논문 2012-49-9-31

신형원전(APR+)을 위한 범용소프트제어기의 내고장성 설계

(Fault Tolerant Design of Universal Soft Controller for Advanced Power Reactor)

예 송 해*, 유 준 **

(Song-Hae Ye and Joon Lyou)

요 약

최근 범용소프트제어기 설계는 원자력발전소의 첨단주제어실에 적용되고 있다. 범용소프트제어기는 고집적 주제어실에서 비안전 기기뿐만이 아니라 안전기기를 제어할 수 있는 소프트웨어 기반의 수동제어 수단이다. 따라서 범용소프트제어기는 신형 주제어실의 단일 워크스테이션 구현을 위한 필수적인 설계특성을 갖고 있다. 전통적인 주제어실은 컴퓨터 기반으로 하는 통합 운전원 인터페이스 체계로 대체되고 있다. 범용소프트제어기의 오작동신호 발생 가능성을 줄이기 위해 어떠한 기기의 조작을 위해서는 2단계의 구분된 운전원 조작을 요구하는 설계를 고려하였다. 범용소프트제어기 오작동 가능성은 매우 낮기 때문에 범용소프트제어기 그자체로 발전소의 트립 가능성을 증가시키지는 않는다. 범용소프트제어기는 원자력발전소의 계측제어분야/인간연계 분야의 혁신을 대표한다. 범용소프트제어기는 인간연계를 기반으로 하는 단일 표시장치에 다양한 디비젼의 제어와 표시기를 통합하고 있다. 범용소프트제어기의 고장으로부터 안전기능 수행의 영향을 막기 위해 안전기기 및 기능에는 공학적 안전설비 신호가 적용된다. 또한 안전등급 수동스위치는 범용소프트제어기의 신호보다 우선한다. 그러므로 범용소프트제어기의 오작동 신호는 안전관련 스위치로부터의 제어신호에 의해 차단되어질 수 있다.

Abstract

Recently, design of Universal Soft Controller(USC) has been applied to the advanced control room for nuclear power plant. USC is software-based manual control means to control safety components as well as non-safety components in the highly-integrated control room. Therefore, design feature of USC is essential for the implementation of a single workstation in the advanced control room. The traditional control room is replaced by computer-driven consolidated operator interfaces. Considering our design has further reduced the probability of USC spurious signals by requiring two distinct operator control actions to generate any control signal. The reality of USC does not increase the probability of reactor trip because the probability of spurious USC signal is negligible. Universal Soft Control represents a significant evolution in nuclear I&C/HSI System. USC integrates the indicators and controls from multiple divisions into a single integrated visual display unit(VDU) based HSI(Human System Interface). In order to prevent adverse influence on safety function performance from USC failure, ESFAS signals are applied to safety components or functions. In addition, safety manual switches have priority over USC's signals. Therefore, spurious USC signals can be momentarily blocked by selecting a soft control command from the safety VDU.

Keywords: Advanced Power Reactor+, Universal Soft Controller, Man Machine Interface System, Human System Interface, Highly-Integrated Control Room

* 정회원, 한수원(주) 중앙연구원
(KHNP CRI)
** 평생회원-교신저자, 충남대학교 전자공학과
(Dept. of Electronics Engineering, Chungnam National University)
※ 본 연구는 지식경제부에서 시행한 지식경제 기술혁신사업의 기술개발 결과임
접수일자: 2011년11월17일, 수정완료일: 2012년8월27일

Ⅰ. 서 론

현재 국내에서 개발 중인 신형원전(APR+)은 기존 발전소와 달리 주제어실내 각 운전원에게 제공되는 운전원 콘솔에 안전계통과 비안전계통의 기기 및 공정을 동시에 제어 할 수 있는 범용소프트제어기(Universal Soft Controller)의 최초 적용을 추진중에 있다. 일반적으로 소형 워크스테이션 기반의 원자력발전소 첨단 주제어실은 정보, 제어, 및 운전원 지원기능이 통합되어 있어 안전계통을 포함한 모든 계통의 운전이 한 개의 워크스테이션에서 동일한 제어방식으로 수행된다.

해외 경쟁노형인 프랑스의 N4원전, AREVA사의 EPR, 미국 웨스팅하우스사의 AP-1000 및 일본 미쓰비시의 APWR 등 해외 경쟁로형들은 일반 산업계의 디지털 제어설비 기반의 신기술 적용을 위한 활동과 규제기관의 신규 규제입장을 반영하여 운전편의성을 향상시킨 범용소프트제어기를 주제어실 내 운전원의 제어수단으로 적용하고 있다.

