2003 춘계학술발표회 논문집
한국원자력학회

원전 디지털시스템 감시타이머의 고장검출범위 정량화 방법

A Quantification Method for the Fault Coverage of Watchdog Timers in NPP Digital Systems

김만철, 김석준, 성풍현
한국과학기술원
대전광역시 유성구 구성동 373-1

전성택
한국수력원자력(주)
경상북도 경주시 양남면 나아리 260

요 약

본 논문에서는 원자력발전소에 적용되는 디지털 시스템에 고장내구성 기법으로써 가장 널리 이용되고 있는 방법론인 감시타이머에 대한 고장검출범위를 정량적으로 평가하는 방법을 제안한다. 감시타이머의 정량적 평가를 위해서는 감시타이머 자체가 아닌 감시의 대상이 되는 시스템에 대한 분석이 더 중요하다는 결론에 따라, 감시의 대상이 되는 시스템을 평가하기 위하여 해석적 방법과 컴퓨터 시뮬레이션을 혼합한 hybrid형 방법을 제시하였다. 개발된 방법을 월성원자력발전소의 디지털 기반 보호계통인 PDC에 적용해서 정량적 평가를 수행해 봄으로써, 개발된 방법론이 적용가능성을 검증하였다.

Abstract

This paper proposes a quantitative assessment method for the fault coverage of watchdog timers which is one of the most widely used fault-tolerant mechanism in digital systems applied to nuclear power plants. Based on the result that for the quantitative assessment of watchdog timers the analysis of the target system is much more important than the analysis of the watchdog timer itself, we developed a hybrid model combining analytic method and computer simulation for the quantitative analysis of the target system. The developed method is applied to PDC which is the

digital-based plant protection system in Wolsung nuclear power plants, and it turned out that the developed method has reasonable applicability.

1. 서 론

근래의 디지털 기술의 급속한 발전과 기존 아날로그 기기의 예비품 부족으로 인한 원전 유지보수비용의 상승에 따라, 신규 원전 혹은 기존 원전의 노후화된 계측제어시스템에 대하여 디지털 기기의 도입이 점차 확대되고 있다. 하지만, 이에 비하여 디지털 기기는 안전성 및 위험도에 대한 평가 방법론은 아직 초기단계에 머무르고 있는 것이 사실이다.

Kang과 Sung[1]은 디지털 기반 발전소보호계통에 대한 확률론적안전성평가 결과에 따라, 디지털 기반의 발전소 보호계통의 안전성에 가장 큰 영향을 미치는 세 가지 인자로써 소프트웨어 고장률, 공통유형고장, 그리고 디지털 시스템의 고장검출범위(fault coverage)를 지적하였다. 이들 중 고장검출범위는 디지털 기기만의 특성으로써, 고장내구성 및 자체검사에 의해 디지털 기기 내부에 존재하는 오류(fault)를 검출 및 그 영향을 최소화할 수 있도록 하는 기능의 효율성에 대한 척도로써 다음과 같이 정의된다. [2]

$$C = Pr\{\text{ Fault processed correctly } | \text{ Fault existence }\} \qquad (1)$$

현재 고장검출을 위해서 가장 널리 쓰이고 있는 방법론은 감시타이머(watchdog timer)이다. 감시타이머의 대략적인 구조는 그림 1에 나타나있다. 그림 1에서 보는 바와 같이 감시대상이 되는 시스템은 감시타이머에게 heartbeat 신호를 생성해서 전해주고, 감시타이머는 시스템에 정상상태일 경우에는 heartbeat 신호를 계속해서 받아들이게 되는데, 만일 감시대상시스템에 어떠한 문제가 발생하여 heartbeat 신호를 감시타이머에게 전달해 주지 못하는 경우에는 감시타이머는 감시대상시스템에 재기동(reset) 신호를 주어, 시스템을 재기동시키게 된다. 이러한 간단한 구조를 통해 감시타이머는 감시대상시스템의 건전성을 확보하며, 이러한 장점으로 인해 현재 많은 디지털 기기에 적용되고 있다.

