KIPS Tr. Comp. and Comm. Sys.
Vol.2, No.12 pp.561~568 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.12.561

Design of Uni-directional Optical Communication Structure Satisfying Defense-In-Depth Characteristics against Cyber Attack

Jeong Kwang Il† · Lee Joon Ku†† · Park Geun Ok†

ABSTRACT

Instrumentation and control system in nuclear power plant performs protecting, controling and monitoring safety operation of Nuclear Power Plant. As cyber attack to the control equipment of instrumentation and control system can cause reactor shutdown and radiation release, it is required to design the instrumentation and control system considering cyber security in accordance with regulatory guides and industrial standards. In this paper, we proposed a design method of uni-directional communication structure which is required in the design of defense-in-depth model according to regulatory guides and industrial standards and we implemented a communication board with the proposed method. This communication board was tested in various test environments and test items and we concluded it can provide uni-directional communication structure required to design of defense-in-depth model against cyber attack by analyzing the results. The proposed method and implemented communication board were applied in the design of SMART (system-integrated modular advanced reactor) I&C (instrumentation and control) systems.

Keywords : Cyber Security, Cyber Attack, Defense-In-Depth, Uni-Directional Communication, Instrumentation and Control System, Nuclear Power Plant

사이버공격에 대비한 심층방호 특성을 만족하는 단방향 광통신 구조 설계

정 광 일† · 이 준 구†† · 박 근 옥†

요 약

원전 계측제어계통의 제어기기에 대한 사이버공격은 원자로 정지 또는 방사선 누출 등의 심각한 재앙을 유발할 가능성이 있다. 그러므로 원전 규제기관 및 산업표준의 요건에 따라 심층방호 특성을 고려한 사이버보안 대책설계가 원전 계측제어계통 설계에 요구된다. 본 논문에서는 사이버공격에 대한 원전 계측제어계통의 심층방호 대처 설계시 필수적으로 요구되는 단방향통신 구조를 구현하기 위한 설계방법을 제안한다. 제안한 단방향 통신 구조 구현방법은 통신보드 내에 구현되었다. 단방향 통신을 지원하는 통신보드는 시험을 통하여 심층방호 설계에 필요한 단방향 통신 구조를 제공하며, 사이버공격에 강인한 특성을 갖는 것으로 분석되었다. 이러한 사이버공격에 대비한 심층방호 대처 설계 및 단방향 통신을 지원하는 통신구조는 일체형원자로(SMART) 계측제어계통 설계에 적용되었다.

키워드 : 사이버보안, 사이버공격, 심층방호, 단방향통신, 계측제어계통, 원자력발전소

1. 서 론

원자력발전소(NPP, nuclear power plant, 이하 원전) 계측제어계통(I&C system, instrumentation and control system)은 보호, 제어 및 감시기능을 자동이나 수동으로 작동하는 제반장치 및 설비를 말하며 원자력발전소의 두뇌 및 신경망에 해당한다. 최근 원전 계측제어계통은 아날로그 기반의 제어기기에서 점차 디지털화된 제어기기 및 이들 제어기기간의 데이터 전송을 위한 통신망을 채택하여 사용하고 있다. 그러나 디지털 기술 기반의 제어기기는 아날로그 기반 기기에 비해 사이버 공격으로부터 매우 취약하다고 보고되고 있다. 원전의 계측제어계통 제어기기에 대한 사이버 공격은 원자로 정지까지 유발할 수 있으며, 심각한 경우 방사선 누출과 같은 심각한 국가적 재앙을 유발할 수도 있다. 이와 같이 디지털 기술의 취약성을 악용한 사이버 공격은

※ 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2012M2A8A4025979).
† 정 회 원 : 한국원자력연구원 연구로공학부 책임연구원
†† 비 회 원 : 한국원자력연구원 연구로공학부 선임연구원
논문접수 : 2013년 10월 14일
심사완료 : 2013년 11월 28일
* Corresponding Author : Jeong Kwang Il(hisunny@kaeri.re.kr)

원전의 운전 및 운영에 위협을 주는 등 국내외적으로 중요한 문제로 부각되고 있다.

최근 사이버공격 사례로서 2003년 미국 데이비스 베시(Davis-Besse) 원전의 컴퓨터 네트워크에 슬래머웜 침투 사례, 2007년 DHS (department of homeland security)의 사이버 공격 시험을 통하여 실제 원전의 디젤발전기 정지 사례, 2008년 미국 회계감사원의 미국 최대 국립전력회사인 TVA (tennessee valley authority)사의 제어시스템을 모의해킹하여 발전소 제어시스템에 침투한 사례, 그리고 2010년 스턱스넷 (stuxnet) 바이러스가 원전 제어시스템 침투하여 이란의 나탄즈 원자력 원심분리기가 일부 기능을 마비시키는 공격사례 등 여러 공격사례가 있었다. 이러한 공격사례들을 통하여 원전은 사이버 해커들이 고의로 공격하고자 하면 위협 및 침해받을 수 있는 다양한 루트가 존재함을 알 수 있다. 이와 같이 원전의 계측제어계통의 통신망은 내부 및 외부 공격에 의한 사이버 공격으로부터 안전하게 보호하기 위한 다양한 사이버보안 기술을 접목할 필요가 있으며, 사이버보안 기술 접목으로 인한 통신망 성능 저하를 최소화할 수 있는 방법 또한 강구되어야 한다.

