IE Interfaces
Vol. 21, No. 1, pp. 85-95, March 2008.

일체형 원자로 보호계통의 디지털 신호 처리 모듈에 대한 신뢰도 예측

이상용[1†] · 정재현[1] · 공명복[2]

[1]삼창기업(주) 원자력사업본부 / [2]울산대학교 산업정보경영공학부

Reliability Prediction for the DSP module in the SMART Protection System

Sang-Yong Lee[1] · Jae-Hyun Jung[1] · MyungBock Kong[2]

[1]Nuclear Power Division Head Office, SAMCHANG ENTERPRISE CO., LTD, Ulsan, 689-871

[2]Department of Industrial Engineering, Ulsan University, Ulsan, 680-749

Reliability prediction serves many purposes during the life of a system, so several methods have been developed to predict the parts and systems reliability. MIL-HDBK-217F, among the those methods, has been widely used as a requisite tool for the reliability prediction which is applied to nuclear power plants and their safety regulations.

This paper presents the reliability prediction for the DSP(Digital Signal Processor) module composed of three assemblies. One of the assemblies has a monitoring and self test function which is used to enhance the module reliability. The reliability of each assembly is predicted by MIL-HDBK-217F. Based on these predicted values, Markov modelling is finally used to predict the module reliability.

Relax 7.7 software of Relax software corporation is used because it has many part libraries and easily handles Markov processes modelling.

Keyword: reliability prediction, DSP, MIL-HDBK-217, markov processes

1. 서 론

작동중인 원자로의 비정상 상태 시에 원자로를 안전하게 정지시키는 보호계통을 포함한 원자력 발전소의 많은 계통들은 오랫동안 아날로그 기기를 사용하여 그 기능을 수행해왔다. 그러나 최근의 세계적인 추세는 가동되고 있는 원자력 발전소의 안전과 직결되는 보호계통에서 마저도 아날로그 기기들을 디지털 기기로 대체하고 있다. 우리나라도 울진 5, 6호기에 이러한 추세가 반영되어 디지털 기기가 도입되었으며, 가동 중인 다른 원자력 발전소의 안전과 비 안전 계통에 있는 노후 기기들에 대하여 디지털 기기의 도입 및 대체가 추진되고 있다. 따라서 기기의 디지털 화에 따른 신뢰도 예측이 절실히 필요하다. 원자력 발전소의 안전에 관련되는 기기 및 계통들은 원자력 법규나 규제지침에 따라 높은 신뢰성이 요구되고 있으며 지금까지 원자력 발전소의 대부분의 기기에 대한 신뢰도 예측값은 외국의 기기 공급자가 제공한 결과를 그대로 수용하여 왔으며 국내에서 기기의 신뢰도를 직접 예측하는 경우는 많지 않았다. 전자 기기의 신뢰도의 예측은 수명기간 동안 여러 목적에 이용될 수 있다. 예를 들면, 설계단계에서는 온도나 전기적 스트레스가 설계에 미칠 영향을 알기 위하여 그리고 개발단계에서는 사용 환경에서의 신뢰도 목표를 설정하기 위하여 사용될 수 있다. 따라서 부품이나 시스템의 신뢰도 예측에 사

†연락저자 : 이상용 이사, 689-871 울산광역시 울주군 웅촌면 고연리 974-1번지 삼창기업(주) 원자력 사업 본부, FAX : 052-260-7230, E-mail : lsy010@samchang.com

2007년 05월 접수, 2회 수정 후 2007년 09월 게재확정.

용되는 많은 절차들이 이미 개발되어 있다.

Bowles(1992)는 6가지 절차(MIL-HDBK-217, Bellcore 신뢰도 예측 절차, NTT 절차, CNET 절차, British Telecom HRD4, Siemens 절차)를 마이크로 전자 부품에 적용하는 것을 개관하고 이를 64K DRAM에 적용한 결과는 절차마다 예측값에 차이가 많고 British Telecom HRD4를 제외한 다른 5가지 절차가 마이크로 전자 부품의 신뢰성이 개선되는 것을 반영한 예측을 하지 못함을 밝혔다. 즉, 부품의 신뢰성 예측 모형이 전자분야 기술의 급속한 성장과 디지털화에 따른 부품의 성능 향상을 반영하지 못하고 있으며, 예측모형마다 각기 다른 고장 영향 인자와 가중치를 부여하여 예측모형마다 다른 신뢰도 값이 계산되고 있다. 이에 대한 대안으로 Wong(1995)은 부품의 수명을 지수분포가 아닌 와이블분포로 하고 여러 인자를 고려하여 부품의 신뢰성을 예측하는 절차를 제안하였다. So and Kang(1997)은 가속수명시험을 설계하기 위한 입력데이터로 축전기에 대한 고장률을 MIL-HDBK-217 절차로 예측하였다.

한편 시스템에 대한 신뢰도 예측에서 Jones and Hayes(1999)는 5가지 절차(MIL-HDBK-217, Bellcore 신뢰도 예측 절차, CNET 절차, British Telecom HRD4, Siemens 절차)를 여러 형태의 회로기판에 대한 신뢰도 예측에 적용하여 절차마다 예측값이 서로 다르고 이들이 현장값과도 매우 다르다는 것을 보였다. 또한 예측에 사용되는 절차마다 서로 다른 물리적 모수에 민감하였으며 특히 MIL-HDBK-217은 환경과 품질인자에 가장 민감하였다. 따라서 Cassannel *et al*.(2005) 등은 시스템의 신뢰성 예측에 MIL-HDBK-217, CNET 절차 등에 의한 경험적 신뢰성 예측값에 현장에서 얻어진 데이터 분석결과와 시험 또는 고장분석을 통한 결과를 반영하여 예측하는 방법을 제시하고 있다. Jung *et al*.(2000) 등은 디지털 기기의 하드웨어 신뢰도를 예측하는 5가지의 절차에 대하여 조사 연구를 하였다. 특히 MIL-HDBK-217와 Bellcore의 신뢰도 예측 절차를 자세히 비교하였으며 MIL-HDBK-217이 더 많은 인자를 고려하고 있어 정확하고 세계적으로도 폭넓게 많이 사용되고 있다고 하였다.

시스템의 신뢰성 예측은 부품, 설계, 제조과정, 기대되는 사용 환경 등에 대한 정보를 필요로 한다. 그러나 대부분의 시스템 신뢰성 예측 절차는 설계부분에서 시스템이 부품들의 직렬구조로 설계되어 있다고 간주하고 시스템의 신뢰성을 예측하고 있다. 따라서 최근에 안전과 관련한 시스템에서 디지털 기기를 사용하는 경우 디지털 기기의 특성상 신뢰성을 향상시키는 다양한 설계가 가능하지만 이를 반영한 신뢰도 예측은 거의 없다. Yun and Yun(1999)은 부품들의 직렬구조인 아날로그 원자로 보호 모듈들에 대하여 MIL-HDBK-217을 사용하여 신뢰도를 예측하고 이에 기초하여 보호계통의 신뢰도를 예측하고 경년화에 의한 신뢰도 변화를 계산하였다.

본 논문은 국내에서 원자력 중장기 사업의 일환으로 순수 국내 기술로 개발되고 있는 원자로 주기기를 단일 압력 용기에 내장한 가압 경수로 중소형 원자로인 일체형 원자로(SMART: System integrated Modular Advanced ReacTor)의 디지털 신호 처리(DSP: Digital Signal Processor) 모듈에 대하여 신뢰도 예측을 수행한다.

원자력 발전소 제어 및 보호계통의 정량적 신뢰도 분석 요건인 EPRI URD에서는 MIL-HDBK-338 및 MIL-HDBK-217의 요건에 따라 정량적 신뢰도 분석을 수행할 것을 요구하고 있다. 디지털 신호 처리 모듈의 기능 분석을 통하여 기기를 어셈블리로 분류하여 각 어셈블리에 대하여 신뢰도를 계산하였다. 한편 디지털 신호 처리 모듈은 원자로 보호계통으로 신뢰성을 향상시키기 위한 설계가 반영되어 있으므로 이러한 특성을 고려하여 기기의 신뢰도를 예측하고자 한다. 모듈을 구성하는 어셈블리의 고장률 예측과 마코프 모형화에 의한 모듈의 신뢰도 예측은 신뢰성 분석 소프트웨어 Relex를 이용하였다.

