원전 디지털 제어계통을 위한 고장허용설계방법론에 관한 연구

論 文
49D - 1 - 1

A Study on Fault-Tolerance Design Methods for Nuclear Digital Control Systems

高 浚 錫* · 崔 重 仁**
(Won-Suk Ko · Jung-In Choi)

Abstract - In this paper, a design method of fault-tolerance is presented for the nuclear digital control systems composed of software and hardware. As a quantitative design method measure of fault-tolerance, we used Reliability, Availability and Safety. To implement the proposed fault-tolerance, a prototype system has been devised for the digital control systems and a quantitative method of 'Markovian Model' is applied. The results provide the appropriate degree of redundancy and diversity, and fail-safe.

Key Words : Fault-Tolerance, Redundancy, Diversity, Fail-safe, Reliability, Availability, Safety

1. 서 론

원자력 발전소의 제어 개념은, 최적의 성능을 유지하기보다는 운전 변수들을 항상 안전 제한치 이내에 유지하는 것이 중요하다. 특히 계통을 불안정하게 하는 외란에 대하여 안정된 대처 능력이 매우 중요한 요구 사항이다[1]. 디지털 계통의 고장 허용성이란 하드웨어적인 고장 혹은 소프트웨어적인 에러에도 계통이 주어진 성능을 수행할 수 있는 특성을 의미한다. 이는 모든 계통의 설계에서 필요한 특성이지만 특히 고신뢰성이 요구되는 분야에서는 더욱 중요한 요건이다[2]. 본 논문에서는 다중성(Redundancy)과 다양성(Diversity)을 적용한 고장 허용 설계 방법을 이용하여 하드웨어 및 소프트웨어로 구성된 원전 디지털 제어 계통인 MDS(Megawatt Demand Setter)의 프로토타입을 구현하고, Markov 모델을 사용한 정량적인 평가결과를 이용하여 신뢰도(Reliability), 가용도(Availability), 안전도(Safety)를 지표로 한 고장 허용 설계의 기준을 제시하고자 한다.

2. 프로토타입 디지털 제어계통 구성[1, 5]

그림 1에 있는 프로토타입의 디지털 제어 계통은 병렬 기능을 지닌 DSP 인 PC40 을 적용한다. 또한 각 모듈을 통과한 신호의 검증을 위해 각 모듈에 D/A, A/D 컨버터를 달아 계측기를 통해 아날로그 신호의 특성을 측정할 수 있도록 한다. 프로토타입의 디지털 제어 계통을 구성함에 있어 하나의 모듈이 고장났을 경우에 대비한 하드웨어 리던던시를 위해 다른 모듈을 채택한 것과 마찬가지로, 아래의 보여진 모듈도 보드상에 두 개의 프로세서가 있어 200%의 리던던시를 지니고 있다. 프로토타입의 디지털 제어 계통은 원자력 발전소의 공정을 모의하는 소프트웨어 모듈과 디지털 계통인 하드웨어 모듈, 그리고 두 계통을 연결하는 연계모듈로 구성된다.

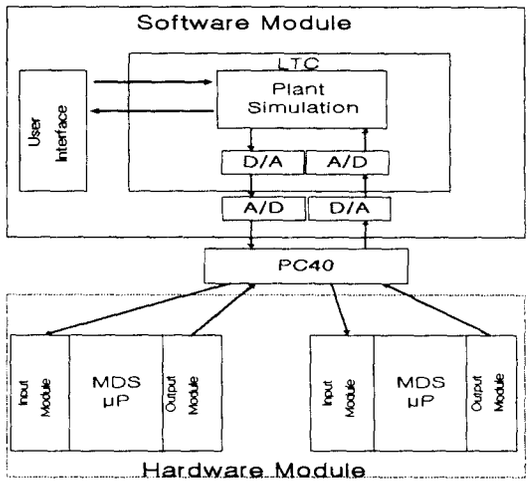

그림 1 프로토타입 디지털 제한계통
Fig. 1 Prototype of Digital Limitation System

2.1 소프트웨어 모듈

이는 원자력 발전소의 모든 공정을 모의하는 시뮬레이터로서 현재는 PC 상에 구현되어 있다. 그림 1에서 소프트웨어 모듈은 PC 모니터 상에 구현된 사용자 연계 화면을 통하여 다양한 발전소 거동을 모의하며 또한 그 거동을 보여주고 있다. 이렇게 모의된 발전소의 공정 변수는 D/A 컨버터를 통하

*正 會 員 : 曉園大 電氣電子工學科 碩士
**正 會 員 : 曉園大 電氣電子工學科 副敎授 · 工博
接受日字 : 1999年 6月 23日
最終完了 : 1999年 12月 10日

여 아날로그 신호로 바뀌고 A/D 컨버터를 통해 DSP(Digital Signal Processor) 보드에 전송되어 실제 발전소 센서로부터 나오는 것처럼 온라인으로 디지털 제어 계통인 MDS 로 전송된다. MDS는 디지털 자동 감시 제한 계통으로서 터빈 제어 계통을 통하여 터빈 부하를 제한함으로써 이 효과가 발전소 계통에 궤환되도록 하며, 여기서 사용되는 제한 알고리즘은 다음과 같다. MDS의 궤환 제한 알고리즘은 먼저 터빈 제어 계통을 통하여 제한 조치를 수행함으로써 그 영향이 발전소 운전 변수들을 제한하도록 한다. MDS는 자동급전계통에서 보내지는 부하 요구 혹은 운전자가 운전자 연계 모듈을 통하여 입력한 부하 요구를 출력과 비교한다. 이 차이에 따라 터빈 부하율이 결정되며, 이는 설계 제한치 혹은 운전원이 정한 설정치에 의해 제한된다. 이렇게 하여 결정된 값은 MDS의 제한 프로그램을 통하여 계산된 값에 의해 비교되어 이 보다 클 경우 제한된다. 제한 프로그램은 발전소 주요 트립 관련 변수값과 트립 설정치 및 부하 요구량을 입력으로 하여 각각의 변수에 대하여 정상 운전 제한치내에 제한 설정치를 결정하게 된다. 이 제한 설정치가 궤환 제한 알고리즘이 작동하는 기준이 되며 알고리즘 작동 영역은 제한 설정치로부터 트립 설정치 사이가 된다. 또한 MDS 의 제한 알고리즘 수행 후 나오는 출력은 다시 D/A , A/D 컨버터를 통하여 소프트웨어 모듈로 전송되어 마치 액추에이터를 통하여 발전소 공정에 입력되듯이 온라인으로 LTC(Long Term Cooling) 코드의 입력이 된다. LTC 코드는 이 입력에 대한 전 계통의 동적 거동을 모의한다.

