2003년도 대한전자공학회 하계종합학술대회 논문집 제26권 제1호

원전 원자로보호계통 통신망 설계 방안

김창회, 박주현, 한재복
한국원자력연구소 계측제어인간공학연구부

Communication System Design Issues for Reactor Protection System in Nuclear Power Plants

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

Abstract

원자로보호계통은 비정상운전으로부터 원자로를 보호하기 위해 안전센서 신호를 감시하고, 그 값이 트립 설정치를 초과할 경우 자동으로 원자로 트립 또는/및 공학적 안전설비 작동 신호를 개시한다. 따라서, 원자로보호계통은 4 개의 채널로 구성되며, 각 채널간 및 채널 내에서는 데이터 통신망을 통해 원자로 트립신호와 운전정보를 전송한다. 이러한 기능을 수행하는 데이터 통신망은 실시간 및 결정론적 프로토콜을 만족해야 한다. 특히, 원자로 트립신호를 전송하는 안전등급 통신망은 채널간 격리 및 브로드 캐스팅(Broadcasting) 요건을 만족해야 한다.

본 논문에서는 원자로보호계통에 적용되는 데이터 통신망 설계기준과 프로토콜 설계방안에 대해 기술한다.

I. 서론

KNICS 원자로보호계통은 4 개의 채널로 구성되며, 각 채널은 동일한 하드웨어 및 소프트웨어를 갖는다. 원자로보호계통 각 채널은 하나의 캐비닛으로 구성되며, 각 캐비닛은 전기적 물리적으로 격리된 방에 설치된다. 각 방은 주제어실과 동일한 운전환경을 갖는다. 원자로보호계통 각 채널은 다음과 같은 기기들로 구성된다(그림 1 참조).

- 비교논리프로세서(BP) : PLC
- 동시논리프로세서(CP) : PLC
- 자동시험 및 연계프로세서(ATIP) : PLC
- 캐비닛운전원모듈(COM) : 산업용 컴퓨터 및 터치화면
- 기타 : 개시회로 및 기타 하드웨어 장치들

각 채널의 비교논리 프로세서는 입력모듈을 통해 취득된 트립변수를 트립 설정치와 비교한 후 트립 및 예비트립 상태신호를 출력한다. 이 출력신호는 안전데이터링크(SDL)를 통해 동일 채널 및 타 채널의 동시논리 프로세서로 전송된다.

동시논리 프로세서는 동일 채널 및 타 채널의 트립 상태신호를 안전데이터링크(SDL)를 통해 입력 받아 2/4 동시논리를 수행하고, 트립 조건이 만족될 때 마다 원자로 트립 및 공학적 안전설비작동 개시신호를 발생시킨다.

자동시험 및 연계프로세서는 비교논리 프로세서 및 동시논리 프로세서의 기능이 정확하게 작동하고 있는지를 시험한다. 또한, 각 채널의 운전상태를 타 채널로 전송하고, 공학적안전설비-기기제어계통과 연계하여 이 계통으로부터 상태정보를 제공받는다.

캐비닛 운전원모듈은 터치화면과 컴퓨터로 구성되며, 터치화면을 통해 일부 제어기능과 시험을 수행하고, 각 채널의 운전상태와 유지보수 화면을 제공한다.

4 개의 채널로 구성된 원자로보호계통은 각 채널간

및 채널 내의 데이터를 전송하기 위해 다음과 같은 데이터 통신망을 사용한다.

- 안전데이터링크(SDL) : 비교논리프로세서의 트립 상태신호를 동일 채널 및 타 채널의 동시논리 프로세서로 전송한다.
- 채널내부통신망(ICN) : 각 채널 내에 설치된 디지털 제어기기와 캐비닛 운전원모듈을 연결하며, 운전상태 및 정보신호를 교환한다.
- 채널간 데이터통신망(ICDN) : 각 채널간의 정보를 공유하기 위한 통신망으로 이중화 구성을 갖는다.