최근 세계 각국의 원전 규제기관 및 산업표준 기관 등은 원전 사이버보안과 관련하여 새로운 규제지침 및 산업표준을 제시하는 등 원전에서 사이버 공격에 대비한 사이버보안 기술의 적용을 위한 연구가 진행되고 있으며, 원전에 적용할 수 있는 요건, 규제지침 및 산업표준을 잇따라 내놓거나 수정 및 개정하고 있다. 원전 운영자 및 설계자들은 이러한 원전관련 규제지침 및 산업표준에 따라서 운영 및 설계하여야 한다. 따라서 원전 계측제어계통의 계통설계 및 통신 시스템 설계 또한 원전관련 규제지침 및 산업표준을 따르도록 설계되어야 한다.

따라서 본 논문은 원전 계측제어계통에서 사이버공격으로부터 방어할 수 있는 수단으로 원전관련 규제지침 및 산업표준에서 제시하는 심층방호 보호모델에 대해서 기술한다. 또한 심층방호 보호모델에서 필수적으로 사용되는 단방향 통신에 적용되는 산업표준 요건인 통신독립성 요건에 대해서 기술한다. 그리고 통신독립성 요건을 만족하기 위해서 제안하는 단방향통신 구조를 가지는 통신보드(CMB : communication board) 개발에 관해서 기술한다. 마지막으로 시험을 통하여 단방향통신 구조를 가지는 통신보드가 심층방호 보호 모델 특성 및 통신독립성 요건을 만족하는지 확인함으로써 사이버공격에 강인하도록 개발되었음을 확인한다.

2장에서는 원전 사이버보안 설계를 위한 원전 계측제어계통 설계에 적용되는 규제지침 및 산업표준, 심층방호 특성, 통신독립성에 대해서 기술하고, 3장에서 제안하는 단방향 통신구조를 적용한 통신보드 구현에 대해서 기술한다. 4장은 단방향 통신 구조를 적용한 통신보드로 구성한 원전 계측제어계통 제어기기를 이용한 시험환경 및 시험결과를 기술하고, 5장에서 결론을 기술한다.

2. 원자력발전소 사이버보안

2.1 개요

원전 계측제어계통은 보호, 제어 및 감시기능을 자동이나 수동으로 작동하는 제반장치 및 설비이며, 원전 계측제어계통은 사이버공격으로 인하여 고장이나 이상 발생 시에 고장안전(fail-safe) 개념에 의하여 원자로의 정지 및 심각한 경우 방사선 누출 등의 중대사고까지 이어질 수 있다. 따라서 최근 원전 관련 규제기관 및 산업표준 기관은 원전 계측제어계통의 설계 및 운영시 필요한 사이버보안 계획, 정책, 이행 및 운영 방안을 제시하고 이를 준수하여 설계, 개발 및 운영하도록 요구한다.

2.2 규제지침 및 산업표준

국내 원전에서 많이 적용되는 규제지침으로는 미국의 원전 규제기관인 미국 원자력 규제위원회 (U.S. NRC : U.S. Nuclear Regulatory Commission)에서 발행한 10CFR(Code of Federal Regulatory) 및 Regulatory Guide(이하 R.G)가 있으며, 원전에 많이 적용되는 산업표준으로서 IEEE에서 발행하는 표준문서가 있다.

R.G 1.152 (2006년) "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"는 원전에서 디지털 안전계통을 설계할 때 생명주기(life cycle)에 따라 사이버보안을 적용하여 설계하여야 한다는 사이버보안 지침을 기술한다[1]. R.G 5.71은 어떤 시스템을 원전에 적용하기 위해서는 적용되는 사이버보안 계획, 정책을 비롯하여 설계, 구현, 시험, 설치, 운영 등 각 생명주기 단계별로 적용되어야 할 기술적/관리적/행정적 조치 사항을 상세하게 기술하고 있으며, 기술적으로는 사이버공격에 대비하여 심층방호(Defense-in-Depth) 보호모델을 수립하고 이에 따른 계측제어계통 구조를 설계할 것을 요구한다[2]. 원전 안전계통에 디지털 컴퓨터 사용에 대한 산업표준인 IEEE Std. 7-4.3.2 (2010년)는 R.G 1.152(2006년)의 사이버보안 내용을 반영하여 5.9절 “접속제어”을 통하여 인적보안, 물리적보안 및 사이버보안에 대한 내용 및 생명주기에 따른 보안 요건을 제시하며, 부록 E를 통하여 통신독립성 요건을 제시하고 있다[3].

