# 디지털 보호계통 기술 개발

한재복, 김창회 / 한국원자력연구소


## 요 약

원전의 보호계통은 발전소의 비정상 운전시 원자로를 보호하고, 관련 기기를 작동시켜 사고를 완화시키는 기능을 수행한다. 따라서, 보호계통은 안전등급으로 분류되고, 안전기준에 따라 개발되어야 한다. 본 기고에서는 우리나라를 비롯한 원자력선진국의 보호계통 개발동향을 기술한다. 또한, 원전 계측제어계통 개발 사업을 통해 개발되고 있는 보호계통과 안전등급 PLC(Programmable Logic Controller)에 대한 설계특징과 그 구성에 대해 논의한다.


## 서 론

우리나라는 1978년 고리 1호기 상업운전을 시작으로 현재 18기의 원전이 상업운전 중에 있으며, 2015년까지 10기의 원전이 건설될 예정이며, 세계 6위의 원자력발전 국가이다.

원자력발전소는 우라늄이 핵분열하여 열에너지를 만드는 원자로, 원자로의 열에너지를 전달하는 원자로냉각재계통, 열에너지를 전달받아 고온 고압의 증기를 생성하는 증기발생기, 증기발생기의 증기를 이용하여 전기를 생산하는 Turbine Generator 및 운전 및 감시에 필요한 계측제어계통 등으로 구성된다.

계측제어계통은 발전소 운전에 따른 공정의 변화를 측정하는 계측계통(Instrumentation System), 발전소를 제어하기 위한 제어계통(Control System), 사고시 발전소를 안전하게 유지하기 위한 보호계통(Protection System), 발전소 운전상태를 감시하고, 필요할 경우 경보를 발생시키는 감시계통(Monitoring System)으로 크게 나누어진다. 특히, 보호계통은 발전소가 비정상 상태일 때 원자로를 정지시켜 핵연료 피복재의 손상을 방지하고, 원자로냉각재계통의 건전성을 유지하여 사고를 완화시키는 등 발전소 안전에 관련된 중요한 기능을 수행한다. 이런 이유로 보호계통은 안전등급(Class 1E) 및 내진등급 I(Category I)를 만족해야 한다.

1980년대 이전의 원전에서는 아날로그 논리회로와 계전기를 사용하여 보호계통을 설계하였으나 1980년대 이후에는 프랑스 EdF, 카나다의 AECL, 미국의 웨스팅하우스 및 CE 등에서 디지털 보호계통이 개발되기 시작하였다. 80년대 초기에는 보드(Board) 단위의 디지털 제어기기를 개발하여 보호계통을 설계하였지만, 확장성 및 유지보수 등의 문제로 인해 1980년대 후반에는 산업체에서 널리 사용되어 그 신뢰성이 인증된 PLC(Programmable Logic Controller)를 사용하여 보호계통을 설계, 개발하였다.

원전 계측제어기술을 자립하기 위해서는 계측제어계통 설계기술뿐만 아니라, 계측제어계통 구성에 사용되는 제어기기의 기기설계 및 제작기술이 전체적으로 완성되어야 한다. 원전설계기술의 경우

1984년부터 시작된 원전기술자립계획에 따라 국산화가 이루어졌으며, 그 기술을 바탕으로 울진 3&4호기 및 영광 5&6호기의 한국 표준형 원전(KSNP)이 개발되었다. 그러나 이러한 설계기술 국산화에도 불구하고 보호계통에 사용될 안전등급 제어기기가 개발되지 않아 현재 상업운전 중인 원전뿐만 아니라 2004년에 가동 예정인 울진 5&6호기 보호계통에도 여전히 외국사의 제품이 적용되고 있다.

원전계측제어계통 개발사업에서는 이러한 문제점을 해결하기 위해 최적화된 디지털 보호계통을 개발하고, 핵심 기기인 안전등급 PLC를 개발하고 있다. 이 PLC는 최적화된 디지털 보호계통 구성을 위해 다양한 통신망을 제공하고, 엄격한 실시간 요건을 만족하며, 외국의 안전등급 PLC에 비해 높은 신뢰도와 성능을 가지도록 개발되고 있다. 따라서, 본 사업을 통해 개발되는 보호계통과 안전등급 제어기기는 외국사인 웨스팅하우스나 지멘스사의 제품을 대신하여 기존발전소의 노후설비 교체나 신규원전에 적용될 수 있다.

