EPLD를 이용한 안전성이 고려된 NMR PPC의 보팅메카니즘 설계와 신뢰도 분석

°유동완* · 박희윤** · 구인수** · 서보혁*
경북대학교 전기공학과* · 한국원자력연구소**

Design of a Voting Mechanism considering Safety for NMR PPC Using EPLD and Reliability Analysis

°Dong-Wan Ryoo* · Heui-Youn Park** · In-Soo Koo** · Bo-Hyeok Seo*
Dept.of Electrical Eng. Kyungpook Nat. Univ.* · KAERI**

Abstract- The protection system of the nuclear reactor and chemical reactor are representative of PPC(Plant Protection Controller). This PPC must be designed based on reliability as well as concept of safety, which is a failed system go a way of safe. PPC is consist of part of data acquisition, calculator, communication with redundancy, and a voter is important factor of reliability. Because it is serial connected. This paper presents a Design and Analysis of a Voting Mechanism considering Safety for NMR PPC Using EPLD. In the case of digital implementation a coincidence logic(voter) of PPC, it needs CPU and memory, so increase a number of units. Therefore the failure rate and cost is increased. On the contrary when it is designed EPLD or FPGA.

1. 서 론

예전에 단독으로 운전되는 기계의 고장은 장치의 운용 손실로 끝나게 되지만 요즘의 공장자동화(FA)에서는 전체공정에 치명적으로 작용하고 그로 인한 주변의 손실들이 많게 작용한다. 그리고 복잡하고 정교한 시스템일수록 고장률이 높아지게 되며 신뢰성에 근거를 둔 제어기의 설계는 중요한 위치를 차지하게 되었다.[1-5] 플랜트 보호 제어기는 플랜트의 여러 상태를 입력 받아 플랜트가 이상동작이 고장과 사고로 진단될 때 제어기가 동작해 플랜트의 동작을 정지시켜 플랜트와 인명 등을 보호하는 제어기이다. 원자력 발전소의 원자로보호계통, 화학 반응로가 대표적인 예이다. 이러한 플랜트 보호제어기는 신뢰성뿐 만 아니라 제어기 자체의 고장시 안전성을 고려한 방향으로 고장을 유도하는 안전공학적 설계를 바탕으로 설계되어야 한다. PPC(Plant Protection Controller)는 다중성을 가지는 데이터 취득부, 알고리듬 계산부, 통신인터페이스등으로 구성되지만 그중 보터부분은 각 채널에 직렬로 연결되므로 전체신뢰도에 중요한 요소로 작용한다.[6-7] 본 논문에서는 EPLD를 이용한 안전성을 고려한 NMR(N-Module Redundancy) PPC의 보팅 메카니즘을 설계하고 마르코프모델을 사용하여 신뢰도와 안전성을 분석하였다. 동시논리부(보팅)를 디지털 프로세서로 설계할 경우 프로세서와 프로그램을 저장, 실행할 메모리(램, 롬)가 있어야하므로, EPLD, 또는 FPGA로 설계될 경우에 비해부품의 개수가 증가하므로, 고장률이 높아지며, 가격 역시 높아진다. 그리고 EPLD나 FPGA는 분산제어나 속도면에서도 좋은 결과를 가져올 수 있다.

2. 플랜트 보호 제어기(PPC)의 신뢰도와 안전성

플랜트 보호 제어기는 플랜트의 여러 상태를 입력 받아 플랜트가 비정상상태이거나 고장으로 진단될 때 플랜트의 동작을 정지시켜 플랜트와 인명 등을 보호하는 제어기이다. 원자력 발전소의 원자로보호계통이 대표적인 예이다. 플랜트 보호 제어기는 그림 1과 같이 플랜트의 상태를 입력 받는다. 한 채널의 입력은 벡터 형태이다. 즉 원자력 발전소의 경우 압력, 증기발생기의 수위, 온도, 유량 등에 대한 측정변수를 입력받아 동작한다. 네 채널로 구성된 플랜트 보호 제어기는 각 채널별로 동일변수에 대한 독립된 센서를 통해 입력을 받는다. 각 채널은 고장진단기능을 하는 제어기로 동작한다. 그리고 신뢰성을 재고하기 위하여 병렬로 다중화(Redundancy) 시켰다. 동시논리부(Voter)는 4개중 2개 이상이 일치해야 동작하는 역할을 하는 2/4동시발생논리를 가진다. 바이패스는 운전자가 한 채널을 보수유지 위해 또는 운전자의 판단에 따라 제어기의 동작에서 우회(분리)시킬 필요가 있을 때 분리시키는 역할을 한다.

