신뢰성응용연구 신뢰성기술
제10권, 제2호. pp.149-160, 2010

원자력발전소의 제어계측 시스템에 대한 가용도 평가 방법 연구

이동희*·남경현**

한국산업기술시험원*·경기대학교**

A Study on the Availability Assessment Method for Instrumentation and Control System of Nuclear Power Plant

Dong Hee Lee*·Kyung H. Nam**

Korea Testing Laboratory*·Kyonggi University**

Abstract

This paper presents a study of an availability evaluation for I&C(Instrumentation and Control) System which it applied for nuclear power plant. The system availability assessment have been implemented to the reactor protection system by the adoption of Markov process. Results are satisfied to the requirement of EPRI and APR1400. Based on the research of I&C system assessment, it will contribute to improve the availability of system and impact the design concept with new design optimization.

Keywords : Reliability, Availability Assessment, Instrumentation and Control System, Nuclear Power Plant

논문접수일 : 2010년 02월 23일 논문수정일 : 2010년 03월 10일 게재확정일 : 2010년 03월 19일

1. 서론

현대 과학기술의 발전으로 인하여 더욱 복잡하고 정교한 시스템의 개발과 생산이 가능하게 됨에 따라, 신뢰도의 개념은 모든 공학 및 과학 분야에서 중요한 위치를 차지하게 되었다. 복잡하고 정교한 시스템일수록 고장률이 높아지게 되면서 시스템 신뢰도는 제조기업의 제품 생산 과정에서도 대단히 중요한 관심분야로 등장하게 되었고 기계, 전기 또는 화학시스템 등 신뢰성 공학에 대부분 적용되고 있다. 이중 원자력발전소, 항공기, 병원시스템과 같이 인간의 생명과 안전에 연관되는 시스템에서는 매우 높은 신뢰도를 요구하고 있다.

이중 원자력발전소의 두뇌와 신경망에 해당되고, 원자력발전소의 안전 운전을 보장하며 사고 예방에 필수적인 시스템이 원자력발전소의 제어계측(Instrumentation and Control, I&C) 시스템이다. 제어계측 시스템은 주기적으로 계측을 수행하고 많은 수의 센서를 짧은 시간에 자동으로 계측할 수 있으며, human error의 최소화, 위험 발생 시의 조기경보를 실시함으로써 동적 측정을 실시할 수 있는 시스템이다. 원자력 시설에 방사능 누출사고가 발생할 경우에도 시설 종사자는 물론 주변 환경이 방사능 영향으로부터 안전하게 보호되어야 하므로, 이러한 측면에서 제어계측 시스템에서 신뢰성은 중요한 키워드이며, 이를 정량적으로 평가할 수 있는 정형화되고 객관적인 방법이 필요하다.

원전의 가용성은 안전성과 상반되는 개념으로 정상적으로 운전되어야 할 상황에서 고장에 의하여 원자로가 정지되는 경우를 고려한다. 원전은 고장안전 요건에 따라 설계되어 있으므로, 제어계측 시스템에 고장이 발생하면 원자로를 안전하게 정지시키는 방향으로 작동한다. 제어계측시스템에 발생한 고장으로 발전소가 정지되면 운영자 측면에서 경제적인 손실이 발생되므로 이를 최소화하기 위하여 원자력발전소 운영자는 안전성 분석과는 별도로 가용도에 대한 정량적인 평가를 요구하고 있다. 제어계측 시스템의 고장으로 인한 원자로 불시정지의 척도는 평균고장시간(mean time between failure of system, MTBFS)으로 표시된다. 원전의 안전성 향상 및 MTBFS를 개선하기 위하여 제어계측 시스템은 일반적으로 4중화 구조로 설계되어 있다. 다중화 된 제어계측 시스템은 2개 이상의 채널에서 설정치를 초과한 신호가 입력될 때 원자로정지 신호를 발생하는 2-out-of-4 로직으로 구성되어 있다. 즉, 2-out-of-4 로직은 동일한 기능을 하는 4개의 채널 중에서 1개의 채널에서만 고장이 발생한 경우에는 불필요한 원자로 정지가 발생하지 않으나 4개의 채널 중 2개 이상의 채널에서 고장이 발생하면 원자로가 정지된다.

