Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.6.681

HPD 개발수명주기를 적용한 원전 FPGA 기반 제어기의 설계와 검증

이준구* · 정광일** · 박근옥** · 손광영***

Design and Qualification of FPGA-based Controller applying HPD Development Life-Cycle for Nuclear Instrumentation and Control System

Joon-Ku Lee* · Kwang-Il Jeong** · Geun-Ok Park** · Kwang-Young Sohn***

요 약

원자력 산업계는 최근 원전 계측제어계통 설비의 단종과 같은 예상치 못한 환경에 직면해오고 있으며, 이러한 문제를 근본적으로 해결하고자 노력하고 있다. IAEA, IEC, 등의 연구결과에 따르면, FPGA는 단종이 예상되는 제어계통에의 대체수단으로 주목받고 있다. FPGA가 원자력 플랜트의 PLC(Programmable Logic Controller)를 대체하기 위해서는 높은 건정성과 신뢰성을 가져야 한다. 따라서, FPGA 기반 제어기의 건전성과 신뢰성을 향상시키기 위하여 HDL 개발수명주기를 적용하여 개발하였다. 또한, 원전 계측제어계통에 적용하기 위하여 번인시험과 환경시험의 기기검증이 수행되었다. 시험수행결과, 352시간의 번인시험과 92시간의 환경시험 중에 정상적인 기능 및 성능을 수행함을 확인할 수 있었다.

ABSTRACT

Nuclear industries have faced unfavorable circumstances such as an obsolescence of the instrumentation and control system, and therefore nuclear society is striving to resolve this issue fundamentally. IEC and IAEA judge that FPGA technology is a good replacement for Programmable Logic Controller (PLC) of Nuclear Instrumentation and Control System. FPGAs are currently highlighted as an alternative means for obsolete control systems. Because the main function inside an FPGA is initially developed as software, good software quality can impact the reliability of an FPGA-based controller. Therefore, it is necessary to establish a software development aspect strategy that enhances the reliability of an FPGA-based controller. In terms of software development, HDL-Programmed Device (HPD) Development Life Cycle is applied into FPGA-based Controller. The burn-in test and environmental(temperature) test should be performed in order to apply into nuclear instrumentation and control system. Therefore it is ensured that the developed FPGA-based controller are normally operated for 352 hours and 92 hours in test chamber of Korea Institute of Machinery and Materials (KIMM).

키워드

Field Programmable Gate Arrary, Programmable Logic Controller, Nuclear Power Plant. Instrumentation and Control System, Burn-In Test, Environmental Test, Hardware Description Language

필드 프로그래머블 게이트 어레이, 프로그래머블 논리처리기, 원자력 플랜트, 계측제어계통, 번인시험, 환경시험, 하드웨어 기술언어

* 교신저자(corresponding author) : 한국원자력연구원(jklee@kaeri.re.kr)

** 한국원자력연구원(hisunny@kaeri.re.kr, gopark@kaeri.re.kr) *** ㈜미래엔(kwangyoung.sohn@mirae-en.co.kr)

접수일자 : 2014. 04. 21 심사(수정)일자 : 2014. 05. 19 게재확정일자 : 2014. 06. 16

Ⅰ. 서 론

산업계 전반에 걸친 디지털 컴퓨터 및 정보처리기술의 급속한 발전에 힘입어 아날로그 기술의 쇠퇴와 함께 디지털 기술로의 대전환이 이루어졌다. 한편, 원자력플랜트에 사용 중인 아날로그 기반의 계측제어계통은 부품단종 및 기술지원의 어려움으로 인하여 보수 및 교체가 어려운 상황이다. 이러한 문제를 해결하기 위하여 1990년대부터 본격적으로 PLC(Programm-able Logic Controller)가 원전 계측제어계통에 적용되었으나, PLC 또한 단종문제로 인한 유지보수의 어려움이 발생하였다. 특히, 아날로그 기기와는 달리 PLC가 소프트웨어에 의해 운영되는 특성은 주요부품 단종시에 운영체제 또는 지원 소프트웨어를 변경해야 하는 상황을 가져왔으며, 이에 따른 인허가 심사가 별도로 요구되었다. 이러한 문제를 극복하기 위하여 설계시점에는 소프트웨어이나, 통합시에는 단일 칩내의 회로로 구성되는 FPGA(Field Programmable Gate Array)에 대한 원자력 산업계의 관심이 집중되고 있다.