하지만, 감시타이머가 감시대상시스템의 모든 고장에 대해서 재기동 신호를 줄 수 있는 것은 아

그림 1 감시타이머의 기본 구조

그림 2 Heatbeat 신호 생성 알고리즘과 감시타이머

니다. 특별한 경우에 있어서는 감시대상시스템에 오류가 발생하였음에도 불구하고 감시타이머에게는 계속 heartbeat 신호를 전달해 줌으로써 감시대상시스템의 오류를 검출하지 못하는 것이다. 이러한 경우의 수는 (1)에서 언급한 바와 같이 확률로써 표현이 되는데, (1)이 의미하는 것은 바로 고장이 발생하였을 경우에 대해서 고장을 검출할 수 있는 확률을 나타내는 것이다. 이러한 고장검출범위에 대한 확률값을 구하기 위하여 수많은 연구들이 수행되어져서 많은 이론적인 모델들과 이론적인 모델들의 변수값들을 통계적으로 구하기 위한 방법론들이 제시되어 왔다. 이러한 모델들에 대해서는 [2]에 잘 정리되어 있다.

하지만, 고장검출범위의 정량화와 관련한 최근의 추세는 실제 고장주입실험(fault injection experiment)에 의한 실험적인 평가이다. 감시타이머의 경우 Miremadi와 Torin [3]이 Motorola MC6809E 8비트 CPU에 대해 수행한 실험에서, 두 종류의 소프트웨어 기반의 알고리즘과 감시타이머의 조합을 이용했을 때, 87%의 모든 오류와 93%의 제어흐름오류를 검출할 수 있으며, 고장타이머만을 이용하였을 때에는 62%의 오류를 검출할 수 있었다는 실험결과를 발표하였다. Schmid et al.[4]는 감시프로세서를 이용하여 약 73%의 고장을 검출할 수 있었다는 결과를 발표한 바 있다. 하지만, 이러한 고장주입실험에 의해 얻어진 실험결과는 특정 시스템에 대해서, 특정 실험조건에 대한 결과이므로, 디지털 기기의 안전성 및 위험성 평가를 위한 일반적인 정량화 방법론에 적합하다고 할 수 없다. 이에 따라, 본 연구는 고장 검출범위의 정량화를 위한 보다 근본적이고, 이론적인 접근을 시도하여, 이를 바탕으로 대상시스템을 선정하여 그에 대한 고장검출범위 평가를 수행하였다.

2. 고장검출범위 정량화에 대한 고찰

디지털 기기의 고장검출범위에 대한 국내전문가와의 상의 결과 그림 1의 감시타이머의 고장검출범위를 구하기 위해서는 감시타이머에 대한 분석보다는 감시대상시스템 자체에 대한 분석이 필요하다는 결론을 얻을 수 있었다. 이는 감시타이머의 경우 고장 검출범위가 대상이 되는 디지털계통에서 생성되어서 감시타이머로 전해지는 heartbeat 신호에 대한 의존성이 절대적이기 때문이며, 결국 heartbeat 신호는 디지털계통 내부의 알고리즘에 의해서 생성되기 때문이다. 현재 디지털 계통에서 감시타이머를 위해 생성하는 heartbeat 신호는 생성되는 위치에 따라 크게 응용소프트웨어(Application Software, AS)에서 생성되는 경우, 운영체제(Operating System, OS)에서 생성되는