그러나 현재 원전의 제어계측 시스템의 가용도를 평가하기 위한 연구가 중요함에도 불구하고 현재까지 많은 연구가 이루어지지 못하였다. 현진우(2006)는 차세대원전 기술개발에서 사용하였던 외국원전 자료를 토대로 원자력발전소의 디지털 분산제어 적용 시 고려해야 할 핵심 요소 중 신뢰도에 초점을 맞추어 다중화를 통한 이중구조(병렬구조) 분산제어기의 신뢰도를 계산하여 신뢰도 향상을 이론적으로 고찰하였으며, 네트워크 형태별 프로토콜을 분석하여 통신망 설계에 관한 방법을 제시하였다. 오연경(2006)은 제어계측 설비의 객관적이고 체계적인 평가방법을 적용한 인터넷 기반을 구축하여 가동원전 제어계측 설비평가, 제어계측 설비정보 및 신뢰성 확인, 설비개선계획 및 정비계획 수립지원 등을 용이하도록 지원하였다. 김만철(2004)은 계측제어계통, 인간기계연계(MMI), 운전원에 대한 정량적 안전성 평가를 위하여

시스템 신뢰도분석 방법인 reliability graph with general gates(RGGG) 방법을 제안하였으며, 인간신뢰도분석을 위한 방법으로 운전원의 상황판단에 대한 정량적인 모형을 제안하였다. 이동영(2005)은 디지털 원자로보호계통의 안전성 평가에 적합한 고장률 예측기법 및 원자로보호계통의 고장으로 인한 원자로 불시정지의 평가척도인 평균고장발생주기를 구하는 기법을 제안하였다. 또한 조영조(1989)는 가법적 중복적응 제어기를 이용하여 마코프 과정에서 제어시스템의 신뢰도 향상을 위한 연구를 수행하였다.

이러한 여러 선행연구 중에서 이동영(2005)은 제어계측 시스템의 확률론적 안전성분석에 사용하고 있는 고장나무 분석기법이 고장영향의 파급 및 유지보수의 효과를 모형에 반영하기 어려운 단점이 있다고 지적하였다. 이러한 문제점을 해결하기 위하여 본 논문에서는 독립사건 확률계산에 활용되고 있는 이항분포 기법을 확장하여 2-out-of-n 다중화 시스템의 MTBFS를 예측하였다. 이를 위하여 고장수리가 수반되는 다중화 시스템의 MTBFS를 계산하기 위해 마코프 과정(Markov process) 기법을 활용하였으며 제어계측 시스템의 고장률 및 MTBFS를 추정하였다. 추정은 실제 PLC 모듈에 접목시켜 추정하였으며 선행연구의 결과와 비교하였다.

2. 원자력발전소의 제어계측 시스템

2.1 제어계측 시스템의 개요

우리나라는 1978년 처음으로 원자력발전소 가동을 시작하여 30년에 걸쳐 원전기술 자립을 위한 노력을 해 온 결과 30년 만에 기술 완전자립을 이뤘다. 두산중공업에서 '원자력발전소 제어계측기술 시스템(MMIS : Man-Machine Interface System)'을 국내기술로 개발한 것은 원자력발전소의 상태감시 및 제어보호 등을 담당하는 원전의 두뇌이자 신경조직에 해당하는 기술이라 할 수 있다. 이 기술은 미국, 프랑스, 캐나다 등 원전 선진국들만이 보유하고 있는 원전 핵심기술로 우리나라가 원전기술 완전자립을 위한 마지막 해결과제였다. MMIS의 개발로 원전 1호기당 1,000억 원 가량의 수입 대체효과를 거두게 됐으며 원전에 대한 토털 솔루션(total solution)을 제공할 수 있어 원자력발전소를 통째로 수출할 수 있게 되었다.

원전 MMIS는 제어계측과 MMI 및 인간공학을 포괄하는 개념으로 최근의 UAE 원전수주에 관한 언론보도에서 원전 제어계측 시스템(MMIS)으로 사용되고 있다. 제어계측 시스템은 원전의 두뇌와 신경망에 해당하는 계통으로 원전의 운전 상태를 감시 및 제어하고 이상상태가 발생하였을 때 원자로를 안전하게 정지하도록 하는 보호기능을 수행하는 원전 안전에 필수적인 주요 설비이다. 원전에서는 보수적인 입장과 인증기술을 요구하는 기술적 특성으로 인해 몇 년 전까지는 아날로그기술로 구현되어 노후화와 기술의 낙후성으로 인해 운전 및 유지보수비용이 증가하고 안전성까지 위협받고 있었다. 최근에 들어서야 컴퓨터 기반의 디지털기술을 채택하고 있는 실정이다. 일반 산업체와는 달리 원전에서 발생하는 사고의 여파는 일반 국민에게 방사능 누출과 방사성물질의 피해를 입힐 수 있는 가능성을 내재하고 있어 이러한 가능성을