본 논문에서는 이들 통신망의 설계기준과 설계 방안에 대해 기술한다.

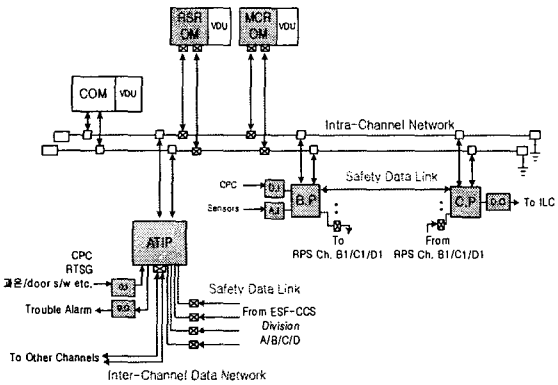

그림 1. KNICS 원자로보호계통 한 채널의 구성

II. 통신망 설계기준

원전 보호계통에 적용되는 통신망은 Reg Guide 1.75[1], IEEE Std. 384[2], IEEE Std. 7-4.3.2 Annex G[3]에 언급된 안전요건을 만족해야 한다.

데이터 통신망에 사용되는 하드웨어는 통신모듈, 광섬유케이블, 광섬유모뎀, 동축케이블로 구성되며, 이들 하드웨어 품질은 다음과 같이 분류된다.

- 안전등급 : 전기안전 1 등급 (Class 1E)
- 품질등급 : 품질등급 1 (Quality Class 1)
- 내진요건 : 내진등급 I (Seismic Category I)

통신망에 적용되는 소프트웨어는 통신 드라이브 및 응용 소프트웨어로 구성되며, 안전기능 수행여부에 따라 다음과 같이 분류된다.

- 안전데이터링크(SDL) : 필수 안전등급
- 채널내부통신망(ICN) : 안전관련 등급
- 채널간 데이터통신망(ICDN) : 안전관련 등급

안전데이터링크(SDL)는 원자로 트립신호를 전송하는 통신망으로 참고문헌 [1,2,3]의 기준에 따라 결정론적 프로토콜을 사용하고, 실시간 성능을 만족해야 한다. 또한, 안전데이터링크는 각 채널간의 통신시 데이터 흐름은 단방향이어야 하고, 브로드캐스팅(Broadcasting) 방식을 사용해야 한다. 그러나 동일 채널 내에서는 양방향 통신을 허용한다. 안전데이터링크에 사용되는 통신 프로토콜은 다양한 기능 보다는 최소 기능으로 설계되어야 하며, 자가진단 및 보안-인증 기능을 가져야 한다.

채널내부통신망(ICN) 및 채널간 데이터통신망(ICDN)은 비교논리 및 동시논리프로세서, 자동시험연계 프로세서, 그리고 캐비닛운전원모듈 간에 운전정보를 공유하기 위한 통신망이다. 이 통신망은 이중화 구성을 가져야 하며, 실시간 프로토콜을 만족해야 한다.

데이터 통신망은 전송기능 상실시 계통이 안전한 상태로 가도록 설계되어야 한다. 그리고 통신모듈, 광섬유모뎀, 전송로 등 기기의 고장으로 인한 데이터 송수신 오류, 오류 데이터 전송 등을 포함한 고장유형 및 영향분석(FMEA)을 수행해야 한다.

데이터 통신망은 안전데이터링크는 채널간 연계시 전기적 격리 및 독립성을 유지해야 한다.

데이터 통신망 모듈은 자가진단시험 및 지시기능을 가져야한다.

데이터 통신망 모듈 및 전송로는 IEEE TR-102323[4]에서 요구하는 EMI/RFI 요건을 만족해야 한다.

III. 통신망 설계 고려사항

앞 절의 통신망 설계기준에 따른 통신망 설계 시 고려해야 할 사항은 다음과 같다.

