'2000 춘계학술발표회 논문집
한국원자력학회

원전 안전계통에 사용된 디지털 컴퓨터시스템에 대한 실시간 성능 분석

Analysis on the Real-Time Performance of Digital Computer Systems used in Nuclear Power Plant Safety Systems

김복렬, 오성헌, 주운표, 정윤형

한국원자력안전기술원
대전광역시 유성구 구성동 19

요 약

원전 안전계통에 사용된 디지털 컴퓨터시스템은 사고 상황에 따른 타이밍 요구 제한치 이내에 응답해야 하므로 그 설계에는 엄격한 성능요건(예, 응답시간)이 부과된다. 특히, 시스템 응답시간의 관점에서 디지털 계통은 아날로그 계통과 상당한 차이를 갖고 있다. 본 논문에서는 그 차이를 분석하고, 월성 원전 제2정지계통에 사용된 디지털 컴퓨터시스템의 타이밍 및 스케줄링 분석을 통해 시스템 응답시간의 만족 여부와 실시간 성능을 평가하였다. 그 분석에서는 실행 모듈에 대한 스케줄러 동작모델, 실행 알고리즘 그리고 각 모듈의 실행에 따른 타이밍 도면을 작성하여 타이밍 데드라인을 정성적으로 평가하였다. 그 결과 디지털 컴퓨터의 스케줄 가능성을 확인하였고 실시간 성능은 검증시험을 통해 측정된 각 정지 변수의 응답시간이 50ms 이하로서 성능 타이밍 요건(100ms)에 대비하여 50% 이상의 타이밍 여유를 확보한 것으로 평가되었다.

Abstract

As digital computer systems used in the safety systems of nuclear power plants should be responded within timing requirements to accident situations, strict performance requirements (e.g., response time) are imposed upon the design of the computer systems. Especially, with respect to system response time, digital systems are largely different from analog systems. This paper analyzed the differences, performed the timing and scheduling analyses of digital computers used in Shutdown System No. 2 at Wolsong nuclear power plants, and evaluated whether the system response time and real-time performance are complied with. We analyzed the operation model, execution algorithm and execution timing diagram of a scheduler for execution modules, and assessed their timing deadlines qualitatively. We concluded the digital computer systems are capable of scheduling on demand and evaluated the real-time performance of the systems has the timing margin of more than 50% as compared with performance timing requirement (100ms), since the response time for each trip parameter measured through validation tests was less than 50ms.

1. 서 론

가동중 원전의 계측제어계통이 노후화 됨에 따라 유지, 보수에 따른 어려움과 비용 증대 등의 이유로 원전 사업자들은 노후화된 설비 또는 계통을 디지털 계통으로 교체해 가고 있다. 디지털 계통은 기능적인 관점에서 보면 아날로그 계통과 다르지 않지만, 운전 특성은 크게 다르다. 디지털 계통은 소프트웨어를 이용하여 복잡한 기능들을 순차적으로 수행하는 반면에 아날로그 계통은 병렬 처리가 일반화되어 있다. 이와 같이 순차적인 운전 특성을 갖는 디지털 계통이 원전의 안전계통에 사용될 때에는 아날로그 계통과는 다른 성능(performance) 문제를 안고 있다. 특히, 실시간 디지털 계통은 실제 공정에서 요구하는 타이밍 요구 제한치 이내에 응답해야 하므로, 동 계통의 설계에는 엄격한 성능요건(예, 응답시간)들이 부여되며, 이 같은 성능요건은 하드웨어와 소프트웨어 구조, 운영체제의 특성과 응용 요구사항, 그리고 프로그래밍 설계에 따라 크게 좌우될 수 있다. 일반적으로 원자로 보호계통이나 안전관련 계측제어계통의 성능을 평가하는 최소 척도로는 시스템 응답시간, 정확도와 측정 범위를 들고 있다[1]. 시스템 응답시간은 어떤 감시변수가 그 채널의 동작 설정치를 초과하는 시점에서부터 최종작동장치가 소정의 기능을 수행할 때까지 경과하는 시간을 의미한다. 정확도는 센서 또는 운전원의 입력 오차가 생기지 않은 정도, 측정값과 참값이 일치하는 정도, 그리고 작동기의 출력 오차가 생기지 않은 정도를 의미한다. 측정 범위는 어떤 물리량이 측정되는 하한과 상한 값의 간격을 나타낸다[2]. 이 척도들 중에 실시간 디지털 계통의 성능에 직접적인 영향을 미치는 것은 시스템 응답시간이다. 원전 안전계통의 응답시간은 원자로 출력 진동억제, 핵연료 설계 제한치 초과 방지, 노심 냉각구조 손상방지 등과 같은 사고해석 또는 기술지침서의 응답시간에 근거하여 설정되어야 한다. 본 논문에서는 디지털 컴퓨터시스템의 응답시간을 비교·분석하고, 월성 원전 2,3,4호기 제2정지계통에 사용된 디지털 컴퓨터시스템의 타이밍 및 스케줄링 분석을 통하여 시스템 응답시간의 만족 여부와 실시간 성능을 평가한다.