배제하는 디지털 제어계측 시스템을 개발하기 위해서는 안전성과 신뢰도 확보가 무엇보다도 중요하다. 그중에서도 높은 신뢰도의 안전성이 요구되는 보호기능을 수행하는 디지털 원자로 안전계통은 더욱 중요하다. 2005년에 준공된 울진 원자로 5·6호기에 디지털 원자로안전계통이 국내에서는 처음으로 채택되었을 정도로 보수적이다. 원전제어계측 시스템이 디지털화되면서 예전에 아날로그 계기가 회로로 구현되던 감시제어 및 보호기능의 대부분이 하드웨어 플랫폼을 기반으로 하는 내장형 소프트웨어로 구현되고 있다.

2.2 제어계측 시스템의 구성요소

원전 제어계측 시스템을 구성하는 주요 하드웨어 플랫폼은 PLC(Programmable Logic Controller), DCS(Distributed Control System)와 PC이다. 안전에 중요한 기능을 구현하는 디지털 안전계통에는 PLC가 사용되고 있다. 원전 PLC가 실시간 운영체제를 포함하는 프로세서 모델, 통신모듈 및 입출력 모듈로 구성되는 것은 일반 산업체에 적용되는 PLC와 같으나 처음부터 원전의 규제요건과 품질활동 하에서 제작되어 사전에 규제기관의 인허가 승인을 획득하여야 한다. 전 세계적으로 이런 요건을 만족하는 PLC는 프랑스 아레바의 Teleperm-XS, 미국 웨스팅하우스의 AC-160 정도이다. 우리나라에서는 최근에 원전의 요건을 만족하는 PLC를 국내기술로 개발하여 국제기관의 인허가를 획득함으로써 국내 원전 제어계측 시스템에 적용할 예정이다.

DCS는 비안전 제어계통에 사용되며, DCS의 주요 소프트웨어로는 system builder, logic builder, graphic builder, report builder, 그리고 상용 데이터베이스를 기반으로 하는 history data server와 operator information station으로 구성된다. 최근의 추세는 DCS가 제어 기능을 담당하면서 감시를 위한 정보 및 그래픽 화면까지 제공하고 있어 예전에 사용되던 감시정보 제공을 위한 플랜트 프로세스 컴퓨터(plant process computer)는 더 이상 사용되지 않는다.

원전에서 PC가 안전등급으로 활용되는 경우, 원자력에 사용할 수 있도록 사용인증과정을 거쳐야 한다. 하드웨어적으로는 원전규제 요건을 만족하여야 하며, 소프트웨어적으로는 장착되는 운영체계의 결정론적 실시간성, 교착상태 회피, 방지 또는 회복 메커니즘, 우선순위 전도, 그리고 multi-tasking 동기상태 등의 요건을 만족하는지 고려하여야 한다. PC는 주로 정보표시나 정보처리를 위한 프로세서로 사용된다.

3. 제어계측 시스템의 가용성 평가

3.1 가용도 분석기법

3.1.1 이항분포를 이용한 가용도 분석기법

T_1, T_2, $\cdots$, T_n을 n개의 채널의 수명을 표시하는 확률변수이고, T가 시스템의 수명을 표시하는 확률변수라고 하자. 만일 시점 t에서의 n개의 채널의 상태를 나타내는 변수를 $X_1(t)$, $X_2(t)$, $\cdots$, $X_n(t)$로 표시하면 $i=1,2,\cdots,n$에 대하여

$$X_i(t)=\begin{cases}1, & T_i>t\\ 0, & T_i\le t\end{cases} \tag{4.1}$$

을 나타내며, 그에 대응하는 채널의 상태벡터와 시스템의 상태는 다음과 같이 표시된다.

$$\underline{X}(t)=(X_1(t),X_2(t),\cdots,X_n(t))\text{과 } \phi(\underline{X}(t)) \tag{4.2}$$

