

## 원자력 안전등급 제어기기의 통신망을 위한 통신보드 설계

이동일<sup>1</sup> · 류광기<sup>2\*</sup>

### Design of Communication Board for Communication Network of Nuclear Safety Class Control Equipment

Dongil Lee<sup>1</sup> · Kwangki Ryoo<sup>2\*</sup>

<sup>1</sup>Research Institute, PONUTech Co., Ltd., Seoul, Korea

<sup>2</sup>Department of Information and Communication Engineering, Hanbat National University, Daejeon, Korea

#### 요 약

본 논문에서는 원자력 안전등급 제어기기의 안전 통신망 구현을 위한 원자력 안전등급 통신 보드를 제안한다. 원자로 보호시스템이 아날로그에서 디지털화되면서 디지털 통신망을 사용하게 되었다. 디지털 통신망은 원자력 안전등급에 사용되는 통신망으로 안전등급에서 요구하는 성능 및 시험을 통과한 통신보드가 제공되어야 한다. 통신 프로토콜 계층은 OSI 7 계층 중 물리계층, 데이터링크 계층, 어플리케이션계층만을 사용한다. 데이터 링크 계층에서는 사이버 보안을 위해 데이터 패키지를 변경하였다. 데이터 건전성을 위해 CRC32를 사용 하였으며 데이터 수신에 대해서는 재요청 및 응답을 하지 않는 단방향 통신만을 함으로써 원자력 안전시스템에 영향을 주지 않게 설계 되었다. 또한 원자력안전등급을 획득하기 위해서 요건, 설계, 검증의 절차에 따라 설계하였다. 하드웨어검증을 위해 전자파 시험, 노화분석 시험, 육안검사, 번인시험, 내환경 시험 및 내진 시험과 같은 기기 검증을 수행 하였다. 또한 FPGA 펌웨어 검증을 위해 IEEE 1074의 생명주기를 준수하여 단위시험과 통합 시험을 실행 하였다[1-3].

#### ABSTRACT

This paper suggest the safety class communication board in order to design the safety network of the nuclear safety class controller. The reactor protection system use the digitized networks because from analog system to digital system. The communication board shall be provided to pass the required performance and test of the safety class in the digital network used in the nuclear safety class. Communication protocol is composed of physical layer(PHY), data link layer(MAC: Medium Access Control), the application layer in the OSI 7 layer only. The data link layer data package for the cyber security has changed. CRC32 were used for data quality and the using one way communication ,not requests and not responses for receiving data, does not affect the nuclear safety system. It has been designed in accordance with requirements, design, verification and procedure for the approving the nuclear safety class. For hardware verification such as electromagnetic test, aging test, inspection, burn-in test, seismic test and environmental test in was performed. FPGA firmware to verify compliance with the life-cycle of IEEE 1074 was performed by the component testing and integration testing.

**키워드** : 안전통신망, 원자력 제어기기, 원자력 통신보드

**Key word** : Safety communication, MMIS, Nuclear communication board

접수일자 : 2014. 11. 17 심사완료일자 : 2014. 12. 12 게재확정일자 : 2014. 12. 26

\* **Corresponding Author** Kwangki Ryoo(E-mail:kkryoo@gmail.com, Tel:+82-42-821-1710)

Department of Information and Communication Engineering, Hanbat National University, Daejeon 305-791, Korea

**Open Access** <http://dx.doi.org/10.6109/jkiice.2015.19.1.185>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.  
Copyright © The Korea Institute of Information and Communication Engineering.

## I. 서 론

기존의 아날로그 기술을 이용한 가동 원전의 계측제어계통은 기기 및 부품의 노후화로 성능과 신뢰성의 저하, 불시정지 발생빈도의 증가, 이용률 제고를 위한 신기술의 적용곤란, 기기의 단종문제 등으로 운전 및 유지보수 측면에서 경제적 부담이 가중되는 추세이다. 기존 원자력발전소의 노후화된 기기의 교체가 심각한 문제로 대두되고 있고 이러한 문제점을 해결하기 위하여 전반적인 디지털 기술의 도입과 새로운 기술 및 기법이 적용되고 있는 추세이며, 신규 원자력발전소, 중소형 원자로 및 연구용 원자로의 계측제어계통 설계에도 디지털 기술의 적용이 불가피한 실정이다[4].