현재, 국내 원전에는 FPGA 기술의 적용이 미비한 반면, 해외에서는 이미 FPGA 기술을 이용한 제어기가 원전에 적용되고 있다. 국내적용 경험이 없는 FPGA의 원전적용을 위해서는 안전성 측면이 중요하므로, FPGA 제어기의 신뢰성 및 건전성 확보가 중요하다. 따라서, FPGA 기반의 제어기 개발시에 하드웨어와 주요 기능을 수행하기 위한 소프트웨어 등의 체계적인 개발이 필요하다. 제어기를 구성하는 하드웨어는 검증된 부품을 사용하고, 신뢰성 높은 설계를 함으로써 그 신뢰성을 향상시킬 수 있다. 또한, 소프트웨어의 경우에는 HPD (HDL-Programmed Devices) 개발수명주기를 적용하여 체계적으로 개발함으로써 소프트웨어의 품질을 향상시킬 수 있으며, 궁극적으로는 제어기의 신뢰성을 향상시키게 된다.

본 본문에서는 원전 사용을 위한 FPGA 기반 제어기 개발을 위한 HPD 개발수명주기를 제시하고, 개발된 제어기에 대한 기기검증을 통하여, 기존 PLC를 대체할 만큼 충분히 신뢰성 있음을 제시하였다.

Ⅱ. 결함 유형

원전적용을 위해서는 설계 및 구현단계에서 예상되는 설계오류 및 결함유형의 인식은 필수적이다. 설계자는 하드웨어와 소프트웨어의 관점에서 FPGA의 결함유형을 고려해야 한다. 하드웨어 결함유형은 FPGA 회로에서의 “short” 또는 “open”과 관련된다. 이런 결함은 제조과정에서의 결함에 의해 야기되며, “stuck-at-faults(stuck-at-0 또는 stuck-at-1)”는 이러한 결함의 유형들이다. Baraza [1]은 이러한 결함유형들을 탐지하는 매커니즘을 제시하였다.

표 1. 결함유형의 분류
Table 1. Classification of fault modes

Fault Modes	Characteristics
Clock slack	Loose state of clock timing
Clock skew	Different clock input times between flip flops in spite of that the same clock is used in logic design
Glitch	Glitch in digital logic is a short-lived fault in the logic system owing to a change at the input. Glitch is the inherent characteristic of logic design caused by asynchronous timing
Metastability	Metastability is an undefined state, in case that the output of the flip-flop is not 0 or 1

또한, 하드웨어 자체의 결함이 아닌 소프트웨어 측면의 오류가 발생할 수 있으며, 개발수명주기에 따른 확인 및 검증활동에 의하여 이러한 설계오류 등을 모두 제거해야 한다.

소프트웨어 결함유형은 설계자에 의해 야기되는 설계오류이며, 이러한 설계오류를 줄이기 위하여 설계자에 대한 교육과 함께 최종 생산품이 고장에 대한 내성을 갖도록 해야 한다. 표 1은 설계 및 구현단계에서 예상되는 결함유형의 분류를 보여준다[2-3]. 확인 및 검증활동은 이러한 FPGA의 특성을 고려하여 수행되어야 한다. 설계자는 프로그램동안 발생할 수 있는 결함을 조사하고, 수집할 필요가 있다.

이러한 원전 안전에 영향을 미치는 PLC를 대체하기 위해서는 높은 신뢰성과 건전성을 가져야 하며, 개발수명주기를 적용하여 체계적인 제어기 개발이 수행되어야 한다. 개발수명주기의 확인 및 검증활동에 의

하여 결함유형이 제거되어야 한다.

III. 개발수명주기

3.1 원전 디지털시스템 관련 기술기준

국내 인허가 기관은 원전에의 디지털 시스템 적용 시에 하드웨어 및 소프트웨어 관련 기술기준 준용을 요구하고 있다. 소프트웨어 건전성을 유지하기 위하여 소프트웨어 개발수명주기 적용과 함께 다음의 활동을 수행해야 한다.

- 소프트웨어 품질보증
- 소프트웨어 형상관리
- 소프트웨어 확인 및 검증

상기의 기술기준은 일반적으로 PLC와 같은 소프트웨어 기반의 디지털 설비에 적용되는 것이다. 즉, 단일 칩에 다운로드 이후에는 하드웨어로 분류되나, HDL로 개발과정에는 소프트웨어로 분류되는 FPGA의 특성으로 인하여 일반적인 소프트웨어 공정과 유사한 개발절차 및 활동이 확립되어야 한다.