2.3 심층방호 보호 모델

원전의 안전계통을 설계함에 있어 안전성과 높은 신뢰도를 확보하는 것이 중요하다. 이러한 요건을 해결하기 위해서는 다중성을 통한 신뢰성 확보와 안전성 확보 등의 방법이 있다. 일반적으로 원전의 안전계통은 다중성을 위하여 네 채널을 구성하지만, 네 채널로 구성된 다중 계통에서 하나의 원인으로 인한 공통원인고장(common cause failure)의 발생 시에 다중성을 통하여 구축해 놓은 안전성과 높은 신뢰성이 동시에 무너져 안전계통이 원하는 기능을 수행하지 못하는 문제점이 있어 왔다. 이에 따라 원전의 안전성을 확보하기 위하여 제어계층, 보호계층(또는 원자로정지계층), 공학적안전설비작동계층 그리고 감시 및 수동조치계층으로

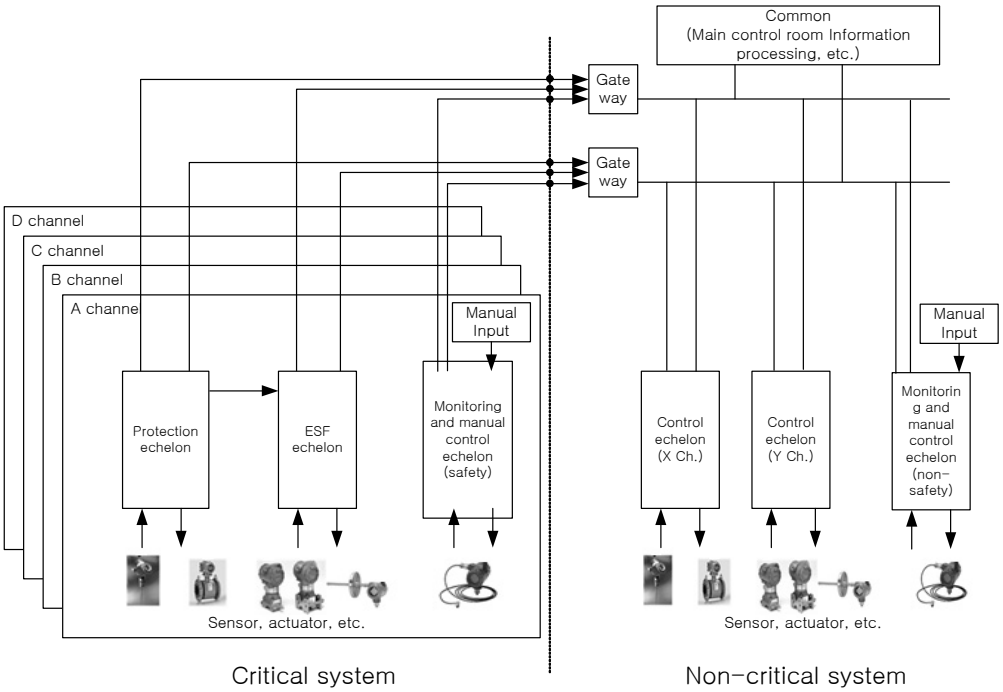


Fig. 1. Defense-in-depth hierarchical structure in I&C system of NPP

구성되는 심층방호 및 다양성을 만족하도록 설계하여 공통원인고장에 대비하도록 요구한다. 그리고 네 개의 방어계층들 중에서 적어도 두 계층의 기능들이 공통원인고장에 의해 동시에 영향을 받지 않아야 함을 요구한다.

이러한 심층방호 보호 개념은 사이버보안과 관련해서 필수계통(critical system)과 비필수계통(non-critical system), 그 외 지원계통 및 행정계통 간의 접근 전략으로 적용된다. 여기에서 필수계통은 원전의 안전 및 보호에 관련한 기능을 수행하는 안전계통 및 안전등급 기기이다. 비필수계통은 필수계통으로 분류되지 않는 계통들을 말한다. 위에서 언급한 심층방호 4개 계층 중에서 보호계층 및 공학적안전설비작동계층이 필수계통에 해당하며, 제어계층은 비필수계통에 해당한다. 감시 및 수동조치계층은 필수계통 및 비필수계통에 필요한 설비를 제공한다. Fig. 1은 원전 심층방호 계층 개념의 일반적인 연계 구조를 보여준다.

사이버보안과 관련한 심층방호 보호 모델은 사이버공격에 대응하고 사이버공격으로 인한 피해를 완화하고, 복구를 위한 총체적 보호 전략이다. 심층방호 보호 모델의 심층방호 구조는 방벽으로 보호하는 다중의 계층 구조로서 단일 보호 방벽의 훼손 또는 단일 보안 통제의 무력화가 원자력발전소의 안전 및 안전 관련 기능에 손상을 주지 않도록 다단계로 방지하는 역할을 수행한다[4].

R.G 5.71은 심층방호 보호모델에 관한 예시와 구체적인 허용 가능한 심층방호 보호 구조로서 아래와 같은 사항을 계측제어계통 설계에 포함하여야 한다고 제시한다[2].