2. 디지털 신호처리(DSP) 모듈의 설명 및 기능

2.1 디지털 신호처리 모듈 설명

디지털 신호 처리 모듈은 SMART의 보호계통에서 중앙처리장치(CPU) 역할을 하는 모듈로서, 아날로그 시스템의 여러 모듈로 나누어진 기능을 디지털 신호처리 모듈로 묶어 현장의 신호들을 산술 및 논리에 의해 제어하고 처리하는 핵심 모듈이다. 또한, 디지털 신호 처리 모듈은 각종 처리상태 표시와 고장 시에 경보기능, 자가진단 기능 등의 자체 성능 감시 기능을 지닌다. 디지털 신호 처리 모듈 내에 장착된 디지털 신호 처리 칩은 대부분의 응용 분야에서 실시간으로 많은 양의 데이터를 계산하거나 처리할 목적으로 사용되며 특히 디지털 신호 처리를 위하여 특수하게 제작된 프로세서이다.

원자력 발전소에서 지금까지 사용되고 있는 아날로그 신호 처리 모듈은 구성 요소가 아날로그이므로 열과 잡음, 부품의 수명, 그리고 주위 온도에 영향을 받아 그 기능에 있어서 불안정성의 문제를 지닌다. 그러나 디지털 기기인 디지털 신호 처리 모듈은 신호처리 내용(filtering, convolution, correlation, 신호의 정류, 증폭, 변환)이 소프트웨어로 구현되어 간단히 변경될 수 있고, 적은 수의 부품으로 구성되어 있다. 따라서 고성능에 안정성과 정밀도가 뛰어나며 높은 잡음 제거능력과 저전력 소모 구조로 되어 있어 기기의 크기를 소형화 할 수 있다.

디지털 신호 처리 모듈의 거의 모든 기능은 디지털 신호 처리 칩을 통해서 통제되고 처리되는데, 디지털 신호 처리 칩의 일반적인 작동을 설명하면 다음과 같다. 디지털 신호 처리 칩의 가장 핵심적인 부분은 코어(Core)인데, 코어의 구조를 살펴보면 프로그램 제어 장치, 번지 발생 장치(AGU: Address Generation Unit) 그리고 산술과 논리 장치(ALU: Arithmetic and Logic Unit)로 구성된다. 프로그래머가 에디터에서 프로그램을 작성하면 프로그램 제어 장치에서 명령어를 읽어 오고 거기에 해당되는 메모리 번지를 번지 발생 장치에서 발생해 데이터를 산술 논리 장치의 레지스터로 이동시켜 산술 논리 장치에서 산술 연산을 한 후 결과를 번지 발생 장치에서 만든 번지로 데이터를 이동시킨다. 디지털 신호 처리 칩의 성능은 산술과 논리적 연산의 처리 능력을 기준으로 한다.

2.2 디지털 신호 처리 모듈의 기능

디지털 신호 처리 모듈은 컴퓨터와 같이 디지털 입력 신호를 받아 처리하며 동시에 신호처리의 이상을 감시하고 자가진단 후에 복구하는 역할도 지니고 있다. <그림 1>은 디지털 신호 처리 모듈의 간략화된 기능 블록도이다. 그림에서 실선으로 연결된 기능들은 모듈의 필수적인 기능을 담당하며 파선으로 연결된 기능들은 서로 종속적인 관계를 가지고 있다. 점선으로 연결된 기능들 사이에는 감시관계를 가진다.

모듈의 기능은 크게 7가지로 대별할 수 있으며 이들 기능에 대하여 설명하면 다음과 같다.

2.2.1 Clock & Reset 블록

감시 및 자가진단 기능을 수행하는 곳으로, 일정 시간 동안의 신호를 카운트하고 일정 시간이 경과했는데도 다시 처음부터 카운트 되지 않을 때, 디지털 신호 처리 블록을 고장(정지)으로 간주하고 디지털 신호 처리 블록과 마스터 제어 블록을 리셋하게 된다. 워치독과 주변 부품들로 구성되며 두 가지 고장이 가능하다. “낮은 상태 고장”은 모듈의 리셋을 반복시켜 모듈의 필수기능에 영향을 주지만 “높은 상태의 고장”은 감시 및 자가진단 기능의 수행이 정지될 뿐 모듈의 필수기능에는 영향을 미치지 않는다. 그러나 낮은 상태의 고장은 발생률이 극히 작다.

2.2.2 Boot Logic 블록

디지털 신호 처리 모듈에 전원이 인가될 때, UVEPROM에 저장되어 있는 응용프로그램이 메모리 제어 블록 내의 로컬 메모리의 특정 번지에 복사되도록 한다. 모듈의 초기화 때에만 필요하다. 그러나 자가진단 기능에 의하여 모듈이 복구될 수 있도록 항상 작동할 수 있어야 하므로 모듈의 필수기능으로 처리한다.

2.2.3 UVEPROM(Ultra Violet Erasable PROM)

메모리 제어블록 내의 로컬메모리에 복사될 응용프로그램을 저장하게 된다. 모듈의 초기화 때에만 필요하다. 그러나 자가진단 기능에 의하여 모듈이 복구될 수 있도록 항상 작동할 수 있어야 하므로 모듈의 필수기능으로 처리한다.

2.2.4 디지털 신호 처리블록

마스터 제어블록의 제어에 의해 전송되는 데이터를 연산처리하거나, 응용프로그램을 수행한다. 고속의 고정소수점 또는 부동소수점을 처리하거나, 메모리에 대한 다중 엑세스 기능을 갖고 있으며, 주소와 데이터 버스가 분리된 구조를 가진다.

2.2.5 제어신호 처리 및 디스플레이 블록

디지털 신호 처리 제어 펌웨어, 마스터 제어 펌웨어, 메모리 제어 펌웨어, VME(VERSA Module Eurocard, 32비트 버스 규격) 통신 펌웨어, 기타 제어 펌웨어가 내장되어있다. 디스플레이는 프로그램형 논리 소자(PLD)에 의해 디지털 신호 처리의 상태를 DOT-MATRIX를 통해 문자로 표시한다.

2.2.6 메모리 제어블록

글로벌 메모리와 로컬 메모리로 구성되어 있다. 글로벌 메모리는 프로그램형 논리 소자에 의하여 글로벌 메모리 전체 번지를 읽기 및 쓰기를 수행하며, VME 버스 및 통신카드를 통해 전송되는 데이터를 저장하고, 로컬메모리에 상주하고 있는 응용프로그램의 DSP칩을 통한 실행결과 값을 복사하여 저장하고 VME 버스와 통신 카드를 통하여 전송한다. 로컬 메모리는 디지털 신호 처리 칩에서 처리되거나 수행되는 데이터를 저장하거나, 응용프로그램을 저장한다

2.2.7 마스터 제어블록

컨넥터를 통해 입출력되는 데이터를 제어하며, 디지털 신호처리를 통한 VME 데이터 전송 가능 회로를 구현, 독립적인 클럭을 사용함으로서 디지털 신호처리기와 비동기식 통신을 통해 제어알고리즘 처리 값을 보내고 받는 역할을 한다.

디지털 신호 처리 모듈의 기능 블록도를 살펴보면 디지털 신호 처리 모듈은 분류된 기능의 단순한 직렬 결합으로 표현되지 않는다. 더욱이 기능들은 동적으로 복잡하게 관련되어 상호 작용하며 종속적이다. 본 논문에서는 모듈의 필수 기능들이 독립적이라고 가정하고 모듈의 신뢰도를 향상시키는 감시 및 자가진단 기능이라는 디지털 기기의 설계 특성을 고려하여 신뢰도 분석을 행한다.

