전은 다음과 같이 미

국 NRC의 Minimum Inventory 요건을 만족한다.

(1) 비상운전절차 수행을 위한 경보 및 표시 기능을 제공할 수 있도록 필수 (Critical) 안전 기능 상태 표시를 위해 필요한 주요 변수, Preferred/Credited Success Path Performance 표시기, 발전소 안전 정지를 확인하는데 필요한 표시기 및 Regulatory Guide 1.97 Category 1 변수를 제공한다.[2]

(2) 비상운전절차 수행을 위한 제어 기능을 제공한다. 이러한 제어 기능은 Major Flow Path 상의 Preferred/Credited Success Path 기기와 발전소 안전 정지에 필요한 기기에 적용된다.

2.3 공통모드고장 (Common Mode Failure)

디지탈 계측제어계통은 소프트웨어 에러에 의한 공통모드고장에 취약하며, 이러한 공통고장은 하드웨어 구조에 의한 다중성 (Redundancy)를 무력화시킬 수 있다. 그리고 디지탈 계측제어계통에 대한 미국 NRC의 주요 고려 사항은 동일 소프트웨어를 사용하는 계통 또는 채널에 공통모드 고장이 발생할 가능성이 없다는 것을 증명하기가 어렵다는 것이다. 이에 따라 미국 NRC는 디지탈 계측제어계통에 대해서 Defense in Depth and Diversity (D-in-D&D) 평가를 수행할 것을 요구하고 있다[3]. 차세대원전에서는 다음과 같은 두 가지 상황의 공통모드고장이 고려된다.

(1) 안전계통 소프트웨어의 공통모드고장

안전계통 (발전소보호계통 및 공학적안전설비계통) 에 공통모드고장이 발생하는 경우 발전소를 안전하게 정지시킬 수 있도록 비안전계통의 제어기능을 사용한다. 이 경우 운전원은 Workstation 상의 제어기를 이용하여 비안전 기기를 제어하고 다양성보호계통 (Alternate Protection System) 이 사용된다. 그리고 다양한 수동 공학적안전설비 작동 기능이 사용된다.

(2) Workstation 제어기 고장

차세대원전에서는 Non Class 1E로 정의된 제어기 (Softcontroller)를 통하여 안전계통 및 비안전계통 모두를 제어한다. 따라서 동일한 소프트웨어를 사용하는 제어기에 고장이 발생하는 경우 운전원은 Normal Workstation 에서 안전계통과 비안전계통 모두 제어할 수 없게된다. 이러한 경우 발전소를 안전하게 정지시킬 수 있도록 Safety Console에 품질보증된 (Qualified) 계통 레벨의 동작 기능과 표시기 그리고 기기 제어기가 제공된다.

2.4 Safety Console 설계 기준

앞에서 살펴본 바와 같이, 본 연구에서는 차세대원자로의 MMIS 설계 개발의 일부로서 주제어실에 설치될 Safety Console에 대해서 Safety Console의 기능을 정의하고 제공되어야 할 안전 기기 제어 능력 그리고 디지탈 기기를 사용하는 데에 따른 공통모드고장 대처 방안을 평가하였다. 그 평가 결과로서 Safety Console에 대한 설계 기준을 다음과 같이 정립하였다.

(1) Safety Console에서 안전 기능을 수행하는 제어기는 IEEE Std.-603 의 Class 1E 요건을 만족한다.

(2) Safety Console은 설계기준사건 발생시 또는 그 이후에 모든 Class 1E 기기를 운전하는데 필요한 Class 1E 제어기와 품질보증된 경보 및 표시가 제공한다.

(3) Safety Console은 설계기준사건 N+1, 비상운전절차 사건, 그리고 발전소 안전 정지시에 안전

기능을 수행하는데 필요한 Class 1E 제어기 및 품질보증된 경보 및 표시가 제공된다.

(4) Safety Console은 Preferred/Credited Success Path 기기, 안전 정지를 수행하는데 필요한 기기 그리고 발전소신뢰도평가를 통해 결정된 상위 10가지의 필수 직무를 수행하는데 필요한 기기를 제어하기 위하여 "Fixed Position"의 Minimum Inventory를 제공한다.