국내에서는 처음으로 APR1400(신고리 3,4호기)에서 워크스테이션 기반의 운전원 콘솔에 정상운전을 위한 수동제어수단으로 소프트제어기를 적용함으로써 기존 OPR1000(한국표준형 원전) 제어콘솔의 크기를 획기적으로 감소시켰다. 그러나 APR1400 소프트제어기는 안전급 소프트제어기 (ESF-CCS Soft Control Module, ESCM)와 비안전급 소프트제어기 (Information FPD)로 분리되게 설계됨으로써 계통 안전성 및 통신 독립성을 높이고 있음에도 불구하고 해외경쟁노형이 채택하고 있는 범용 소프트제어기에서의 운전편의성 및 설계 단순화 측면에서 개선이 요구된다[1].

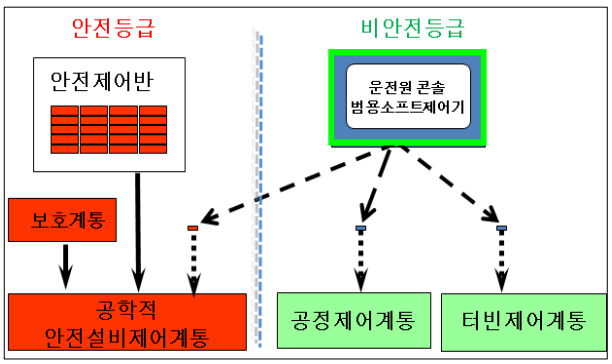

그림 1. 범용소프트제어기 개념도
Fig. 1. A conceptual diagram of Universal Soft Controller.

국내 신형원전(APR+)을 위한 범용소프트제어기는 최근 미국 NRC가 제시한 첨단 주제어실의 통신독립성 현안에 대한 규제요건(ISG-04)을 만족하도록 설계하였으며 범용소프트제어기의 고장이 발전소 안전기능에 영향을 주지 않는 설계특성을 갖도록 하였다(그림 1 참조).

범용소프트제어기의 오조작 발생확률을 낮추기 위해 강화된 품질등급을 적용하여 소프트웨어를 개발하고 운전원 2단계 조작개념을 설계에 적용하였다. 또한 범용소프트제어기 운전개념에도 기기일시확인(Command Temporary Enable, CTE) 스위치 개념을 적용함으로써 어느 경우에도 안전성분석보고서(SAR) 15장에서 고려하고 있는 사고들의 범주를 벗어날 수 없으며, 다중 오류에 대한 거짓신호 전송은 발생 가능한 사고로 고려되지 않는다. 따라서 신형원전에서의 범용소프트제어기 적용은 기존 원전이 갖고 있는 소프트제어기의 안전급과 비안전급으로 구분되는 소프트제어기의 비효율적인 운전성을 개선하고 가용성을 향상할 수 있으며, 원전 인간 기계 연계계통(MMIS, Man Machine Interface System)의 설계 단순화, 설비비용 감소, 운전원의 2차 직무 감소, 운전원 콘솔 크기감소, 유지보수 업무 감소 등의 개선효과를 기대할 수 있다.

Ⅱ. 범용소프트제어기 설계목표 및 구현

1. 설계목표

신형원전(APR+)은 가용성이 향상되고 규제요건을 만족시키는 비안전급 범용소프트제어기를 안전계통 및 비안전계통 기기제어에 적용한다. 범용소프트제어기 고장에 의한 안전계통 기기 오동작의 발생 가능성이 없도록 충분한 설계특성을 반영하였다. 이를 구현하기 위한 설계목표는 다음과 같다.

- 발전소 정상운전 시 범용 소프트제어기를 통한 안전계통 제어기기 및 비안전계통 제어기기를 통합제어한다.
- 발전소 사고 시에 운전원 콘솔이 가용할 경우 범용소프트제어기를 포함한 운전원 콘솔을 이용한 발전소 과도상태 대처를 위한 운전개념을 적용한다.
- 운전원 콘솔이 가용하지 않을 경우 안전급 수동제어수단을 통해 발전소를 안전 정지시키고 안전 상태로 유지시킬 수 있는 후비제어수단을 주제어실

안전제어반에 제공한다.

- 규제요건을 만족하는 안전계통과 비안전계통 간의 연계신호에 대한 독립성을 만족한다.
- 최신 관련규제요건 및 지침이 반영된 인간-기계 연계계통(Man-Machine Interface System, MMIS) 설계한다.
- 인간공학 요건에 따라 운전원의 운전부하를 경감시키고, 운전편의성을 향상시킨 운전원 콘솔을 설계한다.
- 범용소프트제어기 고장으로 인한 안전등급 기기 오동작 발생가능성을 최소화한다.
- 다양성 및 심층방어(Diversity and Defense-In-Depth: D3)를 고려한 설계를 한다[2, 6].