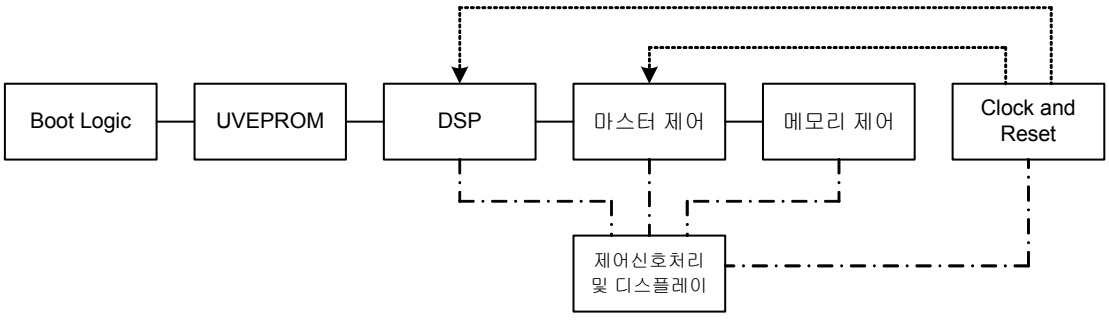

그림 1. 디지털 신호 처리 모듈의 간략화된 기능 블록도

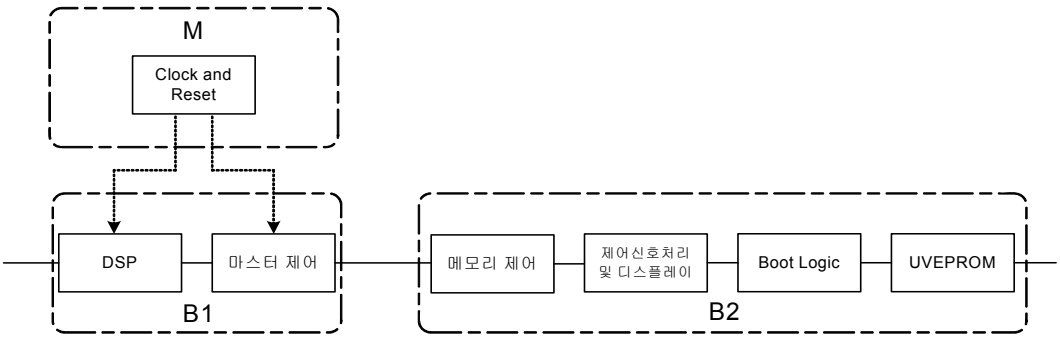

그림 2. 디지털 신호 처리 모듈 RBD

3. 디지털 신호 처리 모듈의 신뢰도 계산

모듈은 대별하면 7가지의 기능을 가지고 있으나 신호처리 및 제어 관련부분으로 모듈의 필수기능을 담당하는 부분과 신뢰성 향상을 위한 감시 및 자가진단 기능을 하는 clock and reset 블록으로 구성된 부분으로 분류될 수 있다. 다시 모듈의 필수기능은 고장이 발생했을 때 clock and reset 블록의 감시기능에 의하여 감시가 가능한 부분(B1)과 고장이 발생했으나 clock and reset 블록의 감시기능에 의하여 감시가 불가능한 부분(B2)으로 분류하여 M, B1, B2 의 3개의 어셈블리로 구분될 수 있다. <그림 2>는 이를 나타낸 것이다.

이것과 관련하여 중요한 가정은 다음과 같다.

1) 각 어셈블리 내의 부품들은 고장시간이 지수분포를 따르며 직렬결합으로 간주한다.
2) 모듈은 소프트웨어를 포함하지만 신뢰도 예측은 오직 하드웨어만을 대상으로 한다.
3) 물리적으로 분할된 어셈블리의 고장은 서로 독립하다.
4) 감시 및 자가진단 기능을 하는 어셈블리의 고장은 모듈의 필수기능에 영향을 미치지 않는다.
5) 자가진단 기능에 의하여 감시 가능한 어셈블리가 고장에서 복구되는 경우 복구되는 시간은 지수분포를 따른다.

표 1. 디지털 신호 처리 모듈 부품 목록

부 품	범 주	하위범주	수 량
DSP	Integrated Circuit	Microprocessor	1
PLD	Integrated Circuit	PAL, PLA	1
watchdog timer	Integrated Circuit	Linear	4
SRAM	Integrated Circuit	Memory	1
UVEPROM	Integrated Circuit	Memory	1
Bus interface controller	Integrated Circuit	VHSIC/VLSI CMOS	1
Transceiver (buffer)	Integrated Circuit	Logic, CGA or ASIC	7
Inverter	Integrated Circuit	Logic, CGA or ASIC	1
D filp-flop	Integrated Circuit	Logic, CGA or ASIC	2
AND gate	Integrated Circuit	Logic, CGA or ASIC	2
OSC 1,2	Miscellaneous	Quartz Crystal	2
dot-matrix	Semiconductor	Alphanumeric Display	1
LED (RED, GREEN)	Semiconductor	Detector, Isolator, Emitter, LED, Standard	2
Resistor(6종)	Resistor	RM	69
Capacitor	Capacitor	CDR	87
PCB edge connector	Connection	PCB edge	1

모듈의 신뢰도 예측에 앞서 모듈을 구성하는 부품에 대하여 목록을 보여주는 것이 <표 1>이다. 부품은 16종에 총 183개의 부품이 사용되고 있다. 모듈을 구성하는 3개의 어셈블리에 대하여 MIL-HDBK-217F의 부품-스트레스 방법을 적용하기 위한 환경 인자는 이 모듈이 항온, 항습이 유지되는 매우 양호한 환경에서 사용되므로 GB(Ground Benign), 대기 온도(Ambient Temperature)는 30℃로 설정하였다. 한편 모듈은 PCB 측면 커넥터, 시험용 커넥터, 칩 내부의 신호 분석용 커넥터, 스위치, IC 소켓, PCB 등의 부품도 포함한다. 그러나 PCB 측면 커넥터를 제외한 이들 기계적 부품류 및 구조물은 고장률이 매우 낮으므로 신뢰도 예측에서 제외하였다.

<표 2>는 MIL-HDBK-217F의 부품-스트레스 방법을 적용하여 부품의 고장률을 계산 할 때 사용되는 고장률 모형을 나타낸다.

표 2. 부품의 고장률 모형

부 품	고장률 계산식($1/10^6$시간)
Microcircuit	
-gate/logic arrays and microprocessor	$\lambda_P = (C_1\pi_T + C_2\pi_E)\pi_Q\pi_L$
-memories	$\lambda_P = (C_1\pi_T + C_2\pi_E + \lambda_{cyc})\pi_Q\pi_L$
-VHSIC/VHSIC-like and VLSI CMOS	$\lambda_P = \lambda_{BD}\pi_{MFG}\pi_T\pi_{CD} + \lambda_{BP}\pi_E\pi_Q\pi_{PT} + \lambda_{EOS}$
resistors	$\lambda_P = \lambda_b\pi_T\pi_P\pi_S\pi_Q\pi_E$
capacitors	$\lambda_P = \lambda_b\pi_T\pi_C\pi_V\pi_{SR}\pi_Q\pi_E$
quartz crystals	$\lambda_P = \lambda_b\pi_Q\pi_E$
general connectors	$\lambda_P = \lambda_b\pi_T\pi_K\pi_Q\pi_E$
optoelectronics, alphanumeric displays	$\lambda_P = \lambda_b\pi_T\pi_Q\pi_E$
optoelectronics, detectors, isolators, emitters	$\lambda_P = \lambda_b\pi_T\pi_Q\pi_E$

표 3. 부품의 고장률 모형의 인자값

어셈블리	부품	λb	πT	πQ	πE	C1	C2	기타 인자	수량
M (감시 및 자기진단 어셈블리)	watchdog timer	N/A	1.345191	1	0.5	0.06	0.003401	πL = 1	4
	inverter	N/A	0.415677	1	0.5	0.0025	0.006225	πL = 1	1
	D filp-flop	N/A	0.415677	1	0.5	0.0025	0.007190	πL = 1	2
	AND gate	N/A	0.415677	1	0.5	0.0025	0.006225	πL = 1	2
	quartz crystal1	0.033336	N/A	1	1	N/A	N/A	N/A	1
	resistor	0.0037	1.106443	1	1	N/A	N/A	πP = 0.76313, πS = 1.230610	10
	capacitor	0.002	1.556644	1	1	N/A	N/A	πC = 0.812831, πSR = 1, πV = 1.008827	4
B1 (감시 가능한 어셈블리)	DSP	N/A	0.259324	1	0.5	0.56	0.144541	πL = 1	1
	bus interface controller	N/A	0.23097	1	0.5	N/A	N/A	λBD = 0.24 λBP = 0.007343 λEOS = 0.065087 πCD = 24.989739 πL = 1 πPT = 2.2 πMFG = 0.55	1
	quartz crystal2	0.028849	N/A	1	1	N/A	N/A	N/A	1
	resistor	0.0037	1.106443	1	1	N/A	N/A	πP = 0.76313, πS = 1.230610	38
	capacitor	0.002	1.556644	1	1	N/A	N/A	πC = 0.812831, πSR = 1, πV = 1.008827	64
B2 (감시 불가능한 어셈블리)	PLD	N/A	0.425126	10	0.5	0.0034	0.130955	πL = 1	1
	SRAM	N/A	1.362173	10	0.5	0.062	0.021440	πL = 1	1
	UVEPROM	N/A	0.297813	10	0.5	0.0034	0.010235	πL = 1	1
	transceiver(buffer)	N/A	1.494212	1	0.5	0.0025	0.00915	πL = 1	7
	dot-matrix	0.00026	1.355235	5.5	1	N/A	N/A	N/A	1
	LED	0.00023	1.355235	5.5	1	N/A	N/A	N/A	2
	resistor	0.0037	1.106443	1	1	N/A	N/A	πP = 0.76313, πS = 1.230610	21
	capacitor	0.002	1.556644	1	1	N/A	N/A	πC = 0.812831, πSR = 1, πV = 1.008827	19
	PCB edge connector	0.04	1.193647	1	1	N/A	N/A	πK = 1	1