2. 디지털 컴퓨터시스템의 응답시간에 대한 분석

위에서 언급한 바와 같이 시스템 응답시간 관점에서 디지털 계통은 아날로그 계통과 크게 차이가 있다. 먼저, 아날로그 계통은 모든 측정변수가 각각 3-4개의 해당 채널들을 갖고 있기 때문에 관련 기능들이 동시 다발적으로 병렬 처리가 가능하다. 반면에 디지털 계통은 일반적으로 각 채널이 센서 및/또는 신호처리회로를 제외하고는 그림 1과 같이 공통된 자원(예, CPU, 메모리)을 공유하게 된다. 이와 같은 구조를 갖는 디지털 계통은 각 채널에 속한 모든 측정변수들이 한 개의 프로세서만을 공유하므로 병렬 처리가 이루어지지 않고 순차적으로 그 프로세서에서 각 측정변수마다 할당된 시간 내에 처리해야 한다. 예를 들어, 그림 1에서 비교논리부분의 할당시간 t_3의 경우 아날로그 계통은 각 채널이 독립적이므로 비교논리 회로가 할당된 시간(=t_3)을 모두 사용하지만, 디지털 계통은 비교논리 프로세서를 공유하는 모든 측정변수들이 t_3 시간을 다시 분할, 사용해야 함으로 각 측정변수에 할당된 시간 프레임(frame)은 t_3/n (n=측정변수의 개수) 이다. 이것은 다음과 같이 표현된다.

- 시스템의 전체응답시간: $t_1+t_2+t_3+t_4+t_5+t_6+t_7 \leq t$ (응답시간 요구 값)

- 비교논리 프로세서의 응답시간: $t_3 = t_{31}+t_{32}+t_{33}+ \cdots +t_{3m}$ (t_{3i}=비교논리 프로세서에서 각 측정변수에 할당된 시간 프레임)
- 동시논리 프로세서의 응답시간: $t_4 = t_{41}+t_{42}+t_{43}+ \cdots +t_{4n}+t'$ (t_{4i}=동시논리 프로세서에서 2/4 동시논리 구현을 위해 할당된 시간 프레임)

  여기서 t'는 다른 채널 또는 프로세서간의 데이터 통신에 따른 지연시간이다.

즉, 디지털 계통의 응답시간은 각 프로세서에서 할당한 시간 프레임과 다른 채널 또는 프로세서간의 데이터 통신에 따른 지연시간을 고려하여 합산한 전체응답시간이 사고해석 또는 기술지침서의 응답시간 요구 값보다 적거나 또는 같으면 적합한 것으로 평가한다. 따라서 안전관련 디지털 계통의 응답시간에 대한 성능현안 평가는 첫째 각 프로세서에서 각 측정변수에 할당한 시간 프레임과 통신 지연시간을 합산한 전체응답시간이 사고해석 또는 기술지침서의 요구 값보다 적거나 또는 같은지, 둘째 각 프로세서에서 각 측정변수를 그 시간 프레임 내에 적절히 스케줄링 할 것인지가 주요 관건이다. 첫 번째 현안은 시스템 구성요소들에 대한 타이밍 분석(예, 모듈)을 통하여 확인 및 검증해야 할 사항이고, 두 번째 현안은 관련 변수(또는 하부 모듈)들에 대한 실행가능성 또는 스케줄가능성 분석을 통해 확인되어야 한다. 본 논문에서는 첫 번째 현안과 관련하여 제2정지계통에 사용된 디지털 컴퓨터시스템에 할당된 성능 타이밍 요건(100ms)에 근거하여 각 실행 모듈에 대한 타이밍 분석을 수행하였고, 두 번째 현안과 관련하여 실행 모듈들에 대한 스케줄링 분석을 통해 실시간 성능을 평가하였다.