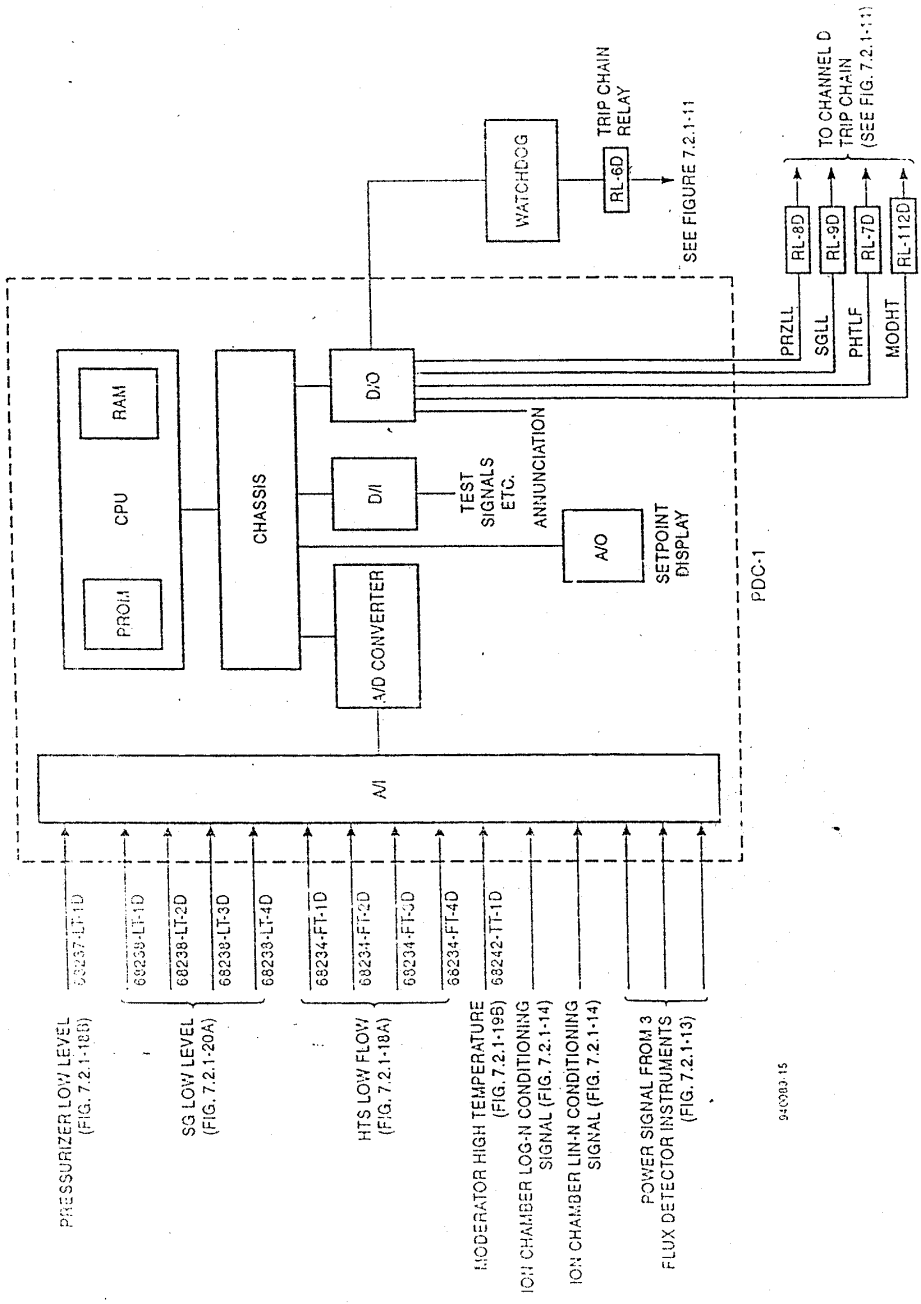

그림 3 Channel D PDC-1 and Watchdog

경우, 그리고 디지털 계통의 자체검사에 따라 생성되는 경우로 나누어 질 수 있다. (그림 2) 이에 따라, 정량화 방법론 역시 이러한 서로 다른 경우에 맞도록 개발되어져야 한다는 결론을 도출하였다.