마찬가지로 비수리 시스템에 대하여

$$\phi(\underline{X}(t))=\begin{cases}1, & T>t\\ 0, & T\le t\end{cases} \tag{4.3}$$

을 표시한다. 따라서 채널 i와 시스템의 신뢰도함수 $R_i(t), R_S(t)$는 다음과 같다.

$$R_i(t)=P(T_i>t)=P(X_i=1)=E[X_i(t)] \tag{4.4}$$

$$R_s(t)=P(T>t)=P(\phi(\underline{X}))=1)=E[\phi(\underline{X}(t))] \tag{4.5}$$

n중 k시스템의 상태는 채널의 상태벡터에 의하여 다음과 같이 결정된다.

$$\phi(\underline{X}(t))=\begin{cases}1, & \sum_{i=1}^{n}X_i(t)\ge k\\ 0, & \sum_{i=1}^{n}X_i(t)<k\end{cases} \tag{4.6}$$

즉, n개의 채널 중에서 k개 이상의 채널이 가동될 때에만 시스템은 가동된다. 만일 모든 부품의 신뢰도 같으면 시스템 신뢰도 $R_s(t)$는 다음과 같다.

$$R_s(t)=\sum_{y=k}^{n}\binom{n}{y}[R(t)]^y[1-R(t)]^{n-y} \tag{4.7}$$

일반적으로 제어계측시스템은 동일한 구조를 갖는 4개의 채널로 구성되며, 2개 이상의 채널에서 고장이 발생하면 원자로 보호계통이 정지되는 2-out-of-4 로직으로 구성되어 있다.
2-out-of-4 구조로 설계된 제어계측시스템은 공통원인고장의 발생을 최소화가기 위하여 각 채널들이 전기적 및 물리적으로 독립되어 있으므로, 한 채널에서 발생한 고장이 다른 채널의

고장에 영향을 미치지 않는 독립사건이다. 즉, 각 채널의 고장이 독립사건이므로 채널의 고장 상태는 상호 독립적인 good 또는 failure 상태로 관찰될 수 있다.
2-out-of-4 제어계측시스템의 어느 한 채널에서 고장이 발생한 경우에는 정상적인 운전이 가능하다. 그러나 동시에 2채널 이상에서 고장이 발생하면 원자로가 정지된다. k-out-of-n 시스템은 n개의 채널 중에서 k채널 이상에서 동시에 고장이 발생하면 원자로가 정지된다. 운전 중에 유지보수를 수행하지 않는 경우, k-out-of-n 시스템의 k채널 이상에서 동시에 고장이 발생할 확률은 다음과 같다.

$$\lambda_s = \sum_{y=k}^{n} \binom{n}{y} \lambda^y (1-\lambda)^{n-y} \tag{4.8}$$

여기서, λ_s : k-out-of-n 제어계측시스템 고장률

λ : 제어계측시스템 각 채널의 고장률이며, $0 \le \lambda \le 1$로 제한함

PLC 제어기기는 자체적으로 고장상태를 판단할 수 있는 기능을 보유하고 있다. 이와 같이 고장난 채널을 검출하고 수리하는 시스템의 경우 시스템 운전 중에 한 채널에서 고장이 발생한 상태에서 고장수리가 완료되기 전에(MTTR 시간 내) 다른 채널에서 중복하여 고장이 발생하는 경우에만 원자로보호계통의 기능이 상실된다. 2-out-of-4 로직을 구성하고 있는 4개의 채널 중 어떤 한 채널에서 초기고장이 발생할 확률은 ${}_4C_1\lambda$이다. 고장난 채널의 수리시간 $MTTR$ 동안 나머지 3개 채널 중 어느 한 채널에서 새로운 고장이 발생할 확률은 ${}_3C_1\lambda MTTR$이다. 여기서 λ는 채널의 고장률이다. 그러므로 고장수리가 가능한 2-out-of-4 로직으로 구성된 시스템의 전체 고장률λ_s 및 평균수명 $E_s(t)$는 다음과 같다.