2. 범용소프트제어기 설계

하나의 운전원 콘솔은 네 개의 화면으로 구성되며 정보처리계통(IPS) 비안전 네트워크인 DCN-I 네트워크와 연결되어 있다. 만일 운전원이 정보화면상에서 하나의 기기를 선택하면 분리된 템플릿에 범용소프트제어기 제어템플릿이 보여진다. 그리고 제어템플릿상의 제어명령을 선택하면 제어메시지 건전성을 확인하여 명령 확인 스위치(CTE)를 작동할 때만 제어명령이 전달되게 된다. 운전원 제어명령은 기기선택정보와 명령선택정보의 검증을 통해 CDG로 전송된다. 범용소프트제어기 제어명령은 가장 낮은 우선순위를 가진다. 그러므로 만일 발전소 안전기능 보장을 위한 보호계통 자동동작 신호 및 운전원 개입에 의한 안전등급 수동조작 스위치의 신호가 발생한다면 범용소프트제어기 신호는 차단되고 이러한 안전 신호들에 의도된 안전기능을 수행한다(그림 2 참조).

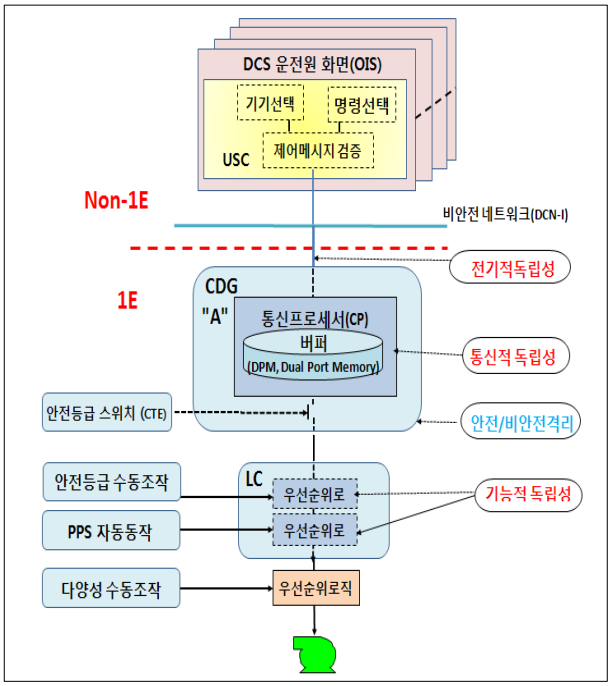

그림 2. 범용소프트제어기 구성도
Fig. 2. The overview of USC.

가. 안전계통 사이의 독립성

안전기능 동작시 범용소프트제어기로 인해 안전기능이 저해되지 않도록 물리적/전기적/통신적/기능적 독리성 요건을 적용하였다[3~5].

(1) 물리적 격리

공학적 안전설비계통(Engineered Safety Facility-Component Control System, ESF-CCS)를 포함하는 안전기기와 USC는 IEEE Std.384 요건을 만족하는 물리적 격리를 제공한다. 광케이블과 물리적 격리된 장소에 기기를 위치시킨다.

(2) 통신적 격리

USC와의 통신을 위한 각각의 제어디비젼케이트웨이(CDG)는 제어(기능)프로세서로부터의 통신연계 격리를 담당하는 DPM(Dual Ported Memory)과 통신 프로세서를 갖고 있다. 또한 USC와의 메시지 교환 기능은 프로세서와 독립적이며 비동기적으로 이루어지며 USC와의 통신이 안전계통내에서의 안전기능 수행에 나쁜 영향을 주지 않는다. 듀얼 포트메모리는 두 개의 CPU가 같은 메모리에 읽기와 쓰기를 독립적으로 수행한다. 또한 듀얼 포트 메모리는 (기능) 프로세서가 통신프로세서보다 우선한 방법으로 메모리에 접근하도록 한다.

이를 위해 통신모듈은 중재로직을 갖고 있으며 듀얼 포트 메모리의 일부분으로 구성된다. 듀얼 포트 메모리의 높은 순위 포트에서는 우선적으로 제어(기능) 프로세서가 할당되며 기능 프로세서가 이러한 포트를 이용한 접근을 시도하면 중재로직은 통신프로세서를 낮은 순의 포트에 연결되는 통신프로세서의 접근을 막는다.

즉 통신프로세서가 듀얼포트 접근이 차단되면 정해진 시간동안 접근이 허용될 때까지 대기하게 되며 정해진 시간동안의 통신이 이루어지지 않게 되면 알람을 발생한다.

(3) 기능적 격리

USC 제어신호들이 안전기기를 제어하기 위해서는 대상기기별로의 전용 우선순위 로직을 통해서만 제어되어져야 한다. USC 제어신호는 안전등급 수동제어기(MI 스위치 혹은 ESCM) 신호와 같이 제어로직으로 전달되며 안전등급 수동제어기 제어명령이 우선순위가 높다[1].