3.2 HPD 개발수명주기

FPGA 제어기는 원전 기술기준인 IEC 61513의 시스템 개발주기에 따라 개발되어야 한다. 또한, 개발시에는 소프트웨어이나 다운로드 이후에는 하드웨어인 특성에 의하여, IEC 60880의 원전 소프트웨어 요건, IEC 60987의 컴퓨터 기반 시스템의 하드웨어 개발요건을 충족하도록 개발되어야 한다. 즉, 원전에서 사용하기 위한 계측제어설비 개발절차는 수명주기가 적용되어야 하며, 이와 함께 품증보증, 형상관리 등도 요구되고 있다. FPGA 제어기의 핵심 설계요건은 HPD에 대하여 기술한 IEC 62566에 기초를 두고 있으며, 설계 및 검증을 위한 수명주기가 그림 1의 HPD 개발수명주기의 V 모델로 기술되고 있다. HPD 개발수명주기는 요건, 설계, 구현, 통합, 검증단계의 각 활동준수를 요구하고 있으며, 각 단계에서는 확인활동이 요구되고 있음을 알 수 있다.

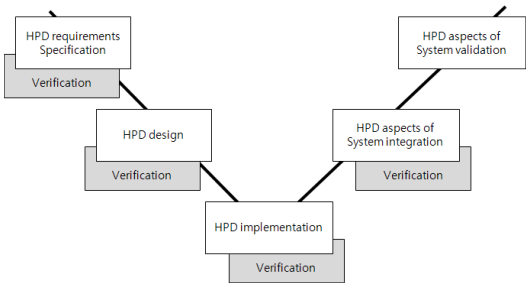


그림 1. HPD 개발수명주기
Fig. 1 Development life cycle of HPD

그러나, HPD 개발수명주기는 소프트웨어 측면에서의 개발수명주기를 위주로 기술하여, 구체적인 FPGA의 설계공정을 반영하지 못한 단점이 있다.

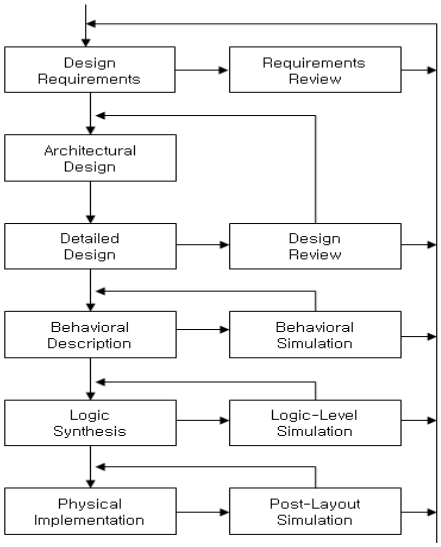


그림 2. 제안된 원전 FPGA 상세 설계공정
Fig. 2 Proposed detailed FPGA design process for nuclear I&C system

그림 2는 HPD 개발수명주기 중, 요건, 설계, 구현 단계를 FPGA 설계공정을 반영하여 제안한 구체화된 FPGA 설계절차이다. FPGA 설계 절차는 각 설계단계와 이에 일치하는 확인단계를 포함하고 있다. 각 확인단계의 결과가 만족스럽지 못한 경우에는 그 이전 개발단계로 되돌아가거나, 개발초기 단계로 되돌아가 처음부터 다시 개발해야 한다.

IV. FPGA 기반 제어기 개발

FPGA 제어기는 VHDL 사용, 하향식설계, 동기설계적용, 결함유형 제거 및 최적화 기법을 활용하여 개발하였다[3, 4, 5]. VHDL는 IEEE Std. 1076에 의해 표준화된 장점이 있으며, 개발시 IP 코어의 사용은 검증자체의 어려움과 원천기술 개발의 필요성으로 인해 사용을 배제하였다.

FPGA 제어기 형상은 그림 3과 같이 FPGA 보드, I/O 보드, 통신보드, 전원모듈, 백플레인 및 쉐시로 구성된다. 이는 원전 다양성보호계통을 구성하는 최소 모듈이며, 제어기는 아날로그 신호를 입력받아 연산처리 후 그 결과를 디지털 신호로 출력하는 기능을 갖고 있다. 제어기는 백플레인 버스를 거쳐 서로 통신으로 연결되어 상호 연계한다.

