신뢰성응용연구 신뢰성기술
제8권, 제2호. pp.101-111, 2008

FMEDA를 활용한 디지털 신호처리기 보드의 진단 유효범위의 측정

금종룡 · 서용석 · 이준구 · 박재윤

한국원자력연구원 계측제어 · 인간공학연구부

Measurement of a Diagnostic Coverage for a Digital Signal Processor Board Using an FMEDA

Jong-yong Keum · Yong-suk Suh · Jun-koo Lee · Je-yun Park

I&C · HFE Division, Korea Atomic Energy Research Institute

Abstract

Good diagnostics improves both the safety and system unavailability of digital safety systems. The measure of a diagnostic capability is called the Coverage Factor. Because the Failure Modes, Effects and Diagnostic Analysis (FMEDA) provides information on the failure rates and failure mode distributions necessary to calculate a diagnostic coverage factor for a component, the FMEDA can be used as a useful tool to calculate it. Through performing FMEDA on a digital signal processor (DSP) board used in a digital safety system, it is shown that some components of the DSP board can be replaced or improved to satisfy the required diagnostic coverage. That is, the FMEDA can serve as a useful verification tool to design a diagnostic capability for the DSP board.

Key Words : diagnostic coverage(진단 유효범위), digital signal processor(디지털 신호처리기), FMEDA(고장 모드, 영향 및 진단 분석), digital safety system(디지털 안전계통), failure mode distribution(고장모드 분포)

1. 서 론

아날로그 기기에 비해 데이터의 전송과 처리 능력이 뛰어나며, 보다 정확하고 신뢰성 있게 신호를 처리할 수 있다는 장점 때문에 디지털 기기들의 사용이 급속히 확산되어 기존의 아날로그

기기를 거의 완전히 대체하고 있다[1]. 또한 디지털 기기는 고장을 탐지하는 광범위한 온라인 진단능력을 제공한다.

디지털 시스템의 우수한 고장 진단능력은 시스템 불가용도(system unavailability)를 개선시키고, 더 나아가 이는 시스템 안전성(safety)을 개선시킨다. 이러한 사실은 고장 내구성 메커니즘(fault tolerant mechanism)의 진단 유효범위(Coverage Factor)에 따라 디지털 시스템의 시스템 불가용도가 수 배에서 수 백배까지 영향을 받는 것으로 확인된 분석 결과를 통해서 알 수 있다[2].

디지털 시스템의 불가용도(unavailability) 및 안전성 측면에서 진단 유효범위를 측정하고 평가하는 것은 중요하다. 고장 진단능력의 척도로써 진단 유효범위를 사용한다. 진단 유효범위는 고장이 발생했을 경우 그 고장이 탐지될 확률을 말한다.

진단 유효범위를 계산하는 과정의 토대는 제품에 대한 잠재적인 고장을 조사하는 방법으로 잘 알려진 FMEA(Failure Modes and Effects Analysis)이다. FMEA는 시스템 고장으로부터 위험도(risk)를 줄이는 근본적인 대책을 확립하는데 도움을 준다. 하지만 FMEA만으로는 진단 유효범위를 계산하는데 한계점을 가지고 있다. 즉 FMEA는 진단 유효범위를 구하는데 필요한 고장모드의 분포 데이터를 가지고 있지 않다. FMEDA는 FMEA의 확장으로 이러한 점을 보완하여 진단 유효범위를 계산해 내는 방법을 제공한다. 본 논문은 FMEDA(Failure Modes, Effects and Diagnostic Analysis)를 활용하여 진단 유효범위를 계산해 내는 방법을 제시한다.

2. FMEDA 개요

2.1 정의

FMEDA [3]는 서브시스템/제품 수준의 고장률, 고장모드 및 진단 유효범위를 생산해 내기 위하여 1988년 이후 개발 중인 체계적인 분석 기법을 기술하기 위하여 1994년에 붙여진 명칭이다(그림 1 참조). FMEDA 기법은 다음의 사항들을 고려한다.

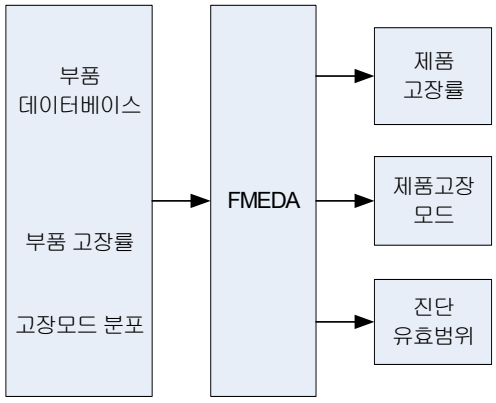
(1) 설계의 모든 부품
(2) 각 부품의 기능성
(3) 각 부품의 고장모드
(4) 제품 기능성에 대한 각 부품의 고장모드의 영향
(5) 고장을 탐지하는 자동진단의 능력