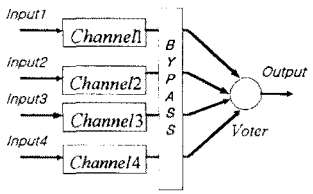


그림 1 플랜트 보호 제어기

플랜트 보호 제어기의 목표 신뢰도가 주어졌다고 가정한다 한 채널의 고장률에 따른 전체 신뢰도를 분석한다면 한 채널의 목표 신뢰도를 구할 수 있다. 그러므로 먼저 한 채널의 고장률에 따른 전체 신뢰도를 분석한다.

2.1 정상상태시 PPC의 신뢰도

한 채널을 바이패스 시키지 않은 정상상태의 플랜트 보호제어기의 신뢰도 분석을 위한 마르코프 모델(Markov model)이다. 각 채널 제어기의 고장률을 상수 λ로 가정한다.

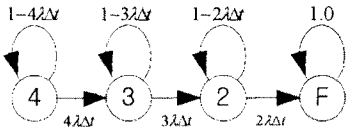


그림 2 정상운전시 플랜트 보호 제어기의 마르코프 모델

아래 $P(t)$는 시각 t 에 각각의 상태에 있을 확률로 두면, 마르코프 모델에 의한 미분 방정식을 아래 식(1)에서(3)과 같이 둘 수 있다.

$$\frac{dP_4(t)}{dt} = -4\lambda P_4(t) \qquad (1)$$

$$\frac{dP_3(t)}{dt} = 4\lambda P_4(t) - 3\lambda P_3(t) \quad (2)$$

$$\frac{dP_2(t)}{dt} = 3\lambda P_3(t) - 2\lambda P_2(t) \quad (3)$$

$$\frac{dP_F(t)}{dt} = 2\lambda P_2(t) \quad (4)$$

여기서 초기값(t=0)은 다음과 같다.

$P_4(0)=1,\ P_3(0)=P_2(0)=P_F(0)=0$

식 (1-3)의 해는 식(5-7)과 같다.

$$P_4 = e^{-4\lambda t} \quad (5)$$

$$P_3 = 4e^{-3\lambda t} - 4e^{-4\lambda t} \quad (6)$$

$$P_2 = 6e^{-2\lambda t} - 12e^{-3\lambda t} + 6e^{-4\lambda t} \quad (7)$$

그러므로 정상상태 즉 1채널이 임의로 바이패스 시키지 않았을 때 신뢰도는 각 상태의 P_4와 P_3와 P_2를 모두 더 하여 식(8)과 같이 나타낼 수 있다.

$$R_{ppc} = P_4 + P_3 + P_2 \quad (8)$$
$$= 6e^{-2\lambda t} - 8e^{-3\lambda t} + 3e^{-4\lambda t}$$

이 보호제어기의 MTTF 다음 식(9)와 같이 나타낼 수 있다.

$$MTTF_{ppc} = \int_0^\infty R_{ppc}(t)\ dt \quad (9)$$
$$= \frac{13}{12\lambda}$$

그리고 보호 제어기의 정상상태의 가용도(steady-state availability: $A(\infty)=A_{ss}$)는 다음과 같이 쓸 수 있다.

$$A_{ss-ppc} = \frac{MTTF}{MTTF+MTTR} \quad (10)$$

$MTTR=\frac{1}{\mu}$,여기서 μ는 수리율(repair rate)이다.

그림 3은 플랜트 보호 제어기의 시간에 따른 신뢰도를 나타내고 있다. A는 한 채널의 고장률(λ)이 $1*10^{-4}$일 때이고, B는 $2*10^{-4}$,그리고 C는 $3*10^{-4}$일 때의 신뢰도를 나타낸다. 그림 4은 플랜트 보호 제어기의 μ는 수리율에 따른 정상상태의 가용도를 나타내고 있다.

