2015년도 대한전기학회 하계학술대회 논문집 2015. 7. 15 - 17

디지털 제어설비 운전 신뢰도 증진방안

이광대*, 임희택, 김민석
㈜한국수력원자력 중앙연구원 계전기술연구실 I&C그룹

Operation Reliability Improvement of Digital Control System for Nuclear Power Plants

Kwang-Dae Lee*, Lim-Hee Taek, Kim-Min Seok
Korea Hydro & Nuclear Power Co. Central Research Institute

Abstract - 원자력발전소 계측제어시스템은 과거의 아날로그 설비에서 디지털설비로 개선되고 있으며, 신규로 건설되는 발전소에서는 모든 시스템이 디지털화 되었다. 디지털설비는 하드웨어와 소프트웨어, 통신기능이 통합된 매우 복잡한 설비이며, 기존 하드웨어를 중심으로한 신뢰도 분석방법으로는 신뢰도를 확인하는데 한계가 있다. 따라서 본 논문에서는 기존의 신뢰도 분석방법의 한계를 극복하기 위하여 신뢰도 검증설비를 구성하여 다양한 시나리오에 의한 장기 종합시험을 수행하는 방식으로 신뢰도를 보증할 수 있는 방법과 구성들을 제시한다.

1. 서 론

디지털 시스템은 소프트웨어에 의하여 동작하는 하드웨어와 통신기기들로 구성되어있으며 대규모 설비의 경우에는 제어 기능이 여러개의 프로세서에 분산되어 동작한다. 기존의 아날로그 시스템에서는 하드웨어의 높은 신뢰도 설계가 전체 설비의 신뢰도를 좌우하였다. 그러나 디지털시스템의 신뢰도를 보증하기 위하여, 국제 표준에서 제시하는 하드웨어의 신뢰도 분석, 소프트웨어 확인검증 방법을 적용하여왔으며, 최종적으로 통합시험을 통하여 건전성을 확인하게된다.

디지털 시스템의 신뢰도는 국제 표준에 의한 짧은 시간동안의 시험과 검증으로는 분명히 한계가 있으며, 이는 발전소 현장에서 오동작하는 디지털 시스템의 현황으로부터 확인된다.

따라서 기존과 같이 완벽하지못한 분석에 의한 신뢰도 보증방법을 보완할 방법이 필요하며, 자동차와 전자기기 들의 최종 장기 운전시험 사례로부터 아이디어를 얻을 수 있다. 일반 산업계에서는 출시한 디지털 기기의 잦은 고장은 리콜 등을 통하여 경제적 손실뿐만 아니라 기업 이미지에 큰 영향을 미친다. 그러므로 개발 과정의 완결성에 더하여 주요 회사에서는 최종 장기 시험을 통하여 개발 과정에서 미쳐 찾아내지 못한 오류들을 점검하여 최종 신뢰도를 높이고 있다.

원전의 디지털 시스템은 국제 표준에 의하여 개발과정 중에 완결성을 보증하도록 확인 검증 과정을 거쳐서 개발된다. 그러나 디지털 설비의 복잡성과 정보 연계성들을 고려하면 기존의 개발과정이 아무리 완결하여도 종합적인 신뢰도 보증에는 부족함이 있다.

본 논문에서는 기존의 원전 디지털 시스템의 신뢰도 검증 방법을 요약하고 문제점들을 정리하였다. 또한 이러한 취약점들을 보완할 개선방안으로 신뢰도 검증설비를 개발하여 적용하는 방안을 제시하였다.

2. 본 론

2.1 디지털 제어설비 신뢰도 검증 방법

원자력발전소의 안전기능을 수행하는 계측제어계통은 IEEE Std 603-1998(IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations)과 원자력 규제지침 8.14(안전등급 계측제어계통 설계)에서 설계단계에서 신뢰도 분석을 수행할 것을 요구하고 있다.