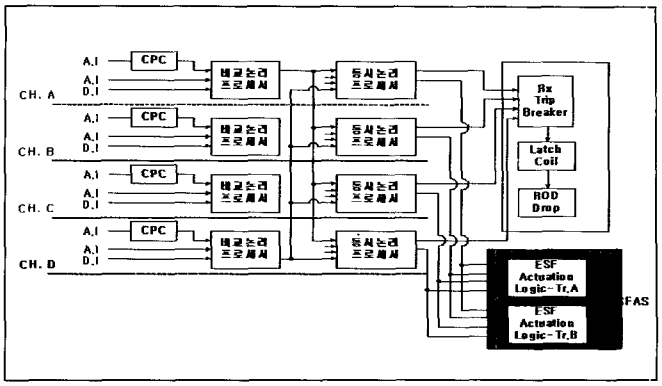



그림 1 보호계통 블럭선도

## 원자력발전소 보호계통 개발 동향

### 보호계통 기능 및 설계요건

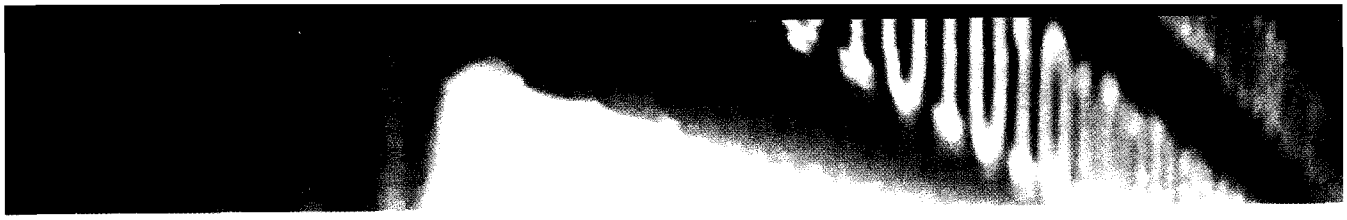
보호계통은 원자로보호계통(Reactor Protection System)과 공학적안전설비작동계통(Engineered Safety Features Actuation System)으로 구성된다. 원자로보호계통은 발전소의 비정상시 원자로를 정지시키며, 공학적안전설비작동계통은 설계기준 사고시 관련 기기를 작동시켜 사고를 완화시키는 역할을 담당한다.

일반적으로 원자로보호계통은 동일한 4개의 다중채널로 구성된다. 원자로보호계통은 다중화된 4개의 Class 1E 계측 채널로부터 공정변수를 취득하고, 그 변수가 원자로 정지설정치를 초과하면 원자로 정지신호를 발생시킨다. 따라서, 원자로보호계통은 입력된 계측 채널의 신호를 설정치와 비교하는 비교논리프로세서(Bistable Processor)와 4채널의 정지신호가 정지논리(2/4 논리)를 만족 하는지를 판단하는 동시논리프로세서(Coincidence Processor), 유지보수 및 시험을 위한 시험프로세서(Test Processor)로 구성된다(그림 1)

공학적안전설비작동계통은 원자로보호계통 각 채널로부터 공학적안전설비 작동신호를 제공받아 4채널 중 2개 이상의 채널이 설정치를 벗어날 경우 관련 기기 작동신호를 발생시킨다. 일반적으로 공학적안전설비는 안전주입, 격납용기 격리, 격납용기 살수, 주증기 격리, 비상급수와 관련된 기기를 작동시키며, 다중화 요건에 따라 2개의 트레인으로 구성되어 있다.

보호계통은 비정상 및 설계기준 사고환경에서 모든 기능이 작동될 수 있도록 설계되어야 한다. 보호계통 설계시 고려해야 할 몇 가지 요건을 간단히 기술하면 다음과 같다.

- 보호계통은 불필요한 트립을 방지하기 위해 우회기능을 제공해야 한다.
- 보호계통은 공통유형고장을 배제하기 위해 다양성을 제공해야 한다.
- 보호계통은 단일고장으로 인해 발전소가 정지되는 것을 방지하기 위해 다중화 채널 로 설계되어야 하며, 다중화 채널간에는 독립성이 유지되어야 한다.
- 보호계통은 그 성능을 주기적으로 확인할 수



있도록 시험기능을 제공해야 한다.