그림 3. 개발된 FPGA 기반 제어기
Fig. 3 Developed FPGA-based controller

FPGA 제어기는 소프트웨어 측면에서는 구체화된 HPD 개발수명주기를 적용하여 체계적인 개발을 하였다. 원전적용을 위한 건전성 확인을 위해서는 제어기가 설치될 원전 계측제어 환경에서의 기능 및 성능시험을 통해 건전성이 입증되어야 한다. 이를 위해 한국기계연구원에서 다음과 같은 검증이 수행되었다.

V. 원전 기기검증

5.1 FPGA 제어기 정확도 시험

개발된 FPGA 제어기는 높은 신뢰도와 함께 EPRI TR-107730에서 요구하는 높은 정확도를 가져야 한다. 이에 그림 4와 같이 교정된 시험 장비를 이용하여 아날로그 입력보드(전류, 전압), 아날로그 출력보드(전류, 전압) 디지털 입력 및 출력보드의 정확도와 동작성을 시험하였다.

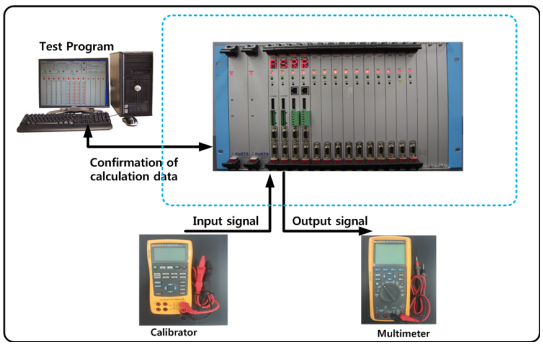


그림 4. 정확도 및 동작성 시험설비
Fig. 4 Accuracy and operability test configuration

FPGA 제어기의 정확도 및 동작성 시험결과는 표 2와 같이 허용기준을 충족하였다. 시험은 공식인증기관인 한국기계연구원에서 수행되었다.

표 2. FPGA 기반 제어기 정확도 및 동작성 시험기준
Table 2. FPGA-based controller accuracy and operability test criteria

EUT	Acceptance Criteria (Accuracy)
Analog Input Board (Voltage)	be equal to or less than ±0.32%
Analog Input Board (Current)	be equal to or less than ±0.35%
Analog Output Board (Voltage)	be equal to or less than ±0.3%
Analog Output Board (Current)	be equal to or less than ±0.32%
Digital Input Board	contact (On/Off) operability
Digital Output Board	contact (On/Off) operability

5.2 FPGA 제어기 번인, 온습도 시험

번인시험은 부품조립 후 초기고장 제거와 전기적 특성치의 극한값까지 운전하여 정상적으로 동작됨을

확인하기 위한 것이다. 또한 온습도 시험은 주어진 사용환경 하에서 기기의 성능특성을 만족시킬 수 있음을 입증하기 위한 것이다. 시험은 원전 기술기준인 EPRI TR-107330 및 IEEE Std. 323 요건에 따라 수행되었으며, 시험은 그림 5와 같이 육안검사, 번인, 온습도 시험의 순서로 수행되었다.

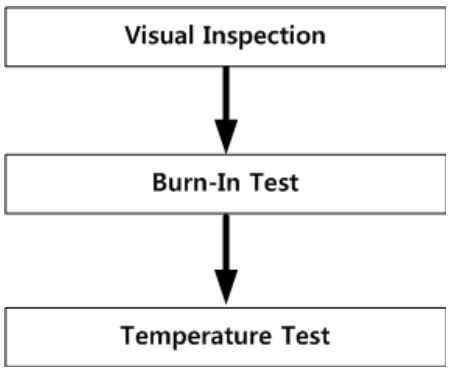


그림 5. 검증시험 순서
Fig. 5 Qualification test procedure

기능 및 성능시험을 위하여 FPGA 제어기에는 원전 다양성보호계통 프로그램이 탑재되었으며, 이는 원자로를 정지하는 기능을 수행한다.

그림 6. 번인 및 환경시험 챔버
Fig. 6 Burn-In and environmental test chamber

시험을 위한 구성은 FPGA 제어기와 외부 모사신호 생성기 및 측정기, 그리고 시험요원을 위한 화면으로 구성된다. FPGA 제어기의 연산기능을 수행하는 FPGA 보드, 아날로그 입출력보드, 디지털 입출력보드, 통신보드, 전원모듈이 탑재된 상태이다. 이후, 그림 6의 시험챔버 환경하에서 FPGA 제어기의 시험 및 성능시험을 기능 시험절차서에 따라 수행하였다. 시험설비는 표 3과 같은 시험챔버 환경하에서 요구되는 기능을 정상적으로 수행할 수 있어야 한다.