IEEE Std 603의 "5.15 Reliability"에서는 안전계통은 정성적 또는 정량적인 신뢰도 목표를 만족하여야하며, 이를 확인하기 위하여 적절한 신뢰도 분석을 수행하는 것을 요구하고 있다. 또한 분석 지침으로 IEEE Std 352-1987 과 IEEE Std 577-1976을 제시하고 있다.

계통설계에서는 Diversity & Defense in Depth, Plant Safety Analysis, Probabilistic Risk Analysis, Cyber Security 등의 활동이 있고, 고장분석에서는 전통적인 신뢰도 분석 방법인 FMEA (Failure Mode & Effect Analysis), FTA(Fault Tree Analysis), Hazards Analysis 등이 사용된다.

IEEE Std 352 에서는 원자력발전소 안전계통 설계시의 신뢰도 분석 방법으로 정성적(Qualitative)/정량적(Quantitative) 분석 방법을 제시하고 있다.

○ Qualitative Analysis
  ① FMEA (Failure Modes & Effects Analysis) : Bottom-Up
  ② FTA (Fault Tress Analysis) : Top-Down
  ③ Reliability Block Diagram
○ Quantitative Analysis
  ① Mathematical Modeling
  ② Tabular Reference to Popular Logic Configuration

2.2 기존 신뢰도 분석 방법의 한계

FMEA, FTA와 같은 전통적인 분석기법은 도미노와 같이 Failure Event에 기초한 고장들의 직접적인 연쇄작용 모델이다. 그러나 최근 디지털시스템의 도입으로 FMEA, FTA와 같은 방법만으로는 최적으로 신뢰도 또는 위해도를 분석하지 못한다는 연구 결과들이 나오고 있으며, Hazard의 원인과 결과의 관계가 항상 직접적인 연쇄 작용이 아님이 드러나고 있다. 또한, 아날로그와 달리 디지털시스템의 고장은 설계와 개발의 특성과 관련된 시스템적 원인으로부터 발생함을 지적하고 있다.

기존 신뢰도 분석방법의 한계를 나열하면 다음과 같다.

① 정성적 분석의 한계
  - 하드웨어 위주의 고장 분석
  - 분석 수준과 대상 고장 모드 정의의 한계성
  - 세부 설계자와 개발자만이 가능
  - 디지털시스템(HW, SW, 통신, 기능분산 등)에는 부적합
② 이론 및 수학적 정량화 분석의 비현실성
  - 부품 신뢰도/고장자료를 신뢰하기 어려움(MIL 데이터 북)
  - 설계/개발/제작 과정의 불확실성 반영에 한계
  - 외부 Stress 요인(환경, 전원품질 등) 반영이 어려움
  - 신뢰도 분석 결과의 신뢰도가 낮음
③ 종합 신뢰도 검증방법의 부재
  - 기기를 조합한 전체 시스템 신뢰도 분석 방법이 부재
  - 전체 디지털시스템 신뢰도 검증(확인) 방법이 부재
  - 기기(환경)검증은 제한된 시간 동안, 제한된 기능만 확인

2.3 일반 산업계의 디지털 종합 검증 사례

원자력발전소 디지털설비의 제작, 설계나 최종 검증 과정은 일반 산업계와 기준과 방법이 다를 뿐 유사한 면이 있다. 원자력발전소의 디지털설비는 내부 제어기기는 상용 제품을 채용하고, 목적에 맞도록 기기들 간의 기능 설계를 한 후에 종합 확인 검증을 하게 된다. 이 과정은 자동차에서 전자 제어기용 상업용 마이크로프로세서를 사용하여 자동차에 적합한 기능 설계를 한 후에 부분 시험과 종합 검증을 하는 과정과 유사하다. 그러나 자동차를 비롯한 상업용 제품들에서 하자가 발생할 경우, 회사의 이미지와 제품 리콜에 따른 경제적 손실 등을 고려하여 제작사들은 하자를 최소화 할 수 있는 방법에 많은 시간과 노력을 기울인다. 품질향상을 위한 6σ 기법은 100만개 당 0.002개의 불량률을 목표로 하며, 기업들이 채택하는 이면에는 하자 최소화를 위한 극한 노력을 보여준다. 본 절에서는 일반 산업계인 자동차, 스마트 폰의 최종 종합 검증 과정을 간략하게 소개하고, 일반 산업계에서 하자를 최소화하기 위한 노력을 확인하고 시사점을 도출하고자한다.