USC 신호는 우선순위가 가장 낮으며 최소재고스위치(MI) 스위치와 안전등급 수동조작신호(ESCM) 신호가 수신될 때는 USC 신호는 이러한 신호에 의해 차단되어지며 제어로직에서 실행되지 않는다.(MI 스위치와 ESCM 신호가 동작되어질 때 USC의 반대 신호는 이러한 신호에 의해 비활성화 된다.) 즉 MI 스위치와 ESCM의 Start/Open 신호는 USC Stop/Close 신호를 차단한다. 그러므로 운전원 MI 스위치 혹은 ESCM을 통해 안전기능을 수행할 때 USC 신호는 우선순위 로직에 의해 차단되기 때문에 안전기능에 나쁜 영향을 주지 않는다. 또한 자동제어명령(ESFAS) 신호가 동작될 때 USC 신호는 차단된다. 자동제어명령(ESFAS) 발생되면 모든 운전 제어신호(USC, MI 스위치, ESCM 신호)에 의해 차단된다. 그러므로 오작동 USC 신호은 ESAFS 기능에 영향을 주지 않는다[1]. (그림 3 참조)

우선순위 로직 기능은 입증 및 확인이 되어야 하며 공학 안전설비계통(ESF-CCS) Loop 제어기와 기기연계모듈(CIM) 상에서 다양하게 구현된다. 다양성 모듈 상에서는 소프트웨어가 아닌 CPLD로 구현되며 소프트웨어에 의한 공통모드고장에 영향을 받지 않는다. USC와 안전등급 수동제어기(MI 스위치와 ESCM) 사이에서의 우선순위 로직은 ESF-CCS 루프제어기에 구현된다.

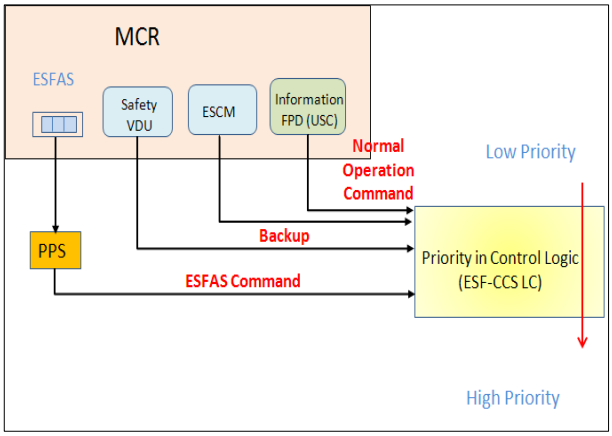

그림 3. 수동제어기기 우선순위
Fig. 3. The priority of manual controllers.

ESFAS 신호는 보호계통(PPS)에서 개시되며 ESF-CCS 그룹제어기에 의해 기동되며 USC로부터의 어떠한 기기제어신호보다 항상 우선권을 가져야 한다.

USC 신호는 기기제어로직에서의 많은 입력신호 중 하나로 처리된다. 또한 ESF-CCS에서 우선순위로직을 포함한 안전관련 소프트웨어는 운전중 변경이 되면 안된다. 소프트웨어 변경방지 설계특성은 어떠한 USC 신호(유효 및 에러 호함) 때문에 잘못된 소프트웨어 변경을 할 수 없게 한다.

우선순위 로직 소프트웨어 혹은 안전기능 소프트웨어는 잘못된 신호에 의해 변경되거나 손상되면 안되며 그것의 건정성은 유지되어야 한다. 따라서 다음과 같은 방법들이 고려되어져야 한다. ESF-CCS 루프제어기의 소프트웨어를 변경하기 위해서는 랙으로부터 물리적으로 분리하여 소프트웨어 변경이 가능하다. 즉 ESFAS-CCS 소프트웨어의 기능은 별도의 기기에 갖춰진 프로세서에 의해 새롭게 수정 변경 로딩하여 랙에 장착한다.

