원자로보호계통의 고장검출기능과 신뢰도의 상관관계 분석

Dependability Analysis of Fault Detection Function and Reliability of Reactor Protection System

김 지 영* · 박 홍 래** · 유 준*** · 이 동 영§ · 최 종 균§
(Ji-Young Kim · Hong-Lae Park · Joon Lyou · Dong-Young Lee · Jong-Gyun Choi)

Abstract - Reliability is an important issue on the digital reactor protection system. This paper presents a quantitative reliability evaluation method to find out an improvement effect of availability for the digital control module with a fault detection function. It is a reliability evaluation model which considers only the electronics parts ocurring a spurious reactor trip by the FMEA(Failure Mode Effect Analysis). Applying the previous and present methods to the reactor protection system, the availability factors are evaluated and compared.

Key Words : 원자로보호계통, 고장검출기능, 신뢰도, 신뢰도 평가모델, 불가용도

1. 서 론

원자로 보호계통은 원자로의 운전상태가 이미 설정된 안전 설정치를 초과하면 발전소를 정지시키는 중요한 설비이다. 국내에서 운전되고 있는 대부분의 원자로보호계통은 아날로그 시스템으로 구성되어 있으며, 최근에 이르러서 비로소 디지털 원자로보호계통이 적용되고 있다. 현재 디지털 시스템으로 구성된 원자로보호계통은 아날로그 시스템과 비교하여 사용된 부품의 수가 많으므로, 부품의 고장률 및 수량만을 이용하여 신뢰도를 계산하는 기존의 고장률 계산기법을 사용하면, 디지털 시스템의 신뢰도가 낮을 수밖에 없다. 또한 디지털 시스템에 설치된 고장진단(surveillance test) 기능은 시스템의 고장상태를 신속히 검출하여 사후보전을 수행할 수 있으므로, 시스템의 가용도가 개선된다. 그러나 이 경우에도 기존의 고장률 계산기법을 사용하면 추가된 부품의 증가에 따라 시스템의 가용도가 저하되는 모순이 발생한다. 이를 해결하기 위하여 본 논문에서는 원자로 보호계통에 고장검출 기능을 추가함에 따라 가용도의 개선효과를 정량적으로 평가할 수 있는 모델을 제안하고, 원자로 보호계통을 구성하는 PLC 제어기기의 디지털 출력모듈에 적용하여 고장검출 기능의 추가에 따라 개선되는 불가용도를 정량적으로 평가하였다.

2. 기존의 신뢰도 계산기법을 이용한 DO모듈의 고장률 평가

* 準 會 員 : 忠南大 工大 電子工學科 碩士課程
** 正 會 員 : 忠南大 工大 電子工學科 博士課程
*** 正 會 員 : 忠南大 工大 情報通信工學部 正敎授 · 工博
§ 韓國原子力硏究所 硏究員

2.1 MIL-HDBK-217F 방법

원자력 분야에서는 일반적으로 Military Standard에서 제안하고 있는 Part Count Method 또는 Part Stress Method를 사용하여 제어기기의 신뢰도를 계산하고 있다[1]. 이들 방법은 제어기기 모듈에 사용된 부품의 수량, 품질계수, 운전환경계수를 이용하여 고장률(failure rate) 및 신뢰도를 예측한다. MIL-HDBK-217F 핸드북은 부품의 신뢰도에 영향을 주는 요인들을 고려하여 각종 전자부품에 대한 고장률 모형을 제시하고 있으며, PLC 제어기기 모듈의 신뢰도는 핸드북에서 제시한 부품들의 신뢰도를 합하여 구한다. 본 연구에서는 PLC 제어기기 모듈의 고장률을 계산하기 위하여 Part Stress Analysis 기법을 사용하였다. 이 기법에서 사용되고 있는 부품고장률 모델은 부품의 종류에 따라 다르나, 고장률 모델을 일반적으로 나타내면 다음과 같다.

