2003년도 대한전자공학회 하계종합학술대회 제26권 제1호

원전 안전등급 PLC 개발 현황

김창회, 박주현, 한재복
한국원자력연구소 계측제어인간공학연구부

Development Status of the Safety Class PLC for Nuclear Power Plants

Changhwoi Kim, Joohyun Park, Jaibok Han
Instrumentation & Control-Human Factors Division, KAERI
E-mail : chkim2@kaeri.re.kr

Abstract

원전 안전계통에 적용될 PLC 는 엄격한 내진, 전자파, 내환경 시험기준을 만족해야 하며, 원전 안전등급에 부합되는 안전성 및 신뢰성을 만족해야 한다. 전 세계에서 안전계통에 적용될 PLC 는 Siemens 의 Teleperm XS, Invensys 의 Triconex, WestingHouse 의 AC-160 이 있으며, 국내에서는 원전 안전계통 개발시 전적으로 이들 PLC 수입에 의존하고 있다.

현재 한국원자력연구소와 국내 PLC 제조회사간에 공동과제를 통해 안전등급 PLC 개발을 수행하고 있으며, 본 논문에서는 개발될 PLC 의 설계기준과 개발된 하드웨어 및 소프트웨어 사양 등 개발현황에 대해 기술한다.

I. 서론

원자력발전소 안전계통은 비정상 운전시 원자로를 정지시켜 핵연료 피복재의 과열을 방지하고, 원자로냉각재계통의 건전성을 유지한다.

국내 상업운전중인 원전의 안전계통은 아날로그 논리회로 또는 릴레이를 사용하고 있다. 그러나 최근에 건설중인 울진 5&6 호기는 안전계통에 웨스팅하우스에서 공급하는 AC-160 PLC 를 사용하였다. 또한, 차세대 원전에서는 웨스팅하우스의 COMMON Q 로 명명된 PLC 기반 안전계통 패키지를 적용할 예정이다.

한편 독일의 지멘스(Siemens)에서는 PLC 를 사용한 안전계통 패키지(Teleperm XS)를 개발하여 헝가리 Paks 발전소 등 유럽 원전의 안전계통 개량화에 널리 적용하고 있다. 최근 미국의 Invensys 사에서는 터빈제어에 사용되어 오던 Triconex PLC 를 안전등급 기준에 맞게 수정 보완하여 NRC 로부터 승인을 받았다.

원전 계측제어계통의 설계기술은 사용되는 제어기기의 특성에 따라 설계변경이 수반되어야 하기 때문에, 기기제작 기술의 자립 없이는 외국 기술의 의존으로부터 탈피할 수 없다.

현재 한국원자력연구소와 국내 PLC 제조회사간에 공동과제를 통해 원전 안전계통에 적용될 PLC 를 개발하고 있다. 개발될 PLC 하드웨어는 전기안전 1 등급(Class 1E), Quality Class 1, 내진등급 I 을 만족해야 한다. 또한, 실시간 운영체제, Firmware, 엔지니어링 도구와 같은 각종 소프트웨어는 error-free 를 위해 software life cycle 에 따라 개발되어야 하며, 각 단계에서 철저한 V&V 를 수행해야 한다. 통신망의 경우 안전등급 기준에 따라 결정론적 프로토콜 및 실시간 프로토콜을 사용해야 하므로 기존 산업체에서 사용되는 것과는 다른 프로토콜을 적용해야 한다.

본 논문에서는 본 과제를 통해 개발되고 있는 안전등급 PLC 설계기준과 하드웨어 및 소프트웨어 사양 등 개발현황에 대해 기술한다.

II. 안전등급 PLC 설계기준

원전 안전계통은 다양한 규제 요건을 만족해야 한다. 기본적인 성능 요건은 발전소 설비 또는 장비의 특성과 여러 가지 안전해석에 따라 결정되어야 한다. 안전등급 PLC 설계기준은 다음과 같다.

응답 시간

PLC 입력단에서 신호를 취득하고, 보호기능을 연산, 처리한 후 출력단에 신호가 나타날 때 까지 소요시간으로 50ms 이내에서 실시간으로 작동해야 한다.