2.2 하드웨어 모듈

하드웨어모듈은 실제 발전소에 구현될 디지털 계통과 동일한 구조와 성능을 갖도록 구성하였다. 먼저 MDS 계통을 동일한 2개의 연계성이 좋은 마이크로프로세서 상에 구현하여 active-parallel 계통과 stand-by 계통으로 구분 200% 리던던시를 적용하고, MDS 제한 알고리즘은 프로그램 하여 ROM으로 다운로드한 것을 적용한다.

2.3 연계 모듈

본 프로토타입 체제 구성에서 소프트웨어와 하드웨어 모듈간의 입출력 실시간 연계 모듈은 평가 체제의 실현화에 매우 중요한 요소이다. 컨버터로는 PC/16IO8을 이용하여 충분한 채널을 확보하였고 디지털 신호 처리를 위하여 PC40을 이용한다.

3. 정량적 평가 모델링[3]

이 계통 설계의 고장허용성에 대한 정량적 평가방법인 Markov 모델을 적용하기 위하여 이 계통을 그림 2 와 같이 시스템 1과 시스템 2 로 모델링한다.

3.1 시스템 1

시스템 1에서 보면 각각의 부계통은 하드웨어와 소프트웨어로 구성되어 있는데 소프트웨어의 고장은 공통모드고장일 가능성이 높기 때문에 이를 별도로 구분하여 고려하였다. 이는 디지털 계통에 대한 인허가에 있어 매우 중요한 요소로 적용된다. 시스템 1의 Markov 모델의 적용을 위한 동적 상태를 다음과 같이 정의한다.

state 0 : 하나의 유니트가 작동중이고, 다른 하나가 대기중인 경우,
state 1 : 하나의 유니트가 수리중이고, 다른 하나가 작동중인 경우,
state 2 : 두 개의 유니트가 고장이고, 둘 중의 하나가 수리중인 경우

이후에는 가용도(availability)해석을 위한 천이행렬을 M_a로 하고 신뢰도(reliability)해석을 위한 천이행렬을 M_r로 표시한다. 행렬 M_r은 M_a의 고장계통상태에 대응하는 열에 0을 적용하여 얻을 수 있다. 또한 고장율을 λ, 수리율은 μ로 정의하여 표시하기로 한다.

3.1.1 가용도 모델

시스템 1은 다음과 같이 두 개의 독립적인 유니트로 구성할 수 있다. 각각의 유니트는 작동중에 순간적인 고장율 λ를 가지며, λ_c는 공통모드고장에 기인하는 유니트의 순간적인 고장율을 나타낸다. 고장은 작동중 고장 혹은 공통고장으로 인해 발생하므로 Δt에서 하나의 유니트의 고장확률은 $(\lambda+\lambda_c)\Delta t$ 가 된다. 유니트의 수리가 고장 발생 후에 임의적이고 순간적으로 이루어진다고 가정할 경우 순간수리율은 μ이다.

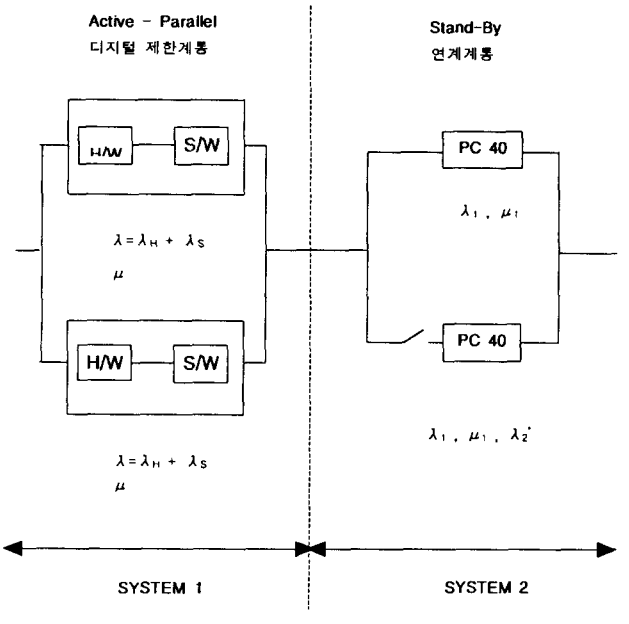

그림 2 고장허용성 정량적 평가모델
Fig. 2 Fault tolerance quantitative Evaluation model

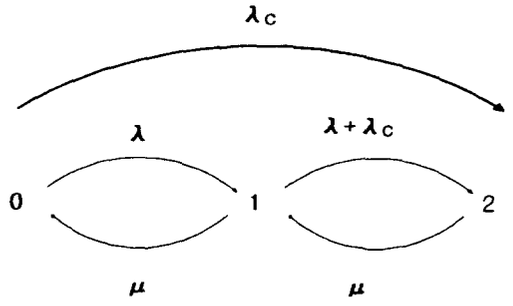

그림 3 시스템 1 의 가용도 해석을 위한 상태천이도
Fig. 3 State transition for availability analysis of system 1

시간 t에서 각각의 상태의 확률 $P_n(t)$의 집합을 전개할 경우 시스템은 n 차이며, 천이는 매우 작은 시간 Δt 동안에 조건확률 $\lambda \Delta t$와 $\mu \Delta t$를 가지고 일어난다

$$\begin{aligned}
\frac{dP_0(t)}{dt} &= -(\lambda+\lambda_c)P_0(t) + \mu P_1(t) \\
\frac{dP_1(t)}{dt} &= \lambda P_0(t) - (\lambda+\lambda_c+\mu)P_1(t) + \mu P_2(t) \\
\frac{dP_2(t)}{dt} &= \lambda_c P_0(t) + (\lambda+\lambda_c)P_1(t) - \mu P_2(t)
\end{aligned} \tag{1}$$

이 식을 행렬의 형태를 이용하여 표현하면,

$$\frac{d}{dt}\begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \end{bmatrix} = \begin{bmatrix} -(\lambda+\lambda_c) & \mu & 0 \\ \lambda & -(\lambda+\lambda_c+\mu) & \mu \\ \lambda_c & \lambda+\lambda_c & -\mu \end{bmatrix} \begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \end{bmatrix} \tag{2}$$

이고, 이 식을 다시 쓰면

$$dP(t)/dt = M_a P(t) \tag{3}$$

여기서

$$M_a = \begin{bmatrix} -(\lambda+\lambda_c) & \mu & 0 \\ \lambda & -(\lambda+\lambda_c+\mu) & \mu \\ \lambda_c & \lambda+\lambda_c & -\mu \end{bmatrix} \tag{4}$$