표 3. 시험 조건
Table 3. Test condition

EUT	Environmental Requirements	
	Burn-in Test	Temperature Test
FPGA-based Controller	A minimum 352 hours	Temp. : 30~50℃ R.H : 60~95% A minimum 92 hours

번인 및 온습도 시험동안 제어기의 요구되는 기능 및 성능을 평가하였다. 번인 시험 중의 기능시험(3차)과 온습도 시험 중의 기능시험(3차)을 실시하여 FPGA 제어기가 표 3의 허용기준을 만족하였음을 확인하였다. 환경시험은 공인기관(한국기계연구원)에서 수행되어 시험기간 중 그 기능 및 성능이 유지됨을 확인하였다.

5.3 원전 다양성보호계통 기능시험

원전 다양성보호계통은 원전 요건인 10CFR50.62의 정지불능예상과도상태(Anticipated Transient Without Scram) 사건의 완화요건을 충족하도록 설계된다. 또한, 원자로보호계통의 공통유형고장(CMF : Common Mode Failure)에 의한 기능불능시에 다양성보호계통은 원자로정지 및 공학적안전설비를 작동하는 기능을 수행한다. 이러한 이유로 다양성보호계통은 센서부터 최종 구동단까지 원자로보호계통과는 물리적으로 분리 및 전기적으로 격리된다.

현 운용중인 원전의 다양성보호계통은 센서부터 최종 구동단까지 두 채널로 구성되며, 원전변수를 지속적으로 감시하여 2-out-of-2 논리에 의해 자동으로 원자로정지 및 공학적안전설비를 작동시킨다.

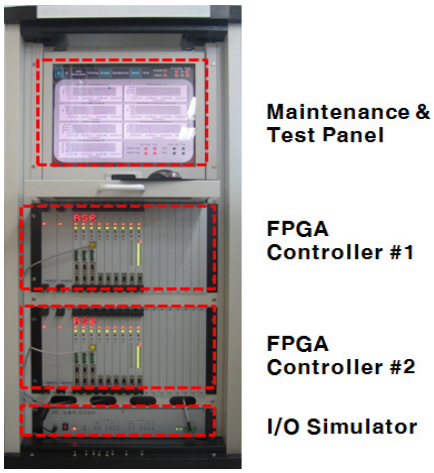


그림 7. 원전 다양성보호계통 시험환경
Fig. 7 System test environment for diverse protection system

개발된 FPGA 제어기에 자동 원자로정지 및 자동 공학적안전설비 작동기능을 수행하는 다양성보호계통을 그림 7과 같이 두(2) 채널의 FPGA 제어기에 탑재하였다. 또한, I/O 시뮬레이터를 장착하여, 그림 8과 같이 사고시의 시나리오에 따라 공정변수를 생성하여 FPGA 제어기로 구성된 다양성보호계통에 대한 기능 및 성능시험을 수행하였다.

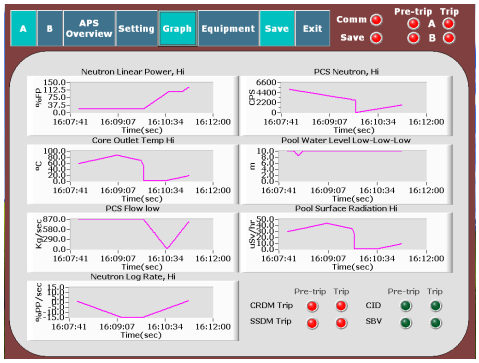


그림 8. 원전 다양성보호계통 시험모드
Fig. 8 Test mode for diverse protection system

이 시험을 통하여 개발된 다양성보호계통의 정상동작여부를 확인하였으며, 이와 수반하여 FPGA 제어기의 기능수행여부를 확인하였다.

VI. 결 론

FPGA 설비가 원전 계측제어계통에 적용되는 PLC 설비를 대체하기 위해서는 PLC 대비 동등수준의 건전성과 신뢰성을 확보해야 하였다. 따라서, 제어기를 구성하는 소프트웨어 측면에서의 구체화된 HPD 개발 수명주기를 제시하였고, 체계적 소프트웨어 개발을 수행하였다. 또한, 개발된 FPGA 제어기를 원전 계측제어계통 환경에 설치하기 위해서는 원전 기기검증 요건에 따른 검증이 수행되어야 한다. 이에 번인, 환경시험을 수행하여 각각 352시간, 92시간동안 정상으로 동작함을 확인하였다. 이러한, 체계적 개발과 검증을 통하여 원전적용 가능성을 확인할 수 있었다.