2.3.1 자동차 종합 검증

자동차는 보다 높은 안전성과 안정성, 승차감을 요구하는 소비자들을 만족시키기 위하여 다양한 기능의 ECU(Electronic Control Unit)를 적용하여왔다. ECU는 자동차 곳곳의 센서로부터 수집된 측정값에 따라 신호 처리 또는 제어 연산에 의하여 기계적인 구동기를 동작시키는 마이크로컴퓨터 기기이다. ECU는 1979년 보다 엄격해지는 자동차 배기가스 제어를 위하여 GM 자동차에 채용된 이후, 80년대에는 엔진 분사 제어에 주로 사용되어 연비를 획기적으로 향상시켰다. ECU는 주요 사용처에 따라서 변속기 제어용에는 TCU(Transmission Control Unit), 파워트레인에는 PCU(Powertrain Control Unit) 등의 이름으로 사용된다. 초기

에는 자동차의 엔진 제어나 자동변속기 제어에 주로 사용되었으나 현대에는 ECU의 숫자가 고급 차량을 대표하고 있으며, 중형차의 경우에는 25개, 고급 차종에는 100개 정도가 사용된다.현재는 ECU의 처리 속도가 높아짐에 따라 많은 숫자의 ECU를 통합하고, 또한 분산된 기능들을 최종 검증하는 것이 과제가 되고 있다. 자동차에서도 내부에 장착되어있는 많은 ECU들 사이에는 원전의 디지털제어설비와 같이 데이터 통신망이 사용되며, 각 ECU의 긴급 정보들은 엔진을 정지시키는 보호기능의 ECU와 연결되어있다. 따라서 자동차를 구성하는 엔진, 트랜스미션, 변속기와 같은 기계장치들 뿐 만 아니라 ECU 장치들의 연동시험을 종합적으로 확인하는 과정이 반드시 필요하다. 상용 자동차 제조사들은 최종적으로 상용화하기 전에 법적 규정 만족과는 별도로, 자체적으로 장기 로드 시험을 수행하여 최종 신뢰도를 확인하는 과정을 거친다.

2.3.2 스마트폰 종합 검증

일반 산업계의 컴퓨터 기기 중에서 가장 개발 주기가 빠른 반면에 내구성이 요구되는 기기는 스마트 폰이다. 스마트 폰의 내부 전자회로와 기능, 소프트웨어는 각 개발 팀이나 검증 팀에 의하여 분야별로 시험될 뿐만 아니라 최종 상용화되어 출시 전에 최종 소비자가 사용하는 것과 같은 방법으로 장기 신뢰도 시험을 한다. 사용자의 손가락을 모사하는 구동기 로봇을 이용하여 연속, 반복하여 동작시키면서 기능과 성능을 종합적으로 확인한다. 사용자 관점의 장기 시험은 각 분야별 시험의 완결성에도 불구하고, 각 분야의 상호 연결 과정의 종합적인 신뢰도 보증을 위한 것이다.

2.3.3 일반 산업계 사례 검토 결과

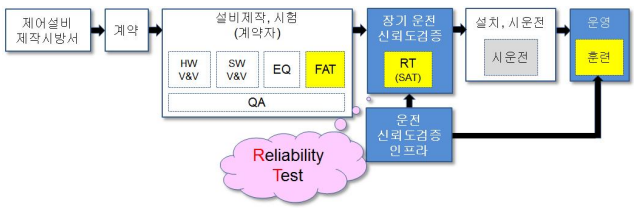
일반 산업계의 경우에도 마이크로프로세서를 가진 디지털 기기로 구성된 경우에는 단일 기기의 건전성 시험과 종합 확인 시험을 수행하고 있으며, 특히 출고전의 장기 운영 시험은 마지막 결함을 찾아내는 최종 관문이다. 특히, 자동차나 스마트 폰과 같은 상업용 제품들은 작은 결함이 회사 이미지와 제품에 미치는 영향이 크고, 리콜이 발생할 경우에는 경제적인 손실도 크므로 최종 시험에 많은 시간과 노력을 기울이는 편이다. 이런 사회 전반적인 신뢰도 증진을 위한 노력을 볼 때, 원자력발전소에서 사용하는 설비들의 신뢰도를 높이기 위해서는 현재 미흡한 설계와 제작후의 최종 시험 또는 장기 운영 시험에 보다 적극적인 적용 검토가 필요하다.