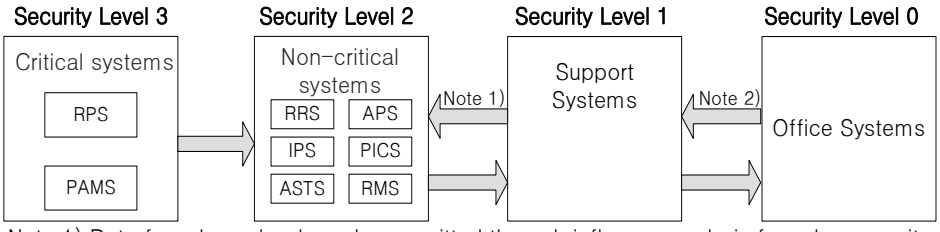
- 필수계통에 사용되는 필수자산은 보안레벨 최고등급으로 설정하고 낮은 보안레벨로부터 보호
- 보안레벨 최고등급에서 다음 하위등급으로는 오직 단방향 데이터 흐름만 허용
- 낮은 보안레벨의 디지털 자산으로부터의 상위 보안레벨 디지털 자산의 통신 개시는 금지
- 사이버공격을 탐지, 예방, 지연, 완화 및 복구할 수 있는 기능을 구비

R.G 5.71에서 가장 핵심적인 부분은 위의 구체적인 요건에서 두 번째 항목, 필수계통으로 구성되는 보안레벨 최고등급에서 비필수계통으로 구성되는 낮은 보안 레벨로의 통신은 단방향 데이터 흐름으로 구성되어야 하며, 세 번째 항목, 역방향의 통신 개시는 금지되어야 한다는 것이다. 이는 원전 계측제어계통의 필수계통 설계시 반드시 준수해야 하는 IEEE Std. 7-4.3.2의 통신독립성 항목과 일치하는 항목이다. 아래 2.4절은 IEEE Std. 7-4.3.2에서 제시하는 통신독립성에 관해서 기술한다.

R.G 5.71의 심층방호 보호 모델을 본 논문에 적용한 원전 계측제어계통의 심층방호 보호 모델의 사용 예시는 Fig. 2와 같다. 필수계통을 보안레벨 3로 최고등급으로 설정하였으며, 보안레벨 3에서 보안레벨 2로 단방향으로 설정하고, 보안레벨 2에서 보안레벨 3로는 역방향의 통신개시가 불가능하도록 설정하였다[4].

2.4 통신독립성

통신독립성이란 원전 계측제어계통 설계 관련 요건 중에서 필수계통의 채널간 통신 또는 필수계통과 비필수계통간의 통신시 적용되는 것으로서, 상기 기기간에는 물리적으로 분리된 기기를 사용하여야 하고 타채널 또는 비필수계통의



Note 1) Data from lower level can be permitted through influence analysis for cyber security and via IDS/IPS security device
Note 2) Data from lower level can be permitted via IDS/IPS security device

Fig. 2. Example of Defense-in-depth model for cyber security in I&C system of NPP

기기가 필수계통 기기의 기능을 저해하지 않아야 한다는 독립성 요건을 만족하기 위한 하나의 필요조건이다. IEEE Std. 7-4.3.2는 원전 안전계통에 디지털 컴퓨터 사용과 관련한 요건 및 지침을 제시하는 산업표준으로서, 디지털시스템이 원전 계측제어계통에 사용되면서 디지털시스템 간 통신이 중요하게 되어 통신독립성에 관련한 지침을 부록 E로 제공한다[3]. IEEE Std. 7-4.3.2에서 제시하는 통신독립성 요건을 정리하면 아래와 같다.

- 일대일 연결
- 통신격리
- 전기적 분리
- 핸드쉐이킹 및 인터럽트 사용 금지
- 데이터 건전성 검사

Table 1은 제안하는 단방향통신 구조와 기존 원전의 통신구조에서 통신독립성 측면에서 비교한 것이다.

기존 원전의 경우, IP 또는 MAC 주소 해석, 통신경로 확립, 송신된 데이터의 에러 여부 확인 등을 위하여 양방향 통신 및 역방향 신호전송경로가 존재한다. 즉, 비필수계통으로부터 필수계통으로 신호를 전송받는 구조로 설계하여 현재 규제지침 및 산업표준에서 제시하고 있는 심층방호 보호모델 및 통신독립성 요건을 완전히 만족하지 않는 것으로 분석되었다. 그러나 기존 원전의 경우 비필수계통에서 필수계통으로의 역방향 통신은 운전원의 조치에 의한 수동스위치 동작으로 수행되도록 설계하여 안전하게 비필수계통으로부터 필수계통으로 역방향 신호를 처리할 수 있도록 하였다. 이에 반해 본 논문에서 제안하는 단방향 통신을 지원하는 통신보드는 IP 또는 MAC 주소 해석, 통신경로 확립 등을 사용하지 않도록 통신 프로토콜을 자체 개발하여, 필수계통과 비필수계통간의 통신 또는 필수계통간의 채널간 통신시 운전원 조치가 없어도 가능하도록 설계하였다.

Table 1. Communication independence structure of the existing NPP and the proposed method

	Existing NPP	Proposed method
Electrical isolation	optical cable	optical cable
Communication isolation	Buffering circuit	Buffering circuit and broadcasting communication
Handshake	Yes	No
IP or MAC address Resolution	Yes	No
Communication type	bi-directional communication	uni-directional and bi-directional communication
Protocol	IP/Ethernet	Safety communication protocol
Backward data link	Yes	No
Data integrity	CRC	CRC32

3. 단방향 광통신 구조 설계 및 구현

3.1 단방향 광통신 구조 설계

위에서 기술한 통신독립성을 만족하도록 단방향 통신을 지원하는 통신구조를 제안하고 구현하였다. 먼저 원전 계측제어계통의 통신 구조에 대한 기본적인 방향은 아래와 같이 설정하였다.