본 연구는 펌웨어 개발수명주기에 따른 계획단계, 요건단계, 설계단계, 구현단계와 통합 및 검증단계의 단계별 확인 및 검증에 대한 내용을 포함하고 있다.

안전통신망 통신 보드는 디지털 계측제어계통의 제어기에 적용할 수 있도록 설계되고 제작되었다. 디지털 계측제어계통에의 제어기기 안전등급 통신보드를 도입함으로써 부품단종 문제점 해결 및 예비부품 확보를 용이하게 하였으며, 단방향 데이터링크 사용으로 인한 통신의 복잡성 감소와 광케이블 사용으로 전기적 격리 용이성 및 전자파 영향 감소를 시켰다.

안전등급 통신보드는 원자력 디지털 계측제어계통의 안전등급 통신망 설계에 적용하기 위하여 개발하였고, 펌웨어 개발 수명주기에 따라 확인 및 검증 업무를 수행하였으며, 내진 시험, 내환경 시험 및 전자파 시험을 포함하는 기기검증 시험을 수행하여 성능을 확인하였기에 원자력 디지털 계측제어계통의 안전등급 통신망에 적용할 수 있음을 입증하였다.

## II. 관련 연구

### 2.1. 원자력 안전등급 분류

품목 또는 용역이 원자력발전소 안전성 및 신뢰성에 미치는 영향의 중요도에 따라 다음과 같이 품질등급을 Q, A, S로 구분하여 운영한다.

#### 2.1.1. 안전성등급(Q)

고장 또는 결함 발생시 일반인에게 방사선 장애를 직

접 또는 간접으로 미칠 가능성이 있는 원자로 및 원자로의 안전에 관련된 품목 또는 용역에 적용된다.

#### 2.1.2. 안전성영향등급(A)

안전관련 구조물, 계통 및 기기에 해당되지 않으나 다음의 각 항에 해당하는 품목 또는 용역은 A등급으로 분류 관리하며, 설계, 구매, 시공 및 운전을 위해 지정되어 있는 적절한 품질보증요건이 적용된다.

#### 2.1.3. 일반산업 등급(S)

상기 Q, A등급으로 분류되지 않은 품목이나 용역에 적용된다.

## 2.2. 원자력 안전등급 제어기기 설계

프로세서 보드, 통신 보드, 아날로그 입력 보드, 아날로그 출력 보드, 디지털 입력 보드, 디지털 출력 보드, 전원공급기 등으로 이루어진다. 서브랙 크기는 19인치 6U 사이즈로 제작되며, 최대 15슬롯까지 장착 가능하도록 설계되어 있다. 버스의 기본 주파수는 50Mhz를 사용하며, Data, Adress, nCS, nRD, nWR, WnR, nREADY, nSYSRST 신호를 사용한다.

## III. 구 현

### 3.1. 안전통신망

#### 3.1.1. 안전통신망 구조

안전제어기기 플랫폼을 구성하는 노심보호계통(SCOPS), 플랜트보호계통(BSM & CCM), 계측계통(IS) 및 MTP는 그림 1과 같이 일대일 데이터 링크를 사용하여 연계된다.

#### 3.1.2. 안전통신망의 기능 요건

안전통신망은 OSI(Open System Interconnection)에서 제시하는 7 계층의 프로토콜에서 1계층(물리계층(Physical Layer)), 2계층(데이터 링크 계층(Data Link Layer)) 및 7계층(애플리케이션 계층(Application Layer))을 사용하여야한다. 물리계층은 물리매체를 통하여 데이터 전송 및 수신에 필요한 기능을 가지며, 데이터 전송을 위한 물리적 매체는 전기적 격리 및 EMI(Electro-Magnetic Interference) 특성이 우수한 광케이블을 사용

한다. 또한 4B/5B의 블록 코딩 방식과 DC Component의 방지를 위한 NRZI (Non-Return-to- Zero-Invert) 인코딩 방식을 사용한다.