IEC 61508 Part 4 [4]는 위험성 고장(dangerous failure)을 안전-관련 시스템을 고장 상태로 가져갈 잠재성을 가진 고장으로 정의한다. 또한 이 표준은 안전성 고장(safe

failure)을 시스템을 고장 상태로 가져갈 잠재성을 가지고 있지 않는 고장으로 정의한다. 위험성 고장은 온라인 진단에 의해 탐지할 수 있느냐 없느냐에 따라 위험성 탐지 가능 고장(dangerous detected failure) 또는 위험성 탐지 불능 고장(dangerous undetected failure)으로 분류한다. 마찬가지로 안전성 고장(safe failure)은 온라인 진단에 의해 탐지할 수 있느냐 없느냐에 따라 안전성 탐지 가능 고장(safe detected failure) 또는 안전성 탐지 불능 고장(safe undetected failure)으로 분류한다.

대부분의 부품들은 다양한 고장모드를 가지고 있으며, 이들 고장 모드는 그것들이 특정 설계에서 어떻게 사용되느냐에 따라 그 중요성이 결정된다. 어떤 부품이 안전기능의 일부이지만 안전기능에 영향을 미치지 않는 특별한 고장모드가 존재한다. 이러한 고장모드를 "영향 없음(No Effect)" 고장모드라고 부른다. 어떤 부품들은 디지털 안전계통의 기능을 제공하는 회로의 일부가 아닌 인간연계표시 및 보조 기능을 지원하는 것이 그 부품의 목적일 수 있다. 그러한 부품들은 원하는 안전기능 구현하는 부분이 아니기 때문에 이러한 부류의 부품들은 "일부가 아님(Not a Part)"라고 부른다.

FMEDA는 잘 입증된 FMEA의 확장이다. FMEDA는 FMEA 분석 과정에 두 가지 부가적인 정보를 추가한다. 첫번째 정보는 분석되는 모든 부품들에 대한 정량적인 데이터(고장률 및 고장모드의 분포)를 제공한다. 두번째 정보는 시스템 (또는 서브시스템)이 온라인 자동 진단에 의해 내부 고장을 탐지해 내는 능력이다. FMEDA는 안전성 모델에서 안전성 탐지 가능 고장, 안전성 탐지 불능 고장, 위험성 탐지 가능 고장, 위험성 탐지 불능 고장에 대한 각각의 고장률을 생성하는데 추천되는 기법의 하나이다[5].



<그림 1> FMEDA의 입력 및 출력

2.2 FMEDA의 제한 사항

FMEDFA는 효율적이기는 하나 제한사항을 가지고 있다. FMEDA는 부품의 고장 모드가

잘 알려져 있을 경우에만 진단을 가능하게 한다. 광범위한 정보가 데이터베이스에 존재한다고 해도 새로운 전자 부품은 모든 고장모드가 잘 알려져 있지 않을 수도 있다. 이러한 부품들은 고장모드에 “unknown″를 표기하고, 고장률을 할당함으로써 FMEDA를 수행할 수 있다.

앞서 언급했지만 FMEDA는 부품의 모든 고장모드를 잘 알고 있는 것을 전제로 한다. 고장모드가 잘 알려지지 않은 부품의 경우, 부품 제조업자로부터의 수명시험 데이터(life test data) 또는 고장모드 핸드북을 기반으로 하여 고장모드에 대한 추정치를 생산해 낼 수 있다. 안전 관련 기능을 가진 이런 부품의 경우 좀 더 철저한 분석이 요구된다. 이런 잘 알려지지 않은 부품은 고장주입기법(fault injection techniques)[6,7]을 사용해 진단 유효범위를 제공할 수 있다. 고장주입기법의 분석 결과를 FMEDA에 편입시켜 사용한다.

3. 유효범위의 측정

3.1 분석 수준

디지털 기술의 급격한 발전에 따른 초미세 기술(submicron technology)의 사용은 결과적으로 많은 새로운 형태의 결함(fault) 및 고장모드를 초래하였다 [8]. 디지털 신호 처리기를 구성하는 게이트와 트랜지스터의 수는 수백만 개에서 수 천만 개에 달하기 때문에 이들 수준에서의 FMEA는 거의 불가능하다. 따라서 디지털 처리기의 FMEA 분석 수준은 부품 수준으로 정하였다. 표 1은 디지털 신호 처리기를 구성하는 부품들을 나타낸다.