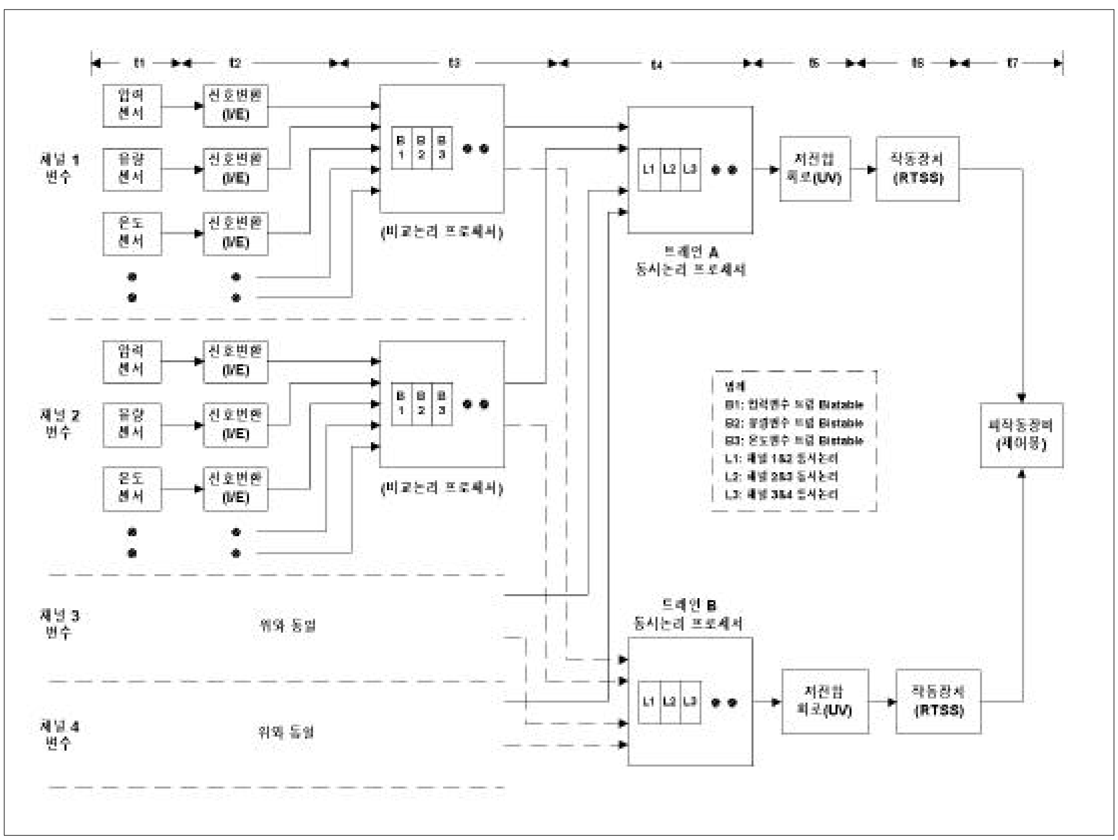

그림 1. 대표적인 디지털 계측제어계통과 응답시간에 대한 모델

3. 제2정지계통 디지털 컴퓨터시스템과 실행 모듈의 타이밍 분석

3.1 디지털 컴퓨터시스템에 대한 개요

월성 원전의 원자로 정지계통은 캐나다 AECB 규제문서 R-8[3]과 R-10[4]의 요건에 따라 제1 정지계통과 제2정지계통으로 설계되어 있다. 제1 및 제2 정지계통의 기본적인 기능요건은 AECB C-6 문서[5]에 명시된 공정계통의 심각한 고장에 대비하여 원자로를 안전정지상태로 도달 및 유지시키고, 허용방사선량의 초과 방지, 그리고 노심의 에너지 생성율과 격납건물로 방출된 에너지를 제한함으로써 격납건물의 건전성을 보장하는데 있다. 각 정지계통의 비교논리회로는 각 채널마다 두 개의 디지털 컴퓨터시스템(PDC1과 PDC2)을 이용하여 출력 변화에 따른 설정치 계산과 정지 기능을 수행한다. 한편 사고해석 또는 기술지침서의 루프응답시간 계산에서는 각 정지 컴퓨터의 응답시간을 100ms로 할당하였다[6,7]. 따라서 각 정지 컴퓨터(예, PDC1)는 A/D 변환기에서 처리된 공정 신호를 받아서 정지 여부를 결정하고 필요하다면 100ms 내에 디지털 출력접점을 개방해야 한다. 이를 위해 각 정지 컴퓨터는 100ms 이내에 관련 감시 및 제어변수를 실행 모듈별로 할당된 타이밍 데드라인 내에 처리해야 한다.

3.2 실행 모듈의 타이밍 분석

제2정지계통의 디지털 정지 컴퓨터(PDC1)의 주요 기능은 가압기 저수위, 일차열수송계통의 저유량, 그리고 증기발생기 저수위에 의한 원자로 정지기능을 수행한다. 또한 상기와 같은 정지기능뿐만 아니라 자가진단기능 및 지시기능들을 수행하게 된다. 이와 같은 기능을 실행 주기별로 분류한 것이 하나의 주기적인 실행 모듈을 형성한다. 그 중에서 가압기 저수위 정지 모듈, "PUD7 (PZLTripFunc)"에 대한 모듈 타이밍을 분석하기 위한 내부 데이터 흐름을 보면 그림 2와 같다[8]. 그림 2에서 /m_PrzL/은 입력변수이고, //c_PZLTrip//은 출력제어변수이며, 원(circle)은 실행처리 단위를 나타낸다. 이 그림에 근거하여 가압기 저수위 정지 모듈들에 대해서 보다 세부화된 타이밍 요구사항은 표 1과 같다. 각 실행 모듈의 타이밍 요건은 출력제어변수, c_PZLTrip의 성능 타이밍 요건(100ms)을 만족할 수 있도록 분할·선정되었다. 실행 모듈의 타이밍 분석결과가 타이밍요건(100ms)을 실제로 만족할 것인지는 실행프로그램을 목표 기종(target machine)에 장착한 이후에 검증시험을 통하여 확인된다.