(5) 주제어실에 설치될 Large Display Panel은 Safety Console에서 볼 수 있어야 한다.

(6) Safety Console은 주제어실에서 제어되는 모든 안전 기기의 주기 점검, 시험 및 보수유지를 수행하는데 필요한 모든 경보, 표시 및 제어 기능을 제공한다.

(7) EPRI URD 10장의 요건에 따라 발전소 트립 이후에 세 번째 운전원을 수용할 수 있는 제어반을 제공한다.

2.5 *Safety Console* 초기 설계

본 연구에서는 차세대원자로의 MMIS 설계 개발의 일부로서 주제어실에 설치될 Safety Console에 대해서 설계 기준을 제시하였고 이에 따른 초기 설계 방안을 다음과 같이 제시한다.

(1) Safety Console은 안전 기기를 제어하기 위한 Class 1E 제어 기능을 제공한다. 이와 관련하여 Fixed position의 Minimum inventory 제어를 위한 누름 스위치가 제공되어야 하며, 공학적안전설비 계통 레벨 동작과 다양한 수동 공학적안전설비 작동을 위해 설정된 Hardwired 스위치가 제공되어야 한다. 그리고 설계기준사건을 만족하기 위해서 필요한 모든 제어 운전을 제공할 수 있도록 각 채널별로 독립적인 운전원 모듈이 제공되어야 한다. 이 운전원 모듈은 안전 기기의 점검, 시험 및 보수유지를 위한 제어 및 표시 기능을 포함한다.

(2) Safety Console은 안전 계통을 감시할 수 있는 기능을 제공한다. 이와 관련하여 필요한 N-채널 안전표시및경보계통 (Safety Indication and Alarm System) 표시기가 제공되어야 한다.

(3) Safety Console은 Regulatory Guide 1.97 Category 1 변수를 표시하는 기능을 제공한다. 이와 관련하여 PAMI (Post Accident Monitoring Indication) Category 1 변수를 위한 P-채널 안전표시및경보계통 (SIAS) 표시기가 제공되어야 한다.

(4) Safety Console은 EPRI URD 10장의 요건에 따라 세 번째 운전원을 수용할 수 있도록 주제실 내에 위치하여야 하며 패널 구성이 이루어져야 한다. 이와 관련하여 Safety Console은 대형정보표시판 (Large Display Panel)을 볼 수 있는 위치에 있어야하며 주제어실 Supervisor 와 Workstation에 있는 운전원과 쉽게 대화할 수 있는 위치에 설치되어야 한다. 그리고 주제어실 내의 다른 운전원이 대형정보표시판을 보는데 방해되지 않아야 한다.

(5) Safety Console은 안전 및 비안전 계통을 감시하는데 사용될 수 있도록 정보처리계통 (Information Processing System) 표시기를 제공하여야 한다.

그림 1 및 2 는 각각 주제어실에서 Safety Console의 위치와 Safety Console 구성을 간략히 나타낸 것이다.

3. 결론

현재 개발이 진행중인 차세대원전의 MMIS 설계는 기존 원자력발전소와 달리 Compact

Workstation 개념 적용을 목표로 하고 있다. 그리고 차세대 원전에서는 Compact Workstation을 적용하면서 안전 계통과 비안전 계통 모두를 동일한 제어기로 제어하는 방식을 고려하고 있다. 따라서 Workstation 고장시에 발전소를 안전하게 정지시키고 그 상태를 유지하기 위해서 Safety Console이 필요하며, 본 연구에서는 차세대원전의 MMIS 설계 개발의 일부로서 주제어실에 설치될 Safety Console을 설계하기 위하여, 우선적으로 Safety Console의 기능을 정의하고 안전 기기 제어 능력 그리고 디지탈 기기를 사용하는 데에 따른 공통모드고장 대처 방안을 평가하였다. 그리고 평가 결과로서 Safety Console에 대한 설계 기준 및 설계 방향을 초기 설계 방향을 제안하였다.