- 보호계통은 설계기준 사고환경에서 주어진 성능을 만족한다는 것을 보증하기 위해 내환경, 전자파, 내진 등의 기기 검증요건을 만족해야 한다.
- 보호계통에 사용되는 소프트웨어들은 관련 규제요건에 따라 확인 및 검증이 되어야 한다.

### 보호계통 개발 동향

프랑스 EdF는 1977년부터 8비트 마이크로프로세서를 사용하여 개발한 디지털 보호계통을 1984년 Palue 1호기를 시작으로 1992년까지 모든 1300MWe P4 시리즈 발전소에 적용하였다. 또한, 1987년경에는 모토롤러 68000 CPU를 사용한 보호계통(SPIN) 개발을 시작하여 1990년 중반에 프로토타입을 통한 검증연구를 수행한 후 N4 발전소(Choose B)에 적용하였다. SPIN은 비교논리프로세서에 해당하는 부분을 5개 FU(Functional Unit)로 나누어 기능적 다양성을 확보하였고, 채널 내에서 뿐만 아니라 채널 간 데이터 전송을 위해 실시간 이더넷을 적용하였다. 또한, 네트워크를 통해 시험장치(CTU)를 각 채널에 연결하여 수동개시 자동시험이 이루어질 수 있도록 설계하였다.

웨스팅하우스에서는 1978년경 Q 시리즈라 명명된 디지털 보호계통을 개발하였다. 이것은 8비트 마이크로프로세서와 아날로그회로가 혼재된 하이브리드 타입이었다. 1986년에는 디지털 보호계통 및 제어시스템 패키지인 Eagle Family 21을 개발하기 시작하였다. Eagle Family 21은 Sizewell B와 체코의 Temelin 발전소에 적용되었다. Temelin 발전소의 경우 완공되었지만, 인허가 문제가 해결되지 않아 상업운전을 하지 못하고 있다.

AECL은 1970년대 후반부터 PDC(programmable Digital Comparator)를 개발하기 시작하여 CANDU-6 플랜트에 적용하였다. 1980년대에는 디지털 보호계통(SDS #1 & #2)을 개발하여 Darington 발전소에 적용하였다.

또 다른 원전 산업체에서는 1980년대 후반부터 산업체에 사용되어 그 신뢰성이 입증된 PLC를 원전 안전등급 기준에 맞게 수정보완하고, 상용등급인증(COTS) 후 보호계통 패키지 개발에 적용하였다. 독일의 지멘스사는 PLC 기반의 보호계통 패키지(Teleperm XS)를 개발하여 헝가리 Paks 발전소 등 유럽 원전의 안전계통 교체에 널리 적용하고 있다. Teleperm XS는 안전에 관련된 데이터는 Profibus FDL을 통해 전송하고, 정보데이터는 실시간 이더넷(IEEE 802.3)을 통해 전송하는 구조를 갖는다.

미국의 ABB-CE사는 산업체에서 사용되고 있던 Advant PLC를 안전등급 PLC(AC-160)로 상용등급인증(COTS) 하여 보호계통을 개발한 후 울진 5&6호기에 적용하였다. AC-160은 안전에 관련된 데이터는 RS-422 기반의 HSL(High Speed Link)을 통해 전송하고, 정보데이터는 AF-100(IEEE 802.4)을 통해 전송한다. 웨스팅하우스는 ABB-CE의 원자력 부문을 인수한 후 AC-160 기반의 보호계통 패키지를 Common Q로 명명하였다. 이 패키지는 신고리 3&4호기 원전에 적용될 예정이다.

영국의 Invensys사는 발전소 터빈 제어계통 등에 사용되고 있던 Triconex PLC를 안전등급 PLC로 상용등급인증(COTS)하였다. 그러나 NRC에서 검토결과 Triconex PLC가 안전등급 기준을 만족하는 통신망을 갖고 있지 않아 보호계통에 적용하는 것은 문제가 있다고 발표하였다.

표 1은 특정주제보고서(Topical Report)를 미국 NRC에서 제출하여 승인된 각 사의 PLC 기반 보호계통 패키지를 나타내며, 그림 2는 디지털 보호계통 캐비닛을 보여준다.

**표 1 Topical Report Review Status**

| Vendor | Platform | Submittal Date | Status |
|---|---|---|---|
| Siemens | Teleperm XS | 98/10/5 | Review completed on 2000/3 |
| Westinghouse | Common Q | 99/4/26 | Review completed on 2001/12 |
| Invensys | Triconex | 00/10/5 | Review completed on 2001/10 |

Teleperm XS　　Common Q　　Triconex

그림 2 PLC 기반 보호계통 캐비닛 예

## KNICS 보호계통

KNICS 사업을 통해 개발되고 있는 KNICS 보호계통 패키지는 다음과 같은 주요 설계특징을 갖는다.