<표 3>은 모듈을 3개의 어셈블리로 분해하고 각 어셈블리에 속하는 부품들에 대하여 <표 2>의 고장률 모형을 적용할 때 사용될 적용 인자 값을 신뢰성 분석 소프트웨어 Relex를 이용하여 산출한 결과이다.

모듈의 신뢰도 예측을 위한 구성 어셈블리 사이의 작용은 다음과 같다. 감시 및 자가진단 기능을 하는 어셈블리(M)는 감시 가능한 어셈블리(B1)를 감시하고 진단하여 복구(재동작)시키지만 감시 불가능한 어셈블리(B2)의 고장에 대하여는 어떠한 역할도 하지 못한다. 또한 감시 가능한 어셈블리(B1)에 대해서도 고장이 발생했을 때 복구시키는 역할은 완전하지 못하다. 따라서 감시 가능한 어셈블리(B1)의 고장에 대하여 자가진단 기능에 의해 복구되는 비율 α를 고려하여 신뢰도 예측을 수행한다.

본 연구에서와 흡사하게 Kang *et al.*(2000)은 워치독 타이머(watchdog timer)가 사용되는 고장 내구성 시스템에 대하여 정적인 안전성을 평가하고 있다. 여기서 감시타이머 자체의 고장 확률, 감시타이머가 시스템의 필수기능이 고장을 일으켰을 때 고장을 감지할 확률, 감지한 고장을 복구할 확률을 고려하여 시스템을 분석하고 있다.

<표 2>와 <표 3>을 가지고 각 어셈블리에 대하여 MIL-

HDBK-217F의 절차에 따라 계산한 고장률은 <표 4>와 같다. 결과는 어셈블리 M은 작은 고장률을 가지며 10배 정도 고장률이 큰 어셈블리 B1에 대하여 감시와 이에 따른 복구 기능을 수행하고 있다. 한편 어셈블리 B1과 B2의 고장률을 비교해 보면 B2의 고장률이 4배 정도 크다. 그러나 이것은 하드웨어적 고장만을 고려한 것으로 실제로 어셈블리 B1은 소프트웨어 고장을 포함하여 큰 고장률을 가지고 있다.

마코프 모형화로 디지털 신호 처리 모듈의 신뢰도를 예측하기 위하여 시간에 따른 모듈의 상태를 (M의 상태, B1의 상태, B2의 상태)와 같이 나타내고 어셈블리의 상태 0은 정상, 1은 고장을 나타낸다고 하자. 그러면 모듈의 상태(0, 0, 0)은 모든 어셈블리가 정상인 경우이다. 상태(1, 0, 0)은 감시 및 자가진단 어셈블리만 고장인 경우로 모듈은 필수 기능을 수행하므로 모듈은 정상과 같다. 상태(1, 1, 0)은 감시 및 자가진단 어셈블리와 감시 가능한 어셈블리가 고장인 경우로 모듈은 진단되어 복구될 수 없으므로 계속적으로 필수 기능의 일부를 수행하지 못하므로 고장상태이다. 상태(0, 1, 1)은 감시 및 자가 진단 어셈블리만 작동하는 상태로 모듈은 필수기능을 수행하지 못하므로 고장이다. 상태(0, 1, 0)은 감시 가능한 어셈블리가 고장난 잠정적 고장상태로 감시 및 자가진단 어셈블리에 의하여 고장이 진단되고 복구되어 상태(0, 0, 0)으로 되거나 아니면 자가진단 어셈블리에 의하여 고장이 진단되지만 복구되지 못하는 상태(0, 1, 0)*으로 된다. 또한 추가적으로 다른 어셈블리가 고장을 일으켜 상태(0, 1, 1)이나 (1, 1, 0)으로 진행된다. 상태(0, 1, 0)에서 상태 (0, 0, 0)으로 복구되는 비율은 α이고 복구되지 못하고 상태 (0, 1, 0)*으로 진행되는 비율은 (1-α)이다. 상태(0, 0, 1)과 (1, 0, 1)은 감시 불가능한 어셈블리가 고장인 경우로 모듈은 고장이다.

따라서 모듈의 상태를 (0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 1, 0)*, (0, 0, 1), (1, 1, 0), (1, 0, 1), (0, 1, 1)의 순서로 했을 때 마코프 모형화를 위한 천이율행렬을 보여주는 것이 <그림 3>이다. 여기서 λ_M, λ_{B1}, λ_{B2}은 각각 M, B1, B2 어셈블리의 고장률이며 μ는 복구 발생률, α는 복구되는 비율을 나타낸다.

<그림 3>의 천이율행렬로 부터 Kolmogorov의 전방향 미분 방정식을 작성하면 다음과 같다.

$$p_{(0,0,0)}'(t) = -(\lambda_M+\lambda_{B1}+\lambda_{B2})p_{(0,0,0)}(t)+\alpha\mu p_{(0,1,0)}(t) \quad (1.a)$$
$$p_{(1,0,0)}'(t) = \lambda_M p_{(0,0,0)}(t)-(\lambda_{B1}+\lambda_{B2})p_{(1,0,0)}(t) \quad (1.b)$$
$$p_{(0,1,0)}'(t) = \lambda_{B1} p_{(0,0,0)}(t)-(\mu+\lambda_M+\lambda_{B2})p_{(0,1,0)}(t) \quad (1.c)$$
$$p_{(0,1,0)^*}'(t) = (1-\alpha)\mu p_{(0,1,0)}(t) \quad (1.d)$$
$$p_{(0,0,1)}'(t) = \lambda_{B2} p_{(0,0,0)}(t) \quad (1.e)$$
$$p_{(1,1,0)}'(t) = \lambda_{B1} p_{(1,0,0)}(t)+\lambda_M p_{(0,1,0)}(t) \quad (1.f)$$
$$p_{(1,0,1)}'(t) = \lambda_{B2} p_{(1,0,0)}(t) \quad (1.g)$$
$$p_{(0,1,1)}'(t) = \lambda_{B2} p_{(0,1,0)}(t) \quad (1.h)$$

한편 $p_{(0,0,0)}(0)=1$, $p_{(1,0,0)}(0)=0$, $p_{(0,1,0)}(0)=0$, $p_{(0,1,0)^*}(0)=0$, $p_{(0,0,1)}(0)=0$, $p_{(1,1,0)}(0)=0$,
$p_{(1,0,1)}(0)=0$, $p_{(0,1,1)}(0)=0$이라는 초기치를 이용하여 각

표 4. 부품 고장률과 모듈 고장률 계산 결과

어셈블리 기호	어셈블리 설명	기능블록	기능블록 고장률	어셈블리 고장률
B1	감시 가능한 어셈블리	디지털신호처리	0.38×10^{-6}	1.39×10^{-6}
		마스터제어	1.01×10^{-6}	
B2	감시 불가능한 어셈블리	Booting Logic	0.04×10^{-6}	4.73×10^{-6}
		UVEPROM	0.06×10^{-6}	
		제어신호처리, 디스플레이	0.83×10^{-6}	
		메모리제어	3.80×10^{-6}	
M	감시 및 자가진단 어셈블리	Clock & Reset	0.18×10^{-6}	0.18×10^{-6}

$$\begin{pmatrix} -(\lambda_M+\lambda_{B1}+\lambda_{B2}) & \lambda_M & \lambda_{B1} & 0 & \lambda_{B2} & 0 & 0 & 0 \\ 0 & -(\lambda_{B1}+\lambda_{B2}) & 0 & 0 & 0 & \lambda_{B1} & \lambda_{B2} & 0 \\ \alpha\mu & 0 & -(\mu+\lambda_M+\lambda_{B2}) & (1-\alpha)\mu & 0 & \lambda_M & 0 & \lambda_{B2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