$$\lambda_i = \lambda_b \pi_T \pi_Q \pi_E \pi_{oth} \quad Failures/\ 10^6 Hours$$

여기서

λ_i = 부품고장률(Failure/10^6 hours)

λ_b = 기본고장률(Base Failure Rate)

π_T = 부품 운전온도계수(Quality Factor)

π_Q = 부품 품질계수(Environment Factor)

π_E = 부품 운전환경계수(Environment Factor)

π_{oth} = Other Factor($\pi_A, \pi_R, \pi_S, \pi_C, \pi_V, \pi_P$)

를 나타낸다. 위의 부품고장률을 바탕으로 DO모듈의 고장률은 다음과 같이 표시된다.

$$\lambda_S = \sum_{i=1}^{n} \lambda_i \quad (1)$$

여기서 λ_i는 부품의 고장률, λ_s는 모듈의 고장률이다.

2.2 MIL-HDBK-217F를 이용한 DO모듈의 고장률 평가

식 (1)을 이용하여 고장검출 기능이 없는 PLC 제어기기의 기본 DO모듈 고장률을 분석한 결과 2.65E-06 Failures/Hour의 고장률을 나타내었다[4]. 추가된 DO모듈의 고장검출 기능은 입력단 신호와 출력단 신호의 시간차를 보상하는 타이밍 제어장치, 저장장치 및 비교기로 구성되어 있다. 이들 고장검출 기능을 구성하고 있는 부품에 의한 고장률은 0.990954E-06 Failures/Hour을 나타내었다[4]. 고장검출 기능을 포함한 전체 DO모듈의 고장률은 앞에서 구한 DO모듈의 고장률과 고장검출 기능의 고장률의 합으로 표현된다. 고장률 계산 결과는 표 1과 같이 신뢰도 개선을 위해 주기시험 기능을 포함한 DO모듈의 고장률이 고장검출 기능이 없는 기본 DO모듈의 고장률보다 나쁘게 평가되었다.

표 1. 고장률 비교

구분	고장률
기본 DO모듈의 고장률 ①	2.650952E-06
고장검출 기능의 고장률 ②	0.990954E-06
고장검출 기능을 포함한 DO모듈의 고장률 (①+②)	3.641906E-06

이상에서 신뢰도 개선을 위해 추가된 고장검출 기능이 모듈의 고장률을 악화시키는 것으로 평가되었다. 이를 해결하기 위하여 Markov 모델을 이용하여 DO모듈에 대한 가용도를 평가함으로써 신뢰도 개선효과에 대한 정량화 방법(안)의 가능성을 입증하였다[4].

3. 4-기능 분류 신뢰도 평가기법 제안

원자로보호계통을 구성하는 PLC 제어기기에 주기시험 기능을 추가하면 고장상태를 조기에 검출할 수 있으므로 원전 불시정지의 횟수가 줄어든다. 그럼에도 불구하고 Military Handbook에서 제시하고 있는 고장률 계산방법은 주기시험 기능의 구현에 사용된 부품의 수만큼 신뢰도가 나빠진다. 부품수에 따른 고장률 계산방법을 보완하기 위해 제어기기 모듈을 기능에 따라 4가지 세부기능으로 분류하여 신뢰도를 평가하는 모델을 제안하였다.

3.1 4-기능 분류 신뢰도 평가모델

하드웨어 제어기기의 신뢰도를 평가하기 위해서는 각 제어기기들의 기능 및 제어기기 내부에 구현되어 있는 자가진단 및 복구기능에 대한 정확한 분석이 이루어져야 한다[6]. 따라서 각 제어기기가 계통 내부에서 갖는 기능 및 자가진단기능을 고려해서 신뢰도 평가모델을 제시한다.