데이터링크 계층은 OSI 표준에서 정의하는 데이터링크 계층은 매체접근제어 계층(MAC, Medium Access Control)과 논리링크제어 계층(LLC, Logical Link Control)으로 세분화된다. 논리링크제어 계층은 OSI 계층구조에서 3계층인 네트워크 계층과 연계하는 세분화된 계층으로서, SECOP-Q 데이터 통신은 3계층의 네트워크 계층을 사용하지 않으므로, 논리링크제어 계층은 사용하지 않는다.

안전통신망은 매체접근제어를 위해서 주소 체계를 각 데이터 프레임에 송신지 주소 및 목적지 주소를 할당하여 통신 노드 간에 데이터 프레임의 교환이 가능하도록 별도의 주소체계를 사전에 설정하여 사용한다.

어플리케이션 계층은 프로세서보드에서 어플리케이션 계층에 해당하는 실제 데이터 전송, 실제 데이터 수신, 다른 통신 노드 감시, 통신보드의 송·수신 버퍼 상태 감시의 기능을 수행한다.

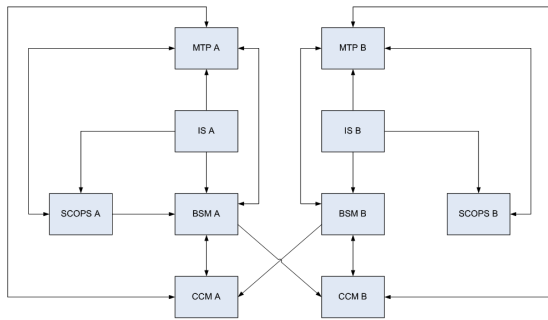


그림 1. 안전제어기기 안전통신망 구조도  
Fig. 1 Structure diagram of safety communication

### 3.2. 안전등급 통신보드 하드웨어

#### 3.2.1. 하드웨어 구조

통신보드는 프로세서보드(CPB : CPU Board)의 데이터를 연계된 서브랙과 송·수신하며, 통신보드는 FPGA(Field Programmable Gate Array), 물리계층 칩(PHY 칩), Transmitter, Receiver와 전면에 모듈의 상태를 표시하는 Dot-Matrix 등으로 구성된다. 또한 프로그램을 다운로드할 수 있는 JTAG(Joint Test Action Group) 포트가 제공된다.

### 3.3. 안전등급 통신보드 펌웨어(FPGA)

#### 3.3.1. 개발환경

JTAG 에뮬레이터를 통해 FPGA에 데이터를 다운로드할 수 있는 개발 연계를 제공하며, 펌웨어 개발을 위하여 그림 2과 같은 개발 환경을 제공하여야 한다.

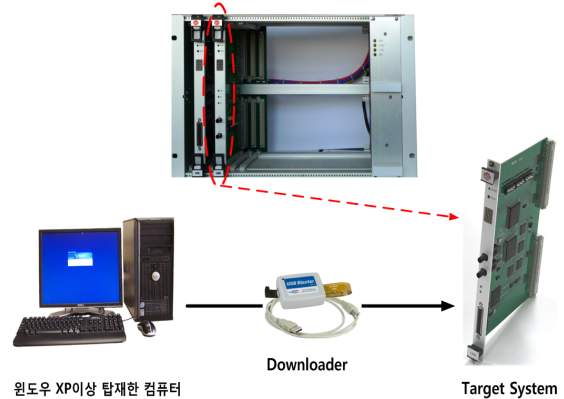


그림 2. 펌웨어 개발 환경  
Fig. 2 Firmware development environment

#### 3.3.2. 펌웨어 구조

통신은 모두 단방향 링크만 허용되므로, 통신 프로토콜은 Feedback 정보를 사용할 수 없는 제한사항을 가지고 있다. 따라서 송신데이터의 정상 전송 확인 및 흐름 제어 등의 기능들은 사용할 수 없다.