신뢰도 요건

신뢰도 계산은 IEEE Std. 352[1]에 부합되어야 한다(부품의 신뢰도 계산방법은 MIL Std 217F[2]를 따른다). 신뢰도 계산은 각 모듈단위로 랜덤 하드웨어 고장율을 적용하여 가용도 분석을 수행해야 한다. PLC 의 전체 가용도 목표는 0.99 이다.

PLC 모듈의 부품 고장이 PLC 성능에 미치는 영향을 분석하기 위해 FMEA 를 수행해야 한다. FMEA 는 출력 상태에 대한 고장(fail high, fail low, fail as is)과 PLC 의 운전상의 고장(메인 프로세서 작동 불가, 몇 개의 I/O 작동 불가 등)에 대한 고장의 영향을 평가해야 한다.

내환경 요건

PLC 는 다음의 운전 환경내에서 주어진 성능을 만족해야 한다.

- 온도 범위 : 주변 온도 4 °C ~ 50 °C(40 °F ~ 120 °F) 범위에서 작동해야 한다. 이때 주변 온도란 자연 냉각일 경우는 새시의 바닥, 강제 순환 냉각일 경우는 팬 입구측 근처를 말한다.
- 습도 : PLC 는 상대 습도 10 % ~ 95 % (비응축) 범위에서 작동해야 한다.
- 방사능 : 10^3 RADS 노출에 대해서 작동해야 한다.

EMI/RFI 내성요건

PLC 는 EPRI TR-102323[3](or MIL Std. 461/462D)[4,5]의 EMI/RFI 기준을 만족해야 한다. EPRI TR-102323 에서 만족되어야 할 EMI/RFI 기준은 다음과 같다.

- Radiated Susceptibility per Appendix B Section 3.1.2
- Conducted Susceptibility per Appendix B Section 3.2.2
- Radiated Emission per Section 7
- Conducted Emissions Testing per mandatory tests in Section 7

위 기준에 대해 PLC 는 다음을 만족해야 한다.

- 메인 프로세서 및 어떤 Coprocessor 도 그 기능이 유지되어야 한다.
- I/O 데이터의 전송이 중단 또는 상실되지 말아야 한다.
- 디지털 I/O 상태가 변화되지 말아야 한다.
- 아날로그 I/O 레벨이 3% 이상 변하지 말아야 한다.

정전기 방전(ESD) 내성요건

PLC 플랫폼 및 관련 장치들이 PLC 새시에 설치되었을 때 PLC 플랫폼과 관련 장치들은 EPRI TR-102323 appendix B, Section 3.5(or IEC 61000-4) 기준에 따라 Esd 내성 요건(PLC 가 이런 Esd 레벨에 노출되었을 때 어떤 손상이나 운전 손실이 발생되지 않아야 함)을 만족해야 한다. 다중화 기능을 갖는 PLC 일 경우, ESD 레벨에 노출되었을 때 하나 또는 그 이상의 모듈에 고장이 발생하더라도 PLC 기능을 상실하지 않으면 허용할 수 있다.

서지 내성요건

PLC 는 IEEE Std. C62.41[6]의 0.5us 상승시간을 갖는 100kHz 표준 링 웨이브와 표준 1.2/50us ~ 8/20us 의 조합 웨이브 둘 다에 대한 서지 내성을 만족해야 한다. 내서지 레벨은 3000V 피크 인가 전압을 적용한다. 서지 레벨을 어떤 특정 부분에 인가하였을 때, PLC 내부의 어떤 부품(device)이나 어떤 모듈이 손상되지 않아야 하고, 트립 발생 기능이 손상되지 않아야 한다.

안전 및 비안전 격리요건

PLC 모듈에 최소한 교류 600V 및 직류 250V 의 전압을 30 초 동안 인가하였을 때 격리가 유지되어야 한다. 격리 특성은 IEEE Std. 384[7]에 제시된 기준에 따라 Class 1E 및 Non-1E 연결에 대한 계측 및 제어 요건을 만족해야 한다. 격리 성능시험은 PLC 모듈 및 보조 격리장치에 대해 수행되어야 한다. 이미 검증된 외부 격리장치를 사용할 경우는 이 시험을 하지 않아도 된다.