이 행렬의 고유치는 다음과 같이 계산된다.

$$\begin{aligned}
&|sI - M| = 0 \\
&s_0 = 0, \\
&s_1 = -(\lambda+\lambda_c+\mu) - (\mu\lambda)^{1/2} \\
&s_2 = -(\lambda+\lambda_c+\mu) + (\mu\lambda)^{1/2}
\end{aligned} \tag{5}$$

모든 상태 확률의 합에서 가용도의 확률을 빼주면 비가용도가 된다. 비가용도를 Q(t) 라고 하면,

$$Q(t) = 1 - A(t) = \sum_{n=N_u+1}^{N} P_n(t)$$
(N: state의 총수 , N_u: upstate의 수) (6)

여기서 A(t) 는 $\sum_{n=0}^{N_u} P_n(t)$ 이다. 따라서, 이 계통의 가용도 해석을 위해 $P_2(s)$ 의 값을 구하고 역라플라스변환을 행하면, $P_n(s) = [cof(sI-M)^T]_{n0}/\Delta$ 의 형태로 구하고, 여기서 Δ = (s - s_0) (s - s_1) ⋯ (s - s_N) 이다.

$$\begin{aligned}
P_2(s) &= \frac{(-1)^2}{\Delta}\begin{vmatrix} -\lambda & -\lambda_c \\ s+\lambda+\lambda_c+\mu & -(\lambda+\lambda_c) \end{vmatrix} \\
&= \frac{(\lambda+\lambda_c)^2 + \lambda_c(s+\mu)}{s(s-s_1)(s-s_2)}
\end{aligned} \tag{7}$$

$P_2(s) = A + B + C$ 로 놓고 부분분수 전개를 통해 각각의 값을 구하면,

$$\begin{aligned}
A &= \sum_{j=0}^{2} b_{2j}(s-s_j)^{-1} \\
b_{20} &= (\lambda+\lambda_c)^2/s_1 s_2 \\
b_{21} &= (\lambda+\lambda_c)^2/s_1(s_1-s_2) \\
b_{22} &= -(\lambda+\lambda_c)^2/s_2(s_1-s_2)
\end{aligned} \tag{8}$$

상수 a에 대한 다음 정리에 의하여 역라플라스변환을 행하면,

$$\ell^{-1}[(s-a)^{-K}] = t^{K-1}e^{at}/(k-1)! \qquad k = 1, 2, \cdots$$

$$A = \frac{(\lambda+\lambda_c)^2}{s_1 s_2} + \frac{(\lambda+\lambda_c)^2(s_2 e^{s_1 t} - s_1 e^{s_2 t})}{s_1 s_2(s_1-s_2)} \tag{9}$$

$$\begin{aligned}
B &= \sum_{j=0}^{2} b_{2j}(s-s_j)^{-1} \\
b_{20} &= \mu\lambda_c/s_1 s_2 \\
b_{21} &= \mu\lambda_c/s_1(s_1-s_2) \\
b_{22} &= -\mu\lambda_c/s_2(s_1-s_2)
\end{aligned} \tag{10}$$

$$B = \frac{\mu\lambda_c}{s_1 s_2} + \frac{\mu\lambda_c(s_2 e^{s_1 t} - s_1 e^{s_2 t})}{s_1 s_2(s_1-s_2)} \tag{11}$$

$$\begin{aligned}
C &= \sum_{j=1}^{2} b_{2j}(s-s_j)^{-1} \\
b_{21} &= \lambda_c/(s_1-s_2) \\
b_{22} &= -\lambda_c/(s_1-s_2)
\end{aligned} \tag{12}$$

$$C = \frac{\lambda_c(e^{s_1 t} - e^{s_2 t})}{(s_1-s_2)} \tag{13}$$

$$\begin{aligned}
P_2(t) &= \frac{((\lambda+\lambda_c)^2 + \mu\lambda_c)\cdot((s_1-s_2) + (s_2 e^{s_1 t} - s_1 e^{s_2 t}))}{s_1 s_2(s_1-s_2)} \\
&\quad + \frac{\lambda_c(e^{s_1 t} - e^{s_2 t})}{s_1 - s_2}
\end{aligned} \tag{14}$$

비가용도 확률 $P_2(t)$ 는 식 (14)와 같으므로 시스템 1의 가용도는 $A(t) = 1-P_2(t)$를 통하여 구한다.

3.1.2 신뢰도 모델

고장율 λ 하에서 두 개의 독립적인 유니트중 하나의 유니트가 고장이라면, 계통의 신뢰도는 다음과 같은 형태로 유도한다. 그림 4는 state 2로부터는 수리를 할 수 없는 신뢰도 해석을 위한 상태천이도이다. 단 대기 중에는 고장이 발생하지 않고 하나의 유니트는 계통을 작동할 수 있어야한다.

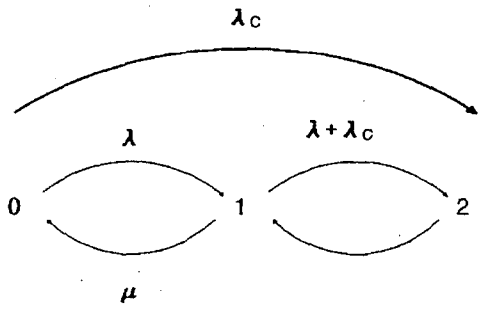

그림 4 시스템 1 의 신뢰도 해석을 위한 상태천이도
Fig. 4 State transition for reliability analysis of system 1

천이행렬은

$$M_r=\begin{bmatrix} -(\lambda+\lambda_c) & \mu & 0 \\ \lambda & -(\lambda+\lambda_c+\mu) & 0 \\ \lambda_c & \lambda+\lambda_c & 0 \end{bmatrix} \tag{15}$$

이 행렬의 고유치는

$$\begin{aligned} s_0 &= 0\ , \\ s_1 &= -1/2\ (2\lambda + 2\lambda_c + \mu) + (\mu^2 + 2\mu\lambda + 2\mu\lambda_c)^{1/2} \\ s_2 &= -1/2\ (2\lambda + 2\lambda_c + \mu) - (\mu^2 + 2\mu\lambda + 2\mu\lambda_c)^{1/2} \end{aligned} \tag{16}$$

상기 과정을 반복하여 얻은 $P_2(t)$ 는

$$P_2(t) = \frac{((\lambda+\lambda_c)^2+\mu\lambda_c)\cdot((s_1-s_2)+(s_2e^{s_1t}-s_1e^{s_2t}))}{s_1s_2(s_1-s_2)} + \frac{\lambda_c(e^{s_1t}-e^{s_2t})}{s_1-s_2} \tag{17}$$

식 (17)의 값을 이용, $R(t) = 1-P_2(t)$ 를 통하여 시스템 1의 신뢰도를 구한다. 식(14) 와 비교하면 가용도 모델과 다른 점은 천이행렬 상의 고유치의 값이고, 행렬의 형태는 같으므로 $P_2(t)$ 의 형식은 같다.