- APR 1400 요건 만족
- 자동주기시험 기능 적용으로 이용률 향상
- 주요 프로세서 완전 이중화로 신뢰도 향상
- 네트워크 확대 적용으로 유지보수 향상

본 사업을 통해 개발되는 보호계통 패키지는 원자로보호계통과 공학적안전설비-기기제어계통(ESF-CCS)으로 구성되며, 이들 계통에 적용될 디지털 제어기기로 안전등급 PLC를 사용한다. 이 PLC는 KNICS 원자로보호계통 및 공학적안전설비-기기제어계통 설계요건과 안전계통에 적용하기 위한 제어기기 일반요건에 따라 국내 PLC 전문회사에서 개발하고 있다. 그림 3은 KNICS 보호계통 구조를 나타낸다.

KNICS 원자로보호계통은 전기적/물리적으로 격리된 4개의 채널로 구성되며, 각 채널에는 PLC로 구현된 비교논리프로세서(BP), 동시논리프로세서(CP), 자동시험 및 연계프로세서(ATIP)가 설치된다. 각 채널의 비교논리프로세서와 동시논리프로세서는 완전 이중화 구성을 가진다. 또한, 캐비닛운전원모듈(COM), 주제어실 및 원격정지실 운전원모듈, 노심보호연산기 등이 각 채널에 포함된다. 각 프로세서들의 운전정보는 이중화된 ICN(Intra-Channel Network, Profibus-FMS)을 통해 전송되고, 비교논리프로세서와 동시논리프로세서간 안전데이터 전송은 SDL(safety Data Network, Profibus-FDL)[1]을 통해 이루어진다. 자동시험 및 연계프로세서는 자동주기시험을 관장하며, 타 채널 및 ESF-CCS와의 연계를 수행한다. 자동주기시험은 비교논리 및 동시논리프로세서 입출력모듈, 비교논리, 동시논리에 대해 정해진 주기마다 자동으로 시험이 개시되고 수행된다. 캐비닛 전면에는 유지보수를 위해 캐비닛 운전원 모듈이 설치되며, ICN을 통해 전송된 각 프로세서의 운전정보가 CRT상에 표시된다. 또한, 캐비닛 운전원 모듈에는 유지보수시 사용될 트립채널우회 및 전채널우회 스위치가 설치되어 있다[2].

공학적안전설비기기제어계통( ESF-CCS)은 전기적/물리적으로 격리된 4개의 디비젼으로 구성되며, 각 디비젼에는 PLC로 구현된 그룹제어기(GC), 루프제어기(LC), 통신 및 시험프로세서(CITP)가 설치된다. 또한, 캐비닛 운전원 모듈과 주제어실 및 원격정지실의 수동제어반이 포함된다. 각 디비젼의 그룹제어기는 완전 이중화로 구성되며, 원자로보호계통에서 전송된 공학적안전설비 작동신호를 취득하여 Full 2/4 논리를 수행한다. 작동신호는 그룹네트워크(GN)을 통해 관련 루프제어기로 전송되고, 루프제어기는 정해진 논리에 따라 관련 기기를 작동시킨다. 그룹네트워크는 안전데이터를 전송하는 네트워크이기 때문에 안전데이터링크와 동일한 안전등급 기준을 만족해야 한다. 각 그룹제어기와 통신 및 시험프로세서 간에는 IDN(Intra-Division Network)을 통해 운전정보를 공유한다. 통신 및 시험프로세서는 그룹제어기의 입출력모듈과 2/4 논리에 대해 자동주기시험을 수행한다. ESF-CCS는 PLC가 갖는 Multi-loop 제어기능을 사용하기 때문에 Single-loop를 사용하는 PCS 캐비닛보다 사이즈가 간결해지고, 모든 제어기들이 네트워크를 통해 연결되기 때문에 유지보수성 및 경제적 측면에서 유리하다고 할 수 있다.