그림 3. 천이율행렬

상태의 확률에 대한 라플라스 변환을 구하면 다음과 같다.

$$p_{(0,0,0)}(s)=\frac{s+\mu+\lambda_M+\lambda_{B2}}{(s+\lambda_M+\lambda_{B1}+\lambda_{B2})(s+\mu+\lambda_M+\lambda_{B2})-\alpha\mu\lambda_{B1}} \quad (2.a)$$

$$p_{(1,0,0)}(s)=\frac{\lambda_M}{s+\lambda_{B1}+\lambda_{B2}}p_{(0,0,0)}(s) \quad (2.b)$$

$$p_{(0,1,0)}(s)=\frac{\lambda_{B1}}{(s+\lambda_M+\lambda_{B1}+\lambda_{B2})(s+\mu+\lambda_M+\lambda_{B2})-\alpha\mu\lambda_{B1}} \quad (2.c)$$

$$p_{(0,1,0)^*}(s)=\frac{(1-\alpha)\mu}{s}p_{(0,1,0)}(s) \quad (2.d)$$

$$p_{(0,0,1)}(s)=\frac{\lambda_{B2}}{s}p_{(0,0,0)}(s) \quad (2.e)$$

$$p_{(1,1,0)}(s)=\frac{\lambda_{B1}}{s}p_{(1,0,0)}(s)+\frac{\lambda_M}{s}p_{(0,1,0)}(s) \quad (2.f)$$

$$p_{(1,0,1)}(s)=\frac{\lambda_{B2}}{s}p_{(1,0,0)}(s) \quad (2.g)$$

$$p_{(0,1,1)}(s)=\frac{\lambda_{B2}}{s}p_{(0,1,0)}(s) \quad (2.h)$$

만약 $(s+\lambda_M+\lambda_{B1}+\lambda_{B2})(s+\mu+\lambda_M+\lambda_{B2})-\alpha\mu\lambda_{B1}=0$의 해를 s_1, s_2로 $s_3=-\lambda_{B1}-\lambda_{B2}$로 나타내고 식 (2.a)~식 (2.h)를 역변환하면 다음과 같은 각 상태의 확률이 구해진다.

$$p_{(0,0,0)}(t)=\frac{s_1+\mu+\lambda_M+\lambda_{B2}}{s_1-s_2}e^{s_1t}+\frac{s_2+\mu+\lambda_M+\lambda_{B2}}{s_2-s_1}e^{s_2t} \quad (3.a)$$

$$p_{(1,0,0)}(t)=\frac{\lambda_M(s_1+\mu+\lambda_M+\lambda_{B2})}{(s_1-s_3)(s_1-s_2)}e^{s_1t} \quad (3.b)$$
$$+\frac{\lambda_M(s_2+\mu+\lambda_M+\lambda_{B2})}{(s_2-s_3)(s_2-s_1)}e^{s_2t}+\frac{\lambda_M(s_3+\mu+\lambda_M+\lambda_{B2})}{(s_3-s_1)(s_3-s_2)}e^{s_3t}$$

$$p_{(0,1,0)}(t)=\frac{\lambda_{B1}}{s_1-s_2}e^{s_1t}+\frac{\lambda_{B1}}{s_2-s_1}e^{s_2t} \quad (3.c)$$

$$p_{(0,1,0)^*}(t)=\frac{(1-\alpha)\mu\lambda_{B1}}{s_1(s_1-s_2)}e^{s_1t}+\frac{(1-\alpha)\mu\lambda_{B1}}{s_2(s_2-s_1)}e^{s_2t} \quad (3.d)$$
$$+\frac{(1-\alpha)\mu\lambda_{B1}}{s_1s_2}$$

$$p_{(0,0,1)}(t)=\frac{\lambda_{B2}(s_1+\mu+\lambda_M+\lambda_{B2})}{s_1(s_1-s_2)}e^{s_1t} \quad (3.e)$$
$$+\frac{\lambda_{B2}(s_2+\mu+\lambda_M+\lambda_{B2})}{s_2(s_2-s_1)}e^{s_2t}+\frac{\lambda_{B2}(\mu+\lambda_M+\lambda_{B2})}{s_1s_2}$$

$$p_{(1,1,0)}(t)=\frac{\lambda_M\lambda_{B1}(s_1+\mu+\lambda_M+\lambda_{B2})}{s_1(s_1-s_3)(s_1-s_2)}e^{s_1t} \quad (3.f)$$
$$+\frac{\lambda_M\lambda_{B1}(s_2+\mu+\lambda_M+\lambda_{B2})}{s_2(s_2-s_3)(s_2-s_1)}e^{s_2t}$$
$$+\frac{\lambda_M\lambda_{B1}(s_3+\mu+\lambda_M+\lambda_{B2})}{s_3(s_3-s_1)(s_3-s_2)}e^{s_3t}$$
$$-\frac{\lambda_M\lambda_{B1}(\mu+\lambda_M+\lambda_{B2})}{s_1s_2s_3}$$
$$+\frac{\lambda_M\lambda_{B1}}{s_1(s_1-s_2)}e^{s_1t}+\frac{\lambda_M\lambda_{B1}}{s_2(s_2-s_1)}e^{s_2t}+\frac{\lambda_M\lambda_{B1}}{s_1s_2}$$

$$p_{(1,0,1)}(t)=\frac{\lambda_M\lambda_{B2}(s_1+\mu+\lambda_M+\lambda_{B2})}{s_1(s_1-s_3)(s_1-s_2)}e^{s_1t} \quad (3.g)$$
$$+\frac{\lambda_M\lambda_{B2}(s_2+\mu+\lambda_M+\lambda_{B2})}{s_2(s_2-s_3)(s_2-s_1)}e^{s_2t}$$
$$+\frac{\lambda_M\lambda_{B2}(s_3+\mu+\lambda_M+\lambda_{B2})}{s_3(s_3-s_1)(s_3-s_2)}e^{s_3t}$$
$$-\frac{\lambda_M\lambda_{B2}(\mu+\lambda_M+\lambda_{B2})}{s_1s_2s_3}$$

$$p_{(0,1,1)}(t)=\frac{\lambda_{B1}\lambda_{B2}}{s_1(s_1-s_2)}e^{s_1t}+\frac{\lambda_{B1}\lambda_{B2}}{s_2(s_2-s_1)}e^{s_2t} \quad (3.h)$$
$$+\frac{\lambda_{B1}\lambda_{B2}}{s_1s_2}$$

흡수상태인(0, 1, 0)*, (0, 0, 1), (1, 1, 0), (1, 0, 1), (0, 1, 1)의 확률은 식 (3.d)~식 (3.h)이고 극한확률을 가지며 이는 각 식에서 지수함수를 제외한 항으로 주어진다. 모듈의 신뢰도는 모듈이 필수 기능을 수행할 수 있는 확률로 일시적 고장 상태(0, 1, 0)에서 자체적으로 빠른 속도로 상태(0, 0, 0)으로 복구되는 경우도 포함한다. 따라서 모듈의 신뢰도는 일시적 상태(0, 0, 0)나 (1, 0, 0)에 존재할 확률인 식 (3.a)와 식 (3.b)의 합으로 다음과 같이 정의한다.

$$R(t)=p_{(0,0,0)}(t)+p_{(1,0,0)}(t) \quad (4)$$
$$=\frac{\alpha\mu\lambda_{B1}}{(s_1-s_2)(s_1-s_3)}e^{s_1t}+\frac{\alpha\mu\lambda_{B1}}{(s_2-s_1)(s_2-s_3)}e^{s_2t}$$
$$+\frac{\lambda_M(s_3+\mu+\lambda_M+\lambda_{B2})}{(s_3-s_1)(s_3-s_2)}e^{s_3t}$$

특별하게 $\alpha=0$에 대하여는 식 (4)가 다음의 식 (5)와 같이 된다.

$$R(t)=e^{-\lambda_{B1}t}e^{-\lambda_{B2}t} \quad (5)$$

이것은 모듈은 B1 또는 B2 어셈블리가 고장을 일으키면 고장이 발생한다. 그러나 어셈블리 M은 고장에는 무관하므로 모듈은 필수기능을 하는 어셈블리로 B1과 B2의 2개로만 구성된 직렬구조로 간주된다. 이는 모듈의 신뢰성 구조상 가장 취약한 구조의 경우이다.