3.1.3 안전도 모델

시스템의 안전도 (Safety)란 고장이 발생하더라도 안전성에는 영향을 주지 않는 경우를 포함한 계통의 정상 상태 확률로서 고장 허용 설계인 실패-안전 (Fail-Safe) 에 대한 정량적 지표이다. 안전도에 대한 정량적 모델은 일반적으로 고장이 나더라도 검출이 되는 경우를 실패-안전 상태로 정의함으로써 검출 할 수 있는 부분은 고장율에서 제거하는 것을 의미한다. 따라서 다음과 같이 생각할 수 있다. 고장상태를 검출 할 수 있는 확률, 즉 검출율을 γ 라고 하면 그림 3에서 고장상태 P_2는 안전한 상태 FS (Fail-Safe) P_{FS}와 안전하지 못한 상태 FU(Fail-Unsafe) P_{FU}로 나누어진다. 이때 $P_{FU} = (1-\gamma)\ P_2$이 되며 안전도 S(t)는 다음과 같이 표현할 수 있다.

$$\begin{aligned} S(t) &= 1 - P_{FU} = 1 - (1-\gamma)\ P_2 \\ &= 1 - (1-\gamma)\ (1-R(t)) \\ &= \gamma + (1-\gamma)\ R(t) \end{aligned} \tag{18}$$

여기서 R(t)는 시스템 1의 주어진 신뢰도이다.

3.2 시스템 2

시스템 1과 같은 방법을 적용하여 해석한다. 시스템 2의 Markov 모델의 적용을 위한 동적 상태는 다음과 같이 정의한다.

state 0 : 유니트 1이 작동중이고
　　유니트 2가 대기하는 경우
state 1 : 유니트 1이 수리중이고
　　유니트 2가 작동중인 경우
state 2 : 유니트 2가 수리중이고
　　유니트 1이 작동중인 경우
state 3 : 두 개의 유니트가 고장나고 수리중인 경우

3.2.1 가용도 모델

시스템 2는 두 개의 독립된 유니트로 구성되어 있으며, 1번 유니트에 대해 2번 유니트는 대기상태이다. 그림 5 로 모델링하였고 시간 t에서 각각의 상태의 확률 $P_n(t)$의 집합을 전개한다. 여기서 λ^*은 대기중 고장이 일어날 확률이다. 시스템은 n 차이고 천이는 매우 작은 시간 Δt 동안에 조건확률 $\lambda\Delta t$와 $\mu\Delta t$를 가지고 일어난다고 하면

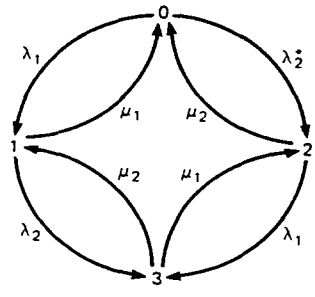

그림 5 시스템 2 의 가용도 해석을 위한 상태천이도
Fig. 5 State transition for availability analysis of system 2

$$\begin{aligned}
\frac{dP_0(t)}{dt} &= -(\lambda_1 + \lambda_2^*)P_0(t) + \mu_1 P_1(t) + \mu_2 P_2(t) \\
\frac{dP_1(t)}{dt} &= \lambda_1 P_0(t) - (\lambda_2 + \mu_1)P_1(t) + \mu_2 P_3(t) \\
\frac{dP_2(t)}{dt} &= \lambda_2^* P_0(t) - (\lambda_1 + \mu_2)P_2(t)' + \mu_1 P_3(t) \\
\frac{dP_3(t)}{dt} &= \lambda_2 P_1(t) + \lambda_1 P_2(t) - (\mu_1 + \mu_2)P_3(t)
\end{aligned} \tag{19}$$

다음과 같은 형태로 다시 쓰면,

$$dP(t) / dt = M_a P(t)$$

여기서,

$$M_a = \begin{bmatrix} -(\lambda_1 + \lambda_2^*) & \mu_1 & \mu_2 & 0 \\ \lambda_1 & -(\lambda_2 + \mu_1) & 0 & \mu_2 \\ \lambda_2^* & 0 & -(\lambda_1 + \mu_2) & \mu_1 \\ 0 & \lambda_2 & \lambda_1 & -(\mu_1 + \mu_2) \end{bmatrix} \tag{20}$$

시스템 1 과 같은 방법으로 고유치를 구하고 비가용도를 구한다. $P_3(s)$ 는

$$\begin{aligned}
P_3(s) &= \frac{(-1)^3}{\Delta} \begin{vmatrix} -\lambda_1 & -\lambda_2^* & 0 \\ s+\lambda_2+\mu_1 & 0 & -\lambda_2 \\ 0 & s+\lambda_1+\mu_2 & -\lambda_1 \end{vmatrix} \\
&= \frac{\lambda_1((\lambda_2^*+\lambda_1)(s+\lambda_2)+(\lambda_2^*\mu_1+\lambda_2\mu_2))}{s(s-s_1)(s-s_2)(s-s_3)}
\end{aligned} \tag{21}$$

$P_3(s) = A - B + C - D + E - F$ 로 놓고 부분분수 전개를 통해 각각의 값을 구하면,

$$\begin{aligned}
A &= \sum_{j=1}^{3} b_{2j}(s-s_j)^{-1} \\
b_{21} &= \lambda_1\lambda_2^* / (s_1-s_2)(s_1-s_3) \\
b_{22} &= \lambda_1\lambda_2^* / (s_2-s_1)(s_2-s_3) \\
b_{23} &= \lambda_1\lambda_2^* / (s_3-s_1)(s_3-s_2)
\end{aligned} \tag{22}$$

$$A = \frac{(\lambda_1\lambda_2^*)((s_2-s_3)e^{s_1t} - (s_1-s_3)e^{s_2t} + (s_1-s_2)e^{s_3t})}{(s_1-s_2)(s_1-s_3)(s_2-s_3)} \tag{23}$$