내진요건

PLC 는 Seismic Category I 기준을 만족해야 한다. 3 축

방향으로 동시에 가해지는 안전정지지진(SSE) 진동 동안 또는 가해진 후에 그 성능 요건을 만족해야 한다. PLC 는 5 번의 운전기준지진(OBE)에 적용된 후 SSE 진동에 견뎌야 한다. PLC 는 SSE 레벨의 진동이 가해진 후 PLC 의 모든 연결부는 손상되지 않고 연결되어 있어야 하며, 모든 모듈들은 충분히 결합되어 있고, 각종 부품들의 성능이 저하되지 않아야 한다. 릴레이 출력 모듈의 경우는 OBE 및 SSE 가 가해지는 동안 릴레이 접점을 변경시킬 수 있어야 한다. 이런 상태로의 변화는 2ms 를 초과하지 말아야 한다.

운영체제(OS)

일반적으로 PLC 에 탑재된 운영체제는 제어행위를 수행하는데 필요한 최소한의 필수 기능만을 가져야 하며, 실시간 성능을 보장해야 한다.

진단요건

PLC 는 자가진단과 점검시험을 통하여 PLC 에 의도된 안전기능을 수행하는데 방해되는 모든 고장을 감지할 수 있도록 충분한 고장진단과 시험능력을 가져야 한다.

전원장치 요건

전원공급장치의 1 차에 공급되는 AC 소스는 90 ~ 150V 이며, 공급 주파수는 57 ~ 63Hz 일 때 정상적으로 동작해야 한다. 직류 소스로 동작되는 전원공급장치는 DC 소스 24VDC ± 15% 내에서 정상적으로 동작해야 한다.

접지 및 차폐 요건

PLC 장비의 접지 및 차폐는 IEEE Std. 1050[8] 요건과 EPRI TR-102323 의 지침서를 만족해야 한다. PLC 새시와 전원공급장치는 대지(earth) 접지와 DC common 에 연결할 수 있는 단자를 가져야 한다. 입/출력 모듈의 단말은 차폐 결선 단자를 제공해야 한다.

주기 점검 시험 요건

IEEE Std. 338[9] 의 기준에 따라 주기점검시험에는 채널 구성에 대한 체크, 교정 검사, 기능 시험, 응답시간 시험, 그리고 로직 시스템의 기능 시험 등이 수행되어야 한다.

통신요건

통신 프로토콜은 결정론적이고, 응용 프로그램의 기능을 정지시키거나 PLC 스캔 사이클을 중지시키는 통신 오류를 발생시키지 말아야 한다. 통신 데이터를 위한 동기화 및 큐(queue)를 제공해야 한다. 메시지 큐 상태에 대한 지시를 응용 소프트웨어에서 오류의 검출 및 회복 방법에 따라 활용 가능해야 한다. '동기를 제공하기 위해 요구되는 대기시간' + '오류 검출 및 회복 시간' + '공칭 루프 시간(nominal loop time)'이 응답 시간 요건을 만족해야 한다. 데이터 품질 검사는 적어도 CRC-16 과 같이 견고한 검사 방법을 사용해야 한다.

III. 안전등급 PLC 제작사양

앞 절의 설계기준에 따라 개발된 중요 제작사양은 다음과 같다.

전원장치 사양

- 정격입력전압 : AC 110V ~ 220V(AC 120V)
- 입력전압 가변범위 : AC 85 ~ 264V
- 입력 주파수 : 47 ~ 63HZ
- 정격출력전압 : DC 5.0V(DC 24.0V)
- 정격최대부하전류 : 22A(0.5A)
- 출력전압 Tolerance : ±1%
- Hold up Time : 40ms 이상(정격출력전압 100% ~ 95%)
- 병렬운전 : Master/Slave 운전

연산모듈 사양

- Micro Processor : TI DSP SMQ320C32PCMM-50M (Military)
- O/S (Real Time) : PCOS (Kernel 10K bytes)
- Hardware Interrupt : OS Time Interrupt 1ms(10ms to 1sec)
- Program 언어 : LD, IL, SFC, FBD, ST
- 명령어 : IEC 1131-3 규격 명령어 채용
- Multi-Task 수 : 6 Task