1) 양방향 통신

계측제어계통의 제어기기간의 양방향 통신은 광케이블을 사용한 일반적인 양방향 통신을 의미하여, 필수계통의 동일 채널내의 제어기기간 통신에 사용된다.

2) 단방향 통신

본 논문에서 사용하는 계측제어계통 제어기기간의 단방향 통신은 자체 개발한 통신보드에서 제안하는 단방향모드 설정 스위치를 통해 단방향 통신으로 설정된 경우에만 수행되며, 필수계통의 다른 채널간의 제어기기간 통신 및 필수계통의 제어기기와 비필수계통의 정보 및 감시기기로의 단방향 통신에 사용된다. 즉 통신보드는 기본적으로 양방향 통신을 수행하며, 단방향 통신이 필요한 경우에만 통신환경 구성시에 단방향 모드로 설정하도록 하여 단방향통신을 수행하도록 설계하였다. 단방향통신구조는 IEEE Std. 7-4.3.2 의 통신독립성을 만족하기 위한 구조로서, 브로드캐스팅 통신 경로를 통한 통신 격리 및 광케이블 사용으로 전기적 격리를 제공한다.

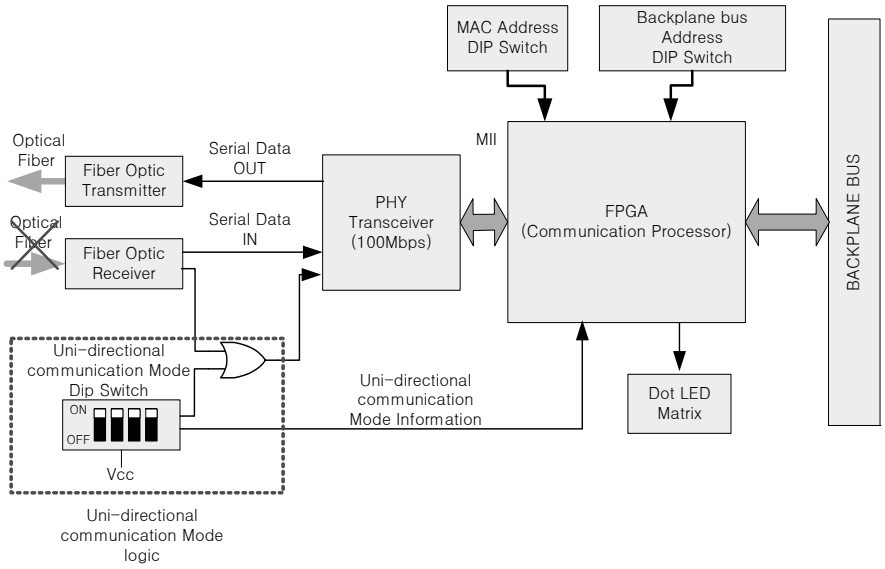


Fig. 3. Design structure of CMB supporting uni-directional communication mode

통신보드는 Fig. 3에서 보이는 단방향 통신모드 설정 스위치의 설정 정보에 따라 단방향 통신 또는 양방향 통신을 수행한다. 기본적으로 단방향 통신 모드가 설정되지 않았을 경우 양방향 통신을 수행한다. 일반적으로 단방향 모드가 설정되지 않았을 경우, 즉 양방향 통신 수행 시에 수신부에 링크가 연결되지 않을 경우 링크가 확립되지 않은 것으로 설정되어 송신부는 데이터 송신이 불가능하게 된다. 그러나 단방향 통신모드가 설정되었을 경우 수신부에 링크가 연결되어 있지 않아도 송신부는 데이터 송신이 가능하도록 하는 것이 본 논문에서 제안하는 단방향 전송모드를 지원하는 통신보드의 핵심 기능이다.

3.2 통신보드 구현

통신보드는 원전 계측제어계통 제어기기간의 통신을 수행하며, 제어기기 내의 중앙처리보드(CPB : CPU Board)로부터 통신 임무를 수행하며, 중앙처리보드와는 독립적으로 동작한다. 단방향 통신 구조를 지원하는 통신보드의 사양은 아래와 같으며, 구현된 통신보드는 Fig. 4와 같다.

- 크기는 6U (1U=44.45mm)
- VME64 백플레인버스 (데이터 및 주소버스 각 32bit)
- 보드 전면에 run, fault 구별 LED
- 보드 전면에 reset 버튼
- 한 쌍의 광 송수신 포트
- 10/100Mbps 급 물리계층 송수신기
- 통신보드 네트워크 물리주소 설정 DIP 스위치
- 제어기기내 VME 주소 설정 DIP 스위치
- 단방향 통신 모드 설정 DIP 스위치
- 송신 및 수신 에러 체크를 위한 CRC32 검사
- LPF (loss pass filter) 및 PLL (phase locked loop)
- ST type의 광 커넥터