$$\begin{aligned}
B &= \sum_{j=1}^{3} b_{2j}(s-s_j)^{-1} \\
b_{21} &= \lambda_1\lambda_2 / (s_1-s_2)(s_1-s_3) \\
b_{22} &= \lambda_1\lambda_2 / (s_2-s_1)(s_2-s_3) \\
b_{23} &= \lambda_1\lambda_2 / (s_3-s_1)(s_3-s_2)
\end{aligned} \tag{24}$$

$$B = \frac{(\lambda_1\lambda_2)((s_2-s_3)e^{s_1t} - (s_1-s_3)e^{s_2t} + (s_1-s_2)e^{s_3t})}{(s_1-s_2)(s_1-s_3)(s_2-s_3)} \tag{25}$$

$$\begin{aligned}
C &= \sum_{j=0}^{3} b_{2j}(s-s_j)^{-1} \\
b_{20} &= \lambda_1\lambda_2^*\lambda_2 / s_1s_2s_3 \\
b_{21} &= \lambda_1\lambda_2^*\lambda_2 / s_1(s_1-s_2)(s_1-s_3) \\
b_{22} &= \lambda_1\lambda_2^*\lambda_2 / s_2(s_2-s_1)(s_2-s_3) \\
b_{23} &= \lambda_1\lambda_2^*\lambda_2 / s_3(s_3-s_1)(s_3-s_2)
\end{aligned} \tag{26}$$

$$C = -\frac{\lambda_1\lambda_2^*\lambda_2}{s_1s_2s_3} + \frac{\lambda_1\lambda_2^*\lambda_2(s_2s_3(s_2-s_3)e^{s_1t} - s_1s_3(s_1-s_3)e^{s_2t} + s_1s_2(s_1-s_2)e^{s_3t})}{s_1s_2s_3(s_1-s_2)(s_1-s_3)(s_2-s_3)} \tag{27}$$

$$\begin{aligned}
D &= \sum_{j=0}^{3} b_{2j}(s-s_j)^{-1} \\
b_{20} &= \lambda_1\lambda_1\lambda_2 / s_1s_2s_3 \\
b_{21} &= \lambda_1\lambda_1\lambda_2 / s_1(s_1-s_2)(s_1-s_3) \\
b_{22} &= \lambda_1\lambda_1\lambda_2 / s_2(s_2-s_1)(s_2-s_3) \\
b_{23} &= \lambda_1\lambda_1\lambda_2 / s_3(s_3-s_1)(s_3-s_2)
\end{aligned} \tag{28}$$

$$D = -\frac{\lambda_1\lambda_1\lambda_2}{s_1s_2s_3} + \frac{\lambda_1\lambda_1\lambda_2(s_2s_3(s_2-s_3)e^{s_1t} - s_1s_3(s_1-s_3)e^{s_2t} + s_1s_2(s_1-s_2)e^{s_3t})}{s_1s_2s_3(s_1-s_2)(s_1-s_3)(s_2-s_3)} \tag{29}$$

$$\begin{aligned}
E &= \sum_{j=0}^{3} b_{2j}(s-s_j)^{-1} \\
b_{20} &= \lambda_1\lambda_2^*\mu_1 / s_1s_2s_3 \\
b_{21} &= \lambda_1\lambda_2^*\mu_1 / s_1(s_1-s_2)(s_1-s_3) \\
b_{22} &= \lambda_1\lambda_2^*\mu_1 / s_2(s_2-s_1)(s_2-s_3) \\
b_{23} &= \lambda_1\lambda_2^*\mu_1 / s_3(s_3-s_1)(s_3-s_2)
\end{aligned} \tag{30}$$

$$E = -\frac{\lambda_1\lambda_2^*\mu_1}{s_1s_2s_3} + \frac{\lambda_1\lambda_2^*\mu_1(s_2s_3(s_2-s_3)e^{s_1t} - s_1s_3(s_1-s_3)e^{s_2t} + s_1s_2(s_1-s_2)e^{s_3t})}{s_1s_2s_3(s_1-s_2)(s_1-s_3)(s_2-s_3)} \tag{31}$$

$$\begin{aligned}
F &= \sum_{j=0}^{3} b_{2j}(s-s_j)^{-1} \\
b_{20} &= -\lambda_1\lambda_2\mu_2 / s_1s_2s_3 \\
b_{21} &= \lambda_1\lambda_2\mu_2 / s_1(s_1-s_2)(s_1-s_3) \\
b_{22} &= \lambda_1\lambda_2\mu_2 / s_2(s_2-s_1)(s_2-s_3) \\
b_{23} &= \lambda_1\lambda_2\mu_2 / s_3(s_3-s_1)(s_3-s_2)
\end{aligned} \tag{32}$$

$$F = \frac{\lambda_1\lambda_2\mu_2}{s_1s_2s_3} + \frac{\lambda_1\lambda_2\mu_2(s_2s_3(s_2-s_3)e^{s_1t} - s_1s_3(s_1-s_3)e^{s_2t} + s_1s_2(s_1-s_2)e^{s_3t})}{s_1s_2s_3(s_1-s_2)(s_1-s_3)(s_2-s_3)} \tag{33}$$

$$A(t) = 1 - P_3(t) \tag{34}$$

식 (34)에서 가용도를 구한다.

3.2.2 신뢰도 모델

시스템 2의 신뢰도의 경우도 시스템 1의 방법을 이용한다. 그림 6과 같이 모델링한 후, 신뢰도 해석을 위한 천이행렬 M_r을 구하면,

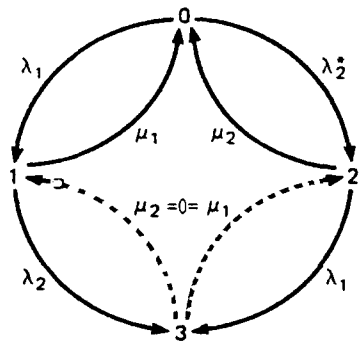

그림 6 시스템 2의 신뢰도 해석을 위한 상태천이도
Fig. 6 State transition for reliability analysis of system 2

$$M_r = \begin{bmatrix} -(\lambda_1 + \lambda_2^*) & \mu_1 & \mu_2 & 0 \\ \lambda_1 & -(\lambda_2 + \mu_1) & 0 & 0 \\ \lambda_2^* & 0 & -(\lambda_1 + \mu_2) & 0 \\ 0 & \lambda_2 & \lambda_1 & 0 \end{bmatrix} \quad (35)$$

$P_3(t)$를 구한 후, $R(t) = 1 - P_3(t)$ (36)
를 통해 신뢰도를 얻는다.