실시간 결정론적 성능

전송 및 처리 등에 관련된 시간이 실시간 결정론적이기 위해서는 Token Bus 방식으로 구현되어야 한다. Token Bus 방식은 일반적인 동작에서 최대 전송시간을 정할 수 있기 때문에 결정론적으로 볼 수 있다. 그러나 CPU 속도와 수행 알고리즘에 따라 처리시간이 달라질 수 있고, 노드들의 추가 또는 제거 시에 논리적 토큰 링 재구성으로 인해 응답 시간에 영향을 줄 수 있기 때문에 이들을 고려하여 프로토콜을 결정하여야 한다.

최소 기능으로 설계

원자로보호계통에 적용되는 안전데이터링크는 정해진 시간에 전송되어야 할 데이터 양이 제한되어 있고, 데이터 처리 측면뿐만 아니라 프로토콜 구현 측면에서도 고 신뢰성을 요구하기 때문에 다양한 기능보다는 최적화된 최소기능의 프로토콜을 요구한다. 따라서, 1 계층과 2 계층을 사용하여 최적화된 프로토콜을 구현해야 한다.

단방향 및 브로드캐스팅 데이터 흐름

원자로보호계통에 적용되는 안전데이터링크는 비교논리프로세서의 트립상태 신호를 각 채널의 동시논리프로세서로 동시에 전송하여야 한다. 이때, 채널간의 격리요건[1]에 따라 타 채널의 동시논리프로세서로부터는 데이터를 받지 않아야 한다. 따라서, 하나의 스테이션을 마스트로 다른 쪽 스테이션을 슬레이브로 설정하고, Send Data with No Acknowledge 방식을 통해 데이터를 전송해야 한다. 또한, 동시에 각 채널로 데이터를 전송하기 위해서는 하나의 공유메모리상에 전송할 데이터를 두면 각 채널 통신보드가 이 데이터를 읽어 가는 방식으로 설계해야 한다.

자가진단 및 감시기능

통신상의 노드 오류, 케이블 오류, 타 연산장치의 오류, 통신 모듈의 H/W 오류, 각 통신 드라이버 보드의 오류, 소프트웨어의 오류, 동시 시작 신호 오류, 데이터 타임아웃 에러 등을 진단하고 표시할 수 있는 기능을 제공해야 한다. 또한, 수신된 데이터는 순환중복검사(Cycle redundancy Check) 등과 같은 방법을 통해 건전성을 감시해야 한다.

보안-인증 기능

비 인가자가 접속하거나 소프트웨어를 변경하는 것을 방지하기 위해 기능을 제공해야 한다. 통신 프로토콜만으로 이것을 해결할 수 없을 경우, 시스템 차원에서 이를 해결해야 한다. 예를 들어 원자로보호계통을 외부망과 분리하고, 타 계통과 데이터 교환이 필요할 경우 보호기능이 있는 gateway 를 사용하고, 안전계통에 접속하기 위한 login 기능을 강화하고, 보호계통 캐비닛 도어의 열림을 감지할 수 있도록 해야 한다.

고장 대처기능

통신모듈의 고장은 통신 케이블의 단락, CPU 등 각 부품들의 고장, 통신상의 에러 프레임의 발생 등이 있을 수 있다. 이러한 고장이 발생될 경우 원자로보호계통은 기본적으로 Fail-safe 하게 작동되어야 한다. 고장 대처 방법 중 하나는 통신모듈 내에 Watchdog Timer 를 설치하고, 매 주기마다 Heartbeat 신호를 전송하는 것이다. 수신 측은 송신측으로부터 Heartbeat 신호가 전송되지 않을 경우 송신측에 어떤 오류가 있다고 판단하고 안전한 방향으로 작동시킨다.