나. 범용소프트제어기 신뢰성 강화

(1) 제어메시지 검증기능

범용소프트제어기는 기기선택기능, 명령선택 기능 및 제어메시지 생성 기능으로 구성되며 각 기능은 독립된 프로그램으로 구현된다. 제어메시지 생성은 기기선택 기능과 명령선택 기능으로부터 제공된 정보를 이용하여 제어메시지를 생성한다. 운전원 운전화면에서 운전원이 기기를 선택하면 기기선택 정보인 기기ID, 채널주소,

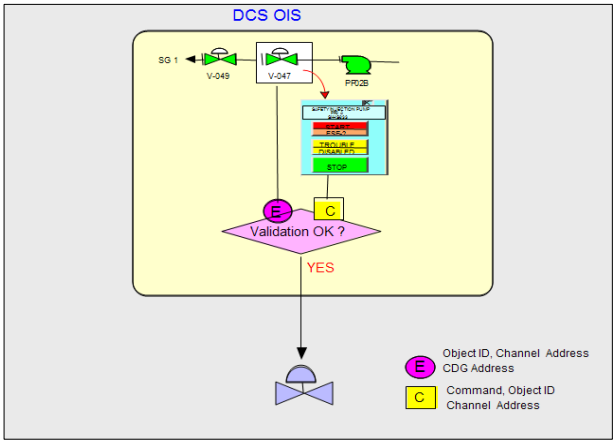

그림 4. 범용소프트제어기 2단계 운전
Fig. 4. Two distinct operation of USC,

ESF-CCS 루프제어기 주소가 검증프로그램으로 전송된다. 다음으로 운전원이 제어명령(Open/Start or Close/Stop)을 선택하면 명령정보인 기기ID, 제어명령이 검증프로그램으로 전송된다. 전송된 두 개의 정보는 검증프로그램에서 메시지의 건전성을 확인하여 ESF-CCS 루프제어기로 전송한다(그림 4 참조)

건전성 확인은 다음과 같이 수행한다.

- 기기정보의 기기ID와 제어명령의 기기ID는 일치하는가?
- 기기정보와 제어명령의 최신 제어명령은 일치하는가?
- 통신에러는 발견되지 않았는가?

범용소프트제어기를 하나의 프로그램으로 구현하는 것보다 각각의 별도의 독립된 프로그램(기기선택, 명령선택, 검증)으로 구현하는 것은 범용소프트제어기 의사작동(Spurious Actuation) 발생확률을 낮출 수 있는 중요한 기술이다.

(2) 발전소 사고해석 범주 확인

범용소프트제어기는 기기선택과 제어명령 선택 후에 기기확인(CTE, Command Temporary Enable) 스위치를 작동할 때만 범용소프트제어기와 CDG를 연결하여 한 개의 제어신호만을 전송하게 된다. 그러므로 범용소프트제어기의 고장으로 인한 잘못된 신호는 근본적으로 안전등급 스위치가 평소 막고 있기 때문에 새로운 유형의 사고는 유발하지 않는다. 또한 범용소프트제어기의 다중 오류에 대한 거짓신호 전송은 발생 가능한 것으로 고려되지 않는다. 그러므로 한 개의 범용소프트제어기 제어신호 전송은 한 개의 제어기기에만 영향을 주게 되며, 이는 어느 경우에도 안전성분석보고서(SAR 15장)에서 고려하고 있는 사고들의 범주를 벗어날 수 없다.

(3) 통신망 오류 검사

신뢰성 있는 통신망 구현을 위해 발생 가능한 오류를 감시하고 이를 대처할 수 있는 플랫폼 차원의 각종 자가진단 기능 및 계통 차원에서의 수단을 제공한다. 제어프로토콜에서는 비트 오류로 인한 잘못된 제어 가능성을 제거하고 아래와 같은 기존 원전에 적용하는 안전등급 플랫폼의 자가진단 기능을 적용한다.

- 워치독 타이머를 이용한 마이크로프로세서 고장
- 코드, 상수, 변수영역에 대한 내부메모리 건전성 진단
- CRC-16 방법에 의한 송수신 데이터 건전성 진단
- 수신선로 단선 진단
- 통신 드라이버 오류

(4) 안전급 수동제어수단 및 감시수단 제공

신형원전 주제어실은 정상운전 시 발전소 저온정지(Cold Shutdown)까지 달성할 수 있는 안전급 제어수단과, 발전소 사고 상황에서 고온정지 (Hot Shutdown)를 달성할 수 있는 충분한 안전급 제어수단을 제공한다. 즉, 수동제어수단(1E 등급) 만으로 발전소를 안전정지시키고 이 상태를 유지할 수 있도록 주제어실내의 안전제어반을 다음과 같이 설계한다.