통신보드는 각 서브랙에 프로세서보드(CPB : CPU Process Board)와 인접하여 장착이 되며, backplane을 통하여 연계된다. CMB의 수신 포트를 통하여 수신되는 데이터 패킷은 backplane을 통하여 CPB로 전달되고 반대로 CPB로부터 타 서브랙의 노드로 송신되는 데이터 패킷은 backplane을 통하여 CMB에 업로드 된다.

통신보드 펌웨어는 통신 연계 제어 모듈, 매체 독립 연계 관리 모듈, BACKPLANE 연계 제어 모듈 및 기타 모듈로 구성된다. 통신보드 전송 속도는 10 Mbps로 펌웨어에서 속도를 제어한다. 또한 DIP 스위치 입력으로부터 MAC 및 Backplane Bus 어드레스를 받아 설정한다.

#### 3.3.3. 펌웨어 설계

통신보드에 대한 블록도는 그림 3과 같은 구조를 가지며, FPGA 내부의 펌웨어 블록도는 그림 4와 같다.

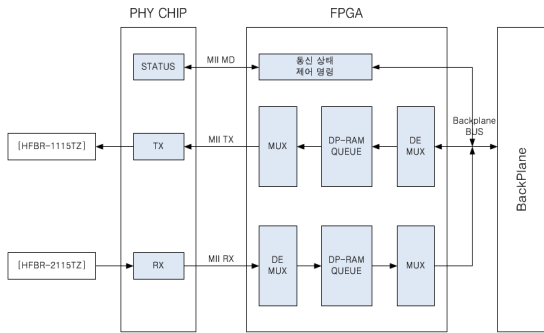


그림 3. 통신보드 블록도  
Fig. 3 Block diagram of communication board

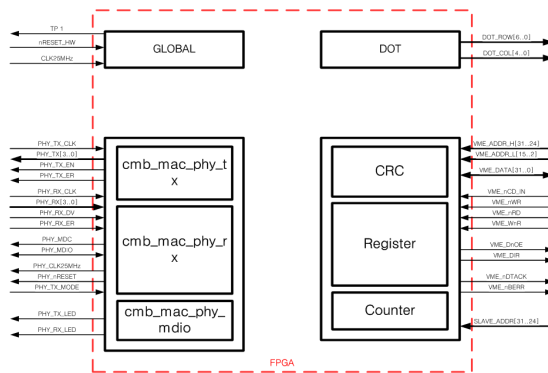


그림 4. 통신보드 펌웨어 블록도  
Fig. 4 Firmware block diagram

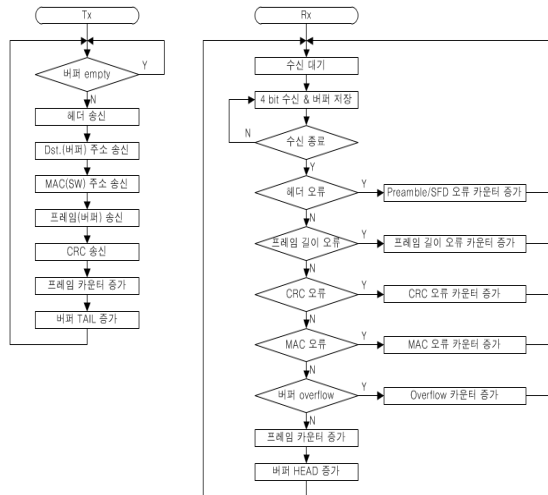


그림 5. 통신보드 펌웨어 내부 Tx(좌), Rx(우) 흐름도  
Fig. 5 Tx(L), Rx(R) flow of communication board

통신보드 펌웨어는 크게 통신 연계 제어 모듈, 매체 독립 연계 관리 모듈, BACKPLANE 연계 제어 모듈 및 기타 모듈로 구성되며, 통신보드 펌웨어의 전체적 흐름을 간략히 그림 5에 나타내었다.

