論 文
55B-12-12

전자연동장치의 안전성 활동에 관한 연구(II)

A Study on Fault Tolerant Digital Controllers for Programmable Electronic Interlocking System(II)

朴 在 煐† · 李 鐘 宇*
(Park Jaeyoung · Lee Jongwoo)

Abstract - Programmable electronic interlocking system plays key role in railway operation and is closely related to railway accidents, in which the programmable electronic controller of interlocking system may become sources. Redundant digital controllers are adopted as the interlocking controllers to prevent the accidents from the controllers being out of order. The redundant digital controllers being fault tolerant are realized through dual or triplex controllers. In this paper, we calculated safety and availability of the redundant digital controllers using Markov models, demonstrated key part to determine the availability ana the safety.

Key Words : 'PES Interlocking System', 'Train Control System', 'Safety', 'Digital Controller', 'TMR'

1. 서 론

전자연동장치는 진로제어, 신호제어 및 운전정리 등 연동장치는 철도운용에서 중요한 역할을 한다. 전자연동장치의 구성은 연동제어기, 현장장치(TFM:Track Functional Module) 및 신호기기로 구성되어 있다. 전자연동장치의 제어기의 안전성과 신뢰성에 대해서 고려하여 보았다.

현재 운전 중인 연동장치의 시스템 설계의 경우, 1970년도 초반 이전의 계전기 기술을 바탕으로 아날로그 계통이 근간을 이루고 있다. 계전연동장치는 제어로직의 복잡성, 단종 부품의 증가, 관련 전문가의 감소 등으로 운전, 유지 및 보수에 어려움이 많을 뿐만 아니라 아날로그 계통의 경직성으로 신기술 이식 등을 통한 성능 향상에 제한을 받고 있다. 따라서 이와 같은 문제점들을 해결하기 위한 방안으로 연동장치의 제어장치의 디지털화가 점차 요구되고 있으며 특히 향후 연동장치 운용에서는 디지털 기술의 적용을 기본 설계 요건으로 제시하고 있다[1].

최근 20여년 동안 마이크로일렉트로닉과 소프트웨어를 이용하여 고장에 잘 대처할 수 있도록 제어 시스템을 설계하고자 하는 연구들이 활발히 수행되어왔으며, 이와 관련된 연구들은 크게 고장진단 분야의 연구들과 진단된 고장정보를 바탕으로 고장을 견뎌낼 수 있는 제어시스템을 개발하고자 하는 연구들로 구별될 수 있다.

특히 제어기는 그 구성부품이 복잡하기 때문에 고장의 발생가능 부위가 많고 고장이 발생하였을 때 그 영향도 매우 크다. 그러나 제어기의 고장에 대한 연구는 아직 많지 않으며, 대부분의 경우 자기진단기능 등을 이용하여 고장을 감지하는 방식을 사용하고 있는 실정이다. 제어기가 디지털 컴퓨터로 구현되는 경우에 고장검출 코드를 사용하는 방법, 프로그램의 수행시간을 고려하여 정해진 시간 안에 수행이 완료되지 않으면 고장으로 판단하는 방법 등을 사용하고 있다[2][3].

전자연동장치의 제어기는, 내고장성 제어와 같은 기능을 갖는 제어기의 하드웨어 모듈들을 여러 개 두는 형태이다. 대표적인 예로 이중화와 삼중화(TMR)를 들 수 있으며, 항공 우주 분야에서는 안전성이 극히 중요하므로 5중화한 경우도 있다[4]. 안전성과 신뢰성의 관계는 상호 보완적인 관계이기도 하지만, 반대로 상호 배타적인 경우도 있다.

전자연동장치의 경우에는 제어기에 발생할 수 있는 제어정보의 변질, 프로세싱의 이상 및 제어기의 고장에 대한 안전성을 높이기 위해서 여분시스템을 구성한다. 2개 이상의 시스템을 비교하여 2개 시스템이 제어기에서 발생할 수 있는 고장을 제거하도록 하여 안전성을 향상시키며, 3 중화를 통하여 신뢰성을 향상시킨다.

본 논문에서는 전자연동장치 제어기의 여분시스템의 구조, 2중화 및 3중화 시스템의 가용성 및 안전성에 대한 문제를 다루었다[5].