- 안전제어반에 운전원 콘솔과 다양성 및 독립성을 갖는 고정형 최소재고스위치 (Minimum Inventory Switch, MI Switch)를 제공하여 다음을 수행한다.
  - 선호되는 경로를 통한 발전소 안전정지 및 안전상태 유지
  - 안전계통을 이용한 비상운전절차
- 발전소 안전상태 및 과도상태 분석결과 요구되는 운전원 조치를 위한 수동제어수단을 안전급으로 제공한다.
  - 각 채널별로 채널전용의 ESCM을 안전급으로 설계하여 제공한다.
- 디지털 설비로 구현된 발전소 보호계통 (PPS)과 공학적안전설비계통(ESF-CCS)의 공통모드고장 시 필수안전기능 수행을 위한 계통수준의 다양성 수동작동스위치 (Diverse Manual Actuation Switch, DMA Switch)를 제공한다.
- R.G. 1.97에서 요구하는 사고 후 감시변수를 표시하는 표시장치를 제공한다.
  - R.G. 1.97에 따른 사고 후 감시변수를 표시하기 위해 채널 A와 B에 전용의 표시장치 QIAS-P FPD 및 안전급 서버를 설치한다. 운전원이 범용소프트제어기를 이용하여 ESF기기를 제어하는 경우 ESF 기기의 상태(예: Open, Close, Start, Stop) 신호는 아래의 경로를 통해 기기상태 정보를 모니터링 한다.(그림 5 참조)

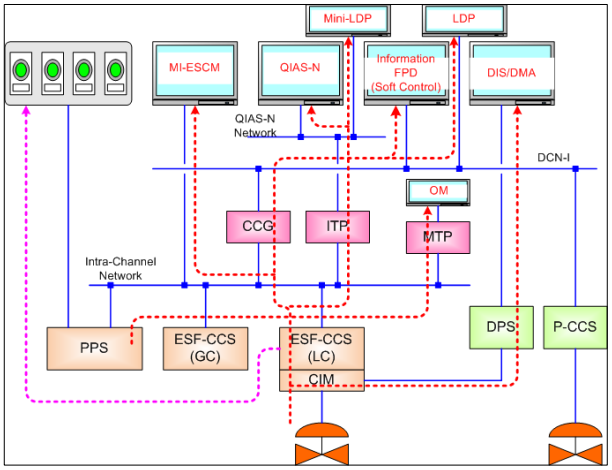

그림 5. 기기상태 모니터링 경로
Fig. 5. The monitoring route for status of components.

✓ 운전화면 (System Mimic 화면) 및 LDP:
ESF 기기 센서 ➔ ESF-CCS LC ➔ Intra-Channel Network ➔ CCG ➔ DCN-I ➔ Information FPD / LDP
✓ 범용소프트제어기 (제어판 스위치 램프):
ESF 기기 센서 ➔ ESF-CCS LC ➔ Intra-Channel Network ➔ CCG ➔ DCN-I ➔ Information FPD
✓ QIAS-N FPD (System Mimic 화면) 및 Mini-LDP:
ESF 기기 센서 ➔ ESF-CCS LC ➔ Intra-Channel Network ➔ ITP ➔ QIAS-N Network ➔ QIAS-N FPD / Mini-LDP
✓ MI-ESCM (제어판 스위치 램프):
ESF 기기 센서 ➔ ESF-CCS LC ➔ Intra-Channel Network ➔ MI-ESCM
✓ DMA/DIS FPD (System Mimic 화면):
ESF 기기 센서 ➔ CIM ➔ DPS Cabinet ➔ DMA/DIS FPD

- 안전제어반에 제공되는 안전급 수동제어수단 및 표시장치는 운전원 콘솔과 충분한 다양성과 독립성이 확보되도록 설계한다.
  - 실배선 스위치 또는 운전원 콘솔과 다른 하드웨어 및 소프트웨어 적용
  - 운전원 콘솔과 전기적 물리적 격리
- 계통수준의 DMA 스위치를 ESF-CCS 루프제어기 하단의 우선회로모듈 (CIM)에 실배선으로 연결하여 최우선으로 작동되게 하여 PPS 및 ESF-CCS 공통유형고장 발생 시 필수안전기능 수행이 보장되게 한다.
  - 기기연계 모듈(CIM)은 PPS 및 ESF-CCS와 다양성을 갖는 하드웨어(CMOS)로 구현하며, 100% 시험 가능하게 한다.
  - CIM 모듈은 안전급으로 설계, 시험, 제작한다.
- 안전제어반의 MI 스위치와 ESCM은 발전소 전 범위 운전모드에서 항상 활성화되게 한다.

(5) 강화된 품질프로그램

범용소프트제어기는 비안전 등급이지만 강화된 품질프로그램 적용을 통해 내진 및 내환경 조건에서 USC 기능을 하는 소프트웨어가 동작을 하여야 하며 지진 등급은 카테고리 2를 만족하여야 한다. 강화된 품질 보증 프로그램은 기기설계와 제작에서 의도된 기능이 보장되어야 하며 기기 전체생명주기 동안의 유지보수와 수리 대체 및 설계변경에 기여하여야 한다.

Ⅲ. 범용소프트제어기 내고장성 강화 운전

범용소프트제어기 운전에 있어 내고장성 강화를 위해 안전계통과의 기능독립성을 만족시키기 위한 다음의 신호연계 및 확인스위치 운전 방안이 적용 및 검토되었다.