2.4 원전의 디지털설비 신뢰도 검증 방안

디지털설비의 신뢰도를 확보하기 위한 설계와 개발, 시험 단계의 검증 기술들은 하드웨어와 소프트웨어, 통신 등의 복잡한 구조로 이루어진 디지털기술의 완결성을 보증하기에는 한계가 있다. FMEA, FTA 등의 신뢰도 분석기술들은 아날로그 기술의 하드웨어 신뢰도 검증 때부터 사용되어온 것들이다. 소프트웨어 신뢰도는 소프트웨어 개발 계획과 단계마다 수행되는 확인 검증 과정을 거쳐서 품질이 보증된다.

하드웨어와 소프트웨어 신뢰도는 두 가지가 통합된 통합 시험단계에서 비로소 기능과 성능시험이 이루어지지만, 현재의 기술수준은 통합 신뢰도라는 정량적인 값으로는 제시하지 못하고 있다.

반면에, 일반 산업계의 제품 최종 시험검증 단계와 하드웨어와 소프트웨어가 결합하여 동작하는 데이터 통신기기들의 신뢰도 검증 방법을 보면 원전 디지털설비의 신뢰도 증진을 위해 추가적으로 필요한 활동들을 알 수 있다. 아무리 완벽한 부분 시험과 검증을 하였더라도, 또한 종합기능과 성능시험을 통과하였다 하더라도 디지털기술의 매우 미세한 비트 오류에 의한 기능 정지는 예상이 어렵다. 또한 이런 오류는 장시간 동안에 수행되는 전 운영범위를 포함하는 매우 잘 짜여진 운영 또는 시험 시나리오에 의해서만이 사전에 발견할 수 있다. 또한 디지털보드들이 인접하게 설치된 전자파 환경에서는 예측이 불가능한 작은 노이즈 환경에서도 오류가 발생할 수 있으며 디지털 부품들의 동작 전압이 낮아짐에 따라 오류 가능성은 높아지고 있다. <그림 1>은 디지털설비의 개발과 시운전과정에서 인수시험(SAT)에서 장기 운전시험을 통하여 최종 운전 신뢰도를 확인한 후에 설치, 운영하도록 하는 개선된 과정을 나타낸다. 이를 위하여 효율적인 운전 신뢰도 시험(RT, Reliability Test)을 위한 시험 인프라가 필요하며, 이 시험 인프라는 운영 과정에서 정비원 훈련용으로 활용할 수 도 있다.

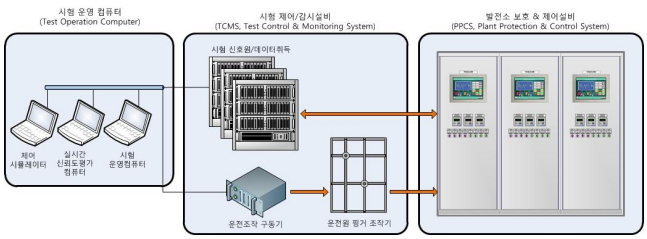


<그림 1> 장기 신뢰도 검증을 반영한 개발 공정

디지털설비의 운전 신뢰도 검증장치의 구성도는 <그림 2>와 같다. 검증장치는 크게 시험 대상설비에 시험용 신호와 운전원 조작을 인가하고 그 결과를 취득하기 위한 시험 제어/감시설비(TCMS, Test Control & Monitoring System), 제어 시뮬레이터, 실시간 신뢰도 평가 컴퓨터, 시험 운영컴퓨터로 구성되어있는 시험 운영시스템(TOS, Test Operation System)으로 구성된다.