또한 $\alpha=1$이고 $\mu\gg\lambda_M$, $\mu\gg\lambda_{B1}$, $\mu\gg\lambda_{B2}$에 대하여는 식 (4)가 근사적 다음의 식 (6)과 같이 된다.

$$R(t)\approx\left(\frac{\lambda_{B1}}{\lambda_{B1}-\lambda_M}e^{-\lambda_Mt}+\frac{\lambda_M}{\lambda_M-\lambda_{B1}}e^{-\lambda_{B1}t}\right)e^{-\lambda_{B2}t} \quad (6)$$

이 경우는 어셈블리 B1의 고장은 거의 복구되어 고장을 일으키지 않는다고 간주되고 모듈의 고장은 어셈블리 B2가 고장을 일으키든지 아니면 어셈블리 M1이 고장난 후에 어셈블리 B1이나 B2가 고장을 일으켜 발생한다. 따라서 신뢰성 구조상 어셈블리 B1에 대하여 M이 대기구조로 주어지고 다시 이것과

직렬로 어셈블리 B2가 연결된 구조이다. 이는 모듈에 대하여 가장 이상적인 구조이다.

모듈의 신뢰도 예측치를 계산하기 위하여 <표 4>의 각 어셈블리의 고장률과 더불어 감시 가능한 어셈블리의 고장에 대한 복구발생률과 복구비율에 대하여 추정해야 한다. 감시 가능한 어셈블리에 대한 복구발생률은 μ=360,000/시간으로 추정되는데 이것은 감시 및 자가진단 어셈블리가 감시 가능한 어셈블리의 고장을 진단하고 복구시키는데 걸리는 평균시간이 약 1/100초 정도 걸리기 때문이다. 한편 자가진단 기능을 하는 어셈블리는 워치독 타이머와 주변 부품들로 이루어지며, 감시 가능한 어셈블리를 구성하는 부품들과 신호를 주고받으며 일정 시간 간격을 초과하여도 응답이 없을 시에 복구시도를 한다. Mahmood and Mccluskey(1988)에 의하면 워치독 타이머의 복구유효범위를 추정하기는 쉽지 않으나, 범위는 대략 60~70% 정도이며, Kim *et al.*(2006)에 의하면 CPU(중앙처리장치)의 고장에 대하여 워치독 타이머가 고장을 복구할 확률은 70% 이상이다. 따라서 본 논문의 자가진단 기능에 의해 복구되는 비율은 이와 비슷할 것으로 간주하여 70%로 추정한다.

따라서 <표 4>의 각 어셈블리의 고장률과 복구발생률 μ=360,000/시간, 복구비율 α = 0.7에 대하여 8가지의 모듈의 상태에서의 확률의 변화를 1,000,000시간까지 보여주는 것이 <그림 4>이다.

계산 결과에 의하면 주어진 5개의 흡수상태 중에서 (1, 1, 0)와 (0, 1, 1)은 모든 시간 구간에서 확률이 매우 작게 나타나고 있다. 상태(0, 1, 0)은 일시적 상태로 모든 시간 구간에서 확률은 거의 0으로 주어지는데 이는 감시 가능한 어셈블리가 고장나면 바로 매우 큰 복구 발생률로 복구 기능이 수행되어 복구된 상태(0, 0, 0)으로 돌아가든지 아니면 복구가 될 수 없는 흡수상태인(0, 1, 0)*로 가기 때문이다. 또한 흡수상태인(1, 1, 0)나 (0, 1, 1)로 갈수 있으나 이 가능성은 상당히 적다. 상태(1, 0, 0)도 일시적상태로 모든 시간 구간에서 확률이 매우 작은데 이는 흡수상태인(1, 1, 0) 이나 (1, 0, 1)로 진행되기 때문이다. 식 (4)로 주어지는 신뢰도는 <그림 4>에서 전 시간구간에서 $p_{(0,0,0)}(t)$ 보다 약간 크게 나타난다. 전자 회로기판의 수명은 보통 20년이므로 <그림 4>의 점선부분인 20년(175200시간)까지 매년 예측된 신뢰도는 다음 <표 5>와 같다.

표 5. 모듈의 예측된 신뢰도

년	예측된 신뢰도
1	0.956
2	0.914
3	0.873
4	0.835
5	0.798
6	0.763
7	0.729
8	0.697
9	0.666
10	0.637
11	0.609
12	0.582
13	0.556
14	0.531
15	0.508
16	0.485
17	0.464
18	0.443
19	0.424
20	0.405

이상과 같은 마코프 문제는 신뢰성 분석 소프트웨어인 Relex를 이용하면 계산을 손쉽게 할 수 있으며 이 후로의 계산

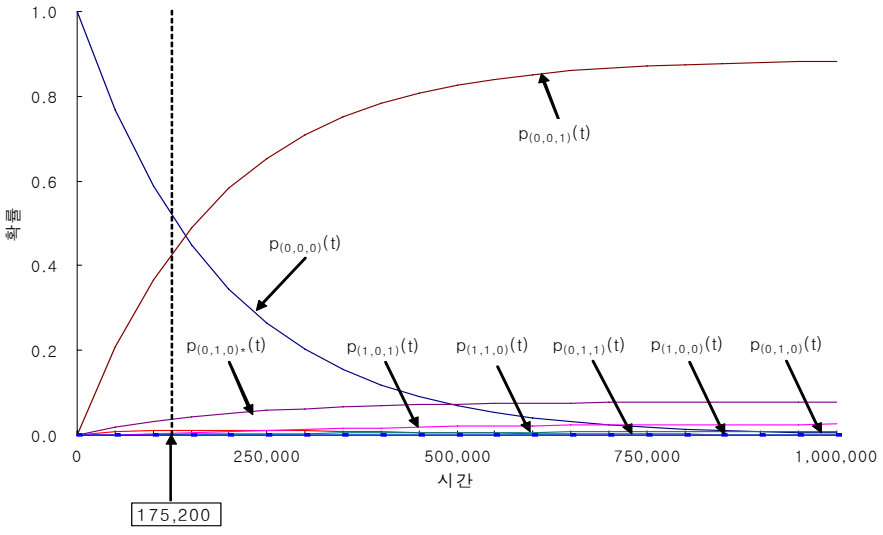

그림 4. 각 상태의 시간에 따른 확률변화

은 이 소프트웨어를 이용한다. Relex를 사용하여 마코프 문제를 풀기 위해서는 마코프 그래프 모형이 입력으로 필요한데 <그림 5>는 본 논문에서 다룬 문제에 대한 모형을 나타낸다.

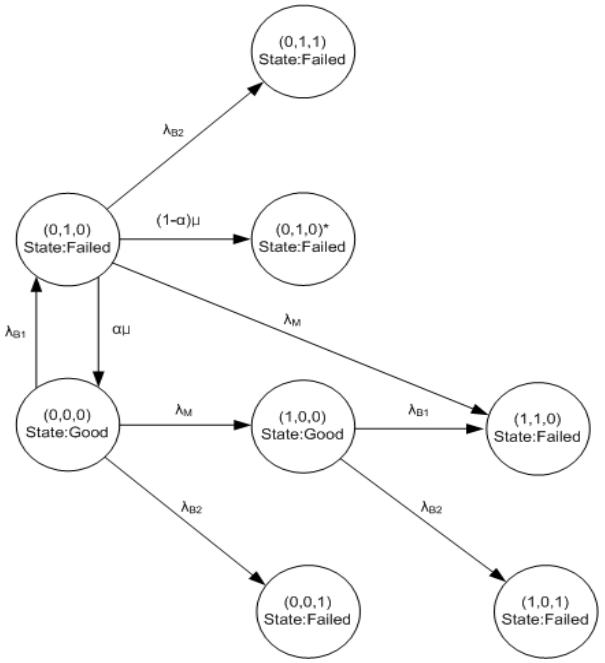

그림 5. 디지털 신호 처리 모듈의 상태변화에 대한 마코프 그래프

임무시간 20년까지의 시간에 대하여 예측된 신뢰도의 민감도에 대하여 살펴보자. <그림 6>은 복구발생률의 변화에 따른 예측 신뢰도의 변화를 보여준다. 이는 상당히 둔감하여 추정된 복구발생률 μ=360,000/시간의 $10^{-8} \sim 10^{8}$ 배의 변화에 대하여도 거의 변화를 보이지 않는다.