2. 여분시스템

2.1 비용적 측면

중복구조에 의한 신뢰도 개선 효과는 목표하는 신뢰도를 이루기 위한 비용(Cost Reliability Ratio)으로 나타낼 수 있으며 다음의 식으로 표현된다.

$$CRR = \frac{nR_M}{R_R - R_M} = n\frac{1}{\frac{R_R}{R_M} - 1} \qquad \text{식(1)}$$

† 교신저자, 正會員 : 서울産業大學 鐵道專門大學院 鐵道電氣信號工學科博士課程
E-mail : pjy7717@paran.com
* 正 會 員 : 서울産業大學 鐵道專門大學院 鐵道電氣信號工學科工學博士
接受日字 : 2006年 10月 25日
最終完了 : 2006年 11月 8日

여기서 R_M, R_R, n은 각각 단위 모듈의 신뢰도, 전체 시스템의 신뢰도 그리고 중복 여분의 개수이다. 위의 관계에서 단위 모듈의 신뢰도 R_M이 낮을수록 중복구조에서의 신뢰도 개선의 효과는 보다 적은 비용으로 높게 됨을 알 수 있다. 따라서 고 신뢰도를 위하여 제어 시스템에 부가되는 여분은 감지기(Sensor), 구동기(Actuator), 그리고 제어기(Controller) 등의 각 구성요소에 부가할 수 있으나, 그 구성요소중 제어기는 시스템의 동작 특성에 가장 큰 영향을 주며 다른 구성요소에 비해 그 구조가 복잡하고 상대적으로 단위 모듈의 신뢰도가 낮으므로 제어기 부분을 중복구조로 하는 것이 전체 시스템의 신뢰도 향상의 측면에서 매우 효과적이라고 할 수 있다.

2.2 여분의 결정

시스템의 신뢰성을 향상시키고 내고장성 시스템을 구축하기 위해 어느 정도의 여분을 유지해야 하는지는 매우 중요하다.

실질적으로 현장에서 운용되는 많은 시스템의 경우, N 개의 구성요소를 가진 시스템은 n 개의 여분을 가지고 운전된다. 운전 중인 N 개의 시스템 중 하나의 구성요소에서 고장이 발생하면 매우 짧은 시간에 여분으로 교체하여 고장없이 계속 운전되는 시스템을 고려할 경우, 이러한 시스템을 구현하기 위하여 다음과 같이 가정한다[7].

1) 구성요소의 교체는 신속하게 이루어져야 한다.
2) 시스템은 교체가능한 여분이 있는 한 정지없이 동작한다. 따라서 고장난 구성요소는 수리할 수 없으므로 제거(Discard)시킨다.
3) 모든 구성요소의 고장시간은 지수분포에 따른다.

여기서, λ는 일정한 값을 갖는 고장으로 정의한다. 만약 모든 구성요소 N이 시스템의 정상 가동에 필요하다면 이들은 논리적으로 연속적이고, 모든 고장율은 $N\lambda$와 같으므로 시간 t에서 k 개의 구성요소에서 고장이 발생한 경우 정상 가동 확률은 식(2)과 같이 표현할 수 있고, 전체 시스템의 신뢰도는 식(3)과 같다.

$$P = \frac{(N\lambda t)^k}{k!} e^{-N\lambda t} \qquad \text{식(2)}$$

$$R(t) = e^{-N\lambda t}\left(1 + N\lambda t + \frac{(N\lambda t)^2}{2!} + \cdots + \frac{(N\lambda t)^n}{n!}\right) = e^{-N\lambda t}\sum_{k=0}^{n}\frac{(N\lambda t)^k}{k!} \qquad \text{식(3)}$$

이 경우 평균 수명 시간(MTTF)은 다음과 같이 주어진다.

$$MTTF_R = \int_0^\infty R(t)\,dt = \frac{n+1}{N\lambda} \qquad \text{식(4)}$$

여분이 없는 시스템의 평균 수명 시간은 식(5)와 같다.

$$MTTF_0 = \int_0^\infty R_0(t)\;dt = \frac{1}{N\lambda} \qquad \text{식(5)}$$

또한, 여분이 없는 시스템 신뢰도에 대한 여분을 가진 시스템 신뢰도의 비율을 신뢰도 증가율(Reliability Improvement Ratio)이라고 하면 n 여분을 가진 시스템 신뢰도의 증가율은 다음과 같이 정의할 수 있다.

$$\mathrm{RIR} \equiv \frac{R(t)\text{with } n\text{spares}}{R_0(t)\text{with no spares}} = \sum_{k=0}^{n}\frac{(N\lambda t)^k}{k!} \qquad \text{식(6)}$$

λt = 0.1인 경우에 각각 다른 N 값에 있어서 여분 n의 개수에 대한 RIR 그래프를 그림 1에 나타내었다. 여기서 λt = 0.1은 임무 시간(Mission time)이 각 구성요소의 평균 수명 시간의 10%에 해당함을 의미한다.