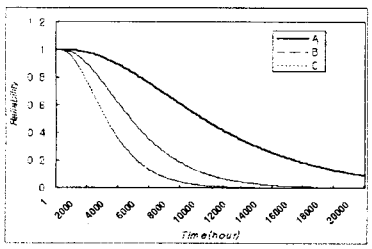


그림 3 PPC의 고장률에 따른 신뢰도
(A: $1*10^{-4}$, B: $2*10^{-4}$, C: $3*10^{-4}$)

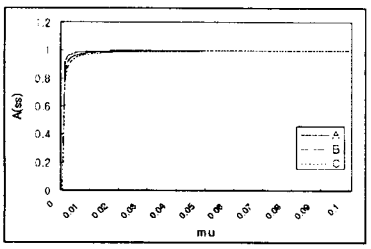


그림 4 PPC 의 MTTR(1/mu)에 따른 정상상태 가용도
(A: $1*10^{-4}$, B: $2*10^{-4}$, C: $3*10^{-4}$)

2.2 한 채널 바이패스시 PPC의 신뢰도

바이패스는 운전자가 한 채널을 보수유지 위해 또는 운전자의 판단에 따라 제어기의 동작에서 우회(분리)시킬 필요가 있을 때 우회시키는 역할을 하며 한 채널이 바이패스 되었을 때 보호 제어기의 신뢰도 분석을 위한 마르코프 모델(Markov model)이다. 여기서는 2/3의 동시논리로 동작한다. 각 채널 제어기의 고장률을 역시 상수 λ로 가정한다.

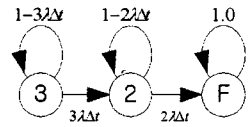


그림 5. 한 채널 바이패스시 PPC의 마르코프 모델

아래 $P(t)$는 시각 t 에 각각의 상태에 있을 확률로 두면, 마르코프 모델에 의한 미분 방정식을 아래 식(11-13)과 같이 둘 수 있다.

$$\frac{dP_3(t)}{dt} = -3\lambda P_3(t) \quad (11)$$

$$\frac{dP_2(t)}{dt} = 3\lambda P_3(t) - 2\lambda P_2(t) \quad (12)$$

$$\frac{dP_F(t)}{dt} = 2\lambda P_2(t) \quad (13)$$

여기서 초기값(t=0)은 다음과 같다.

$P_3(0)=1,\ P_2(0)=P_F(0)=0$ 식 (11-12)의 해는 식(14-15)과 같다.

$$P_3 = e^{-3\lambda t} \quad (14)$$

$$P_2 = 3e^{-2\lambda t} - 2e^{-3\lambda t} \quad (15)$$

그러므로 1채널이 임의로 바이패스 시켰을 때 신뢰도는 각 상태의 P_3와 P_2를 모두 더 하여 식(16)과 같이 나타낼 수 있다.

$$R_{bypass} = P_3 + P_2 \quad (16)$$
$$= 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

그리고 바이패스시 보호 제어기의 MTTF 다음 식(17)와 같이 나타낼 수 있으며, 보호 제어기의 정상상태의 가용도(steady-state availability: $A(\infty)=A_{ss}$)도 역시 다음과 같이 쓸 수 있다.

$$MTTF_{bypass} = \int_0^\infty R_{bypass}(t)\ dt = \frac{5}{6\lambda} \quad (17)$$

$$A_{ss-bypass} = \frac{MTTF}{MTTF+MTTR} \quad (MTTR=\frac{1}{\mu})$$

그림 6은 바이패스된 플랜트 고장 제어기의 시간에 따른 신뢰도를 나타내고 있다. A는 한 채널의 고장률(λ)이 $1*10^{-4}$일 때이고, B는 $2*10^{-4}$,그리고 C는 $3*10^{-4}$일 때의 신뢰도를 나타낸다. 그림 7은 바이패스된 플랜트 고장 제어기의 MTTR($1/\mu$)에 따른 정상상태의 가용도를 나타내고 있다.