1. 공학적안전설비(ESF) 신호연계 확장 적용방안

공학적안전설비(ESF)를 포함한 모든 안전급 기기에 ESFAS 동작신호를 연결하여 USC로부터의 신호를 차단함으로써 안전기능 동작 요구시 안전기능에 영향을 주지 않는다. 비록 범용소프트제어기로 인한 오작동으로 안전기기가 원하지 않는 위치에 있더라도 안전기기의 초기상태를 미리 설정하여 신호를 준다면 발전소의 안전기능 유지는 보장된다. 또한 공학적안전설비의 어떠한 신호가 발생하더라도 G-ESFAS 신호를 이용하여 범용소프트제어기로부터의 신호를 차단함으로써 안전기능에 영향이 없도록 한다(그림 6. 참조).

이러한 신호의 연계는 기능적 독립성 규제요건(ISG-04)에서 요구하는 안전해석 범주안에 있으며 새로운 유형의 사건/사고를 발생시키지 않음을 입증해야 하는 어려움이 있다. 따라서 선행호기에서도 적용된 바 있는 제어명령 확인 기능을 추가적인 설계로 제시하고 있다. 이는 선행호기에서의 채널 확인 개념에서 벗어나

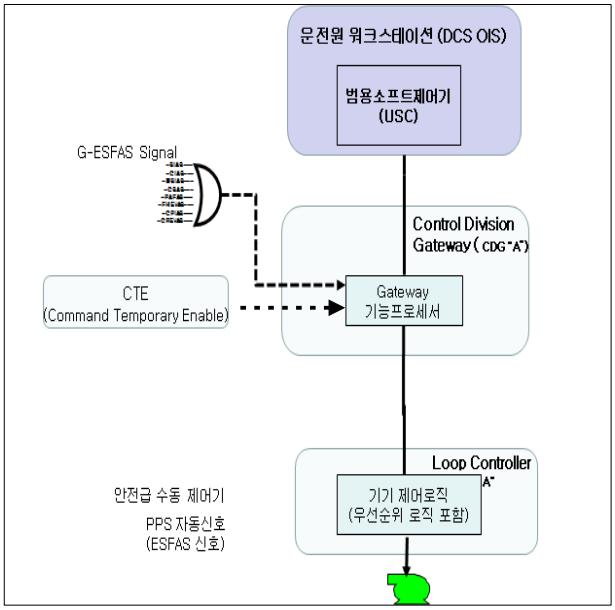

그림 6. 기능독립성을 위한 신호차단
Fig. 6. The signal interception for functional independence.

표 1. ESFAS 신호연계
Table 1. The signal interface of ESFAS.

안전등급기기 구분	USC 운전	ESFAS 신호연계
- Initiation Event/ FMEA 영향기기 - 기존 ESFAS기기 (200개)	CTE	G-ESFAS 신호, 기 신호연계
- 안전기능에 영향을 주는 기기 - LO, LC 적용기기 (100개 정도)	CTE	기기별 신호연계
- 안전기능에 영향이 없는 기기 (Support 기기)	허용	기기별 신호연계
- 나머지 안전기기 (Dependency)	허용	신호연계(제외)

기기선택과 제어명령 선택 후 확인스위치(CTE)를 작동할 때만 범용소프트제어기와 CDG를 연결하여 한 개의 제어신호만을 전송한다.

공학적 안전설비 신호연계를 위한 안전등급 기기에 대한 분석을 표 1과 같이 수행하였다. 원전 안적등급 기기는 설계특성을 고려해 볼 때 ESFAS신호 연계기기, 안전기능에 영향을 주는 기기, 안전기능에 영향을 주지 않는 기기, 안전기능에 영향 없는 기기와 나머지 안전기기로 구분할 수 있다.

USC 운전을 위해서는 USC 오작동 영향이 새로운 유형의 사건을 유발하거나 안전해석에 어려움이 있을 경우에는 CTE를 적용하는 것이 고려되었다. 따라서 정확한 분석 및 제시를 위해서는 설계사의 정확한 분석 및 입증이 필요함에 따라 본 단계에서는 적용을 위한 검토는 수행되지 못하였다 (표 1 참조).

2 운전확인 개념

범용소프트제어기의 오작동 발생확률을 낮추기 위한 운전원 2단계 조작 개념(기기선택, 제어명령 선택)이 적용이 되었으며 아울러 운전확인 스위치에 대한 설계개념과 운전방안에 대한 검토가 수행되었다. 선행호기에서 기 적용되고 있는 채널확인 스위치를 운전원 화면 각각 설치하는 것과 달리 운전원 콘솔에 1대 설치함으로써 설계의 단순화에 기여할 수 있었으며 채널별 선택에서 기기별 선택으로의 개선을 통해 운전편의성을 개선할 수 있었다. 다음은 채널선택과 기기선택시의 운전성을 비교 검토하였다.(표 2. 참조)

표 2. 명령확인스위치 운전개념
Table 2. The operation concept for CTE.