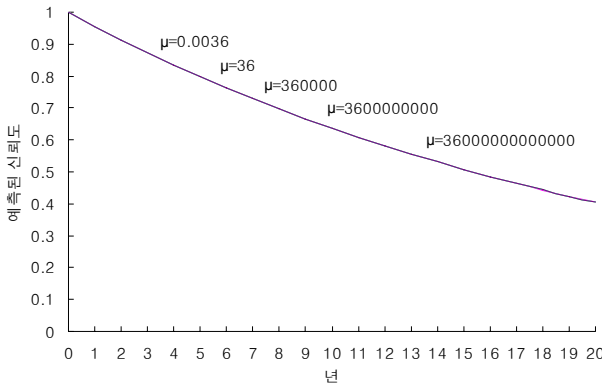

그림 6. 복구 발생률의 변화에 대한 예측된 신뢰도 그래프

한편 추정된 복구발생률 μ=360,000/시간에 대하여 감시 가능한 어셈블리가 복구되는 비율 $\alpha = 0$, $\alpha = 0.7$, 그리고 $\alpha = 1$일 때 임무시간 20년까지의 예측된 모듈의 신뢰도를 나타낸 것이 <그림 7>이다. 복구되는 비율의 증가에 따라 일정시점에서의 신뢰도가 증가하며, 시간이 경과함에 따라 복구되는 비율 $\alpha = 0$과 $\alpha = 1$에 대한 신뢰도 차이가 증가함을 알 수 있다. 특히 복구발생률 α의 의미는 매우 중요하다. 이미 앞에서 언급했듯이 $\alpha = 0$은 분석된 모듈의 구조상 가장 취약한 직렬구조를 나타내며 $\alpha = 1$일 때는 근사적으로 가장 이상적인 구조인 대기구조를 포함한 직렬구조를 나타낸다. 따라서 모듈의 예측된 신뢰도는 이 극단적인 값의 범위 내에 존재한다. 실제로 <그림 7>에서 추정된 $\alpha = 0.7$에서의 신뢰도가 두 곡선의 사이에 존재함을 볼 수 있다. 다음의 <표 6>은 $\alpha = 0$, $\alpha = 1$일 때 계산된 신뢰도와 이들이 <표 5>에 예측된 신뢰도를 기준으로 변화의 백분율을 보여준다. 예를 들면 <표 5>에서 20년의 추정된 신뢰도는 0.405인데 <표 6>의 $\alpha = 0$, $\alpha = 1$일 때 20년의 신뢰도가 각각 0.342와 0.435가 되어 -15.5%와 7.5%만큼 변화되고 있다. 즉 변화가 그리 크지 않음을 알 수 있다.

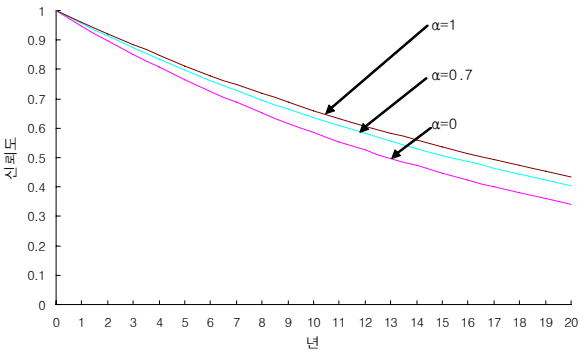

그림 7. 추정된 복구비율과 양 극단의 구조에 대하여 예측된 신뢰도 그래프

표 6. 예측된 신뢰도의 상하 변화 범위 백분율

년	α=0	α=1	하한%	상한%
1	0.948	0.959	-0.8	0.4
2	0.898	0.920	-1.7	0.7
3	0.581	0.883	-2.5	1.1
4	0.807	0.847	-3.3	1.5
5	0.765	0.813	-4.2	1.8
6	0.725	0.780	-5.0	2.2
7	0.687	0.748	-5.8	2.6
8	0.651	0.717	-6.6	2.9
9	0.617	0.688	-7.3	3.3
10	0.585	0.660	-8.1	3.7
11	0.554	0.633	-8.9	4.1
12	0.562	0.607	-9.6	4.4
13	0.498	0.583	-10.4	4.8
14	0.472	0.559	-11.1	5.2
15	0.447	0.536	-11.9	5.6
16	0.424	0.514	-12.6	5.9
17	0.402	0.493	-13.3	6.3
18	0.381	0.473	-14.0	6.7
19	0.361	0.454	-14.8	7.1
20	0.342	0.435	-15.5	7.5

한편 모듈을 구성하는 각 어셈블리의 고장률 예측치의 변화에 대하여 모듈의 예측된 신뢰도 변화를 살펴보자. 복구발생률 360,000/시간과 복구되는 비율 0.7에 대하여 <표 4>와 같이 예측된 각 어셈블리의 고장률을 0배와 10배 변화시켰을 때 <표 5>에 예측된 신뢰도를 기준으로 변화의 백분율을 나타내는 것이 <표 7>이다. 이를 살펴보면 어셈블리 B2가 가장 민감하게 나타났는데 이는 B2 어셈블리는 필수기능을 하는 어셈블리로서 이것의 고장은 직접 모듈의 고장으로 이어지기 때문이다. 또한 어셈블리 B1도 필수 기능을 담당하지만 어셈블리 M에 의하여 복구 가능한 부분이 존재하므로 상당히 둔감하게 나타나고 있다. 앞에서 B1은 소프트웨어의 고장을 포함하여 큰 고장률을 가질 수 있다고 언급하였는데 현재 <표 4>에서 추정된 고장률보다 10배 정도 증가하여도 임무시간 20년에서의 모듈의 신뢰도가 0.405에서 약 48.9% 감소하여 0.207로 된다. 어셈블리 M의 고장은 가장 둔감한데 이것은 감시 및 자가 진단 어셈블리는 절대적인 고장률도 낮을 뿐만 아니라 모듈의 필수기능이 아니기 때문이다.

표 7. 고장률의 변화에 대한 년도별 예측 신뢰도의 변화 백분율

년도	M		B1		B2	
	고장률 ×0	고장률 ×10	고장률 ×0	고장률 ×10	고장률 ×0	고장률 ×10
1	0.0	0.0	0.4	-3.2	4.2	-31.1
2	0.0	0.0	0.7	-6.4	8.6	-52.6
3	0.0	-0.1	1.1	-9.4	13.2	-67.3
4	0.0	-0.1	1.5	-12.4	18.0	-77.5
5	0.0	-0.1	1.9	-15.3	23.0	-84.5
6	0.0	-0.2	2.2	-18.1	28.2	-89.3
7	0.0	-0.3	2.6	-20.7	33.6	-92.6
8	0.0	-0.4	3.0	-23.4	39.3	-94.9
9	0.1	-0.5	3.4	-25.9	45.2	-96.5
10	0.1	-0.6	3.8	-28.3	61.3	-97.6
11	0.1	-0.7	4.2	-30.7	57.7	-98.3
12	0.1	-0.8	4.6	-33.0	64.4	-98.9
13	0.1	-0.9	5.0	-35.2	71.4	-99.2
14	0.1	-1.1	5.4	-37.4	78.6	-99.5
15	0.1	-1.2	5.8	-39.5	86.2	-99.6
16	0.2	-1.4	6.2	-41.5	94.1	-99.7
17	0.2	-1.5	6.6	-43.4	102.3	-99.8
18	0.2	-1.7	7.0	-45.3	110.8	-99.9
19	0.2	-1.9	7.4	-47.1	119.7	-99.9
20	0.3	-2.0	7.9	-48.9	129.0	-99.9

<그림 8>은 임무시간 20년에서 각 어셈블리의 고장률이 0배부터 10배까지 변화할 때 모듈의 신뢰도의 변화를 보여준다. 특히, 점선으로 표시된 1배에서의 신뢰도는 <표 4>의 예측된 각 어셈블리의 고장률에 대하여 모듈의 신뢰도를 나타낸다. 이 점선를 중심으로 B2의 고장률이 매우 민감하게 변화됨을 알 수 있다.