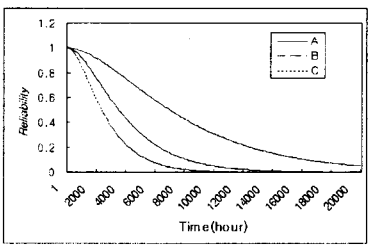


그림 6 바이패스된 ppc의 고장률에 따른 신뢰도
(A: $1*10^{-4}$, B: $2*10^{-4}$, C: $3*10^{-4}$)

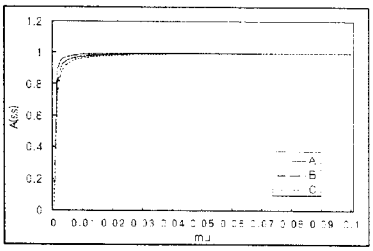


그림 7 Bypassed PPC 의 MTTR에 따른 정상상태 가용도
(A: $1^{*}10^{-4}$, B: $2^{*}10^{-4}$, C: $3^{*}10^{-4}$)

그림 8은 정상상태의 플랜트 보호 제어기와 한 채널 바이패스된 상태에서의 플랜트 보호 제어기 신뢰도 비교를 나타내었다. 그림 9는 정상상태 가용도를 나타내었다. 여기서 고장률은 $1^{*}10^{-4}$이다.

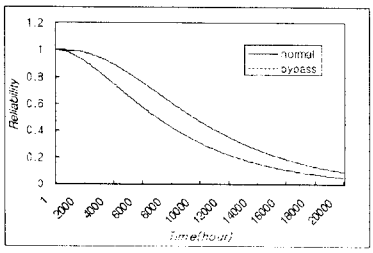


그림 8 normal case PPC 와 bypass case PPC 신뢰도 비교

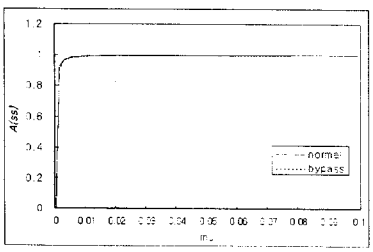


그림 9 normal case ppc 와 bypass case ppc 가용도 비교

2.3 플랜트 보호 제어기의 안전성(Safety)

시스템의 고장은 다시 분류할 수 있는데 하나는 안전한 방향으로 가는 고장과 다른 하나는 비안전 방향으로 가는 고장으로 구분할 수 있다. 실제 원자력 발전소 등과 같은 시스템의 제어기는 제어시스템의 고장발생시 안전한 방향으로 고장이 나는 안전공학적 설계로 가야한다. 아래 그림10에서 보듯이 정상운전 중인 제어기가 고장날 때 안전방향으로 가는 고장과 비안전 방향으로 가는 고장에 대해 안전성을 해석하기 위한 마르코프 모델을 나타내고 있다.

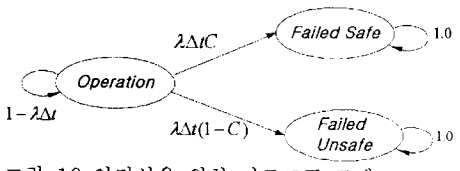


그림 10 안전성을 위한 마르코프 모델

$P_o(t)$는 제어시스템이 정상 동작중 일 때 , $P_{FS}(t)$는 제어시스템이 고장이 일어났으나 안전한 방향으로의 고장, $P_{FU}(t)$는 고장이 일어났으나 비 안전한 방향으로의 고장이 나는 경우에 대해서 각각의 상태에 있을 확률로 두면, 마르코프 모델에 의한 미분 방정식을 아래 식 (18-20)과 같이 둘 수 있다.

$$\frac{dP_o(t)}{dt} = -\lambda P_o(t) \quad (18)$$

$$\frac{dP_{FS}(t)}{dt} = \lambda C P_o(t) \quad (19)$$

$$\frac{dP_{FU}(t)}{dt} = \lambda(1-C) P_o(t) \quad (20)$$

여기서 초기값(t=0)은 다음과 같다.