표 1. 실행 모듈 PUD7에 대한 할당된 타이밍 요구사항

데이터 흐름	모듈 유형	시간	비고
/m_PrzL/	주기	50 ms	
GPumpMde	주기	50 ms	f_PumpMde
GFaveC	주기	50 ms	sf_FlxIrr, sf_FaveC,f_Gdr
GFlog	주기	50 ms	f_Flog
GmPrzL	주기	50 ms	m_PzrL,i_PrzL
GPZLSp	주기	50 ms	f_PZLSp
GPZLCond	주기	50 ms	f_PZLCond
GPZLSnr	주기	50 ms	f_PZLSnr
//c_PZLTrip//	-		

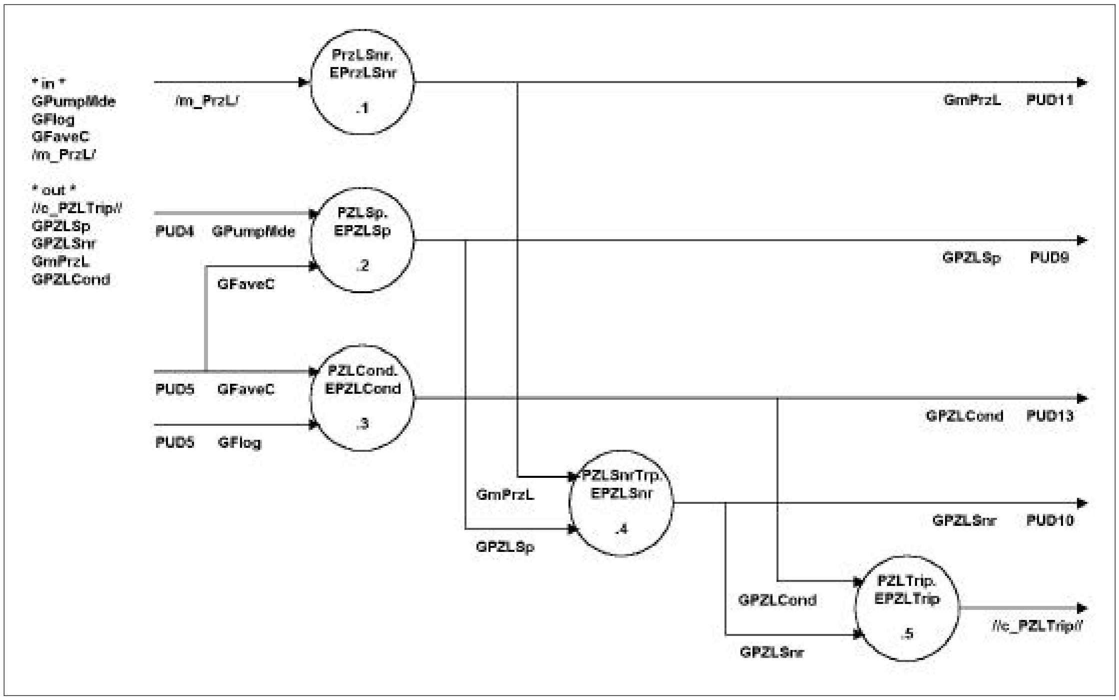

그림 2. 실행 모듈 PUD7의 내부 데이터 흐름도

4. 실행 모듈에 대한 스케줄링 분석 및 성능 평가

디지털 정지 컴퓨터의 실행 모듈들은 주기적인 무한 실행루프를 돌게 된다. 이와 같은 실행루프는 오래 전부터 안전관련 실시간 보호 또는 제어계통에 널리 사용되어온 순환 실행(cyclic executives) 스케줄러에 의해서 이루어진다[9]. 순환 실행 스케줄러는 모듈 실행을 관리하는 소프트웨어이며, 그 실행 구조는 실행 모듈들에 대한 일정한 순서를 결정하고 수행하는 메인(main) 루프로 구성된다. 예를 들어, 순환 실행 순서는 모듈 PUD 1, 2, ⋯, n 순으로 논리적인 루프를 형성하며, 각 모듈은 메인 루프의 관리하에서 실행된다. 모듈의 호출은 주기적인 순서에 따라 이루어지고 마지막 모듈 n이 수행된 다음에 클록 함수를 호출하여 그 루프의 한 주기 시간과 비교해서 남은 시간동안 첫 번째 모듈 PUD1을 지연시켰다가 다시 순환·실행한다. 그래서 모듈들간의 동시 실행은 발생하지 않으며 서로 독립되고 주기적인 실행특성을 갖게 된다. 또한 모듈 PUD1의 시작은 반드시 클록에서 정한 일정한 시간간격으로만 이루어진다. 이와 같이 정해진 일정한 시간간격을 시간 프레임이라 하며, 모든 실행 모듈들은 일정한 시간 프레임 내에 종료되어야 한다.

4.1 분석 방법

서로 독립되고 주기적인 실행 모듈들에 대한 대표적인 스케줄링 분석방법은 비율-기반이론(rate monotonic theory)에 근거한 이용도 한계(utilization bound) 분석방법과 종료시간(completion time) 분석방법이 있다[10]. 이용도(C/T) 한계분석은 실행 모듈들이 관련 데드라인을 만족한다면 그 모듈들에 대한 스케줄링이 가능한 것으로 본다. 즉, 이용도 한계분석은 만약 n개의 독립되고 주기적인 실행 모듈들이 있을 경우 각 모듈에 대한 이용도 합계가 전체 CPU 이용도 상한 값 [$U(n)$]

이하이면 그 모듈은 반드시 데드라인을 만족하게 된다. 이를 수식으로 표현하면 식(1)과 같다.

$$\frac{C_1}{T_1} + \cdots + \frac{C_n}{T_n} \le n(2^{1/n} - 1) = U(n) \quad \cdots\cdots\cdots\cdots\cdots \quad (1)$$