3. 대상시스템 선정 및 분석

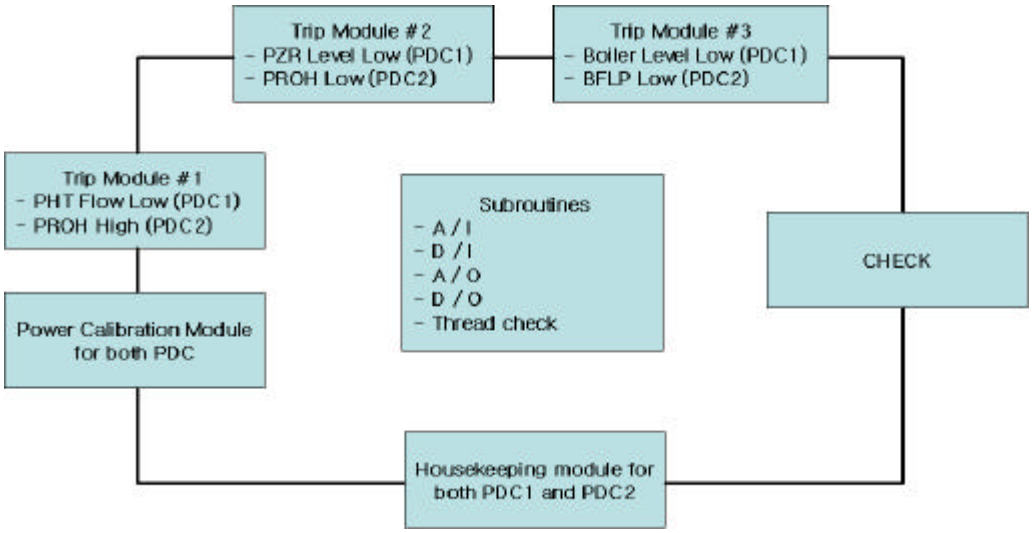

그림 4 PDC 소프트웨어의 구조

대상이 되는 디지털 계통에 대한 분석이 중요해짐에 따라, 실제 원자력발전소의 디지털 계통에서 감시타이머와 같은 고장 내구성기법이 어떻게 적용되고 있는지 그 실태조사를 위하여 월성 원자력발전소의 보호계통인 PDC(Programmable Digital Comparator)에 대한 자료조산 및 분석을 수행하였다. 월성 원자력발전소는 CANDU형의 발전소로써 경수로형 발전소 노형과는 달리 오래전부터 디지털 계통을 제어 및 보호계통에까지 적용하여, 월성 1호기의 경우 운전이력이 20년이 되어간다. 그림 3은 PDC 한 채널에 대한 전체적인 구조 및 감시타이머의 적용실태를 보여주고 있다. 그림 3에서 볼 수 있는 바와 같이 PDC 소프트웨어의 연산결과에 따라 Digital Output (D/O)를 통해서 감시타이머로 heartbeat 신호를 발생시키게 되는데, 만일 감시타이머가 heartbeat 신호를 적절하게 받아들이지 못할 경우 trip chain relay를 끊어버림으로써 해당 채널의 PDC를 trip 상태가 되도록 한다.

그림 4는 감시타이머로 향하는 heartbeat 신호를 생성하는 PDC 소프트웨어의 구조를 나타내고 있다. 그림 4에서 볼 수 있는 바와 같이 PDC 소프트웨어는 Loop형의 구조를 가지고 있으며, 발전소 상태에 따라 trip 여부를 결정하는 모듈을 실행한 후, 한번씩 PDC 계통에 대한 자체검사를 담당하는 CHECK 모듈을 수행한다. 감시타이머로의 heartbeat 신호는 위의 CHECK 모듈에 의해 생성되게 된다. 이러한 형태는 위의 이론적 고찰에서 언급한, 응용 소프트웨어에 의하여 heartbeat 신호가 생성되는 경우에 해당한다.

그림 4에 나타난 CHECK 모듈을 분석해 본 결과, CHECK 모듈은 PDC 각각의 하드웨어에 대한 자체검사 routine들로 이루어져 있고, 분석결과 감시타이머에 대한 heartbeat 신호의 생성은 이들 routine의 자체검사결과와 관련성을 가진다. 이에 따라, 감시타이머가 가지는 고장 검출범위는 CHECK 모듈내부의 자체검사 routine들의 고장 검출범위의 함수로 표현될 수 있다는 결론을 내릴

수가 있다.