본 연구에서 제시한 Safety Console의 설계 개념은 앞으로 차세대원자로 (II) 단계 설계 개발 과정을 통하여 그 규모 및 기능에 대한 보다 깊이 있는 검토가 진행될 것이며, 그 결과로서 보다 확실한 Safety Console의 설계가 이루어질 것으로 기대된다.

4. 참고 문헌

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

[2] Reg. Guide 1.97, Instrumentation for Light Water Cooled Nuclear Power plants to Assess Plant Conditions During and Following an Accident

[3] Branch Technical Position HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer Based I&C Systems

[4] CE Standard Safety Analysis Report Design Certificate (CESSAR DC) Ch. 18

[5] EPRI Utility Requirement Document Ch. 10 Man-Machine Interface System

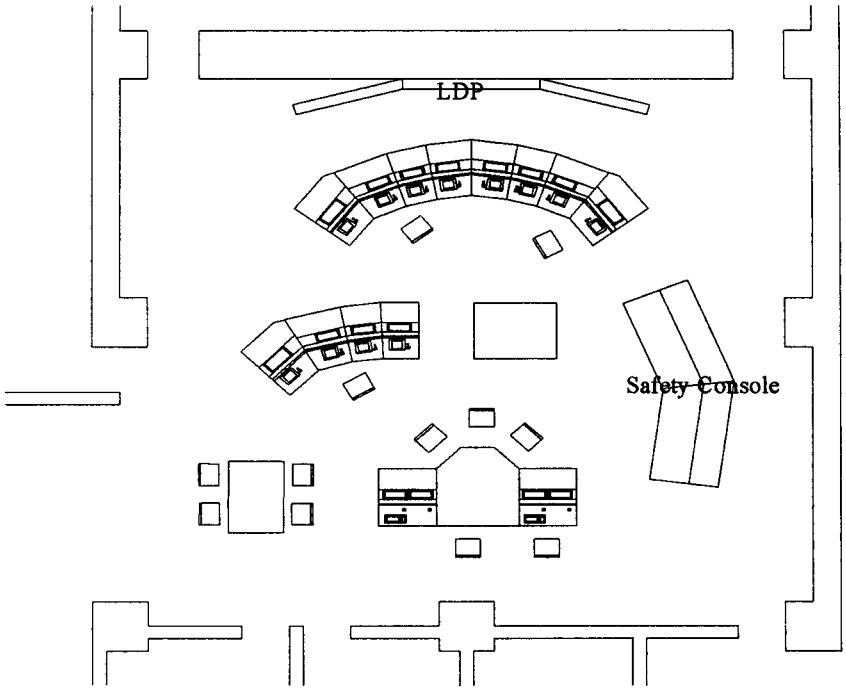

그림 1. Control Room Layout

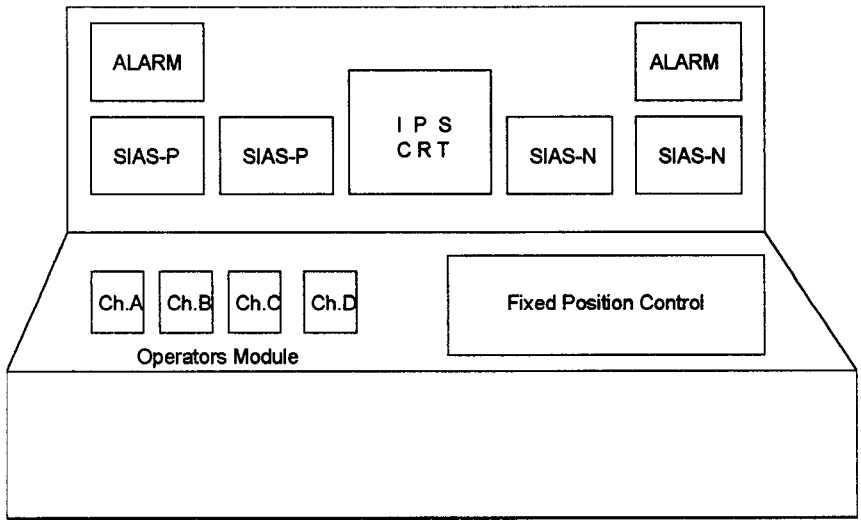

그림 2. Safety Console Layout