여기서 C_i = 실행 모듈 i의 실행시간, T_i = 실행 모듈 i의 주기

n = 독립된 실행 모듈의 개수, $U(n)$ = n개 모듈의 이용도 상한 값

만약 실행 모듈들이 이용도 상한 값을 초과하면, 보다 정확한 스케줄링 기준을 제시한 종료시간 분석방법을 이용하여 분석해 볼 수 있다. 종료시간 분석은 모든 실행 모듈들이 동시에 실행하는 최악의 경우를 가정한다. 만약 어느 한 모듈이 자신의 첫 번째 주기 이전에 실행을 종료한다면 그 이후에는 결코 데드라인을 놓칠 염려가 없다는 것이다. 따라서 종료시간 분석은 각 모듈이 자신의 첫 번째 주기 이전에 실행을 종료할 수 있는지 여부를 점검하게 된다. 종료시간 분석방법을 다시 정리하면 서로 독립되고 주기적인 모듈들이 동시에 시작할 경우 만약 각 모듈이 자신의 첫 번째 데드라인을 만족한다면 그 이후에는 시작시점이 어떻게 조합되더라도 그 데드라인을 모두 만족할 것이다. 각 실행 모듈의 종료시간은 다음 식 (2)과 같은 반복공식에 의해 계산될 수 있다.

$$W_i(m+1) = C_i + \sum_{j<i}^{N} \left[\frac{W_{i(m)}}{T_j} \right] C_j, \; W_i(0) = 0 \quad \cdots\cdots\cdots\cdots\cdots \quad (2)$$

여기서 W_i = 실행 모듈 i의 종료시간

i = 실행 모듈 번호

m = 데드라인 횟수$(1, 2, \cdots, m, \cdots, N)$

T = 실행모듈 i의 주기

상기의 이용도 한계 또는 종료시간 분석방법은 주기적인 실행 모듈들에 대한 스케줄링 가능성을 정량적으로 평가할 수 있는 좋은 방법이지만, 이러한 방법을 적용함에 있어서 선행사항은 각 모듈의 실행시간을 측정할 수 있어야 한다. 만약 각 모듈의 실행시간을 측정 또는 추정할 수 없다면 정량적인 스케줄링 분석은 사실상 불가능하다. 실제로, 각 모듈의 실행시간은 하드웨어의 구조와 동작 특성에 따라 달라질 수 있으며 복잡한 시스템의 경우 각 모듈의 실행시간을 조건별로 모의하여 측정하기란 매우 어렵다. 따라서, 본 논문에서는 각 모듈의 실행시간을 직접적으로 측정할 수가 없어서 정량적인 분석방법에 따른 구체적인 계산결과를 도출하지 못하고, 실행 모듈에 대한 스케줄러 동작모델, 실행 알고리즘 그리고 각 모듈의 실행에 따른 타이밍 도면을 작성하여 타이밍 데드라인을 정성적으로 분석·평가하였다.

4.2 분석 결과

디지털 정지 컴퓨터(PDC1)의 실행 모듈들은 표 2에 기술된 바와 같이 총 14개이며 스케줄러는 각 실행 모듈을 그 실행주기에 따라 프로세서(CPU)에 배정하게 된다. 표 2의 모듈들을 실행 주기별로 다섯 개의 루프, 즉 루프1 (50ms), 루프2 (250ms), 루프3 (500ms), 루프4 (1000ms) 그리고 루프5 (1hr)로 분류하였다. 이 루프들을 실행 주기별로 스케줄링 해 주는 스케줄러의 동작을 그림 3과 같이 모델링 하였으며, 그 스케줄러의 실행 알고리즘을 도식화하면 그림 4와 같다.

표 2. 디지털 트립 컴퓨터(PDC1)에 대한 주기적인 실행 모듈

모듈 유형	스케줄링 요건	모듈 유형	스케줄링 요건
PUD01-AOChkFunc	@ 1sec	PUD08-SLLTripFunc	50 ms
PUD02-DOChkFunc	@ 1hour	PUD09-DisplayFunc	250 ms
PUD03-CheckFunc	50 ms	PUD10-TripAlarmFunc	500 ms
PUD04-SwitchesInput	50 ms	PUD11-SigAlarmFunc	250 ms
PUD05-PowerFunc	50 ms	PUD12-CheckAlarmFunc	500 ms
PUD06-PDLTripFunc	50 ms	PUD13-AnnunFunc	250 ms
PUD07-PZLTripFunc	50 ms	PUD14-Watchdog	@ 20 ms