#### IV. 안전등급 통신보드 검증

##### 4.1. 통신 보드 형상

통신보드의 실물외형은 그림 6와 같다. 안전등급 요건을 충족하기 위한 ST type의 광케이블 커넥터가 좌상에 위치 해있으며, FPGA가 중앙에 있는 것을 확인할 수 있다.

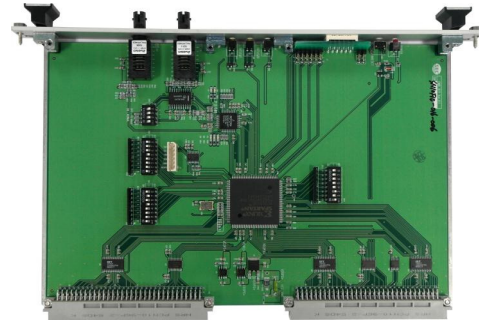


그림 6. 통신보드 실물형상  
Fig. 6 Shape of communication board

##### 4.2. 펌웨어 검증 모델

원자력 안전등급의 펌웨어는 그림 7의 IEEE1074 V-Model life cycle에 맞게 개발 및 검증이 진행 되어야 한다.

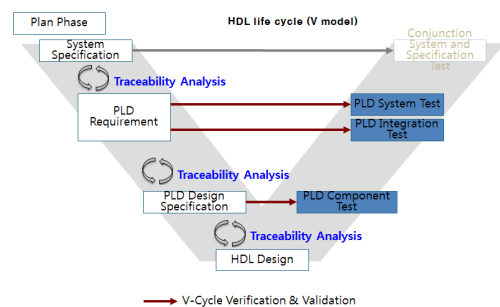


그림 7. IEEE1074 소프트웨어 생명주기 (V-Model)  
Fig. 7 IEEE1074 Software Life Cycle (V-Model)

### 4.3. 하드웨어 단위시험 환경

통신 보드 하드웨어 단위시험 환경은 시험 장비를 통하여 프로세서 보드(CPB)의 주요 부품 및 소자를 시험한다. 통신 보드 하드웨어 단위시험을 위한 기본적인 시험환경은 모든 입출력 변수 및 예상 결과치를 확인할 수 있는 능력이 있어야 한다. 시험에 필요한 장비는 개발 모듈(Target System), 개발 모듈을 장착하는 1개의 서브랙, 확장보드, 서브랙 전원모듈(SPM : Subrack Power Module), 출력확인 장비, Multi-Tester 1대, Oscilloscope 1대 등이다.

### 4.4. 펌웨어 단위시험 환경

통신보드 펌웨어 단위시험을 위해 펌웨어 및 Test Bench를 실행 시킬 수 있는 시뮬레이션 환경이 제공되어야 한다. Test Bench 는 구동되는 시스템 신호를 기준으로 구현하며, 연계장치를 모델링하여 구성하거나 연계신호에 대한 Timing을 생성할 수 있어야 한다. 통신 보드 펌웨어 단위시험을 위한 필요 장비는 시뮬레이션을 위한 Host 컴퓨터와 검증도구(ModelSim, NC-Sim)이다.

### 4.5. 펌웨어 통합시험 환경 및 선수 조건

#### 4.5.1. 하드웨어

시험환경의 하드웨어 구성은 윈도우XP 이상의 운영 체계를 탑재한 Host 컴퓨터와 프로세서가 탑재된 Target System 및 Host 컴퓨터와 Target System을 연결하는 에뮬레이터로 구성된다.

통신보드 펌웨어 통합시험을 수행하기 위한 환경과 입출력 시험에 필요한 장비로 개발 모듈(Target System)을 장착하는 1개의 서브랙, Emulator 1 set, Host Computer 1 대, 시험 소프트웨어 (Code Composer Studio v3.3), 출력 확인 장비인 Multi-Tester 1대, Logic Analyzer 1대이다(그림 8).

#### 4.5.2. 단위시험

통신보드 펌웨어 통합시험을 위해 제공되는 펌웨어 소스코드는 단위시험이 완료된 상태의 버전이어야 한다.