그림에서 n=1 일 때 시스템 신뢰도에 가장 큰 향상을 가져오게 됨을 알 수 있다. 또한 시스템에서 구성요소 N이 크면 클수록 처음 몇 개의 여분으로 인한 신뢰도 향상의 효과가 더 커진다. 따라서 원하는 시스템 신뢰도를 얻기 위한 최소 여분의 개수를 이 그래프를 통하여 찾을 수 있다.

또한 시스템의 평균 수명 시간 증가율(MTTFIR ; MTTF improvement ratio)은 식(4) 및 식(5)로 부터 다음과 같이 표현된다.

$$MTTFIR \equiv \frac{MTTF\text{ with spares}}{MTTF\text{with no spares}} = n+1 \qquad \text{식(7)}$$

즉, 시스템 MTTF는 여분의 개수에 따라 선형적으로 증가함을 알 수 있다.

시스템 신뢰도 향상과 여분의 설비로 인한 MTTF의 증가는 전체 시스템 비용을 증가시킨다. 결국, 여분의 개수를 선택하는 것은 개선되지 않은 시스템의 운전비용과 여기에 여분을 갖는 시스템의 추가 비용을 바탕으로 경제적인 측면에서 결정되어야 한다. 따라서 다음과 같은 고장허용 시스템을 고려한다.

첫째, 신뢰도 향상의 효과가 가장 큰 제어기의 여분을 1개 혹은 2개를 갖는 중복 시스템

둘째, 고장난 제어기를 즉시 교체 가능한 구조.

그러므로 이들 조건을 만족하는 시스템으로 일반적인 능동형 이중화 구조와 삼중화 구조를 채택하여 각각의 신뢰도를 비교하고자 한다.

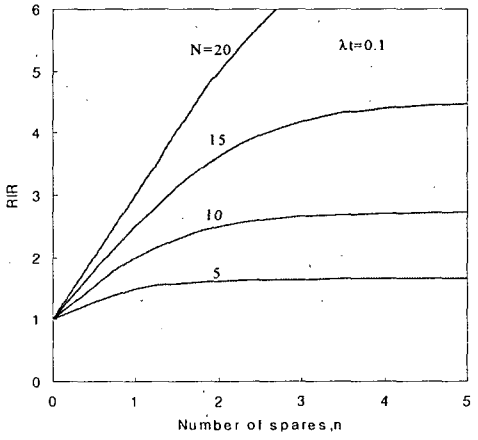


그림 1 여분시스템에 따른 신뢰도 증가율
Fig. 1 Dependence of RIR on number of spares

3. 여분 시스템 신뢰도 분석

3.1 능동형 이중화 시스템

능동형 이중화 시스템은 주 제어기 C_1이 동작하다가 고장이 나면 부 제어기 C_2로 제어가 절환되는 형태이며, 두 제어기를 중복구조로 하기 위하여 부가되는 고장 감지기의 성능인 고장 감지율(Fault Coverage)을 C_d라 한다. 신뢰도의 측면에서 두 제어기는 같은 고장율 λ_c를 갖는 제어기라 가정하면 제어기의 상태는 그림 2와 같으며 다음과 같이 4가지로 표현할 수 있다.

S_1 : 두 제어기가 정상 동작

S_2 : 주 제어기 고장으로 부 제어기절환

S_3 : 주 제어기 동작, 부 제어기 고장

S_4 : 두 제어기가 모두 고장이거나 주 제어기가 고장이지만 고장이 감지되지 않아 계속 연결된 상태

이 중에서 제어 시스템이 동작할 수 있는 모드는 S_1,S_2 및 S_3이다. 이를 Markov process로 모델링하면 다음과 같다.

먼저, 상태 확률 벡터 (State Probability Vector)를 $s_i(t) = [s_1(t), s_2(t), s_3(t), s_4(t)]^T$라 놓으면 그림 2의 상태도에서 $s_i(t)$, i = 1, 2, 3, 4는 다음과 같다.

$$\begin{aligned}
\frac{ds_1(t)}{dt} &= -2\lambda_c s_1(t) \\
\frac{ds_2(t)}{dt} &= \lambda_c C_d s_1(t) - \lambda_c s_2(t) \\
\frac{ds_3(t)}{dt} &= \lambda_c s_1(t) - \lambda_c s_3(t) \\
\frac{ds_4(t)}{dt} &= \lambda_c (1 - C_d)\, s_1(t) + \lambda_c s_2(t) \\
&\quad + \lambda_c s_3(t)
\end{aligned} \qquad \text{식(8)}$$

이 모델에서 제어 시스템의 신뢰도 함수를 구하면 다음과 같다.