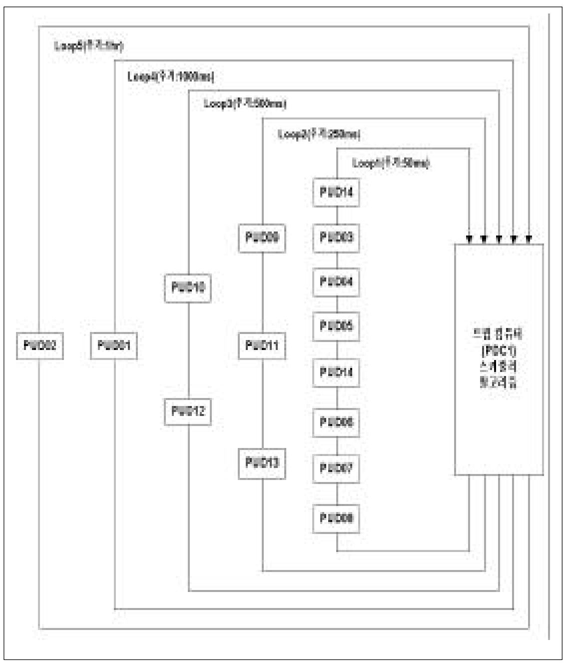

그림 3. 스케줄러의 동작모델

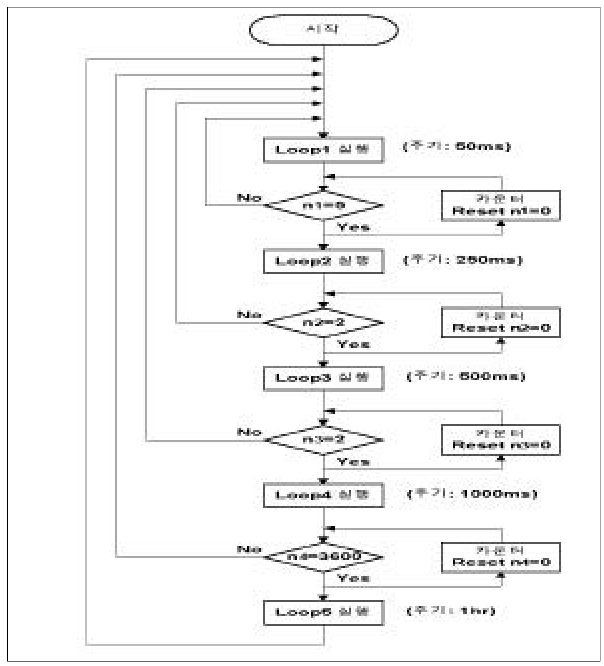

그림 4. 스케줄러의 실행 알고리즘

그림 3과 4에서 스케줄러의 실행 결과를 분석하면 스케줄러는 ① 0 200 ms 기간에서 루프1 모듈들을 4회 반복적으로 실행시키고, ② 201 250 ms 기간에는 루프1과 루프2 모듈들을 순차적으로 실행시키며, ③ 251 450 ms 기간에는 ①의 기간에서처럼 루프1 모듈들만을 다시 4회 반복적으로 실행시킨다. ④ 451 500 ms 기간에는 루프 1, 2, 3의 모듈들을 실행시킨다. 스케줄러는 ⑤ 501 950 ms 기간에 상기 ①과 ② 기간에서처럼 루프1과 루프2를 반복적으로 실행시키며, ⑥ 951 1000 ms 기간에는 루프 1, 2, 3과 4를 모두 실행시킨다. 그 후 1001ms에서부터 (1hr-50ms)까지는 이들 루프가 반복적으로 실행된다. 끝으로 스케줄러는 ⑦ (1hr-50ms) 1hr 기간에 루프 1, 2, 3, 4 그리고 5의 모든 모듈들을 실행시킨다. 특히 ⑦의 기간에는 디지털 컴퓨터시스템이 성능 타이밍 요건(100ms)을 만족하면서 모든 모듈들을 실행해야 하기 때문에 디지털 시스템이 가장 많은 실행 모듈들을 처리해야 하는 최악의 상태이다. 이상과 같은 스케줄러의 실행 결과를 타이밍 도면으로 그려보면 그림 5와 같다. 그리고 표 3은 각 실행 모듈에 대한 타이밍 매트릭스를 나타낸 것이다.

실제로 ⑦ 기간 내에 성능 타이밍 요건을 만족할 것인지는 실행 프로그램을 목표 기종에 장착한 후에 검증시험을 통해 확인될 수 있다.

표 3. 주기적인 실행 모듈에 대한 타이밍 매트릭스

시간	PUD 01	PUD 02	PUD 03	PUD 04	PUD 05	PUD 06	PUD 07	PUD 08	PUD 09	PUD 10	PUD 11	PUD 12	PUD 13	PUD 14
50ms			○	○	○	○	○	○						○/○
100ms			○	○	○	○	○	○						○/○
150ms			○	○	○	○	○	○						○/○
200ms			○	○	○	○	○	○						○/○
250ms			○	○	○	○	○	○	○		○		○	○/○
300ms			○	○	○	○	○	○						○/○
350ms			○	○	○	○	○	○						○/○
400ms			○	○	○	○	○	○						○/○
450ms			○	○	○	○	○	○						○/○
500ms			○	○	○	○	○	○	○	○	○	○	○	○/○
501 950ms	0ms 450ms 구간과 동일함													
1000ms	○		○	○	○	○	○	○	○	○	○	○	○	○/○
1001ms (1hr-50ms)	0ms 1000ms 구간 반복													
1hr	○	○	○	○	○	○	○	○	○	○	○	○	○	○/○