$$\lambda_s = \binom{4}{1}\lambda\binom{3}{1}\lambda MTTR = 12\lambda^2 MTTR \tag{4.9}$$

$$E_s(t) = \frac{1}{\lambda_s} = \frac{1}{12\lambda^2 MTTR}(hour) \tag{4.10}$$

3.2. 마코프 과정을 이용한 가용도 분석

원자력발전소의 제어계측 시스템은 2-out-of-4의 구조로 되어 있어 4개의 채널 중 적어도 3개 이상의 채널이 정상적으로 작동해야 전체 시스템이 안전하게 작동하게 된다. 이러한 시스템 개념을 확장하여 n개의 채널 중 적어도 k개의 채널이 정상적으로 작동해야 전체 시스템이 작동하는 k-out-of-n 구조를 고려하여 보자. 이는 전체 n개의 채널 중 1개의 채널이 고장나게 되면 $n-1$개의 채널이 동작하게 되고 고장난 1개의 채널은 수리과정을 통하여 n개의 정상상태로 전이된다. 이러한 상태전이에 따른 시스템의 정상여부는 n개의 채널 중 k개의 채널이 정상상태일 경우까지 진행되며, $k-1$부터는 시스템이 고장상태로 전이되게 된다. 따라서 이러한 채널간 고장상태의 전이에 따라 각 상태에서의 확률이 결정되게 되며, 이를 이용하여

전체 시스템의 가용도를 계산하는 것이 목적이므로 이를 확률모형으로 전개하면 마코프 과정을 활용할 수 있을 것이다. 다음은 마코프 과정에 대한 정의를 간단히 정리한 것이다 Ross(1997).

유한하고 셀 수 있는 값을 갖는 확률과정 $\{X_n, n=0,1,2,\cdots\}$을 고려하자. 만약 $X_n=i$라면, 확률과정은 시점 n에서 상태 i에 있다고 한다. 이때 상태 i에서 다음 상태인 j로 전이될 고정된 확률 P_{ij}가 있다고 가정하자. 즉, 모든 상태 $i_0, i_1, \cdots, i_{n-1}, i$에 대해서 다음을 가정하자.

$$\Pr\{X_{n+1}=j \mid X_n=i, X_{n-1}=i_{n-1}, \cdots, X_1=i_1, X_0=i_0\}=P_{ij} \qquad (4.11)$$

이러한 확률과정을 마코프 연쇄(Markov chain)라 한다. 식 (4.11)은 과거 상태인 $X_0, X_1, \cdots, X_{n-1}$와 현재 상태인 X_n이 주어졌을 때 미래 상태인 X_{n+1}의 조건부 분포가 과거 상태와는 독립이지만 현재 상태와는 종속으로 주어지는 것을 설명한다. 확률 P_{ij}는 상태 i에 있을 때, 다음 상태인 j로 전이될 확률을 의미하며 다음 조건을 만족한다.

$$P_{ij} \geq 0, \quad i, j \geq 0; \quad \sum_{j=0}^{\infty} P_{ij} = 1, \; i=0,1,2,\cdots.$$

이제 마코프 과정을 이용하여 제어계측 시스템의 가용도 평가를 위하여 다음과 같은 가정을 한다.

가정 1 : 제어계측시스템이 성공적으로 작동하기 위하여 n개의 채널 중 적어도 k ($(1 \leq k \leq n)$개의 채널은 작동해야 한다.

가정 2 : n개의 채널은 서로 독립적이며 각 채널의 고장간 시간 또는 수리시간은 지수분포를 따른다.

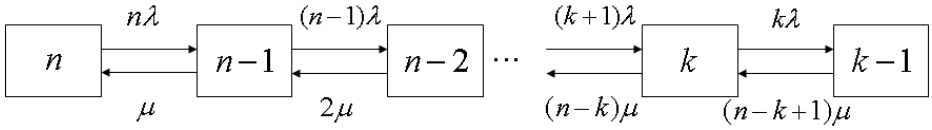
가정 3 : 고장난 채널은 수리가 가능하다.

가정 4 : $n-k+1$개의 채널이 동시에 작동하지 않을 때 제어계측시스템은 작동하지 않으며, 제어계측시스템이 작동하지 않는 경우 더 이상의 채널은 고장나지 않는다.