그림 1은 두 개의 장치(장치 1, 장치 2)로 구성된 시스템을 간략하게 표현한 그림이다. 장치 1은 시스템의 구성품으로 다음의 두 가지 기능을 수행한다. 장치 1의 주 기능은 입력에 따라 의도된 기능을 수행하고 적절한 중간결과를 장치 2에 제공한다. 장치 1의 부 기능은 자가진단 기능으로 장치 1의 출력단에서 출력되는 결과를 피드백 받아서 출력된 결과와 피드백된 결과를 비교하고 그 결과가 일치하지 않으면 출력 불일치 신호를 발생시킨다.

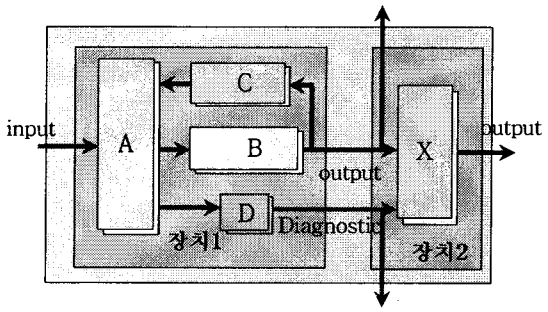

그림 1. 고장검출 기능이 있는 4-기능 신뢰도 모델

부품 A는 입력값을 적절한 출력형태로 변환하여 부품 B로 전달하는 장치 1의 주 기능뿐만 아니라, 피드백된 값과 출력값을 비교하여 출력 불일치 신호를 발생하고 그 결과를 부품 D로 출력하는 부 기능을 수행한다. 부품 B는 A에서 전달된 값을 적절한 출력형태로 변환하여 장치 2로 전달한다. 부품 C는 장치 1의 주 기능과는 관계없이 부품 B의 출력값을 역변환하여 그 값을 부품A에 피드백한다. 부품 D는 부품 A에서 발생한 출력불일치 신호를 받아서 장치 2로 출력하는 기능을 수행한다.

장치 2는 장치 1로부터 결과를 입력받아 다음의 세 가지 기능을 수행한다. 1) 부품 B로부터 입력된 값을 이용하여 의도된 기능을 수행하고 최종결과를 내보낸다. 2) 부품 D에서 전달된 출력불일치 신호를 받아서 장치 1의 건전성을 파악한다. 3) 시스템 외부에서 장치 1의 건전성을 감시할 수 있도록 장치 1의 출력값과 출력불일치 신호를 시스템 외부로 출력한다.

3.2 고장 및 불가용도 모델

3.2.1 고장의 정의

부품 A의 고장은 입력값을 이용하여 적절한 출력형태로 변환하는 기능을 수행하지 못하는 경우 또는 출력값과 피드백값을 비교하는 기능을 적절히 수행하지 못하는 경우로 정의된다. 부품 B, C, D의 고장은 입력값을 이용하여 적절한 출력형태로 변환하는 기능을 수행하지 못하는 경우로 정의된다. 각 부품의 고장률을 각각 λa, λb, λc, λd 라 한다.

다음 표 2는 장치 1을 구성하고 있는 부품들의 고장조합이 장치 1의 주 기능 및 부 기능에 미치는 영향 및 장치 1의 전체 기능에 주는 영향을 나타낸다. 고장조합을 나타낸

표 2의 두번째 항에서 1로 표기한 부품은 정상을 나타내며 0으로 표기한 부품은 고장난 부품을 나타낸다. 이 표에서 주 기능을 수행하는 부품 A 또는 부품 B에 고장이 발생한 경우에 그 영향으로 인하여 장치 1에 고장이 발생하였다. 그러나 세 번째 고장조합 1011에 대해서는 부품 B에 고장이 발생한 경우에도 장치 1의 건전성이 유지되는 것으로 판단하였다. 이는 부품 A가 정상적으로 동작하고 있으므로 부품 B에 발생한 고장을 신속하게 알려주어 즉각적인 보수를 수행할 수 있다. 또한 안전등급 제어기기는 고장안전(Fail-safe) 요건을 만족하여 부품 B에 고장이 발생한 경우에 원자로정지를 유발하는 방향으로 설정이 바뀌도록 설계되어 있으므로 원자로는 안전하게 유지할 수 있다. 이런 측면에서 세 번째 고장조합 1011에 대해서는 부품 B에 고장이 발생한 경우에도 장치 1의 건전성이 유지되는 것으로 판단하였다.