$$\begin{aligned}
R_a(t) &= \mathrm{Prob}\{s_1(t)\} + \mathrm{Prob}\{s_2(t)\} \\
&\quad + \mathrm{Prob}\{s_3(t)\} \\
&= (1 + C_d) e^{-\lambda_c t} - C_d e^{-2\lambda_c t}
\end{aligned} \qquad \text{식(9)}$$

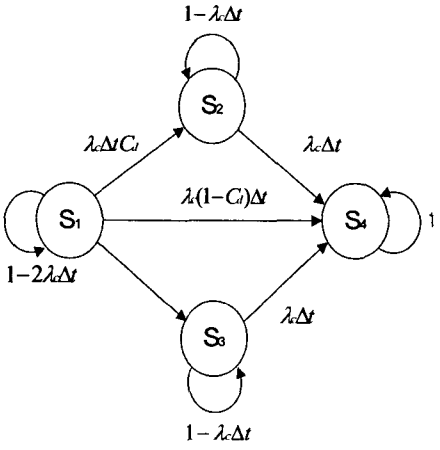


그림 2 능동 DMR 시스템의 Markov 모델

Fig. 2 Markov model of Active DMR system

3.2 삼중화 시스템

삼중화 시스템은 주 시스템과 부 시스템을 특별히 구분하지 않고, 모든 데이터 처리는 세 개의 각각 독립된 커널에서 이루어진다. 어느 한 제어기가 다른 두 제어기와 출력이 다를 경우를 제어에서 제거시키므로 고장 감지 및 재구성을 담당하는 별도의 부 시스템은 필요가 없다. 세 제어기는 같은 제어기이고, 유효 데이터의 산출 방법으로 2 out of 3 voting을 이용하므로 두 제어기가 동시에 고장일 때는 시스템은 동작하지 않는다. 신뢰도의 측면에서 세 제어기는 같은 고장율 λ_c를 갖는 제어기라 가정하면 제어기의 상태는 그림 3과 같으며 다음의 3가지로 표현할 수 있다.

S_1 : 모든 제어기가 정상 동작

S_2 : 두 개의 제어기가 정상 동작

S_3 : 두 개 혹은 모든 제어기가 고장

이 중에서 제어 시스템이 동작할 수 있는 모드는 S_1 및 S_2의 상태이다. 이를 Markov process로 모델링하면 다음과 같다. 먼저, 상태 확률 벡터를 $s_i(t) = [s_1(t), s_2(t), s_3(t)]^T$라 놓으면 그림의 상태도에서 $s_i(t)$, i = 1, 2, 3 은 다음과 같다.

$$\begin{aligned}
\frac{ds_1(t)}{dt} &= -3\lambda_c s_1(t) \\
\frac{ds_2(t)}{dt} &= 3\lambda_c s_1(t) - 2\lambda_c s_2(t) \\
\frac{ds_3(t)}{dt} &= 2\lambda_c s_2(t)
\end{aligned} \qquad \text{식(10)}$$

이 모델에서 제어 시스템의 신뢰도 함수를 구하면 다음과 같다.

$$\begin{aligned}
R_{TMR}(t) &= \mathrm{Prob}\{s_1(t)\} + \mathrm{Prob}\{s_2(t)\} \\
&= 3e^{-2\lambda_c t} - 2e^{-3\lambda_c t}
\end{aligned} \qquad \text{식(11)}$$

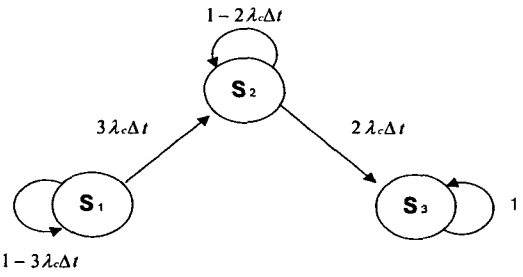


그림 3 TMR 시스템의 Markov 모델

Fig. 3 Markov model of TMR system

3.3 절 신뢰도 비교 및 검토

능동형 이중화 구조와 삼중화 시스템의 평균 수명 시간을 계산하면 각각 다음과 같다.

$$MTTF_a = \frac{1}{\lambda_c} + \frac{C_d}{2\lambda_c} \qquad \text{식(12)}$$

$$MTTF_{TMR} = \frac{5}{6\lambda_c} \qquad \text{식(13)}$$

단일 제어기 시스템의 MTTF는 $1/\lambda_c$ 이므로, 이 방식에서의 신뢰도 개선 효과는 $C_d/2\lambda_c$이다. 즉, 능동형 제어기 시스템에서 신뢰도 개선의 효과는 고장 감지기의 성능 C_d에 크게 의존함을 알 수 있다. 고장 감지기가 고장을 감지하지 못하면 신뢰도 향상의 효과는 기대할 수 없으므로 단일 제어기 시스템의 경우와 같이 된다. 만일 고장 감지기의 감지율이 C_d = 1 이라면 제어 시스템의 평균 수명 시간은 $3/2\lambda_c$이므로, 여분을 갖지 않는 단일 제어기 시스템에 비하여 50[%]의 신뢰도 개선 효과가 있음을 알 수 있다.