$P_o(0)=1,\ P_{FS}(0)=P_{FU}(0)=0$

여기서 C는 고장감지보상(fault detection coverage)이다. 식 (18-20)의 해는 식(21-23)과 같다.

$$P_o(t) = e^{-\lambda t} \quad (21)$$

$$P_{FS}(t) = C - Ce^{-\lambda t} \quad (22)$$

$$P_{FU}(t) = (1-C) - (1-C)e^{-\lambda t} \quad (23)$$

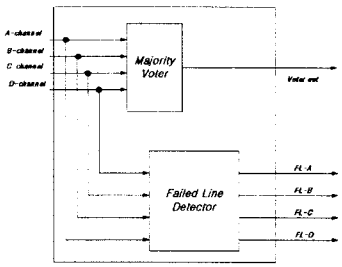
식 (21)은 고장률이 상수 λ인 단일 제어기 시스템의 신뢰도이며, 이 제어시스템의 안전성은 신뢰도($P_o(t)$)와 고장 중 안전한 고장의 확률 ($P_{FS}(t)$)을 더한 식(24)과 같이 나타낼 수 있다.

$$S(t) = P_o(t) + P_{FS}(t) = C + (1-C)e^{\lambda t} \quad (24)$$

즉 안전공학적인 설계에 근거를 두고 시스템이 설계 된다면 안전성이 부과되어 진다. 만약 식 (24)에서 C가 1(perfect) 이라면 $S(\infty)$는 1 이며, 이 시스템은 완전한 안전성을 가지고 C가 어떤 상수라면 정상상태 안전성은 $S(\infty)=C$로 수렴하게 된다. C는 수학적으로 정확하게 계산하기는 어렵지만 안전공학적설계시 분명 0보다는 크다. 즉 안전공학적 설계는 시스템의 안전성을 분명히 높이는 결과를 가져온다.

3. NMR PPC의 보팅 메카니즘의 설계

그림11에서와 같이 PPC의 동시논리부에는 A, B, C, D 채널의 제어신호가 입력이 된다. PPC의 동시논리부(Voter)는 4개중 2개 이상이 일치해야 동작하는 2/4 동시발생논리를 가진다. 보터에 의해 보팅 신호가 출력으로 나간다. 그리고 4개의 채널에 고장채널을 감지하기 위한 고장채널 감지기(Failed line detector)가 연결되어 고장난 채널의 정보를 경보시스템으로 보낸다.



NMR Block with Majority Voter

그림 11 고장감지기능을 가지는 NMR PPC의 동시논리부

본 논문에서는 NMR PPC의 동시논리부를 ALTERA의 설계소프트웨어인 MAXPLUSⅡ를 이용하여 설계하였다. 그림12는 고장감지기능을 가지는 NMR PPC 동시논리부의 회로도이다. 그리고 그림13은 안전성을 고려한 고장감지기능을 가지는 NMR PPC 동시논리부의 회로도이다. 입력으로는 4개의 채널입력과 바이패스신호 등과 출력으로는 보팅출력신호, 그리고 채널고장출력신호 등으로 구성되어 있다.