표 2. 부품고장에 의한 장치고장 경우

번호	고장조합 (ABCD)	주기능	부기능	장치 1
1	1111	정상	정상	정상
2	0111	상실	상실	고장
3	1011	상실	정상	정상
4	1101	정상	상실	정상
5	1110	정상	상실	정상
6	0011	상실	상실	고장
7	0101	상실	상실	고장
8	0110	상실	상실	고장
9	1001	상실	상실	고장
10	1010	상실	상실	고장
11	1100	정상	상실	정상
12	0001	상실	상실	고장
13	0010	상실	상실	고장
14	0100	상실	상실	고장
15	1000	상실	상실	고장
16	0000	상실	상실	고장

각 부품의 고장조합에 따른 장치 1의 고장은 다음과 같은 수식을 이용하여 간단히 표현할 수 있다.

$$
\begin{aligned}
&= \bar{A}BCD + \bar{A}\bar{B}CD + \bar{A}B\bar{C}D + \bar{A}BC\bar{D} + A\bar{B}\bar{C}D \\
&\quad + A\bar{B}C\bar{D} + \bar{A}\bar{B}\bar{C}D + \bar{A}\bar{B}C\bar{D} + \bar{A}B\bar{C}\bar{D} + A\bar{B}\bar{C}\bar{D} + \bar{A}\bar{B}\bar{C}\bar{D} \\
&= \bar{A}CD(B+\bar{B}) + \bar{A}\bar{C}D(B+\bar{B}) + \bar{A}C\bar{D}(B+\bar{B}) \\
&\quad + A\bar{B}\bar{C}(D+\bar{D}) + \bar{A}\bar{C}\bar{D}(B+\bar{B}) + A\bar{B}C\bar{D} \\
&= \bar{A}CD + \bar{A}\bar{C}D + \bar{A}C\bar{D} + A\bar{B}\bar{C} + \bar{A}\bar{C}\bar{D} + A\bar{B}C\bar{D} \\
&= \bar{A}D(C+\bar{C}) + \bar{A}\bar{D}(C+\bar{C}) + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\
&= \bar{A}D + \bar{A}\bar{D} + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\
&= \bar{A}(D+\bar{D}) + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\
&= \bar{A} + A\bar{B}\bar{C} + A\bar{B}C\bar{D} \\
&= \bar{A} + A\bar{B}(\bar{C}+\bar{D})
\end{aligned}
$$

따라서 장치 1의 고장확률은 다음과 같다.

$$
\begin{aligned}
&= P\{\bar{A} + A\bar{B}(\bar{C}+\bar{D})\} \\
&= P(\bar{A}) + P(A)P(\bar{B})P(\bar{C}) + P(A)P(\bar{B})P(\bar{D}) \approx P(\bar{A})
\end{aligned}
$$

장치 1의 고장률은 다음과 같은 근사치로 나타낼 수 있다.

$$\lambda_1 = \lambda_a$$

모듈의 고장 λ_M은 장치 1과 장치 2 고장의 합으로 표현되므로 λ_M은 식 (2)와 같이 장치 1 및 장치 2의 고장률 합으로 Part Count Method를 적용하여 계산할 수 있다.