또한 가용도 계산을 위한 기호는 다음과 같다.

n	제어계측시스템 총 채널의 수
k	시스템이 작동하기 위해 성공적으로 작동해야 하는 최소한의 채널 수
$MTBF_S$	제어계측시스템의 평균고장시간
$MTTR_S$	제어계측시스템의 평균수리시간
$MTTF_I$	개별 채널의 평균고장시간

$MTTR_I$	개별 채널의 평균수리시간
λ	개별 채널의 고장률 $\lambda = 1/MTTF_I$
μ	개별 채널의 수리율 $\mu = 1/MTTR_I$
A	개별 채널의 가용도 $A = (MTTF_I)/(MTTF_I + MTTR_I)$
$\overline{A}$	$\overline{A} = 1 - A \quad \overline{A} = (MTTR_I)/(MTTF_I + MTTR_I)$
A_S	제어계측시스템의 가용도
$N(t)$	시간 t에서 작동하고 있는 채널의 수



<그림 4.2> k-out-of-n 구조의 고장형태

$k \to \infty$일 때, 시간 t에서 시스템이 성공적으로 작동할 확률, 즉

$$\lim_{t\to\infty} \Pr(\text{시간 } t\text{에서 시스템이 성공적으로 작동하는 경우}) = \frac{MTBF_S}{MTBF_S + MTTR_S} = A_s \tag{4.12}$$

이를 $MTBF_S$에 대해 정리하면 다음과 같다.

$$MTBF_S = \frac{MTTR_S A_S}{1 - A_S}. \tag{4.13}$$

시스템이 작동하지 않을 때, $n-k+1$개 채널이 수리를 수행하므로

$$MTTR_S = [\mu(n-k+1)]^{-1} = \frac{MTTR_I}{n-k+1} \tag{4.14}$$

이다. 그러므로 식 (4.14)를 (4.13)에 대입하면 다음과 같다.

$$MTBF_S = \frac{MTTR_I A_s}{(n-k+1)(1-A_S)}. \tag{4.15}$$

수리는 계속 이루어지며, 각 채널들은 독립이기 때문에 시간 t에서 정확하게 j개가 성공적으로 작동하기 위한 확률은 절단된 이항분포를 이용하여 구할 수 있다(여기서, 마코프 과정에 따라 $k-2, k-3, \cdots, 0$은 나타나지 않는다).

$$P(j)=\frac{\binom{n}{j}A^{j}\overline{A}^{n-j}}{\sum_{j=k-1}^{n}\binom{n}{j}A^{j}\overline{A}^{n-j}},\ j=k-1,k,k+1,\cdots,n \tag{4.16}$$

그러므로,

$$\begin{aligned}A_S&=P(k)+P(k+1)+\cdots+P(n)\\&=\left[1+\frac{\binom{n}{k-1}A^{k-1}\overline{A}^{n-k+1}}{\sum_{j=k}^{n}\binom{n}{j}A^{j}\overline{A}^{n-k}}\right]^{-1}\end{aligned} \tag{4.17}$$

이며, (4.15)에 (4.17)을 이용하여 다음과 같이 나타낼 수 있다.

$$\begin{aligned}MTBF_S&=\frac{MTTR_I\sum_{j=k}^{n}\binom{n}{j}A^{j}\overline{A}^{n-j}}{(n-k+1)\binom{n}{k-1}A^{k-1}\overline{A}^{n-k+1}}\\&=\frac{\sum_{j=k}^{n}\binom{n}{j}\left(\frac{\lambda}{\mu}\right)^{n-j}}{\lambda k\binom{n}{k}\left(\frac{\lambda}{\mu}\right)^{n-k}}\end{aligned} \tag{4.18}$$

따라서 시스템의 가용도와 평균수리시간인 $A_S, MTTR_S$는 다음과 같다.

$$A_S=\frac{MTBF_S}{MTBF_S+MTTR_S} \tag{4.19}$$

$$MTTR_S=\frac{MTTR_I}{n-k+1} \tag{4.20}$$

4. 제어계측 시스템의 가용도 분석결과

본 항에서는 선행연구에서 제시한 가용도 평가기법과 마코프 과정을 이용한 가용도 평가를 비교하고자 한다. 즉, 가용도를 분석하기 위하여 원자로보호계통에 적용하여 고장률과 평균 고장시간을 계산하였다. 원자로보호계통은 2-out-of-4 구조로 설계되어 있으며, 각 채널은 이중화된 비교논리 프로세서(BP) 및 동시논리 프로세서(CP), 단일 구조의 자동시험 및 연계 프로세서(ATIP)와 캐비닛 운전원 모듈(COM)로 구성되어 있다.