3.2.3 안전도 모델

시스템 1과 같은 방법으로 구하며 다음과 같다.

$$\begin{aligned} S(t) &= 1 - P_{FU} = 1 - (1-\gamma)\, P_3 \\ &= 1 - (1-\gamma)\,(1-R(t)) \\ &= \gamma + (1-\gamma)\, R(t) \end{aligned} \quad (37)$$

여기서 R(t)는 시스템 2의 신뢰도이다.

4. 정량적 계산결과

구현한 프로토타입 계통에 대하여 고장율 및 수리율의 대표적인 값을 추정 대입하고 불확실한 파라미터에 대한 가용도, 신뢰도, 안전도 해석을 수행하였다. 정량적 평가를 위하여 프로토타입 계통의 주요 구성 요소에 대한 실제적 고장율 데이터를 바탕으로 추정하였다. 이에 근거가 되는 데이터가 표 1에 주어져 있다. 이는 "International Electrotechnical Commission 1508-1"[4]을 통해 얻은 센서와 구동기를 포함하는 전기/전자/디지털 계통 (E/E/PE)에 대한 고장율 및 검출율 데이터이다.

표 1 전기/전자/디지털 논리계통의 고장율 및 검출율 데이터
Table 1 Electric/Electronic/Digital Failure rate and detectable rate of logical system

디지털논리계통

요 소	고장율	검출율(%)
Power supply	5×10^{-6}/Hr	90
Input circuit	0.2×10^{-6}/Hr	50
Input module common part	5×10^{-6}/Hr	50
Main processor	50×10^{-6}/Hr	50
Output circuit	0.2×10^{-6}/Hr	50
Output module common part	5×10^{-6}/Hr	50
Watchdog	1×10^{-6}/Hr	50

전자논리계통

요 소	고장율	검출율(%)
Power supply	5×10^{-6}/Hr	90
Input circuit	0.2×10^{-6}/Hr	50
Logic gate	0.1×10^{-6}/Hr	50
Output circuit	0.2×10^{-6}/Hr	50
Timer	1.0×10^{-6}/Hr	50
Trip amplifier	0.4×10^{-6}/Hr	50

전기 논리계통

요 소	고장율	검출율(%)
Power supply	5×10^{-6}/Hr	90
Relay	0.2×10^{-6}/Hr	75
Electromechanical timer	2.5×10^{-6}/Hr	50

센서와 구동기

요 소	고장율	검출율(%)
Sensors	13×10^{-6}/Hr	50
Actuator	13×10^{-6}/Hr	50

4.1 시스템 1

이는 디지털 제한 계통으로서 하드웨어와 소프트웨어로 구성되어 있으므로 표 1에서 디지털논리계통의 데이터를 사용할 수 있다. 이 계통은 한 요소라도 고장이 나면 전체가 고장이 나는 경우이기 때문에 이 계통의 고장율은 각 요소 고장율의 합이다. 즉, $\lambda = 66.4\times10^{-6}$/Hr = 0.58/Yr이며 고장 검출율 γ = 0.5로 정할 수 있다. 여기서 고려하고자 하는 기간은 원전의 운전 기간으로 t = 1[Yr] 및 t=1.5[Yr]인 경우이다. 수리율은 고장이 검출되면 1년 안에 거의 수리가 가능할 것으로 판단되어 μ = 0.5/Yr로 정하였다. 여기서 가장 불확실한 요소가 공통모드고장율 λ_c의 값인데 베타 인자 $\beta = \lambda_c / (\lambda + \lambda_c)$를 0에서 0.2로 변화시켜가면서 민감도 해석을 수행하였다. 이는 주로 소프트웨어에

서 기인하는 것으로 소프트웨어 설계에 다양성 적용의 정도에 따라 변하게 된다.

4.2 시스템 2

이는 디지털 제한 계통과 원전 시뮬레이터 사이의 연계 계통으로 실제로는 원전의 공정 변수를 측정하여 이를 제한 계통에 입력하며 또한 제한 계통의 출력값을 구동기를 통하여 원전 공정에 입력하는 과정을 모의한 것이다. 따라서 이는 표1에서 센서와 구동기 계통의 데이터를 사용하는 것이 타당할 것이다.

즉 $\lambda_1, \lambda_2 = 26 \times 10^{-6}$ /Hr = 0.23 /Yr

그리고 고장검출율 γ = 0.5이다. 고려하는 시간 역시 시스템 1과 동일하게 t= 1[Yr] 및 1.5[Yr] 하였으며 수리율은 μ_1, μ_2 = 0.2/Yr로 정하였다.

4.3 계산 결과

이상의 데이터를 정리하면 다음과 같다.

표 2 프로토타입 계통의 데이터
Table 2 Data of Prototype System

λ	μ	γ_1	λ_1, λ_2	μ_1, μ_2	γ_2
0.58 /Yr	0.5 /Yr	0.5	0.23 /Yr	0.2/Yr	0.5

이를 바탕으로 각각 β가 0에서 0.2까지 변할 때 가용도 A(t), 신뢰도 R(t) 및 안전도 S(t)를 구하였다. 먼저 전체 시스템의 가용도 A = $A_1 \times A_2$ 로서 A_1은 시스템 1의 가용도로서(14) 에서, A_2는 시스템 2의 가용도로서 (34) 에서 계산된다. 이 결과가 표 3에 주어져 있다. 또한 전체 시스템의 신뢰도는 R(t) = $R_1 \times R_2$ 로서 R_1 은 시스템 1의 신뢰도로서 (17)에서, R_2는 시스템 2의 신뢰도로서 (36)에서 계산된다. 이 결과가 표 4에 주어져 있다.

표 3 프로토타입 계통의 가용도
Table 3 Availability of Prototype System

β	A_1 (1)	A_2 (1)	A (1)	A_1 (1.5)	A_2 (1.5)	A (1.5)
0.00	0.9358		0.9175	0.8924		0.8590
0.05	0.9170		0.8990	0.8686		0.8361
0.10	0.8965	0.9804	0.8789	0.8432	0.9626	0.8117
0.15	0.8732		0.8561	0.8160		0.7855
0.20	0.8503		0.8336	0.7866		0.7572

표 4 프로토타입 계통의 신뢰도
Table 4 Reliability of Prototype System

β	R_1 (1)	R_2 (1)	R (1)	R_1 (1.5)	R_2 (1.5)	R (1.5)
0.00	0.9227		0.9022	0.8590		0.8202
0.05	0.8988		0.8788	0.8258		0.7885
0.10	0.8728	0.9778	0.8534	0.7903	0.9548	0.7546
0.15	0.8448		0.8260	0.7526		0.7186
0.20	0.8143		0.7962	0.7122		0.6800

또한 전체 시스템의 안전도는 S(t) = $S_1 \times S_2$ 로서 S_1은 시스템 1의 안전도로서 (18)에서, S_2 는 시스템 2의 안전도로서 (37)에서 계산된다. 이 결과가 표 5 에 주어져 있다.