삼중화 구조의 경우 시스템의 평균 수명 시간은 식(13)과 같고 단일 제어기의 경우보다 평균 수명 시간이 작게 나타난다. 그러나 중복 제어 시스템은 높은 신뢰도를 보장하면서 동작하는 경우가 대부분이므로 고 신뢰도를 보장하는 임무 시간의 관점에서 보면 단일 제어기 시스템보다 신뢰도 개선이 이루어진다.

예를 들어 단일 시스템의 시간당 고장률 λ = 0.01, r = 0.86 일 때 삼중화 시스템의 임무 시간 증가를 계산하면 다음과 같다.

$$MT_s[0.86] \simeq 15.0823$$
$$MT_{TMR}[0.86] \simeq 26.8272$$

즉, 임무 시간은 단순 시스템에서는 15.08 이지만 삼중화 시스템에서는 26.83으로 늘어남을 알 수 있다. 이것은 삼중화 시스템을 채택함으로써 임무 시간이 단순 시스템에 비해 약 1.8배정도 증가함을 의미한다. 이러한 관계를 그림 4에 나타내었다. 같은 방법으로 신뢰도가 0.95 및 0.99일 경우에 임무 시간을 계산해보면 각각 2.8배, 6배로 증가한다. 즉 고신뢰도 시스템일수록 임무 시간은 증가함을 알 수 있다. 또한 삼중화 시스템은 능동형 이중화 시스템보다 신뢰도 0.99 이상을 유지하는 시간이 C_d=0.5에서는 약 3배, C_d=0.8에서는 약 1.4배 더 길게 나타남을 알 수 있으며, 그림 5에 C_d=0.5 일 때의 그래프를 나타내었다.

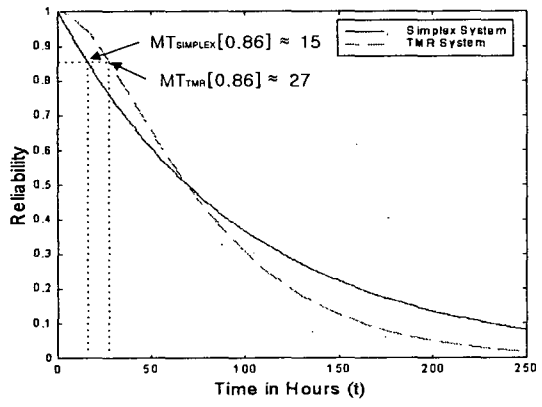
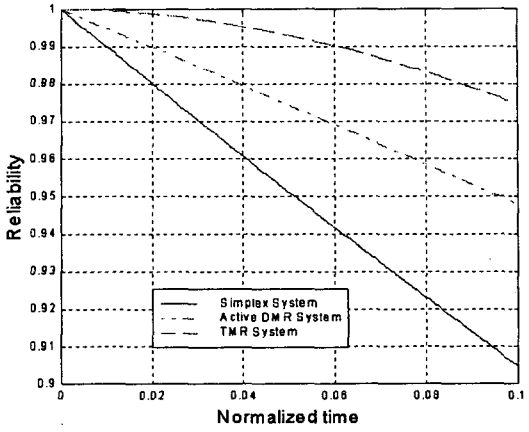


그림 4 동작시간 비교
Fig. 4 Comparison of mission time



$\lambda = 1.0, \quad C_d = 0.5$

그림 5 신뢰성 비교
Fig. 5 Comparison of reliability

4. 여분시스템 안전성 검토

4.1 제어기의 안전성

연동장치를 구성하는 제어기는 안전성에 대한 논의는 논문[]에서 언급하였다. 제어기의 고장은 중대 사고를 발생시킬 수 있다. 제어기의 안전성을 구현하는 방법은 여분시스템을 이용한다. 앞 절에서는 여분 시스템의 신뢰성을 검토하였고, 본 절에서는 여분 시스템의 안전성을 검토한다. PES 제어기의 경우 특정 방향으로 고장이 발생하지 않고 랜덤하게 고장이 발생하므로 안전성 대책을 하기가 어렵다. PES 제어기에서 가장 많이 쓰는 방법으로 여분시스템을 이용한 안전성확보이다. 2개의 제어기 중 하나가 고장이 발생하였을 경우에는 출력에서 서로 불일치가 발생하며, 이것을 이용하여 시스템을 안전 측으로 작동하게 한다. 본 절에서는 여분 제어기 안전성을 검토한다.