비교논리 프로세서는 원자로보호계통에 입력되는 신호가 설정치를 초과할 경우 로직레벨 원자로정시 신호를 발생한다. 동시논리 프로세서는 4개 채널의 비교논리 프로세서로부터 로직레벨 원자로정지 신호를 받아 2-out-of-4 논리를 수행한다. 자동시험 및 연계 프로세서는 원자로보호계통의 동작상태를 감시하고 비교논리 프로세서 및 동시논리 프로세서의 주기시험을 관장한다. 또한 캐비닛 운전원 모듈은 유지보수 및 시험 시에 원자로보호계통의 동작상태 및 각종 시험결과를 화면에 표시한다. 비교논리 프로세서, 동시논리 프로세서, 자동시험 및 연계 프로세서는 PLC로 구성되어 있으며, 캐비닛 운전원 모듈은 산업용 PC와 Flat Panel Display(FPD)로 구성되어 있다.

<표 4.1>은 PLC 모듈의 고장률을 나타낸다. 고장률 예측에 필요한 주변온도는 실제 원전에서의 운전환경을 고려하여 30℃로 설정하고, PLC 운용환경을 Ground Benign으로 고장률을 예측하였다. PLC의 평균수리시간은 8시간으로 가정하였다.

<표 4.1> PLC 모듈의 고장률

모듈명	고장률($10^{-6}/hour$)	MTBF
버스장치	0.92E-06/hr	1.09E06hr
전원모듈	8.72E-06/hr	1.15E05hr
프로세서모듈	13.25E-06/hr	7.55E04hr
통신모듈	6.39E-06/hr	1.56E05hr
통신드라이버	7.20E-06/hr	1.39E05hr
디지털 입력모듈	6.39E-06/hr	1.56E05hr
아날로그 입력모듈	7.48E-06/hr	1.34E05hr
디지털 출력모듈	6.34E-06/hr	1.58E05hr
디지털 출력모듈(Relay)	7.03E-06/hr	1.42E05hr
아날로그 출력모듈	10.78E-06/hr	9.28E04hr

비교논리 프로세서 및 동시논리 프로세서에서 발생한 고장은 원자로 정지에 직접적한 영향을 미치므로 가용도 분석방법에 포함하였다. 그러나 자동시험 및 연계 프로세서와 캐비닛 운전원 모듈에서 발생한 고장은 원자로 정지에 직접적인 영향을 미치지 않으므로 가용도 분석에서 제외하였다.

비교논리 프로세서(BP)는 노심보호연산기계통에서 디지털 입력신호, 센서 및 노외핵계측계통에서 아날로그 입력신호를 받아서 기준 및 설정치와 비교한 후 로직레벨 원자로정지 신호를 safety data link(SLD)를 통해 명시 논리 프로세서 (CP)로 전송한다. 또한 비교논리 프로세서(ATIP)와 캐비닛 운전원 모듈(COM)에 동작상태 및 시험상태 정보를 제공한다.

동시논리 프로세서(CP)는 비교논리 프로세서(BP)로부터 safety data analysis를 통해 로직레벨 원자로정지 신호를 받는다. 또한 동시논리 프로세서는 Intra Channel Network을 통해 자동시험 및 연계프로세서와 캐비닛 운전원 모듈(COM)에 동작상태 및 시험상태 정보를 제공한다.

<표 4.2>와 <표 4.3>은 비교논리 프로세서와 동시논리 프로세서에서 각 모듈별 개수에 따른 고장률을 계산한 결과이다. 제시된 결과는 각 모듈의 개수에 따라 이중화 또는 2-out-of-n의 형태로 주어진 고장률이다.

<표 4.2> 비교논리(BP) 프로세서의 고장률

모듈명	개수	고장률($10^{-6}/hour$)	Sum
버스장치	1	0.92E-06/hr	0.92E-06/hr
전원모듈	2	8.72E-06/hr	1.00E-09/hr
프로세서모듈	1	13.25E-06/hr	13.25E-06/hr
통신모듈	1	6.39E-06/hr	6.39E-06/hr
통신드라이버	2	7.20E-06/hr	14.4E-06/hr
디지털 입력모듈	2	6.39E-06/hr	12.78E-06/hr
아날로그 입력모듈	3	7.48E-06/hr	22.44E-06/hr
디지털 출력모듈	1	6.34E-06/hr	6.34E-06/hr
비교논리 프로세서 고장률			76.52E-06/hr