표 5 프로토타입 계통의 안전도
Table 5 Safety of Prototype

β	S_1 (1)	S_2 (1)	S (1)	S_1 (1.5)	S_2 (1.5)	S (1.5)
0.00	0.9613		0.9506	0.9295		0.9085
0.05	0.9494		0.9389	0.9129		0.8923
0.10	0.9364	0.9889	0.9260	0.8952	0.9774	0.8750
0.15	0.9224		0.9122	0.8763		0.8565
0.20	0.9072		0.8971	0.8561		0.8368

5. 고장허용 설계평가

프로토타입 디지털 제어 계통에 대한 정량적 평가를 통하여 적용된 고장 허용 설계에 대한 효과를 정량적으로 보여주었다.

5.1 다중화 (Redundancy) 기술

다중화 설계에 대한 평가로 단일프로세서와 단일입출력 계통(Simplex), 이중프로세서와 단일입출력 그리고 프로토타입과 같은 이중프로세서와 이중입출력 시스템설계를 비교 평가하였다. 다중성이란 모델링된 고장을 검출 및 정정 할 수 있도록 계통에 정상적인 운전에 필요한 것 이상의 시스템을 부여하는 것으로 여기서는 하드웨어 리던던시를 이용하였다. 단일프로세서와 단일입출력 계통(Simplex) 구조는 프로토타입에서 시스템 1과 시스템 2가 모두 단일계통으로 이루어진 경우로서

가용도는 $$A(\infty) = \frac{\mu}{\lambda + \mu} \tag{38}$$

에 따르고 신뢰도는 $$R(t) = e^{-\lambda t} \tag{39}$$

그리고 안전도는 $$S(t) = \gamma + (1-\gamma)\, R(t) \tag{40}$$

에 따르게 된다. 따라서 단일계통에 대하여 표 2 에 주어진 데이터를 사용하여 가용도, 신뢰도 및 안전도를 구하면 표 6과 같다. 이중프로세서와 단일 입출력의 경우는 시스템 1은 앞서 구한 프로토타입에 대한 계산값이 사용되며 시스템 2에 대해서는 단일계통의 값이 사용된다. 이를 정리하면 다음과 표 7과 같다. 2×1은 이중프로세서의 단일입출력을 의미하고 2×2는 이중프로세서와 이중입출력을 의미한다.

이중프로세서와 이중입출력 구조는 우리가 구현한 프로토타입 계통과 동일한 설계로서 시스템1 및 시스템 2가 모두 다중화된 경우로서 구한 프로토타입에 대한 계산값을 그대로 사용하면 된다. 이를 정리하면 표 8과 같다. 이상의 3가지 구조의 설계를 비교 정리하면 표 9와 같다. 여기서 다중화의 정도에 따라 고장허용성이 증진됨을 알 수 있다.

표 6 단일계통(1×1)의 가용도, 신뢰도 및 안전도
Table 6 Availability, Reliability, Safety of simplex(1×1)

	A(1.0)	A(1.5)	R(1.0)	R(1.5)	S(1.0)	S(1.5)
시스템1	0.6454	0.5693	0.6065	0.4724	0.8033	0.8362
시스템2	0.8130	0.7096	0.7945	0.7082	0.8972	0.8541
전체	0.5247	0.4040	0.4819	0.3346	0.7207	0.7142

표 7 2×1 계통의 가용도, 신뢰도 및 안전도(β= 0.2)
Table 7 Availability, Reliability, Safety of 2×1 system(β= 0.2)

	A(1.0)	A(1.5)	R(1.0)	R(1.5)	S(1.0)	S(1.5)
시스템1	0.8503	0.7866	0.8143	0.7122	0.9072	0.8561
시스템2	0.8130	0.7096	0.7945	0.7082	0.8972	0.8541
전체	0.6913	0.5582	0.6470	0.5044	0.8139	0.7312

표 8 2×1 계통의 가용도, 신뢰도 및 안전도 (β= 0.2)
Table 8 Availability, Reliability, Safety of 2×1system(β= 0.2)

	A(1.0)	A(1.5)	R(1.0)	R(1.5)	S(1.0)	S(1.5)
시스템1	0.8503	0.7866	0.8143	0.7122	0.9072	0.8561
시스템2	0.9804	0.9626	0.9778	0.9548	0.9889	0.9774
전체	0.8336	0.7572	0.7962	0.6800	0.8971	0.8368

표 9 다중화에 따른 고장허용성 (β= 0.2)
Table 9 Fault-Tolerance for redundancy (β= 0.2)

	A(1.0)	A(1.5)	R(1.0)	R(1.5)	S(1.0)	S(1.5)
1×1	0.5247	0.4040	0.4819	0.3346	0.7207	0.7142
2×1	0.6913	0.5582	0.6470	0.5044	0.8139	0.7312
2×2	0.8336	0.7572	0.7962	0.6800	0.8971	0.8368

5.2 다양성 (Diversity) 적용 기술

소프트웨어 설계에 다양성을 적용함으로써 공통모드고장의 비율 β를 감소시킬 수 있다. 다양성이란 여러 형태의 방법을 이용하여 반복적 혹은 공통적인 고장 확률을 줄이는 것을 의미한다. 이 경우 고장허용성이 증진됨을 표 10에서 볼 수 있다.

표 10 다양성 적용에 따른 고장허용성
Table 10 Fault-Tolerance for diversity

	A(1.0)	A(1.5)	R(1.0)	R(1.5)	S(1.0)	S(1.5)
β = 0.2	0.8336	0.7572	0.7962	0.6800	0.8971	0.8368
β = 0.1	0.8789	0.8117	0.7546	0.7546	0.9260	0.8750
β = 0	0.9175	0.8590	0.8202	0.8202	0.9506	0.9085

5.3 실패-안전 (Fail-Safe) 설계 기술

실패-안전 설계를 위하여 고장 검출 기능을 강화하였을 때 고장허용설계 지표인 안전도가 증진됨을 표 11에서 볼 수 있다.