아날로그 입력모듈

- Number of Input : 16 Single ended or 8 Differential input
- Signal Range : ±10V, ±20mA
- Resolution : 16bit(15bit + sign)
- Conversion Time : 500us per Channel
- Over Range : ±15V, ±30mA
- Loop Back Monitoring : All Channel (Short Circuit Proof/Protection), Output Loop Back (Input Circuit Check)

- Drift(24 개월) and CMRR : ±0.3%(Voltage), ±0.3%(Current)이하, 90dB 이상
- Isolation : Between system and all input, 560Vrms
- Accuracy : 0.1%

아날로그 출력모듈

- Number of Output : 8 Differential output
- Signal Range : ±10V, ±20mA
- Resolution : 16bit(15bit + sign)
- Conversion Time : 1ms per all channel
- Over Range : ±12V, ±28mA
- Loop Back Monitoring : All Channel (Short Circuit Proof/Protection), Output Loop (Read) Back (Output Signal Compare)
- Drift(24 개월) : ±0.3%(Voltage), ±0.3%(Current)이하
- Isolation : Between system and all input, 560Vrms
- Accuracy : 0.1%

DC 입력모듈

- Number of Input : 32 point (42Pin Terminal)
- Input Current and Resistance : 7mA , 3.3KΩ
- Delay Time : Typical 5ms
- Monitoring Input for PV : 4 (in group per 8)
- Loop Back Monitoring : 32 Point
- Common Group : Group per 8

DC 출력모듈

- Number of Input : 32 point (42Pin Terminal)
- Rated Supply Voltage : 24V DC (Load Tolerance Range: 18 ~ 30V DC)
- Switching Current : 5mA ~ 500mA
- Leakage Current (Off) : 2mA 이하
- Loop Back Monitoring : 32 Point
- Common Group : Group per 8

Profibus-FDL Drive

- Micro Processor : EC1-48M X 2EA
- Dual Port Memory : 4 ~ 8 Kbytes X 3
- O/S : PDOS
- Driver 확장 : Maximum 4EA (1Slot/Driver)
- Configuration Port : 2 Serial Port (Internal UART)
- Protocol : PROFIBUS-FDL
- Physical 구조 : RS-485 Electric or Optic
- 통신속도(bps) : 9.6K ~ 12Mbps
- Topology : Bus
- Channel 이중화 : Redundancy

IV. 결론

본 논문에서는 원전 안전계통에 적용될 안전등급 PLC 설계기준과 제작사양에 대해 기술하였다. 개발 중인 PLC 는 Class 1E 하드웨어 제작요건에 따라 현재 1차 시제품이 제작되어 기능시험 중에 있으며, 10 월경에 기기검증 시험을 수행할 예정이다. 소프트웨어는 Safety Critical Software 요건에 따라 개발하고 있으며, 정형기법을 적용하여 정형명세와 정형검증을 수행하고 있다.

감사의 글

본 연구는 과학기술부 중장기 연구개발과제의 일환으로 수행되었으며, 이에 관계자 여러분께 감사드립니다.

참고문헌

[1] IEEE Std 352-1987 Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.

[2] MIL STD 217F, "Reliability Prediction of Electronic Equipment".

[3] EPRI-TR-102323-R1, Guidelines for Electromagnetic Interference Testing in Nuclear Power Plant, EPRI, 1997.

[4] MIL-STD-461D-1993, "Electromagnetic Emissions and Susceptibility Requirements for the Control of Electromagnetic Interference".

[5] MIL-STD-462D-1993, "Measurement of Electromagnetic Interference Characteristics".

[6] IEEE Std C62.41-1991 Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits.

[7] IEEE Std 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits.

[8] IEEE Std 1050-1989 Guide for Instrumentation and Control Equipment Grounding in Generating Stations.

[9] IEEE Std 338-1987 Standard Criteria for Periodic Testing of Nuclear Power Generating Station Safety Systems.