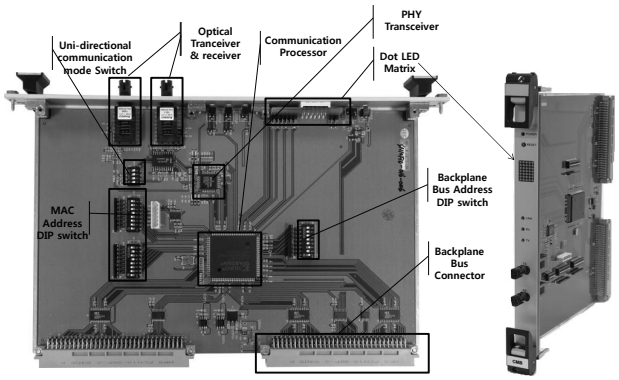


Fig. 4. Implemented structure of CMB

구현된 통신보드는 3 계층의 통신 프로토콜을 사용하며, 이에 따라 통신보드는 3 계층(애플리케이션 계층, 매체접속제어(MAC)계층, 물리계층)의 기능을 수행한다. 애플리케이션 계층에 따른 동작은 중앙처리보드에서 수행되며, 태스크 스케쥴러에 의하여 주기적으로 수행되는 송신 API (application programming interface)와 수신 API를 통하여 통신보드에 송신하려는 데이터를 전송하거나, 통신보드에 수신된 데이터를 애플리케이션이 사용할 수 있도록 가져온다. 통신보드의 MAC계층에서는 데이터프레임의 캡슐화 및 역캡슐화(encapsulation/de-capsulation)를 수행하여 데이터 건전성을 위한 CRC32 검사를 수행한다. 또한 MAC계층에서 단방향통신 모드 설정 정보에 따라 통신보드가 단방향 또는 양방향 통신을 수행하도록 설정된다. 물리계층은 IEEE 802.3 PHY를 사용하며 통신보드와 연결된 링크정보를 MAC계층에 전송 및 전기신호를 광신호로 변환하거나 광신호를 전기신호로 변환하는 등의 기능을 수행한다.

구현된 단방향 통신 구조를 지원하는 통신보드의 요건 적합성을 Table 2와 같이 분석하였으며, 통신보드는 IEEE

Std. 7-4.3.2에서 제시하는 통신독립성 요건을 모두 만족하는 것으로 분석되었다. 또한 통신보드의 통신독립성 요건 만족성은 R.G 5.71에서 제시하는 심층방호 보호모델의 요건을 만족하는 것으로, 심층방호 보호모델의 접근 전략을 만족하는 것으로 검토되었다.

Table 2. CMB Conformance analysis of communication independence

	Conformance	내 용
One-to-one connection	Yes	Supporting one-to-one and one-to-many connection
Communication isolation	Yes	Uni-directional Broadcasting communication
Electrical isolation	Yes	Optical cable as a link media
Handshaking & Interrupt	Yes	- No handshaking for address resolution and link establishment - Independent operation of CMB
Data integrity	Yes	CRC 32 and pre-defined countermeasures

4. 시험 및 결과

4.1 시험환경

개발된 통신보드의 기능 시험을 성능시험을 위하여 제어기기에 통신보드를 탑재하고 아래와 같은 기본적인 9개의 기능시험 항목 및 3개의 성능시험 항목 선정하여 시험계획을 수립하고 시험절차에 따라 수행하였다.

1) 기능 시험 항목
- MAC 주소 인식 기능 시험
- 내부 루프백 (loopback) 기능 시험
- MAC 주소 판별 기능 시험
- 데이터프레임 전송속도 시험
- 양방향 통신 기능 시험
- 단방향 통신 기능 시험
- 통신보드 수신버퍼 기능 시험
- CRC 32 검증 시험
- 보드상태 감지 기능 시험

2) 성능 시험 항목
- 전송속도(transmission speed) 시험
- 전송지연(transmission delay) 시험
- 데이터프레임 손실률(data frame loss rate) 시험

Fig. 5는 단방향 통신 기능 및 성능시험을 위해서 1개의 광케이블을 이용하여 단방향으로만 물리적 링크를 연결한 구성도이며, Fig. 6은 양방향 통신 기능 및 성능시험을 위해서 2개의 광케이블을 이용하여 양방향으로 물리적 링크를 연결한 구성도이다.

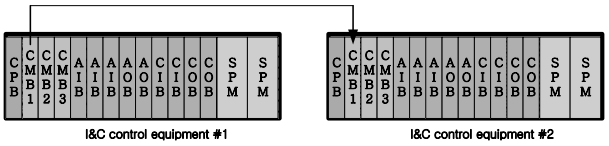


Fig. 5. Uni-directional communication test environment

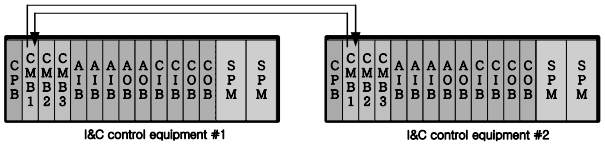


Fig. 6. Bi-directional communication test environment

위 실험에서 사용하는 원전 계측제어계통 제어기기는 모듈 개념으로 안전계통 기능을 수행할 목적으로 개발한 단위제어기로서, 외부로부터 입력신호(아날로그, 접점 및 디지털 신호)를 받아 로직 및 알고리즘 수행을 통한 할당된 제어기능을 수행하고 다른 제어기기로 수행된 결과를 전송하는 기능을 수행한다. Fig. 7은 중앙처리보드 및 여러 입출력보드로 구성된 단위제어기로 구성된 제어기기의 예시이다.