그림 7의 왼쪽에서는 다양성과 다중성에 따른 가용도를 나타내었다. 다양성과 다중성이 증가함에 따라 가용도가 규칙적으로 증대됨을 볼 수 있으며, 다양성과 다중성이 최대일 때 제일 큰 가용도를 볼 수 있다. 고장허용 설계시 70%의 가용도를 고려한다면, 그림 7의 오른쪽과 같이 다중성의 경우는 이중프로세서와 이중입출력을, 다양성의 경우는 공통모드 고장비율을 0.2 이하로 하여 설계하여야 함을 볼 수 있다. 그림 8의 왼쪽에서는 신뢰도를 나타내었다. 다양성과 다중성이 증가함에 따라 신뢰도가 증대됨을 볼 수 있으며, 가용도에 비해서 신뢰도가 낮음을 볼 수 있다. 고장허용 설계시 70%의 신뢰도를 고려한다면, 그림 8의 오른쪽과 같이 다중성의 경우는 이중프로세서와 단일입출력 이상을, 다양성의 경우는 공통모드 고장비율을 0로 하여 설계하여야 함을 볼 수 있다. 그림 9의 왼쪽에서는 다중성과 실패-안정성이 증대될수록 안전도가 증대됨을 볼 수 있다. 고장허용 설계시 70%의 안전도를 고려한다면, 그림 9의 오른쪽과 같이 다중성의 경우는 이중프로세서와 단일입출력 이상을, 고장검출율의 경우는 검출비율을 0.25 이상으로 하여 설계하여야 함을 볼 수 있다.

표 11 실패-안전 설계에 따른 고장허용성
Table 11 Fault-Tolerance according to Fail-safe design

	S(1.0)	S(1.5)
γ =0	0.7962	0.6800
γ =0.25	0.8464	0.7576
γ =0.5	0.8971	0.8368

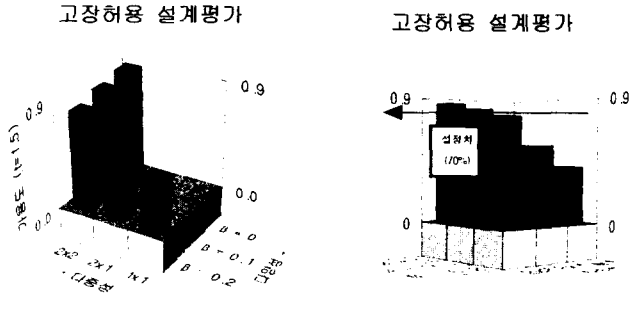

그림 7 다양성과 다중성에 따른 가용도평가
Fig. 7 Availability evaluation for diversity and redundancy

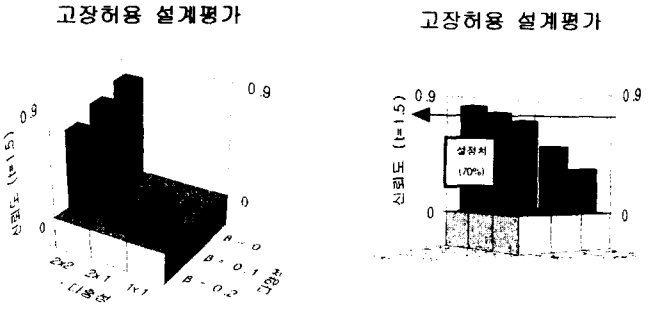

그림 8 다양성과 다중성에 따른 신뢰도평가
Fig. 8 Reliability evaluation for diversity and redundancy

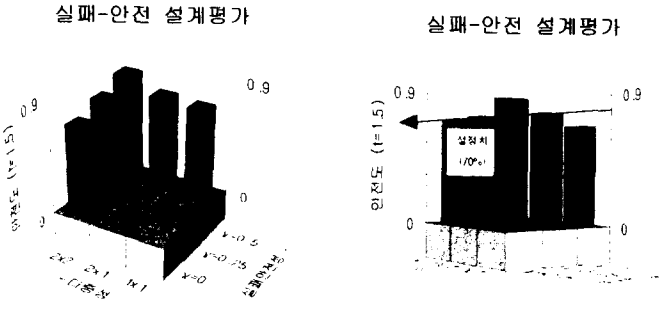

그림 9 다중성과 실패안전성에 따른 안전도평가
Fig. 9 Safety evaluation for redundancy and failure-safe

6. 결 론

본 논문에서는 고장허용설계시 고려할 다중성과 다양성에 대한 기준을 제안하였다. 이를 위하여 프로토타입의 원전 디지털 제어계통을 구현하여 다중화 및 다중성 적용을 하였고, Markov 모델을 이용하여 신뢰도와 가용도에 대한 정량적 평가를 수행하였다. 또한 실패-안전(Fail-Safe) 에 대한 성능지표로 안전도를 제시하였다. 실질적인 고장율 데이터를 이용하여 다중화 및 다양성 적용으로 인한 고장허용성의 정도를 계산하여 가용도와 신뢰도, 안전도가 증진됨을 정량적으로 나타내었다. 최종적으로 이 데이터를 이용, 고장허용설계시 다중성과 다양성, 고장 검출율의 정도를 정할 수 있는 지표로서 사용할 수 있음을 보여주었다.

감사의 글

본 연구는 한국전력공사 전력연구원에서 시행한 '차세대 원자로 기술개발-핵심기술연구(디지털 계측제어계통 기술개발 및 설계평가)' 사업의 지원에 의해 수행되었습니다. 또한 본 연구의 기술적 지원을 하신 배준철, 이건호, 최상철 님께 감사드립니다.

참 고 문 헌

[1] 최중인 외, "디지털 자동감시 제한계통 개발 및 검증", 한국원자력연구소, 1995.
[2] Barry W. Johnson "Design and Analysis of Fault-Tolerant Digital Systems", Addison-Wesley Publishing Company.
[3] Norman J. McCormick "Reliability and Risk Analysis", Academic Press. 1981.
[4] "International Electrotechnical Commission 1508-1", 1997.
[5] 최중인 외, "디지털 계측제어계통 기술개발 및 설계평가",한국전력공사 전력연구원,1999.

저 자 소 개

고 원 석 (高 湲 錫)
1971년 8월 20일 생. 1996년 경원대 전기공학과 졸업. 1998년 경원대 전기전자공학부 졸업(석사).
Tel : 0342-750-5492, Fax : 0342-751-7885
E-mail : kwsiy@mail.kyungwon.ac.kr

최 중 인 (崔 重 仁)
1956년 10월 7일생. 1979년 서울대학교 원자핵공학과 졸업. 1981년 동 대학교 대학원 졸업(석사). 1987년 MIT 계측제어전공(공박). 1988년~1989년 ABB/CE사 연구원. 1987년~1993년 한국원자력연구소 선임연구원. 1993년~현재 경원대학교 전기전자공학부 부교수
Tel : 0342-750-5349
E-mail : jichoi@mail.kyungwon.ac.kr