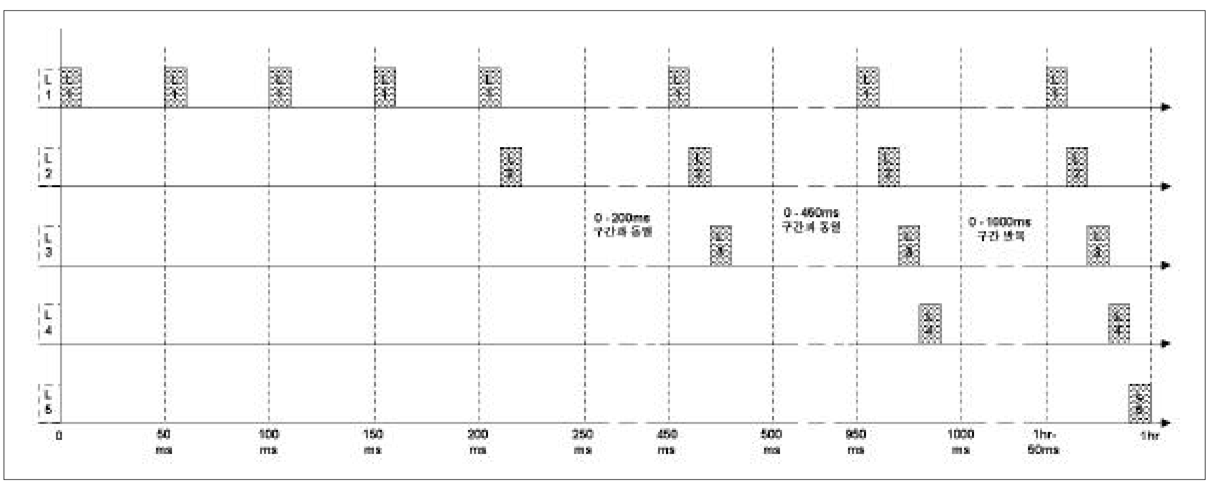

그림 5. 스케줄러의 실행 타이밍 도면

지금까지는 디지털 컴퓨터시스템에서 구현되는 주기적인 모든 실행 모듈들에 대한 스케줄러 동작 모델, 알고리즘, 그리고 실행 결과를 도식적으로 분석하였고, 다음은 각 실행 모듈이 그 주기 안에서 데드라인 시간을 만족할 것인지를 자세히 평가한다. 표 2의 실행 모듈들 중에서 가장 엄격한 스케줄링 요구시간을 갖는 모듈들은 루프 1의 모듈들이다. 루프 1 모듈들의 데드라인을 한 주기, 최대 50ms 까지를 설정할 수도 있지만, 실제 예상된 루프 실행시간은 모든 입력과 출력 하드웨어

의 처리 지연시간(대략 10ms)을 고려하여 40ms를 결정론적 데드라인으로 선정한다. 이 같은 데드라인 선정은 두 차례의 Watchdog 토글간격(20ms) 때문에 그렇게 제한될 수밖에 없다. 결정론적 데드라인 40ms를 구현하기 위해서 스케줄링 루프는 20ms씩 두 부분으로 구분하여 각 부분(20ms)마다 이루어지고 그때마다 Watchdog 토글이 한번씩 일어난다. Watchdog 모듈을 제외한 나머지 모듈(예, PUD 3-8)들은 두 부분 중의 어느 한 부분에서 실행되도록 스케줄링이 이루어진다. 만약 루프 실행시간이 실제로 각 부분에 할당된 시간(20ms)을 초과하면 치명적인 루프실행 타임아웃(timeout) 오류가 발생하고 시스템 응답시간을 만족하지 못하게 된다.

모든 정지변수 관련 모듈들은 단순하게 각 루프가 통과할 때(예, 40ms)마다 실행될 것이다. 다만 PUD1과 PUD2는 루프 실행주기(20ms)보다 훨씬 긴 주기로 실행된다. PUD9, PUD10, PUD11, PUD12, 그리고 PUD13 모듈들은 덜 엄격한 성능 타이밍 요건들을 갖기 때문에 교번(staggered) 루프 구조를 이용한 서로 다른 루프가 통과할 때에 실행된다. 이와 같이 긴 주기의 모듈들은 종료시간 분석방법에 근거하여 첫 번째 데드라인을 만족하면 시작 시점이 어떻게 조합되더라도 나중에는 그 데드라인을 만족할 수 있다. 따라서 주기 50ms인 루프 1의 실행 모듈들이 디지털 컴퓨터 시스템의 실시간 성능을 좌우하게 된다. 루프 1의 모듈들에 대한 실행시간을 측정할 수 없지만, 각 명령문의 실행시간이 수 μs[11]인 점을 감안하면 각 모듈이 데드라인을 만족할 것이고 스케줄링 가능성을 확보한 것으로 평가된다.

4.3 검증 시험

디지털 컴퓨터시스템에서 구현되는 실행 모듈들에 대한 확인 및 검증(V&V) 활동의 일환으로 그 프로그램을 목표 기종에 장착한 후 검증시험이 수행되었다[12]. 검증시험은 블랙박스(black box) 개념, 즉 기능요건의 확인에만 역점을 두었으며 시험방법은 디지털 컴퓨터의 입력부분에 공정조건을 모의하고 그것의 성공 혹은 실패를 출력부분에서 확인하였다. 각 정지 변수의 타이밍 시험에서는 표 4와 같이 각 정지 변수가 50ms 이내의 응답시간을 보였으며 성능 타이밍 요건(100ms)을 만족한 것으로 측정되었다.