검토 항목	CES (Channel Enable S/W)	CTE (Command Temporary Enable)
조작 방법	1번의 Enable로 여러 개의 기기를(5분 동안) 조작가능 : 2단계 조작	매번 3단계 조작
운전원 안전기능	WDS (Workstation Disable S/W)	WDS Bypass 수행 불필요
운전 모드	운전모드 3가지: Workstation, 안전제어반, WS+SC	운전모드 단순 : Workstation, 안전제어반
운전 편의성	WS+SC : 워크스테이션과 안전제어반 번갈아 이동하면서 운전	이동운전 불필요
운전원 Cross Check	운전원 해당채널 운전상태 확인	확인 불필요
운전개념	해당채널 Exclusive 개념	Non-Exclusive

Ⅵ. 결 론

범용소프트제어기에 의한 안전기기 제어를 위해 비안전급인 범용소프트제어기로부터의 어떠한 발생 가능한 고장도 안전계통의 고유 안전기능 수행을 방해하지 않도록 범용소프트제어기와 안전계통 간에는 물리적, 전기적 격리 및 통신 독립성을 보장하였다. 또한 범용소프트제어기의 중요 설계특성 중 운전원 2단계 조작과 제어메시지의 검증기능 등을 통해 오작동 발생확률을 낮출 수 있도록 하였다.

운전원 워크스테이션 내에서의 제어메시지 검증을 통해 제어신호에 대한 신뢰성 확보를 하였으며, 발전소 안전기능 보장을 위해 우선순위로직(Priority Logic)을 적용 구현하였다. 그러므로 범용소프트제어기는 안전과 비안전간의 기능적 독립요건을 만족시켜 비효율적 운전성과 기기 제어에 대한 설계 복잡성을 개선할 수 있었다. 또한 범용소프트제어기로부터의 어떠한 오작동 영향에 대한 안전기능 수행 보장을 위해 공학적 안전설비 신호(ESFAS) 확대 연계방안 검토수행과 기기확인 기능(CTE)의 운전방안 적용을 통해 범용소프트제어기에 대한 신뢰성 확보에 크게 기여할 수 있게 되었다.

신형원전(APR+) 범용소프트제어기는 최근 미국 NRC가 제시한 첨단 주제어실의 통신독립성 현안에 대한 규제요건(ISG-04)을 만족하도록 설계하였으며 범용소프트제어기 고장이 발전소 안전기능에 영향을 주지 않는 설계특성을 갖도록 하였다. 따라서 기존 원전이 갖고 있는 소프트제어기의 안전급과 비안전급으로 구분되는 소프트제어기의 비효율적인 운전성을 개선하고 가용성을 향상할 수 있으며, 원전 MMI의 설계 단순성, 설비비용 감소, 운전원의 2차 직무 감소, 운전원 콘솔 크기감소, 유지보수 업무 감소 등의 개선효과를 기대할 수 있다.

현재 범용소프트제어기에 대한 설계는 신형원전(APR+) 적용을 위해 인허가 기관인 KINS에 기술보고서(TR)를 제출해 놓은 상태이며 추가 질의 및 답변이 진행되고 있다. 본 설계는 인허가 과정을 통해 추가적인 분석 및 입증이 진행될 예정이다.

참 고 문 헌

[1] S.H. Ye, Y.C. Shin, “Priority Logic Design for Advanced Control Room”,2010 Conference on Information and Control System(CICS2010), pp. 77-78, 10. 2010.
[2] Task Working Group 4, “Highly-integrated Control Rooms-Communications Issues (HICRc)”, DI&C-ISG-04, US NRC, 2009.
[3] IEEE 603, Standard Criteria for Safety System for Nuclear Power Generating Stations, 5 November 2009.
[4] IEEE 7.4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
[5] IEEE 384, Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations, 20 December 2008.
[6] NUREG/CR-6635, Soft Control: Technical Basis and Human Factors Review Guidance

저 자 소 개

예 송 해(정회원)
2011년 충남대학교 대학원 전자전파통신공학과 석사 졸업
2011년～현재 충남대학교 대학원 전자공학과 박사과정
1996년～현재 한수원 중앙연구원 선임연구원
<주관심분야 : 원자력발전소 안전계통 설계>

유 준(정회원)
1978년 서울대학교 전자공학과 학사 졸업.
1984년 한국과학기술원 전기전자공학과 박사 졸업.
1984년～현재 충남대학교 전자공학과 교수
<주관심분야 : 산업공정제어, 센서신호처리, IT기반 로봇, 항법시스템>