시험 운영시스템은 제어 시뮬레이터, 실시간 신뢰도평가 컴퓨터, 시험 운영컴퓨터로 구성되며 전반적인 시험 운영 환경을 통제하며 세부 기능은 다음과 같다.

① 대상 설비의 시험에 필요한 계측제어 신호 제공과 제어 결과 데이터의 취득, 입출력 신호원(신호크기, 주기, 특성-주기성/임의성 등) 설정 등
② 대상 설비가 제어하는 발전소 계통 또는 기기의 제어모델을 통한 동적 거동 응답 제공 및 이와 관련된 모델 설정
③ 실시간 운전 신뢰도 평가, 검증 데이터의 저장과 관리, 표기, 인쇄 등
④ 시험 시나리오, 시험 패턴 및 불확도 설정
⑤ 시험 환경에 연결되는 기기들의 네트워크 상수, 기기 파라미터 설정 등



<그림 2> 운전 신뢰도 검증장치 구성도

TCMS는 검증 대상설비인 발전소 보호 & 제어설비에 Hard-Wired 현장 제어신호를 제공하는 시험 신호원과 제어 출력을 감시하기 위한 데이터 취득 장치, 운전원의 조작 동작을 모사하는 운전 조작 구동기와 운전원 핑거 조작기로 구성된다. TCMS 시험 신호원은 시험 운영 컴퓨터가 시험 전 또는 시험 중에 제공하는 시험 패턴에 따라 발전소 현장과 동일한 계측신호를 발생시키고, Hard-Wired 형태 또는 네트워크를 통하여 제공한다. TCMS 데이터 취득 장치는 시험 대상 설비에 제공되는 현장 제어 신호와 제어 출력 결과를 취득하는 역할을 한다. 본 장치는 시험 신호원과 병렬로 연결되지만, 시험 신호원의 크기나 임피던스에 영향을 주지 않아야 한다.

3. 결 론

국내 원전에서는 기존의 아날로그 제어설비가 디지털로 개선되고있으며, 신규 건설 원전에서는 모든 설비가 디지털설비이다. 디지털설비는 하드웨어와 소프트웨어, 통신망을 통한 정보 전달, 기능의 분산 등 구성기기 간에 매우 복잡한 연계관계 구조를 가지고 있다. 원전에서는 안전등급의 주요 제어설비에서는 FMEA, FTA 등의 방법으로 신뢰도 분석을 적용하게되어있으나 하드웨어 기반의 분석방법으로는 디지털설비의 종합 신뢰도를 보증하는데는 한계가 있다.

따라서 본 논문에서는 자동차, 전자기기 등의 일반 산업계에서 수행하는 종합 검증 시험 방법을 디지털 제어설비에 적용하여 신뢰도를 보증하는 방안을 제시하였다.

디지털설비 운전 신뢰도 검증장치는 시험 대상설비의 운영 시나리오와 이때 발생하는 입출력 제어신호와 조작신호 패턴을 가지고있도록 설계하고, 이에 따라서 시험 대상설비의 모든 운전 시나리오를 순차적으로 반복 시험하게된다.

본 검증설비는 향후 본격화되는 디지털설비 업그레이드의 진행여부에 따라서 2018년 경에 개발에 착수할 예정이다.

[참 고 문 헌]

[1] IEEE Std 15288 “System Life Cycle Process”, 2008
[2] IEEE Std 12207 “Software Life Cycle Process”, 2008
[3] IEEE Std 603, “IEEE Standars Criteria for Safety Systems for Nuclear Power Generating Stations”, 1998
[4] IEEE Std 7-4.3.2, “IEEE Standars Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”, 1993
[5] EPRI TR-1022985, “Failure Analysis of Digital I&C Equipment and Systems”, 2011