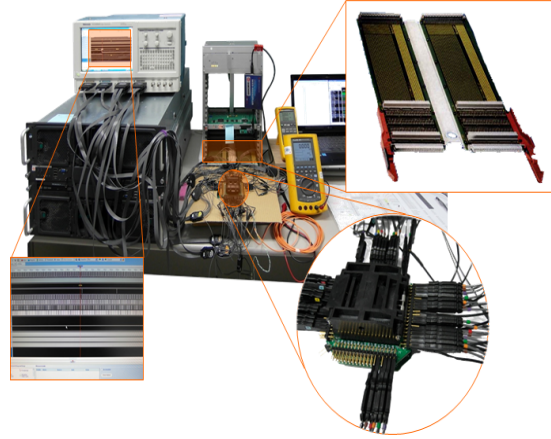


그림 8. 펌웨어 통합시험 환경  
Fig. 8 Firmware integration test environment

#### 4.5.3. 단위시험 및 통합시험 결과

Link 및 Loop-Back 기능과 타이밍에 관한 시험 결과는 각각 그림 9 및 그림 10과 같이 시험 사례의 입력에 따른 시험 출력변수 값이 예상 출력변수 값과 일치하였고 시험 허용기준을 만족하였다.



그림 9. 기능 테스트 (LINK-RSP\_LINK)  
Fig. 9 Functional test (LINK-RSP\_LINK)

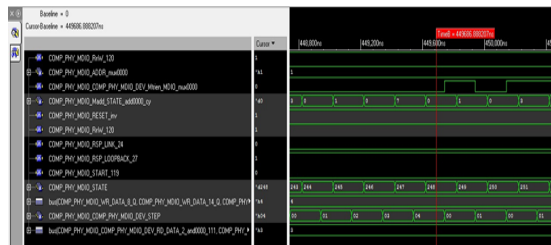


그림 10. 타이밍 테스트 (LINK-RSP\_LINK)  
Fig. 10 Timing test (LINK-RSP\_LINK)

펌웨어 통합시험이 끝난 뒤, 펌웨어가 내장된 FPGA가 삽입된 보드의 견전성을 확인하기 위한 송신 및 수신 시험을 진행한다. 프로세서보드에서 송신 데이터를 생성하고 통신보드를 거쳐 다시 프로세서보드로 수신된 데이터가 동일한지를 그림 11과 같이 확인함으로써 통신보드의 작동 상태를 시험하게 된다. 데이터 정밀도를 측정하기 위해  $10^8$  이상의 데이터 프레임을 전송하여 데이터 손실율(BER)이  $10^{-9}$ 을 만족함을 확인하였다.

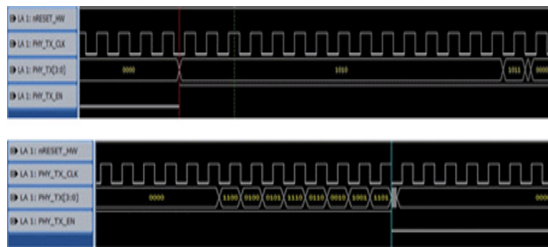


그림 11. 실제 송수신 데이터 비교  
Fig. 11 real data compare for Tx, Rx

#### 4.6. 기기 검증

기기검증은 주어진 온도, 습도, 압력, 방사능에 관한 시험 조건에 따라 그림 12와 같이 전자파 시험, 노화 분석, 육안 검사, 번인 시험, 내환경 시험, 내진 시험을 진행하였다[5,6].