4.2 능동형 2중화시스템

4.2.1 능동형 2중화 구조

능동형 2중화 시스템의 전체 계통도는 그림 6과 같이 CPU 모듈의 2중화와 I/O 스위치모듈의 이중화로 구성된다. CPU 모듈은 각기 독립된 프로세서와 메모리를 내장하고 있으며, 진로설정 등 외부로 부터 입력된 신호를 2개의 CPU 모듈에서 개별적으로 연산 처리한다. 여분관리 장치는 모듈

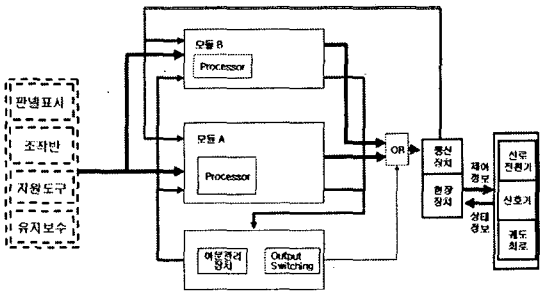


그림 6 절체기를 이용한 시스템 이중화
Fig. 6 Dual Redundancy Controller using Switching

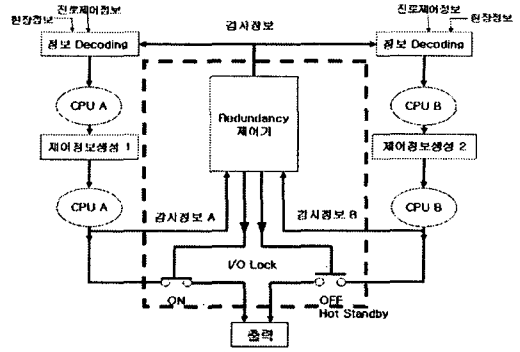


그림 7 능동형 2중화 제어기의 절체시스템

Fig. 7 Switching system for active dual Redundant Controller

A와 B상태를 감시 하며 후 모듈에 이상이 발생하였을 때 I/O를 절체하게 된다.

4.2.2 능동형 2중화 시스템의 안전성 분석

능동형 2중화 시스템의 안전성은 진단기능을 갖는 여분관리 시스템을 이용한다. 여분관리 시스템이 진단을 하여 시스템이 이상이 발생을 하면은 A 제어기에서 B 제어기로 절체를 하고, B 시스템이 고장이 발생하면 시스템의 출력을 발생시키지 않음으로써 제어기의 안전성을 확보한다.

능동형 2중화 시스템의 안전성을 전적으로 여분관리 시스템의 위험 측 고장률에 의존한다.

4.3 3중화 구성

4.3.1 전자연동장치의 3중화 구성

3중화 시스템의 전체 계통도는 그림 8과 같이 CPU 모듈의 삼중화와 I/O 모듈의 이중화로 구성된다. CPU 모듈은 각기 독립된 프로세서와 메모리를 내장하고 있으며, 진로설정 등 외부 센서로부터 입력된 신호를 세 개의 CPU 모듈에서 개별적으로 연산 처리한 후 2 out of 3 voting 방식을 사용하여 유효 출력 제어신호를 결정한다.

CPU A와 CPU C 모듈은 제어권을 가지며, 입력 디바이스로부터 독립적으로 값을 받는다. 열차위치, 선로전환기 위치 등과 같은 중요한 입력 요소는 세 개 또는 그 이상의 센서로부터 입력을 받아 신뢰성을 높이는 것이 일반적이다. CPU A와 CPU C 모듈로 입력된 데이터 값은 CPU 내부 직렬 통신에 의해 세 개의 CPU 모듈이 데이터를 공유하게