표 4. 단일 정지 변수에 대한 응답시간 측정결과

정지 변수	응답시간(ms)	정지 변수	응답시간(ms)
PDC-1G PHTDP	47	PDC-2G PHTHP	45
PDC-1G PRZLL	47	PDC-2G PHTLP	46
PDC-1G SGLL	46	PDC-2G SGFLP	44

4.4 디지털 컴퓨터시스템의 응답시간에 따른 실시간 성능 평가

디지털 컴퓨터시스템은 최악의 부하조건하에서 소정의 기능을 수행할 수 있고, 또한 기능 확장에 대비할 수 있도록 충분한 성능 여유(margin)를 갖게 설계되어야 한다. 일반적으로 디지털 계통은 최악의 부하조건에서도 대략 40%의 여유 용량을 갖도록 설계하는 것이 바람직한 공학적 관례

이다 [13]. 상기의 분석결과를 통해 루프 1의 실행 모듈들이 그들의 데드라인을 만족한 것으로 평가되었으며, 또한 디지털 컴퓨터시스템에 대한 검증시험 결과에서 보면 각 정지 변수의 응답시간이 50ms 이하로서 성능 타이밍 요건(100ms)에 대비하여 50% 이상의 타이밍 여유를 확보한 것으로 확인되었다. 특히 순환 실행 스케줄러는 충분한 타이밍 여유가 없는 상태에서 기능 확장을 실시할 경우 스케줄 가능성을 해칠 수 있다는 단점을 감안해 보더라도 어느 정도의 기능 확장도 가능할 것으로 평가된다.

5. 결 론

원전 안전계통에 사용된 디지털 컴퓨터시스템의 설계에는 엄격한 성능요건(예, 응답시간)들이 부과된다. 특히, 시스템 응답시간의 관점에서 디지털 계통은 아날로그 계통과 상당한 차이를 갖고 있기 때문에 디지털 컴퓨터의 타이밍 및 스케줄링 분석 등에 있어서 신중을 기해야 한다. 본 논문에서는 아날로그 계통과 디지털 계통의 응답시간에 관해서 비교·분석하였고, 월성 원전의 제2정지계통에 사용된 디지털 컴퓨터시스템의 타이밍 및 스케줄링 분석을 통해 시스템 응답시간의 만족 여부와 실시간 성능을 평가하였다. 그러나, 각 모듈의 실행시간을 직접 측정할 수가 없어서 정량적인 분석방법에 따른 구체적인 계산결과를 도출하지는 못하였으나, 실행 모듈에 대한 스케줄러의 동작모델, 실행 알고리즘 그리고 각 모듈의 실행에 따른 타이밍 도면을 작성하여 타이밍 데드라인을 정성적으로 평가하였다. 그 결과로는 스케줄러의 실행 알고리즘이 서로 독립되고 주기적인 단순한 실행 특성을 갖고 있어서 실행 모듈들을 동시에 실행시키지 않으므로, 시스템의 정지(halt) 또는 데드록(deadlock)과 같은 최악의 상태를 초래하지 않고 스케줄이 가능한 것으로 분석되었다. 또한, 검증시험 결과를 보면 각 정지 변수의 응답시간이 대체로 50ms 이하로서 성능 타이밍 요건(100ms)에 대비해 50% 이상의 타이밍 여유를 확보한 것으로 확인하였다. 이 같은 결과는 일반적으로 시스템이 최악의 부하조건에서 대략 40%의 여유 용량을 갖도록 설계하는 것이 바람직하다는 공학적 관례를 만족한 것으로 평가된다.

참고문헌

[1] ANSI/IEEE Std. 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” 1971, Institute of Electrical and Electronics Engineers.

[2] ISA-S51.1-1979, “Process Instrumentation Terminology,” 1979, Instrument Society of America.

[3] AECB R-8, “Requirements for Shutdown Systems for CANDU Nuclear Power Plants,” February 1991.

[4] AECB R-10, “The Use of Two Shutdown Systems in Reactors,” January 1977.

[5] AECB C-6, “Requirements for the Safety Analysis of CANDU Nuclear Power Plants,” Rev.1, May, 1994.

[6] 86-68300-PFS-000, “Program Functional Specification for SDS2 PDC,” Rev.5, October 1995.

[7] 86-68350-SRS-001, “Software Requirements Specification for SDS2 PDCs,” Rev.2,

September 1994.
[8] 86-68350-SDD-001, “Software Design Descriptions for SDS2 PDCs”, Rev.2, March 1995.
[9] **김화수**, **윤창섭**, **송상섭 공저**, “Ada 95**를 이용한 실시간 시스템입문**,” 1999, **집문당**.
[10] Hassan Gomaa, “Software Design Methods for Concurrent and Real-Time Systems.” 1993, Addison-Wesley Publishing Company.
[11] 86-68300-DM-007, “Design Manual: Shutdown System No. 2, Part 7 - Programmable Digital Comparator Hardware,” Rev.0, November, 1994.
[12] 86-68350-TR-001, “SDS2 Final Validation Test Report,” Rev.0, June 1995.
[13] “Advanced Light Water Reactor Utility Requirements Document,” Vol. II, Chapter 10, “Man-Machine Interface Systems,” Rev.7, December 1995, Electric Power Research Institute.