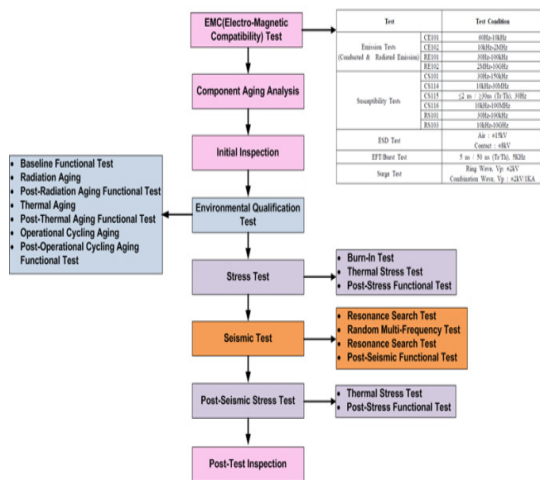


그림 12. 기기검증 절차  
Fig. 12 Equipment verification procedure

## V. 결론

원자력 안전등급 제어기기는 원자력 품질등급 Q등급에 해당하는 제어기기로 원자력 발전소 고장 또는 결함 발생시 일반인에게 방사선 장애를 직접 또는 간접으로 미칠 가능성이 있는 원자로 및 원자로의 안전에 관련된 품목이다. 그러므로 제어기 설계에는 요건에 부합하는 설계과정과 검증을 수행하여 인허가를 획득해야한다.

본 논문에서는 안전등급 제어기기의 안전등급 통신망을 구성하는 통신보드를 설계하여보았다. 원자력 안전등급의 요건을 먼저 분석하고, 개발 절차에 맞는 형상관리로 설계를 하였다. 일반적인 상용 Ethernet Package를 원자력 안전등급 통신망을 위해 Package를 변형 하여 FPGA로 설계하였다.

원자력 안전등급 통신보드 설계에서 가장 중요한 것은 검증 및 시험에 있다. 검증과정은 설계 시작과 동시에 검증에 대한 계획을 수립하고 그에 맞게 진행을 한다. 하드웨어는 전자파 시험, 노화분석, 육안 검사, 번인 시험, 내환경 시험, 내진시험 등과 같은 기기 검증을 통해 검증하였으며, 펌웨어는 Functional Simulation과 Timing Simulation을 포함한 단위시험 그리고 실장 시험인 통합시험을 진행하여 검증하였다. 설계와 검증을 모두 인허가에 맞는 절차를 거쳐 개발됨에 따라, 원자력 안전등급을 획득하여, 원자력 안전등급 제어기기의 통신망을 구성할 수 있게 되었다.

### 감사의 글

본 연구는 교육부와 한국연구재단의 지역혁신인력양성사업(NRF-2012H1B8A2025862)과 미래창조과학부 및 정보통신산업진흥원의 해외인재스카우팅사업(NIPA-HB616-13-1001)의 지원으로 수행되었습니다.

## REFERENCES

- [1] IEEE 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations", 2003.
- [2] IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", 2003.
- [3] IEEE 1074, "IEEE Standard for Developing a Software Project Life Cycle Process", 2004.
- [4] SAMCHANG Co, Ltd, "Topical Report of SECOP-Q Platform", 2011.
- [5] IEEE Std. 802.3, "Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", 2008.
- [6] Regulatory Guide 1.180, "Guideline for Electromagnetic and Radio-Frequency Interference in Safety Related I&C System", 2003.



**이동일(Dongil Lee)**

2005년 동의대학교 공과대학 컴퓨터공학과 공학사  
2014년 한밭대학교 정보통신전문대학원 정보통신공학과 공학석사  
2010년 ~ 현재 (주)포뉴텍 기술연구소 연구원  
※ 관심분야 : SoC 플랫폼 설계 및 검증, 멀티미디어 코덱 설계, 원자력 제어 설계



**류광기(Kwangki Ryoo)**

1986년 한양대학교 공과대학 전자공학과 공학사  
1988년 한양대학교 대학원 전자공학과 공학석사  
2000년 한양대학교 대학원 전자공학과 공학박사  
1991년 ~ 1994년 육군사관학교 교수부 전자공학과 전임강사  
2000년 ~ 2002년 ETRI 시스템IC설계팀 선임연구원  
2010년 ~ 2011년 Univ of Texas at Dallas 방문교수  
2003년 ~ 현재 한밭대학교 공과대학 정보통신공학과 교수  
※ 관심분야 : 공학교육, SoC 플랫폼 설계 및 검증, 멀티미디어 코덱 설계