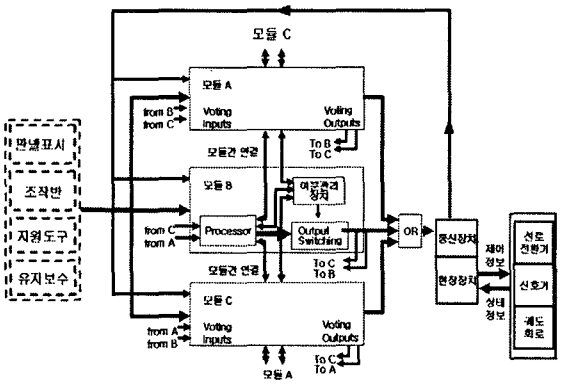


그림 3 3중화 전자연동장치 시스템

Fig 8 Triple Redundancy of PES Interlocking System

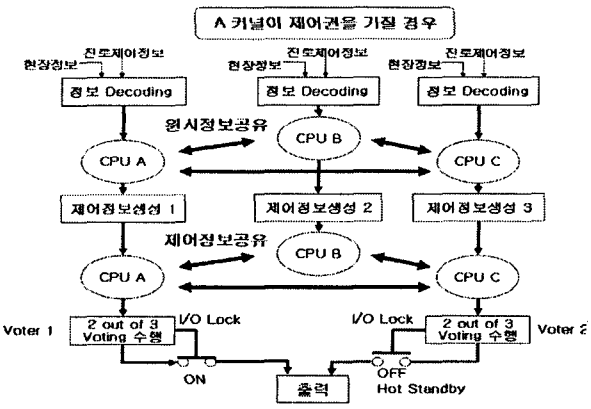


그림 4 2 out of 3 투표방법

Fig. 9 2 out of 3 voting method

되며, 각기 모듈은 독립적으로 연산을 수행한 후 유효 데이터를 재 교환함으로써 각각 2 out of 3 voting을 수행하도록 하였다.

4.3.2 3중화 시스템의 안전성 분석

그림 7에서 제어정보 1을 d_1, 제어정보 2를 d_2, 제어정보 3을 d_3라고 한다. Voter1은 $d_1 = d_2 = d_3$, $d_1 = d_2 \neq d_3$, $d_1 = d_3 \neq d_2$에 동작을 하고, $d_1 \neq d_2 \neq d_3$인 경우에는 동작을 하지 않는다. Voter2는 $d_2 = d_3 \neq d_1$인 경우에만 동작을 하고 $d_1 = d_2 = d_3$, $d_1 = d_2 \neq d_3$, $d_1 = d_3 \neq d_2$, $d_1 \neq d_2 \neq d_3$경우에는 동작을 하지 않는다. 3중화 시스템은 2개의 결과가 동일할 경우에는 출력을 발생하고, 3개의 출력이 서로 다를 경우에는 출력을 하지 않음으로써 안전성을 확보한다.

시스템의 안전성은 Voter에 전적으로 종속된다. 시스템의 안전성을 높이기 위해서는 Voter의 신뢰성을 높여야 하며, 또한 Voter가 고장이 발생하면 한쪽으로 동작되는 특성을 갖도록 설계를 해야 한다.

4.4 여분관리기 및 voter의 안전성 분석

제어기의 고장률을 λ로 하고 고장이 발견될 확률을 C로 한다면, 정상상태는 $1-\lambda\Delta t$, 안전측 고장 $\lambda\Delta t C$, 위험측 고장은 $\lambda\Delta t(1-C)$가 된다.

그림 10의 상태천이도에 따라서 각 상태의 확률은 다음과 같다[9].

$$p_{NS}(t+\Delta t) = (1-\lambda\Delta t)p_{NS}(t) \quad (14)$$

$$p_{FS}(t+\Delta t) = \lambda\Delta t C\, p_{NS}(t) + p_{FS}(t) \quad (15)$$

$$p_{FU}(t+\Delta t) = \lambda\Delta t(1-C)p_{NS}(t) + p_{FU}(t) \quad (16)$$

이 시스템의 상태확률은 다음과 같다.

여분관리기 혹은 Voter의 위험 측 고장률이 동일하다 하면은 능동형 2중계 혹은 3중계 시스템의 안전성을 동일하다. 여분관리기 혹은 Voter를 갖는 제어기의 안전성 요구조건 즉 위험 측 고장률(λ_{fu})을 만족하기 위해서는 다음과 같은 조건을 만족해야 한다.

$$\lambda_{fu} = \lambda_v(1-C) \leq SIL4 \quad (16)$$

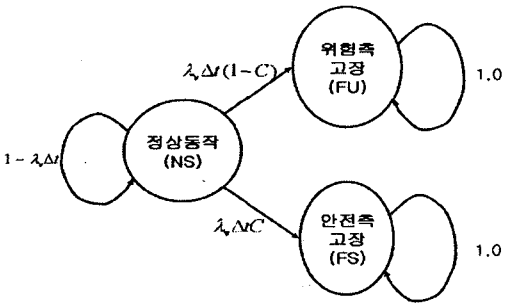


그림 10 여분관리기의 정상, 안전측고장 및 위험측 고장 상태천이도

Fig. 10 Three state Markov modeling for normal, safe failure and unsafe failure of switching controller

5. 여분 제어기의 안전성 및 가용성

여분을 갖는 PES 제어기의 안전성 및 가용성은 다음의 표 4와 같이 표시된다. 두 시스템의 고장발견율이 동일하다고 하면, 안전성 측면에서는 능동형 2중계와 3중계가 동일하고, 가용성 측면에서는 능동형 2중계가 유리하다.