$$\lambda_M = \lambda_1 + \lambda_2 = \lambda_a + \lambda_2 \qquad (2)$$

3.2.2 불가용도 모델

불가용도(unavailability)란 어떤 시점 t 에서 시스템을 사용하려고 할 때 그 시스템이 제대로 동작하지 못할 확률로 정의되며 고장검출 기능이 있는 신뢰도 모델의 불가용도는 다음 식으로 표시된다.[2, 6]

$$Q = \lambda_M \cdot T_a \qquad (3)$$

여기서 T_a 는 고장에 노출된 시간으로 일반적으로 평균 고장수리 시간 MTTR((Mean Time To Repair)이다. MTTR을 감소하기 위해서는 고장발생 시 가능한 빨리 고장발생 여부를 검출하고 신속한 사후보전을 수행하여야 한다. 본 신뢰도 모델은 장치 1의 출력신호 및 출력불일치 신호를 시스템 외부에서 항상 감시할 수 있으므로 시스템에 이상이 발생하면 즉각적으로 유지보수를 수행할 수 있다.

3.3 DO모듈에 대한 4-기능 분류 신뢰도 평가기법 적용

고장모드영향분석 FMEA[7] 결과를 반영하여 제안된 신뢰도 평가모델에 따라 DO모듈을 A,B,C,D의 4가지 세부기능으로 분류하였다. 표 3은 DO모듈에 대한 기능을 분류하고 MIL-HNBK-217F Notice 2의 Part Stress Method를 근거로 하여 DO모듈에서 사용되는 각 부품들의 고장률을 구하였다. DO모듈에서 사용되었으나 모듈의 고장에 전혀 영향을 미치지 않는 부품은 'Don't Care'로 분류하였다.

표 3. 신뢰도 모델에 따라 분류한 고장률 분석

구분		고장률 (단위 : 10^{-6} hr)
장치1	부품 A 고장률 계	0.557244
	부품 B 고장률 계	0.727994
	부품 C 고장률 계	21.601503
	부품 D 고장률 계	0.08833
장치2		7.841439
Don't care		1.57899

3.3.1 고장검출 기능이 없는 DO모듈의 고장률 분석

고장검출 기능이 없는 DO모듈은 부품 A와 부품 B로 분류된 기능만을 수행하도록 설계되어 있다. 즉 DO모듈의 입력값을 적절한 출력형태로 변환하여 장치 2로 넘겨주는 기능을 수행한다. 그러므로 DO모듈의 고장률은 식 (4)와 같이 부품 A와 부품 B 및 장치 2의 고장률의 합으로 표시된다.

$$\lambda_M=\lambda_1+\lambda_2=\lambda_a+\lambda_b+\lambda_2 \quad (4)$$

표 4. 고장검출 기능이 없는 DO모듈의 고장률

구분		고장률(단위 : 10^{-6} hr)
장치1	부품 A 고장률 계	0.557244
	부품 B 고장률 계	0.727994
장치2		7.841439
계		9.126677

3.3.2 고장검출 기능이 있는 DO모듈의 고장률 분석

4-기능 분류 신뢰도 평가기법에서 언급한 바와 같이 고장검출 기능이 있는 DO모듈의 고장률은 식 (5)와 같이 부품 A와 장치 2의 고장률의 합으로 표시된다.

$$\lambda_M=\lambda_1+\lambda_2=\lambda_a+\lambda_2 \quad (5)$$

표 5. 고장검출 기능이 있는 DO모듈의 고장률

구분		고장률(단위 : 10^{-6} hr)
장치1	부품 A 고장률 계	0.557244
장치2		7.841439
계		8.398693

3.3.3 DO모듈의 불가용도 계산

식 (4)와 식 (5)에서 구한 고장률을 이용하여 본 논문에서 신뢰도의 척도로써 사용된 불가용도를 구하면 표 6과 같다.

고장검출기능이 없는 DO모듈에 발생한 고장은 정기검사기간에 DO모듈의 논리검사를 수행하여야만 고장발생을 검출할 수 있다. DO모듈의 논리검사는 30일의 주기로 수행되고 있고 고장은 30일내에서 균일하게 발생할 수 있으므로 논리검사주기를 평균하여 15일로 설정하였다. 그러므로 T는 T = (30일/2) * 24시간 + 8시간 = 368시간이다.