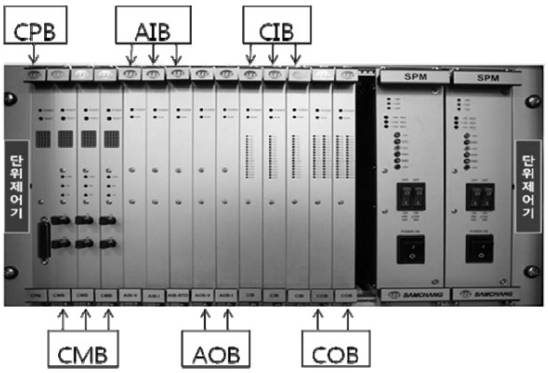


Fig. 7. Example of control module in NPP I&C system

하나의 제어기기는 최대 14장의 보드를 장착할 수 있으며, 중앙처리보드(CPB) 및 다수의 통신보드(CMB), 아날로그입력보드(AIB, analog input board), 아날로그출력보드(AOB, analog output board), 접점입력보드(CIB, contact input board) 및 접점출력보드(COB, contact output board) 등으로 구성할 수 있다. 여기에 2개의 전원공급기(SPM, subrack power module)가 장착된다. 본 실험에서 사용되는 제어기기의 구성은 사용되는 기능 및 목적에 따라 각 보드의 수량을 다르게 할 수 있다.

원전 계측제어계통 제어기기간의 통신을 위해서 여러 개의 제어기기를 이용하여 원전 계측제어계통의 주요 계통인 원자로보호계통을 2채널로 구성하였다. 원자로보호계통은 제어할 수 없는 출력 폭주에 대응해서 원자로 정지와 같이 반응도를 신속하게 줄일 수 있도록 설계된 안전 계통이다. 원자로보호계통의 경우 보팅(voting) 논리를 위하여 보통 4채널로 구성하는데, 본 시험에서는 2채널만을 구성하고 나

머지 2채널은 시뮬레이션 입력을 받아서 처리하도록 설정하여 시험을 구성하였다. Fig. 8과 9는 원자로보호계통 2채널 시험 구성환경 및 시험구성 환경의 논리구조도를 보여준다. 그림에서 PIS(process instrumentation system)는 공정계측계통, NIS(nuclear instrumentation system)은 핵계측계통, SCOPS(SMART core protection system)은 노심보호계통의 계측제어계통을 의미하며, BSM(bistable moduel)은 비교논리모듈, CCM(coincidence module)은 동시논리모듈을 의미하여 원자로보호계통(RPS :reactor protection system)을 구성하는 모듈들이다. 원자로보호계통의 각 모듈은 제어기기로 구성되고, 제어기기기는 여러 통신보드를 이용하여 다른 모듈의 통신보드와 일대일통신(1:1)을 수행한다. 이중에서 보통 4개의 채널로 구성되는 원자로보호계통의 보팅(voting) 논리 수행에 필요한 데이터 교환을 위하여 채널간 통신을 수행하는데, 이때 통신독립성이 요구된다. 본 논문에서 제안된 단방향 통신 구조를 가지는 통신보드는 이러한 채널간 통신에 사용되며, 통신보드를 단방향 통신 모드로 설정하여 단방향으로만 데이터를 전송한다. 이를 통해 수신 받는 쪽의 오류 또는 고장이 송신하는 쪽으로 전송이 불가능하게 되어 송신하는 쪽의 기능을 저해하지 않도록 하였다.

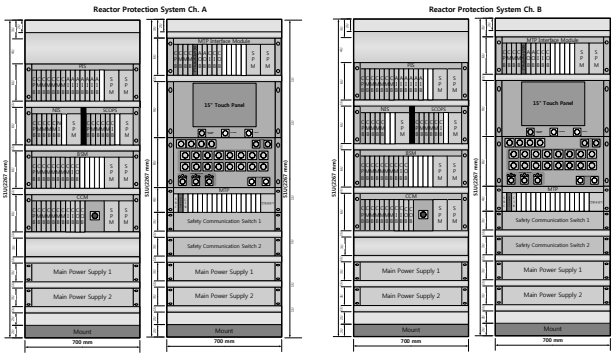


Fig. 8. Test configuration for inter-channel communication independence of critical system
(Reactor protection system 2 channels)

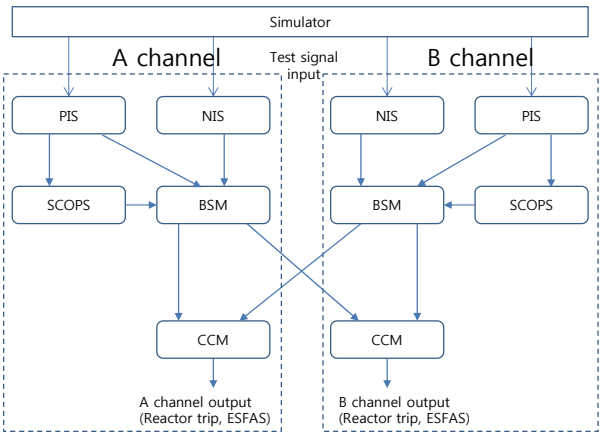


Fig. 9. Logic structure of test configuration for inter-channel communication independence of critical system