여분 제어시스템의 경우는 신뢰성은 제어기의 고장율 λ와 여분구조, 안전성은 C에 의해 결정된다. 시스템의 가용성을 높이기 위해서 여분구조(n)과 제어기의 고장율 λ간의 Trade-off에 의해서 결정될 수 있고, 안전성은 여분관리계의 위험 측 고장률(C)에 의해서 결정된다.

표 4 2중계 및 3중계 제어기의 안전성 및 신뢰성

Table 4 Safety and Reliability for active dual and triplex controller

분류	MTTF	위험 측 출력 고장률	비고
능동형 2 중계	$\frac{1}{\lambda_c}+\frac{C_d}{2\lambda_c}$	$\lambda_v(1-C_d)$	여분관리기와 Voter의 고장 발견률이 동일한 경우 $C=C_v=C_d$
3중계	$\frac{5}{6\lambda_v}$	$\lambda_v(1-C_v)$	

6. 결 론

본 논문에서는 연동장치 제어기의 여분 구성에 따른 가용성과 안전성 특성에 대해 알아보았다.

능동형 2중화 모델과 3중화 시스템에 가용성은 능동형 2중화 시스템이 3중화 시스템보다 유리하고, 안전성의 경우에는 동일하다는 것을 알 수 있었다.

여분 시스템의 제어기를 구성할 경우에는 제어기의 고장률, 여분의 수의 결정에 따라 가용성이 결정되고, 안전성은 여분관리계에 의해서 결정된다. 시스템의 가용성과 안전성 요구조건에 따라 제어기를 설계해야 한다,

<약어>

$\lambda(t)$: 시스템 고장율

$\lambda_{FU}(t)$: 시스템 위험 측 고장율

$\lambda_{FS}(t)$: 시스템 안전 측 고장율

C : Fault Coverage Rate

C_v : Voter Fault Coverage Rate

C_d : 여분관리기의 Fault Coverage Rate

$p_{FU}(t)$: 시스템의 출력 단에서 위험 측 출력확률

$p_{FS}(t)$: 시스템의 출력 단에서 안전 측 출력확률

$p_{NS}(t)$: 시스템의 출력 단에서 정상 출력확률

참 고 문 헌

[1] 한국전력공사, "주파수 조정 운전을 위한 터빈 조속기 및 보일러 제어계의 성능개선", 전력연구원 자동제어연구실, 1987

[2] Aldrich, W. H., "Hot Backup for a Programmable Controller", IEEE Transactions on Industrial Electronics, Vol. IE-29, No. 4, pp. 268-272, Nov. 1982

[3] Patton, R. J., J. Chen, "Optimal Unknown Input Distribution Matrix Selection in Robust Fault Diagnosis", Automatica, Vol. 29, No. 4, pp. 837-842, 1993

[4] Cunningham, G. W., "Space-shuttle Control Systems Reliability : Redundant Processing", SYSTEMS & CONTROL ENCYCLOPEDIA - Theory, Technology, Applications, Vol. 7, pp. 4476-4481, 1987

[5] 한국전력공사, 전력연구원-삼창기업(주)부설연구소, "10MW 인텔리전트 디지털 조속기 개발", 중간보고서, 1997

[6] Johnson, Barry W., "Design and Analysis of Fault-Tolerant Digital Systems", Addison-Wesley Publishing Co., 1989

[7] Ramakumar, R., Engineering Reliability : Fundamentals and Applications, Prentice-Hall, 1993

[8] Ordys, A. W., A. W. Pike, M. A. Johnson, R. M. Katebi and M. J. Grimble, "Modelling and Simulation of Power Generation Plants" , Springer-Verlag, 1994

[9] 이종우 et al, "컴퓨터기반 자동열차제어장치의 안전성", 대한전기학회, 제54B권 제6호, 2005

저 자 소 개

박 재 영 (朴 在 煐)

1951년 4월 8일생. 1989년 서울산업대학교 전기공학과 졸업, 1996년 고려대학교 산업대학원 석사, 2005년~현재 한국철도공사 오송전기사무소장

Tel : 02-3149-2120

E-mail : pjy7717@paran.com

이 종 우 (李 鐘 宇)

1959년 3월 20일생. 1983년 한양대학교 공과대학 기계설계과 졸업, 1986년 Ecole Centrale de Nantes 석사, 1993년 University de Paris VI 공학박사, 2005년~현재 서울산업대학교 철도전문대학원 철도전기 신호공학과 교수

Tel : 02-970-6874

Fax : 02-978-6874

E-mail : saganlee@snut.ac.kr