높은 건전성을 갖는 FPGA 제어기 개발을 통해 해외에 뒤지지 않는 국내기술을 확보할 수 있었으며, FPGA 제어기의 체계적 설계와 건전성 분석을 기반으로 원전에 적용되고 있는 PLC를 대체할 수 있을 것으로 판단된다.

감사의 글

이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(SMART 안전성 향상을 위한 MMIS 연구, No. 2012M2A8A4025979)

References

[1] J. C. Baraza, J. Gracia, D. Gil, and P. Gil, "A prototype of a VHDL based fault injection tool: description and application," *J. of Systems Architecture,* vol. 47, no. 10, 2002, pp. 847-867.

[2] J. LEE, "Design and Verification Process for Developing the FPGA-Based Firmware for NPPs," *1st IAEA Workshop on Applications of Field-Programmable Gate Arrays in Nuclear Power Plants*, Paris, France, Aug. 2008.

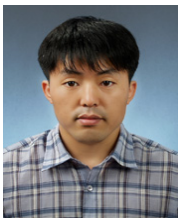
[3] J. LEE and Y. KIM, "Design and Verification of FPGA-Based Applications in Nuclear Power Plants," *J. of Energy and Power Engineering*, vol. 7, no. 3, 2013, pp. 537-544.

[4] J. LEE, "Design Experience for FPGA-based Bistable module of Reactor Protection System," *The 4th IAEA Workshop on Applications of Field-Programmable Gate Arrays in Nuclear Power Plants*, Paris, France, Aug. 2011.
[5] K. Sohn, W. Yi, J. Lee, and I. Koo, "PROTECTION AND CONTROL WITH FPGA," *The 18th Pacific Basin Nuclear Conference (PBNC 2012)*, BEXCO, Busan, Korea, Mar. 2012.
[6] Y. Moon, S. Lim, Y. Lee, and Y. Bae, "Hardware Implementation of Motor Controller Based on Zynq EPP(Extensible Processing Platform)," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 8, no. 11, 2013, pp. 1707-1712.
[7] J. Hong, "A Study on Dual System for Fault Tolerance of PLC," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 6, no. 3, 2011, pp. 397-404.
[8] I. Koo, K. Kim, S. Hong, G. Park, and J. Park, "Digital Asset Analysis Methodology against Cyber Threat to Instrumentation and Control System in Nuclear Power Plants," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 6, no. 6, 2011, pp. 839-847.

저자 소개

이준구(Joon-Ku LEE)

1998년 충남대학교 전기공학교육과(공학사)
2000년 충남대학교 전기공학과(공학석사)
2014년 충남대학교 전기공학과(공학박사)
2000년~현재 한국원자력연구원 연구로계통설계부 선임연구원
2011년~현재 IEC 계측제어전문위원
※ 관심분야 : I&C System, Reliability Analysis



정광일(Jeong-Il Jeong)

1997년 전북대학교 전자공학과(공학사)
1999년 전북대학교 전자공학과(공학석사)
2003년 전북대학교 전자공학과(공학박사)
2003년~2004년 한국표준과학연구원
2004년~현재 한국원자력연구원 연구로계통설계부 책임연구원
※ 관심분야 : I&C System, Cyber Security, Communication System

박근옥(Geun-Ok Park)

1986년 경기공업개방대학 컴퓨터공학과(학사)
1993년 충남대학교 전산학과(석사)
1987년~현재 한국원자력연구원
1987년~현재 한국원자력연구원 연구로계통설계부 책임연구원
※ 관심분야 : I&C System, Cyber Security, Software V&V

손광영(Kwang-Young Sohn)

1988년도 강원대학교 전산학과 졸업(공학사)
1990년도 홍익대학교 전산학과 졸업(공학석사)
1990년~2002년, 한국원자력연구원, 한국전력기술주식회사(대전)
2003년~2008년 스마트 설계센터 위촉연구원
2003년~현재 IEC 위원, 계측제어전문위원
2014년 현재 ㈜미래엔 대표
※ 관심분야 : 디지털 계측제어시스템, CDR(Critical Digital Review), Verification and Validation, Simulator