4.2 시험결과

본 논문에서 제안하는 단방향통신을 지원하는 통신보드는 4.1절에서 기술한 단방향 및 양방향 시험환경(Fig. 5 및 Fig. 6)에서 수행한 기능시험 및 성능시험에서 기능시험 허용기준 및 성능시험 허용기준을 통과하였다. Table 3은 통신보드의 전송속도 성능시험 결과를 보여준다. 통신보드는 10Mbps의 전송속도를 가지도록 설계 및 구현되었으며, 이는 통신보드가 사용하는 고정된 크기의 512byte 데이터프레임을 초당 2,442개를 전송할 수 있음을 의미한다. Table 3과 같이 통신보드는 2,442개의 데이터프레임을 약 0.97 초 내에 전송함으로서 10Mbps의 전송속도를 만족하는 것으로 확인되었다.

Table 3. Test results of CMB transmission speed
(Unit : seconds)

	Average	Min	Max	Std. Dev
Unicast (bidirectional)	0.97656635	0.976345	0.977556	0.000354
Broadcast (bidirectional)	0.97652655	0.975415	0.977556	0.000543
Unicast (uni-directional)	0.97645395	0.975915	0.976824	0.000336
Broadcast (uni-directional)	0.97649645	0.975956	0.976824	0.000307

성능시험 항목인 전송지연 허용기준은 1ms 이하로 설정하였으며, 통신보드의 전송지연 시간은 502 *us*로 허용기준을 만족하였다. 데이터프레임 손실률 허용기준으로 BER (bit error ratio)를 10^{-9} 이내로 설정하였으며, 이는 통신보드가 사용하는 고정된 크기의 512 byte의 데이터프레임을 사용하여 통신시험시 244,141개의 데이터프레임을 오류 없이 전송하는 것과 같다. 데이터프레임 손실률 시험결과는 허용기준을 만족하였다. 또한 통신보드의 통신독립성 시험을 위해 구성한 필수계통 채널간 통신독립성 시험 환경(Fig. 8 및 Fig. 9)에서 A 채널 비교논리모듈 제어기기의 오류 또는 고장신호의 전송시에도 B채널의 동시논리모듈은 정상동작하고 있음을 확인하였으며, 이때 위의 성능시험 항목에 대해서도 동일한 성능을 보여주었다.

5. 결 론

최근 디지털화된 원전 계측제어계통에 대한 사이버공격 위협이 증가하고 있으며, 원전 계측제어계통의 설계는 점차 증가하고 있는 사이버공격 위협으로부터 보호하기 위하여 사이버보안 대책을 수립하고 이를 설계에 반영하여야 한다. 본 논문에서는 사이버보안 대책으로 심층방호 보호모델을 적용함에 있어서 필수적으로 사용되는 단방향 통신을 제공하기 위한 단방향 통신 모드 설정 방법을 제안하였다. 제안한 방법은 원전 계측제어계통 통신에 사용되는 통신보드를

통해 구현하였으며, 통신보드의 기능시험, 성능시험 및 통신 독립성 시험을 통하여 제안하는 단방향통신 모드 설정 방법이 현재 규제지침 및 산업표준에서 제시하고 있는 심층방호 보호모델 및 통신독립성 요건을 만족하고 있는 것으로 확인되었다. 제안된 방법을 포함한 통신보드는 원전 계측제어계통 제어기기에 장착되며, 일체형원자로 계측제어계통 중에서 필수계통에 해당되는 원자로보호계통 및 공학적안전설비 제어계통 구현에 사용되었다.

참 고 문 헌

[1] Regulatory Guide 1.152, Revision 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”, U.S. Nuclear Regulatory Commission, 2006.

[2] Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”, U.S. Nuclear Regulatory Commission, 2010.

[3] IEEE Std. 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”, IEEE Power & Energy Society, 2010.

[4] K. I. Jeong, et al., “Trend of Cyber Security in Instrumentation and Control Systems of Nuclear Power Plant,” Korea Information Processing Society Review, Vol.19, No.05, pp.69-77, 2012.

정 광 일

e-mail : hisunny@kaeri.re.kr

1997년 전북대학교 전자공학과(학사)

1999년 전북대학교 전자공학과(석사)

2003년 전북대학교 전자공학과(박사)

2003년~2004년 한국표준과학연구원

2004년~현 재 한국원자력연구원 연구로공학부 책임연구원

관심분야 : I&C System, Cyber Security, Communication System

이 준 구

e-mail : jklee@kaeri.re.kr

1998년 충남대학교 전기공학과(학사)

2000년 충남대학교 전기공학과(석사)

2011년 충남대학교 전기공학과(박사수료)

2000년~현 재 한국원자력연구원 연구로공학부 선임연구원

관심분야 : I&C System, FPGA, Cyber Security

박 근 옥

e-mail : gopark@kaeri.re.kr

1986년 경기공업개방대학 컴퓨터공학과(학사)

1993년 충남대학교 전산학과(석사)

2006년 공주대학교 전산학과(박사)

1987년~현 재 한국원자력연구원 연구로공학부 책임연구원

관심분야 : I&C System, Cyber Security, Software V&V