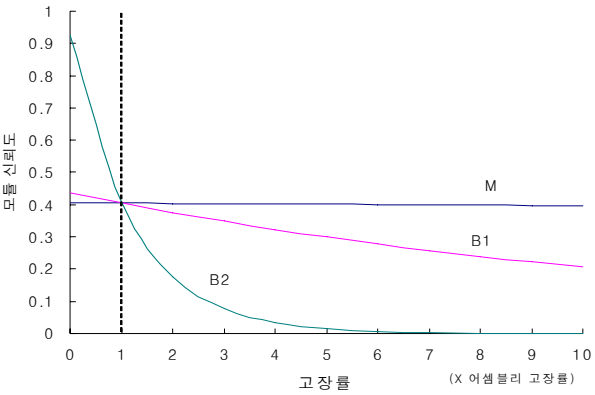

그림 8. 각 어셈블리의 고장률 변화에 따른 임무시간 20년에서의 모듈의 신뢰도 변화

일반적으로 아날로그 기기는 기기를 구성하고 있는 각 부품의 성능 저하에 의하여 고장이 발생하여 고장의 모드가 잘 알려져 있다. 또한 기기의 고장 징후 역시 기기의 성능 저하로 쉽게 알 수 있기 때문에 고장 발생시에 비교적 쉽게 고장 위치를 찾아서 보수 및 교체를 할 수가 있다. 그러나 원자력 발전소의 여러 계통에 사용되고 있는 아날로그 기기들의 고장이나 성능 저하는 부품 단종, 노후화 등의 이유로 더 이상 유지 보수하기가 어려워졌으며 디지털 기기로 대체를 추진하고 있다. <표 8>은 Son *et al.*(2006)에서 인용된 것으로 필드 데이터에 의하여 계산된 원자로 1차 증기라인 압력 신호를 처리하는 아날로그 시스템의 고장률과 신뢰도를 보여준다.

표 10. 1차 증기라인 압력 신호 처리를 위한 아날로그 시스템 신뢰도

구분	NLP2	NLP3	NMD1	NRC10	NAL3	시스템
고장률	1.65 E-06	1.58 E-06	2.91 E-06	3.06 E-06	3.33 E-06	1.253 E-05
신뢰도 (임무시간 20년)	0.749	0.758	0.601	0.585	0.558	0.111

이 아날로그 시스템은 5가지의 기기(NLP2, NLP3, NMD1, NRC10, NAL3)로 구성되어 본 논문에서 분석한 모듈과 유사한 기능을 수행하고 있다. 임무시간 20년을 기준으로 한 신뢰도는 0.111로 본 논문에서 예측된 모듈의 신뢰도 0.405(α = 0.7)에 비하여 상당히 낮음을 알 수 있다. 더욱이 α = 0일 때의 신뢰도 0.342보다도 낮다. 그러나 디지털 기기는 예측하지 못한 원인으로 급격한 고장을 일으킬 수도 있고 그 고장 징후 역시 미리 예측하기가 힘들다. 이러한 디지털 계측 제어 시스템이 가지는 불확실성 때문에 세계 각국의 안전 규제 기관의 견해가 신중하고 유보적인 입장을 견지하고 있지만 디지털 시스템에 고장 내구성 기능을 추가함으로 인해 시스템의 복잡도는 높아지더라도 그것은 자가 진단에 의한 신뢰도 향상의 장점을 상쇄할 만한 것은 아니며 고장 내구성 기법 중 가장 많이 사용되고 있는 감시 타이머를 이용하여 디지털 신호처리 모듈의 신

뢰도 향상을 기대할 수 있다.

4. 결 론

신뢰성 분석 및 평가는 현재 원자력 발전소의 안전과 경제적 운전에서 필수 불가결한 것으로 인식되고 있으며 특히, 디지털 기기의 도입이 확산되면서 다양한 신뢰도 분석방법이 요구되고 있고 적절한 분석 방법들이 연구되어지고 있다.

본 논문은 일체형 원자로의 보호계통에 사용되는 디지털 신호처리 모듈을 대상으로 신뢰도 예측을 수행함에 있어 디지털 기기가 가지는 감시 및 자가진단이라는 특징적인 신뢰도 향상 기법을 고려하였다. 모듈을 3개의 어셈블리로 구분하여 각각의 어셈블리에 대하여는 MIL-HDBK-217F를 적용하여 신뢰도를 예측한 후에 감시 및 자가진단이라는 신뢰도 향상 기법을 마코프 모형화를 통해 반영하여 최종적으로 모듈의 신뢰도를 예측하였다.

감시 및 자가진단이라는 신뢰도 향상 기법이 기기의 신뢰도 향상에 기여하는 정도를 정량적으로 계산함으로써, 추후 개발되는 디지털 기기의 하드웨어의 신뢰도 개선을 위한 방안을 제시하였으며 디지털 기기의 신뢰성 확보에 도움을 주며 나아가서 원자력 발전소 안전과 경제적 운전에 기여할 수 있을 것이다.

참고문헌

Bowles, J. B. (1992), A Survey of Reliability-Prediction Procedures for Microelectronic Devices, *IEEE Transaction on Reliability*, 41(1), 2-12.

Cassannel, G., Mura, G., Cesareti, F., Vanei, M., and Fantini, F. (2005), Reliability Prediction in Electronic Industrial Applications, *Microelectronics Reliability*, 45, 1321-1326.

Jones, J. and Hayes, J. (1999), A comparison of Electronic-Reliability prediction Models, *IEEE Transactions on Reliability*, 48(2), 127-134.

Jung, H. S., Sung, T. Y., Park, J. H., Lee, K. Y., and Park, C. K. (2000), A Survey of Methodologies for the Hardware Reliability Prediction of Electronic Equipment, *Proceedings of the Korean Nuclear Society*, 32.

Kang, H. G., Sung, T. Y., Lee, K. Y., and Park, C. K. (2000), Probabilistic Safety Assessment on the Fault-Tolerant Mechanism of Digital I&C Systems, *Proceedings of the Korean Nuclear Society*, 32.

Kim, S. J. *et al*. (2006), A method for evaluating fault coverage using simulated fault injection for digitalized systems in nuclear power plants, *Reliability Engineering and System Safety*, 91, 614-623.

Mahmood, A and McCluskey, E. J. (1988), Concurrent Error Detection Using Watchdog Processors : A survey, IEEE Trans. *On Computers*, 37(2).

MIL-HDBK-217F (1991), Reliability Prediction of Electronic Equipment, DoD, Washington DC.

MIL-HDBK-338B (1998), Electronic Reliability Design Handbook, DoD, Washington DC.

Relex 7 Visual Reliability Software (1999), Reference Manual, Relex Software Corporation.

So, D. S. and Kang, H. J. (1997), A Study on the Reliability Prediction using MIL-HDBK-217 and the Accelerated Life Testing of Electronic Component, *Journal of the Korean Institute of Plant Engineering*, 2(1), 17-33.

Son, C. H., Lee, S. Y., Kim, S. H., and Lee, P. J. (2006), Developement of Kori Unit 1 Environmental Qualification Review & Environmental Qualification Management Program, Technical Report. Control Technology Research Institute. SamChang Enterprise CO., LTD.

Wong K. L. (1995), A New Framework for Part Failure-Rate Prediction Models, *IEEE Transactions on Reliability*, 44(1), 139-146.

Yun, W. Y. and Yun, M. W. (1999), Reliability Evaluation for Reactor Protection Modules with MIL-HDBK-217 Method, *Proceedings of the Korean Nuclear Society*, 31.

이 상 용
울산대학교 산업정보경영공학부 박사과정 수료
현재: 삼창기업(주) 원자력사업본부 이사
관심분야: 신뢰성공학, 기기내환경 검증, 설비보전, 원전수명관리

공 명 복
서울대학교 공과대학 산업공학과 학사
한국과학기술원 산업공학과 석사
한국과학기술원 산업공학과 박사
미국 Rutgers 대학교 교환 교수
현재: 울산대학교 산업정보경영공학부 정교수
관심분야: 신뢰도 공학, 인간공학, 품질관리

정 재 현
부경대학교 공과대학 전자공학과 학사
현재: 삼창기업(주) 원자력사업본부 제어기술연구소 신뢰성연구팀
관심분야: 계측제어 시스템 신뢰성 분석, 설비 개선