고장검출기능이 있는 DO모듈에 발생한 고장은 자동주기시험 또는 출력불일치 신호에 의해 즉각적으로 판단할 수 있다. 자동주기시험은 8시간마다 한번씩 수행하므로 고장검출에 소요되는 최대시간 T_a는 T_a = 8시간 + 8시간 = 16시간이다. 여기서 고장을 검출하여 수리에 필요한 시간은 EPRI-URD에서 요구하는 8시간을 적용하였다.

표 6. 불가용도 비교

	정상상태 불가용도	정상상태 불가용도값
고장검출기능이 없는 DO모듈	$Q=\lambda_M \cdot \frac{T}{2}$ =9.126677E-06*368	3.358E-03
고장검출기능이 있는 DO모듈	$Q=\lambda_M \cdot T_a$ =8.398683E-06*16	1.34E-04

기존의 디지털 원자로보호계통의 불가용도 평가에 사용된 고장률 평가방법은 제어기기 모듈에 포함된 모든 부품에 고장이 발생하면 원자로불시정지를 일으킬 수 있다는 가정에서 시작하였다. 그러나 본 논문에서 수행한 FMEA 결과에 따르면 디지털 제어기기 모듈에는 고장검출 및 알림기능이 설계되어 있으며, 이들 부품의 고장은 직접적으로 원자로불시정지를 유발하지 않는 것으로 판명되었다.

또한 고장검출 기능을 포함한 PLC 제어기기는 모듈의 고장을 즉각적으로 발견할 수 있으므로 불가용도가 개선됨을 확인하였다.

4. 결 론

기존 원전에서 사용하고 있는 Military Handbook 고장률 계산방법에 추가하여 디지털 기술에 적합한 신뢰도 평가방법론을 개발하므로 제어기기 모듈의 정확한 가용도 및 불가용도를 평가할 수 있다. Markov 모델을 이용하여 고장검출 기능이 추가되었을 때 신뢰도 개선효과의 상관관계를 입증하고, 이를 바탕으로 원전 디지털 제어기기의 신뢰도 예측에 적합한 부품 고장률 계산 및 불가용도 평가기법을 제안하였다. 제안된 방법은 FMEA를 통해 제어기기 모듈의 구성에 사용한 부품을 기능별로 분류하고, 부품의 고장이 원자로불시정지에 전혀 영향을 주지 않는 부품을 고장률 및 불가용도 계산에서 제외하므로 원전의 신뢰도 및 안전성 분석을 정확하게 할 수 있는 기반을 제공하였다.

추후 본 연구내용을 확장하여 디지털 출력(DO) 모듈뿐만 아니라 CPU 모듈, 통신모듈, 각종 입출력 모듈을 포함한 전체 원자로보호계통의 정량적 신뢰도 평가연구가 필요하다.

참 고 문 헌

[1] Military Handbook, "Reliability Prediction of Electronic Equipment : MIL-HDBK-217F"

[2] 이동영, 박주현 외, "계측제어기기 수명평가 현안기술", KAERI/AR-562/2000, 2000.

[3] 모아소프트 신뢰성기술연구소, 신뢰성예측 가이드 (A Guide Book for Reliability Prediction), 교우사.

[4] 김지영, 박홍래, 유준 외, "가용도 분석을 이용한 원자로보호계통 제어기기 출력모듈의 신뢰도 설계", 2003년도 하계종합학술대회 논문집, pp. 2524-2548, 2003. 7, 대한전자공학회.

[5] Krishna B. MISRA, "RELIABILITY ANALYSIS AND PREDICTION : A Methodology Oriented Treatment", Elsevier.

[6] 한국원자력연구소, "원자력 발전소 안전계통에 적용하기 위한 PLC 일반 요건 및 규격, Rev.00.", KAERI/TR-2010/2002, 2002.

[7] ANSI/IEEE Std 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems IEEE, 1987.