CHECK 모듈에서 PROM(Programmable Read Only Memory)에 대한 자체검사는 checksum 검사를 통해서 수행되는데, 이는 수학적으로 결함이 존재하는 경우의 수에 대해서 결함이 검출될 경우의 수를 구할 수 있다. 이러한 경우는 수학을 이용한 이론적 분석에 의해 고장 검출범위를 정량화할 수 있음을 의미한다. 하지만, RAM(Random Access Memory)의 경우는 그 동적인 측면에 의해 결함발생에 대한 결함 검출의 확률을 이론적으로 구하기에는 상당한 어려움이 뒤따른다. 이러한 경우는 시뮬레이션을 통하여 고장 검출범위를 정량화 할 수 있는데, 모델링이 잘 되었을 경우 시뮬레이션을 통해 구해진 고장 검출범위가 실제 고장 검출범위에 매우 근접하게 구해질 수 있을 것으로 예상된다.

4. 월성 PDC에 적용된 감시타이머의 고장검출범위 분석

월성 PDC 소프트웨어의 CHECK 모듈에서 각각의 하드웨어에 대한 자체검사(self-check) 기능에 의한 고장검출범위를 분석하여 보았다. PDC 소프트웨어는 100msec 마다 한 번씩 루프를 돌기 때문에 CHECK 모듈 역시 100msec 마다 한 번씩 수행된다.

아날로그 입출력 (Analog I/O)에 대한 자체검사

아날로그 입출력의 자체검사는 아날로그 출력에서 디지털로 된 값을 아날로그 값으로 변환하여 자체검사신호(self-check signal)을 생성한 뒤, 이를 아날로그 입력에서 읽어들여서, 이를 다시 디지털 값으로 변환하여 원래의 디지털 값과 비교함으로써 이루어진다. 이러한 검사는 0에서 5.0V사이의 범위에서 최소 10군데 이상의 지점에서 수행되어야 하는 것으로 기술지침서에 기술되어있다. 만일 변환 이후에 발생한 오차(error)가 전체 4096 단계(count) 중에서 40 단계 이상으로 오차가 1.0%가 넘게 될 경우에서 PDC의 관련 LED를 켜고, 경보를 발생시켜 운전원에게 이를 알린다. 이 경우에는 단지 경보만 발생시킬 뿐 감시타이머에 heartbeat 신호제공을 중단하지 않으며, 문제가 발생한 조건에서 문제가 해결될 때까지 반복해서 자체검사를 수행한다.

아날로그 입출력에 대한 자체검사 과정에서 4096가 2^{12}이므로 전체적으로 12비트(bit)로 아날로그 값이 디지털 값으로 표현된다. 만일 시험이 12군데의 지점에서 수행된다고 하면, 이러한 시험지점들을 각각의 비트들에 대한 검사를 모두 포함하도록 구성할 수 있다. 아날로그 입출력에서 변환된 디지털 값의 특정 비트가 하나의 값으로 고정되어 버리는 stuck-at-0 또는 stuck-at-1 고장에 대해서, 자체검사는 12비트에 대한 전수검사를 수행하게 됨으로, 오류가 검출되지 않는 경우에 대한 가장 중요한 인자는 운전원이 경보를 인지하지 못하는 사건이 된다. 만일 이를 무시하게 된다면 아날로그 입출력에 대한 고장검출범위는 공학적 판단에 의해 1로 추정할 수 있을 것이다.

PROM에 대한 자체검사

PROM의 경우 매 루프마다 checksum을 수행하여 checksum에서 오류가 발생할 경우 감시타

이머에 heartbeat 신호의 제공을 중단함으로써 해당 PDC가 트립(trip)상태가 되도록 한다. PROM에 대해서 수행하는 checksum의 고장검출범위는 가장 간단한 알고리즘인 패리티 비트 검사(parity bit check)의 고장검출범위를 통해서 유추할 수 있다. 패리티 비티는 1 바이트(byte)에서 1의 개수를 홀수 또는 짝수가 되도록 하는 비트를 추가함으로써 데이터의 오류를 검출하는 기법이다. 패리티 비트는 간단한 알고리즘인 만큼 두 개 이상의 비트가 동시에 고장을 일으킬 경우 오류를 검출할 수 없다는 단점을 가진다. 하나의 비트의 고장률(failure rate)을 λ, 그리고 자체검사주기를 T라고 하면, 8 비트로 구성된 1 바이트에서 동시에 두 개의 비트가 고장날 확률 p는 다음과 같이 주어진다.