고장유형 및 영향분석(FMEA)

통신모듈 설계단계에서부터 통신모듈 내 중요 부품이 고장날 경우 전체 PLC 작동에 미치는 영향을 분석하고, 그 결과를 통신모듈 설계에 반영해야 한다. 또한, 원자로보호계통과 같이 다수의 PLC 가 통신모듈을 통해 연계될 때 각 통신모듈의 고장이 원자로보호계통 안전 기능이 미치는 영향을 분석하고, 그 결과에 따라 통신모듈 또는 계통 구성을 변경하여야 한다.

채널간 전기적 격리

타 채널의 고장이 전기적으로 전파되는 것을 방지하고, EMI/RFI 내성을 갖도록 하기 위해서는 채널간 연계 시에는 가능한 Optic Cable 을 사용해야 한다.

통신 독립성

통신모듈은 Main CPU Module 의 안전 기능 수행에 영향을 주지 않도록 설계해야 한다. 따라서, 통신모듈은 자체 CPU 를 가지도록 하여 통신모듈로 인해 Main CPU Module 이 deadlock 에 빠지거나 실시간 처리가 방해받지 않도록 해야 한다. 또한, 통신 독립성을 유지하기 위해서는 Main CPU Module 과 통신모듈간에 버퍼링 회로를 두어 완충역할을 수행하도록 해야 한다. 버퍼링 회로는 별도의 프로세서나 메모리 카드일 수도 있으며,

확인 및 검증활동에 포함되어야 한다.

하드웨어 및 소프트웨어 상용등급 인증(COTS)

통신모듈을 안전등급 기준에 따라 개발하지 않고 상용등급을 인증 받고자 할 경우 하드웨어 측면에서는 제조사의 QA, 운전이력, 기기검증 결과 등이 필요하다. 그러나 소프트웨어 측면에서는 보다 복잡한 과정이 필요하다. 통신모듈 소프트웨어는 크게 운영시스템(OS) 과 Interface 되는 소프트웨어와 프로토콜 관련부분으로 나누어진다. 따라서, 상용등급 인증을 받기 위해서는 2 가지 소프트웨어 부분에 대해 인증절차를 수행해야 하지만 운영시스템과 연계되는 소프트웨어는 Main CPU Module 에 의존하기 때문에 복잡한 과정이 필요하다. 이런 이유로 프로토콜 관련부분만 인증을 받고 나머지는 Software Life Cycle 에 따라 개발하는 것이 유리하다고 생각된다.

소프트웨어 개발

통신모듈 소프트웨어 개발은 안전등급 소프트웨어 Life Cycle[5]에 따라 개발되어야 한다. 특히, 소프트웨어 요구사항명세(Software Requirement Spec.)[6]와 설계사양(Software Design Spec.)[7] 개발은 가능하면 정형화(Formal Method)된 방법을 사용해야 한다. 정형화된 방법을 통해 개발함으로써 완전성, 일치성, 정확성을 확보할 수 있고, 시뮬레이션 등을 통해 보다 완전한 검증을 수행할 수 있다.

V. 결론

원자로보호계통 통신망은 일반 산업체에서 사용되는 통신망과는 달리 엄격한 실시간 요건 및 Class 1E 기준을 만족해야 한다. 따라서, 본 논문에서는 프로토콜 개발 또는/및 선정 측면에서 고려해야 할 사항과 하드웨어 및 소프트웨어 개발 측면에서 고려할 사항에 대해 제안하였다.

감사의 글

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

참고문헌

[1] USNRC Reg. Guide 1.75, Rev. 02, September. 1978, "Physical Independence of Electric Systems".

[2] IEEE Std. 384-1992 (Reaffirmed 1998), "Standard Criteria for Independence of CIASs IE Equipment and Circuits".

[3] IEEE Std. 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety System of Nuclear Power Generating Stations".

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

[5] IEEE Std. 1074-1997, "Standard for Developing Software Life Cycle Processes"

[6] IEEE Std. 830-1998, "Recommended Practice for Software Requirements Specifications"

[7] IEEE Std. 1016-1998, "Recommended Practice for Software Design Descriptions"

[8] USNRC Reg. Guide 1.173, "Development of Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", 1997