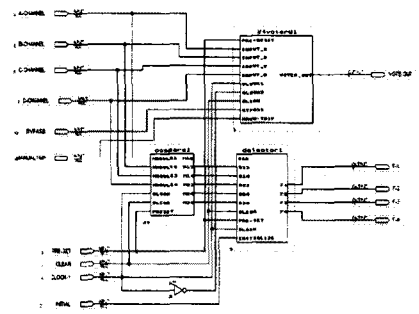


그림 12 고장감지기능을 가지는 동시논리부의 회로

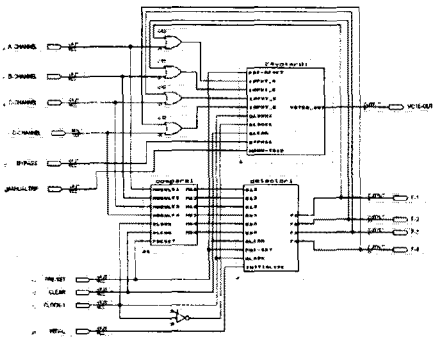


그림 13 안전성을 고려한 NMR PPC 동시논리부의 회로

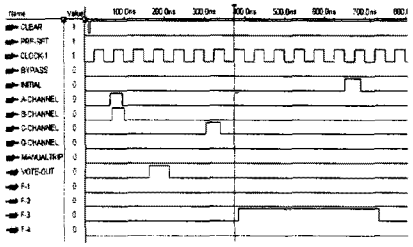


그림 14 NMR PPC 동시논리부의 출력

그림14는 NMR PPC 동시논리부의 출력을 나타내고 있다. A, B 채널에서 제어신호가 들어올 때 동시논리부의 보터에서 2/4 보팅메카니즘에 의한 보팅출력을 보내고 있다. 그리고 만약 C채널(한채널)에서 고장이나, 노이즈에 의해서 단독으로 출력신호를 보낼 때 C채널의 고장감지신호를 발생하고 있으며 그 신호는 래치되어 보터에 귀환된다. 즉 안전한 방향으로의 고장을 유도한다. 이를 경우 운전자는 바이패스 신호로 바이패스를 시키고 해당채널을 테스트 후에 순간적인 노이즈의 경우는 초기화신호(initial signal)을 보내어 고장감지신호를 제거 후 정상운전을 시킬 수 있으며, 한 채널 고장인 경우는 수리 또는 교체하여야 한다. 보터에 도착하는 4채널 신호가 약간의 시간적인차이가 있으므로 동기화를 위하여 래치를 사용하였고 보팅출력은 입력1.5클럭으로 하였다. 감시기는 각 채널의 고장을 감시하며, 고장발생시 해당채널의 고장신호를 발생한다. 만약 A채널(임의의 한 채널)에서만 제어신호가 발생할 때 비교기를 통과하여 들어온 신호에 의해 감시기는 A채널 고장신호를 경보시스템 등으로 보내기 위한 고장신호를 발생하도록 하였다. 역시 초기화 신호(initialize signal)로 고장진단신호를 제거할 수 있다.

4. 결 론

복잡하고 정교한 시스템일수록 고장률이 높아지게 되어 시스템의 신뢰도는 중요한 관심사로 등장하게 되었으며 신뢰성에 근거를 둔 제어기의 설계는 중요한 위치를 차지하게 되었다. 플랜트 보호 제어기는 플랜트의 여러 상태를 입력 받아 플랜트가 이상동작이 고장과 사고로 진단될 때 제어기가 동작해 플랜트의 동작을 정지시켜 플랜트와 인명 등을 보호하는 제어기이다. 이러한 플랜트 보호제어기는 신뢰성뿐 만 아니라 제어기 자체의 고장시 안전성을 고려한 방향으로 고장을 유도하는 안전공학적 설계를 바탕으로 설계되어야 한다. 본 논문에서는 EPLD를 이용한 안전성을 고려한 NMR(N-Module Redundancy) PPC(Plant Protection Controller)의 보팅 메카니즘을 설계하고 신뢰도와 안전성을 분석하였다. 동시논리부(보팅)를 디지털 프로세서로 설계할 경우 프로세서와 프로그램을 저장할 메모리가 있어야하므로, EPLD, 또는 FPGA로 설계될 경우에 비해 고장률이 높아지며, 가격 역시 높아진다. 그리고 EPLD나 FPGA는 분산제어나 속도면에서도 좋은 결과를 가져올 수 있다. 앞으로 추후 연구과제는 플랜트 보호제어기의 안전공학적 설계에 따른 voter의 다중화에 따른 해석, 소프트웨어의 신뢰성에 대한 해석 방법, 제어기 입력 파라메터의 분리(Segmentation)에 따른 해석이다

[참 고 문 헌]

[1] Richard E. Barlow , Reliability and Decision making, Chapman &Hall 1993

[2] Patrick D.T, Practical Reliability Engineering, John Wiely & Sons, 1996

[3] Barry W. Johnson , Design and Analysis of Fault Tolerance Digital Systems, Addison Wesley, 1989

[4] C. GALIKOWSKY " Optimal redundancies for reliability and availability of series systems" Microelectron. Reliability vol 36 No 10 pp.1537-1546 1996

[5] M. Schoenauer & Z. Michalewicz. " Sphere operators and their applicability for constrained parameter optimization problems." In 7th Annual Conference on Evolutionary Programming 1997

[6] C. E Stroud , " Reliability of Majority Voting Based VLSI Circuits" , IEEE Trans. on VLSI systems Vol.2, No. $, pp.516-521, 1994

[7] C. E. Stroud and J.K. Tannehill, " Applying Built-In Self-Test to Majority Voting Fault-tolerant Circuits", Peoc. IEEE VLSI Test Symp., pp 303-308, 1998