$$p = {}_8C_2\,(\lambda T)^2(1-\lambda T)^6 \qquad (2)$$

(2)을 이용하여 월성 PDC의 전체 PROM 용량인 4KB에 대하여 1 바이트라도 오류가 발생할 확률을 구하면 다음과 같다.

$$1 - C = 1 - (1-p)^{4000} \fallingdotseq 4000p \qquad (3)$$

(3)을 이용하여 1 비트 고장율에 대한 고장검출실패확률을 표로 나타내면 표 1과 같다.

1 비트 고장률 (hr^{-1})	10^{-7}	10^{-6}	10^{-5}	10^{-4}	10^{-3}	10^{-2}
고장검출실패확률	10^{-18}	10^{-16}	10^{-14}	10^{-12}	10^{-10}	10^{-18}

표 1 1 비트 고장률에 대한 패리티 비트 검사의 고장검출실패확률

이미 언급한 바와 같이 패리티 비트 검사는 가장 간단한 알고리즘임에도 불구하고, 표 1에서 보는 바와 같이 고장검출실패확률이 거의 무시할 수 있는 수치로 계산되어짐을 확인할 수 있다. 실제 PROM 자체검사에 적용되는 checksum 기법이 패리티 비트 검사에 비해 더욱 정교한 알고리즘임을 감안한다면, PROM의 오류에 대한 고장검출범위가 1로 추정할 수 있다고 할 수 있을 것이다.

RAM에 대한 자체검사

PDC에서 RAM에 대한 자체검사는 한 번의 프로그램 패스(Program pass)당 한 바이트씩 이루어진다. PDC는 4KByte의 RAM을 가지고 있다. 검사가 이루어질 대상바이트에 대해서는 우선 그 바이트의 내용을 저장한 뒤, 모든 비트들을 1(set)로, 모든 bit들을 0(clear)으로 및 "Alternate bits set"과 "Alternate bits clear"를 수행하게 된다. 이후 저장되어있는 본래의 내용을 대상바이트에 다시 저장시켜 원래 상태로 복귀시키는데, 만일 오류가 발생시에는 운전원에게 경보를 발생하고, 감시타이머에 heartbeat 신호의 제공을 중단함으로써 해당 PDC가 트립상태가 되도록 한다.
RAM에 대한 자체검사의 경우 모든 바이트의 모든 비트들에 대한 전수검사를 수행한다. 이에 따라 RAM에 대한 고장검출범위는 공학적 판단에 따라 1로 추정할 수 있을 것이다.

5. 결론

본 논문에서는 디지털 기기의 안전성 및 위험도 평가를 위해 필요한 고장검출범위를 정량화하는 방법에 대해서 기술하였다. 본 연구에서는 고장내구성 기법으로 가장 널리 쓰이는 감시타이머의 고장검출범위를 정량화하기 위한 여러 가지 고찰 및 방법론, 그리고 월성 PDC를 대상시스템으로 선정하여 실제 적용해 봄으로써 개발된 방법론의 타당성을 검증하였다. 본 연구를 통해 감시타이머의 고장검출범위에 대한 정량적 평가를 위한 이론적 분석을 통해서, 감시타이머의 고장검출범위는 감시대상시스템에서 감시타이머에 제공하는 heartbeat 신호를 생성하는 알고리즘에 대한 분석을 통해 구해져야 함을 입증하였다. 이를 뒷받침하기 위하여 대상 시스템으로 월성 PDC를 선정하여 개발된 방법론을 적용한 결과, 월성 PDC에 적용된 감시타이머의 고장검출범위를 추정할 수 있음을 보였다.

참고문헌

[1] Hyun Gook Kang and Taeyong Sung, An analysis of safety-critical digital systems for risk-informed design, Reliability Engineering and System Safety, vol.78, no. 3, pp.307-314, 2002

[2] L. M. Kaufman and B. W. Johnson, Embedded digital system reliability and safety analyses, NUREG-GR-0200, U.S. Nuclear Regulatory Commission, 2001