<표 4.3> 동시논리(CP) 프로세서의 고장률

모듈명	개수	고장률($10^{-6}/hour$)	MTBF
버스장치	1	0.92E-06/hr	0.92E-06/hr
전원모듈	2	8.72E-06/hr	1.00E-09/hr
프로세서모듈	1	13.25E-06/hr	13.25E-06/hr
통신모듈	1	6.39E-06/hr	6.39E-06/hr
통신드라이버	2	7.20E-06/hr	14.4E-06/hr
디지털 입력모듈	2	6.39E-06/hr	12.78E-06/hr
아날로그 입력모듈	1	7.48E-06/hr	6.34E-06/hr
디지털 출력모듈	4	6.34E-06/hr	283.12E-06/hr
동시논리 프로세서 고장률			82.2E-06/hr

위 자료를 이용하여 이동영(2005)의 연구에서 제시한 고장률 및 평균고장시간과 본 논문에서 제시한 고장률 및 평균고장시간을 비교하였다. 결과는 다음과 같다.

<표 4.4> 원자로보호계통의 고장률 및 평균고장시간

모듈형태	고장률(선행연구)	고장률(제안방법)
비교논리프로세서 2-out-of-4	5.62E-07/hr	4.98E-07/hr
동시논리프로세서 2-out-of-4	6.49E-07/hr	5.27E-07/hr
원자로보호계통 2-out-of-4	1.21E-06/hr	1.03E-06/hr
원자로보호계통 MTBFS	93.34 Year	111.37 Year

제안된 방법을 통하여 원자로보호계통의 고장률 및 평균고장시간을 비교한 결과 이항분포를 이용한 방법보다 제안된 방법의 고장률이 낮게 나타나는 것을 알 수 있으며, MTBFS는 크게 나타나는 것을 알 수 있다. 이러한 결과는 미국의 전력연구원이 요구하는 50년의 MTBFS 및 APR1400 원전에서 요구하는 60년의 MTBFS를 동시에 만족하는 것을 알 수 있다.
이러한 정량평가 결과에 나타난 바와 같이 운전 중 유지보수가 가능한 시스템은 다중화된 시스템의 일부에서 고장이 발생한 경우에도 제한된 시간 내에 수리가 완료되면 원자로보호계통의 가용도 요건을 만족할 수 있다는 것이다. 따라서 원전의 안전성과 가용성을 증대시키기 위한 시스템 구조화가 절대적으로 필요하며, 향후 계속된 연구가 필요할 것으로 판단된다.

5. 결론

원자력발전소에서 신뢰성이란 매우 중요한 키워드이다. 이러한 신뢰성을 뒷받침하기 위한 신뢰성 평가 및 검증은 필수적이며, 제어계측 시스템의 가용도를 평가하는 것 또한 중요한 연구일 것이다.
제어계측 시스템의 가용도 분석에 마코프 과정을 이용한 방법을 적용하였으며, 이를 원자로보호계통에 적용하여 가용도를 평가하였다. 그 결과 미국의 전력연구원 및 APR1400에서 요구하는 가용도 기준을 충분히 만족하는 것으로 나타났다. 이러한 연구를 토대로 제어계측 시스템의 가용도를 증가시킬 수 있는 새로운 최적설계방법 연구의 기초연구가 될 것으로 판단되며, 향후 개선된 시스템 설계를 제안할 수 있을 것이다.

참고문헌

[1] 김만철(2004), 운전원을 포함한 원전계측제어시스템의 정량적 안전성 평가 방법 개발, 한국과학기술원 박사학위논문.

[2] 오연경(2006), 웹 기반 원전 I&C 설비 신뢰성 평가시스템 구현, 충남대학교 석사학위논문.

[3] 이동영(2005), 디지털 원자로보호계통 신뢰도분석 기법, 충남대학교 박사학위논문.

[4] 조영조(1989), 가법적 중복 적응 제어기를 이용한 제어시스템 향상에 관한 연구, 한국과학기술원 박사학위논문.

[5] 현진우(2006), 원자력발전소의 디지털 분산제어시스템 적용을 위한 DCS의 신뢰도 평가 및 통신망 설계, 충남대학교 석사학위논문.

[6] Ross, S.M.(1997), Introduction to Probability Models, 6th Ed., Academic Press.