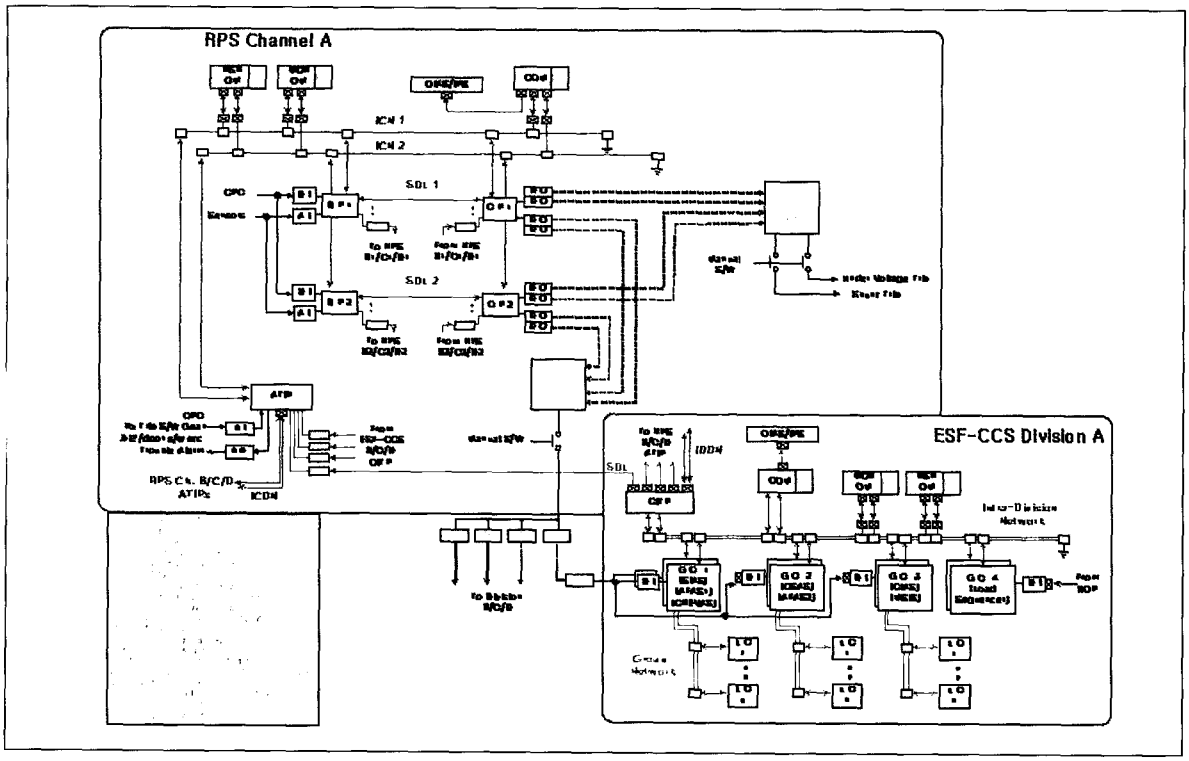



그림 3 KNICS 보호계통 한 채널의 구조

## KNICS 안전등급 제어기기

한국원자력연구소와 국내 PLC 제조회사 간에 공동으로 개발되고 있는 안전등급 PLC는 전기안전등급(Class 1E), Quality Class 1, 내진등급 I을 만족한다. 또한, 실시간운영체제, Firmware, 엔지니어링 도구와 같은 각종 소프트웨어는 error-free를 위해 software life cycle에 따라 개발되며, 요구사항명세서(SRS) 및 설계사양서(SDS)는 정형명세기법을 이용하여 개발하고 있다. 각 생명주기 단계마다 개발된 결과는 독립 검증팀에 의해 V&V가 이루어지고 있다.

KNICS 안전등급 PLC는 다음과 같은 주요 특징을 갖는다.

- 자체 개발된 실시간 운영시스템(RT-OS)을 사용한다.
- 안전데이터 전송을 위해 Profibus-FDL 프로토콜을 사용한다.
- 확장성 및 연계성을 위해 Profibus-FMS/DP, ProfiNet 등 국제 표준 통신망을 사용한다.
- 엔지니어링 도구는 IEC 61131-3 기준을 만족하며, 시뮬레이션 기능을 갖는다.
- 입출력모듈의 각 채널 고장진단을 위해 Loop back 감시기능을 갖는다.
- 다양한 자가진단 기능을 제공한다.
- 이중화된 전원모듈을 사용한다.

개발되는 PLC는 안전계통에 적용하기 위한 PLC 일반요건 및 규격과 EPRI TR-107330 [3]의 사양을 모두 만족한다. 또한, 공정변수를 취득하고, 보호논리를 수행한 후 출력을 발생할 때까지의 응답시간은 50ms 이내에서 실시간으로 작동한다. PLC 각 부품의 신뢰도 계산방법은 MIL Std 217F[4]를 따르며, PLC 각 모듈의 고장율 목표치는 $10^{-6}$/Hr 이다.

개발되는 PLC는 Teleperm XS, AC-160, Triconex의 개발방법과는 다르게 OS를 비롯한 모든 소프트

표 2 안전등급 PLC 주요사양 비교

| | | KNICS (POSAFE-Q) | Teleperm XS | AC-160 |
|---|---|---|---|---|
| CPU | Processor | MIL SMQ320C32PCMM-50 25MIPS | 80486 DX-32M 20MIPS | MC68360QUICC-33M 6MIPS |
| | OS | PCOS RTOS | MICROS | RTOS |
| | User Application | 4MBytes | Up to 4MBytes | 1MByte |
| | Engineering Tool | PSET (표준 IEC 61131-3) | SPACE(비표준) | AMPL(비표준) |
| Analog I/O | Signal Range | ±10V, ±20mA | ±10V, ±20mA | 4~20mA/0-20mA(O) |
| | Resolution | 16 Bit | 16 Bit | 16 Bit |
| | Self Diagnostic | Loop Back (All) | Loop Back (All) | Loop Back (All) |
| Digital I/O | Signal Range | 24VDC, 250VDC/30VDC | 24VDC, 250VDC/30VDC | 24VDC, 48VDC, 60VDC |
| | Self Diagnostic | Loop Back (All) | Loop Back (All) | Loop Back (All) |
| Comm.Driver | Processor | EC1-48M(16Bit) | V25-20M(16Bit) | MC68360QUICC-25M |
| | Interface | Dual Port Memory (16Kbyte) | Dual Port Memory (12Kbyte) | Dual Port Memory |
| | Protocol | Profibus FDL/FMS | Profibus FDL/ IEEE802.3 | HSL/AF-100 |
| EQ Test | Surge | EPRI TR 102323 | Same as left | Same as left |
| | EMI/RFI | EPRI TR 102323 | Same as left | Same as left |
| | Seismic | IEEE Std. 344-1987 | Same as left | Same as left |
| | Environmental | IEEE Std. 323-1983 | Same as left | Same as left |

웨어와 각종 하드웨어를 안전기준에 따라 자체 개발하고 있다. 현재 PLC는 프로토타입이 개발된 상태이며, 기기검증(Equipment Qualification)을 준비하고 있다.

표 2는 개발되는 PLC, Teleperm XS, AC-160의 주요 사양을 나타낸다.

## 결 론

지금까지 원전 계측제어계통의 안전등급 계통인 보호계통 개발 및 안전등급 PLC 개발에 대해 논의하였다. 현재 국내 원전의 계측제어계통은 대부분이 외국의 제작사를 통해 공급 되고 있다. KNICS 사업에서는 원전 계측제어계통의 기자재 국산화 일환으로 보호계통과 핵심제어기기인 안전등급 PLC를 개발하고 있다. 개발되는 보호계통은 기존 보호계통에 비해 디지털 기반이 가지는 장점을 최대로 활용한 구조로 설계되며, 특히 유지보수 및 이용율 향상을 위해 자동주기시험과 완전 이중화 구성을 갖는다. 안전등급 PLC는 OS를 비롯한 모든 소프트웨어와 각종 하드웨어를 안전기준에 따라 국산화된 기술로 개발하고 있다. 따라서, 본 과제를 통해 하드웨어 기반 Safety Critical Software 개발방법, V&V, 안전성 보장, 검증된 하드웨어 개발 등의 기술이 국내 최초로 확립될 것으로 판단되며, 산업체 및 국방분야 산업에 파급효과가 클 것으로 기대된다. 본 과제를 통해 개발되는 보호계통패키지와 안전등급 PLC는 기존발전소 노후 설비 교체나 신규 원전에 적용될 수 있다.

[참고문헌]

[1] 김창회 등, "원전보호계통 통신망 설계방안," 대한전자공학회 하계종합학술대회, 5권. Vol.26, No.1, 2003년 7월

[2] 김창회 등, "KNICS 발전소 안전계통 구조설계," 제2회 계측제어기술 Workshop, 2002년11월

[3] EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants", Dec. 1996

[4] MIL STD 217F, "Realibility Prediction of Electric Equipment"