<표 1> 디지털 신호 처리기의 부품 리스트

Components	Qty	Category	Subcategory
TMS320C40GFL60	1	Integrated Circuit	Microprocessor
EPM7128STC-100-15	1	Integrated Circuit	PAL, PLA
SCV64(CA91C078A-33-EG)	1	Integrated Circuit	VHSIC/VLSI CMOS
DS1232N	1	Integrated Circuit	Linear
74F04	1	Integrated Circuit	Logic, CGA or ASIC
74F08	2	Integrated Circuit	Logic, CGA or ASIC
74F245D	7	Integrated Circuit	Logic, CGA or ASIC
74F175	2	Integrated Circuit	Logic, CGA or ASIC
K6R4016C1D-TC10	4	Integrated Circuit	Memory
M27C256B-12F1	1	Integrated Circuit	Memory
KX0-110 (60Mhz)	1	Miscellaneous	Quartz Crystal
DC015 (32Mhz)	1	Miscellaneous	Quartz Crystal

Components	Qty	Category	Subcategory
0.1UF	87	Capacitor	Chip, Ceramic (CDR)
10K	47	Resistor	Film(RL, RLR, RN, RNR, RM)
330	2	Resistor	Film(RL, RLR, RN, RNR, RM)
120	1	Resistor	Film(RL, RLR, RN, RNR, RM)
4.7K	16	Resistor	Film(RL, RLR, RN, RNR, RM)
180	1	Resistor	Film(RL, RLR, RN, RNR, RM)
22K	2	Resistor	Film(RL, RLR, RN, RNR, RM)
LED(R)	1	Semiconductor	Detector, Isolator, Emitter
LED(G)	1	Semiconductor	Detector, Isolator, Emitter

3.2 FMEDA 수행

표 2에서 1칼럼에서 3칼럼까지는 FMEA와 동일하다. 4칼럼의 고장률은 부품의 특정 고장모드의 고장률을 나타낸다. 4칼럼의 고장률은 부품의 고장률에 고장모드 비율(failure mode ratio)과 부품 개수를 곱한 값을 나타낸다. 표 2의 디지털 신호 처리기 보드의 FMEDA 결과에 표 1의 모든 부품에 대한 FMEDA 결과가 표 2에 나타나지 않았다. 비슷한 부품에 대한 FMEDA 결과는 생략하였다. 7칼럼(SD : Safe Detected))과 8칼럼(SU : Safe Undetected)이 모두 공백인 이유는 FMEDA 결과 안전성 고장이 발견되지 않았기 때문이다.

3칼럼의 영향은 부품의 고장모드가 디지털 신호 처리기에 미치는 영향을 나타낸다. 'No Operating'은 디지털 신호 처리기의 출력이 없음을 의미한다. 'Wrong Operating'은 디지털 신호 처리기가 오동작을 해서 잘못된 신호가 출력됨을 의미한다. 'Operating Delay'는 디지털 신호 처리기의 동작이 지연됨을 의미한다. 'Potential Failure'는 디지털 신호 처리기가 잠재적인 고장을 초래할 수 있음을 의미한다.

표 2에서 5칼럼(탐지유무)부터 10칼럼(DU)은 진단능력 및 진단결과로부터 고장률 유형을 나타내기 위하여 추가되었다. 5번째 칼럼은 온라인 진단에 의해 부품 고장이 탐지될 수 있는지를 나타낸다. "1"은 부품의 고장모드가 탐지 가능하다는 것, "0"은 부품의 고장모드가 탐지 불가능하다는 것을 나타낸다. 6번째 칼럼(모드)은 고장모드를 나타내기 위하여 사용된다. "1"은 고장모드가 안전성 고장모드(safe failure mode)임을, "0"은 고장모드가 위험성 고장모드임(dangerous failure mode)을 나타낸다.

7번째 칼럼(SD)은 안전성 탐지가능 고장률(safe detected failure rate)을 나타낸다. 안전성 탐지가능 고장률은 고장률(4칼럼)에 탐지유무(제5칼럼)와 모드(제6칼럼)를 곱함으로써 구할 수 있다. 8번째 칼럼(SU)은 안전성 탐지불능 고장률(safe undetected failure rate)을 나타낸다. 안전성 탐지불능 고장률은 고장률(4칼럼)에 모드(제6칼럼)와 [1-탐지유무(제5칼럼)]을

곱함으로써 구할 수 있다. 9번째 칼럼(DD)은 위험성 탐지가능 고장률(dangerous detected failure rate)을 나타낸다. 위험성 탐지가능 고장률은 고장률(4칼럼)에 탐지유무(제5칼럼)와 [1-모드(제6칼럼)]을 곱함으로써 구할 수 있다. 10번째 칼럼(DU)은 위험성 탐지불능 고장률(dangerous undetected failure rate)을 나타낸다. 위험성 탐지불능 고장률은 고장률(4칼럼)에 [1-탐지유무(제5칼럼)]과 [1-모드(제6칼럼)]을 곱함으로써 구할 수 있다.

유효범위에 대한 기호는 C로 표기한다. 안전성 유효범위는 C^S로, 위험성 유효범위는 C^D로 표기한다. 디지털 신호 처리기에 대한 안전성 유효범위(C^S)는 안전성 탐지가능 고장률의 합을 안전성 고장률의 합으로 나눔으로써 구할 수 있다. 다음은 C^S에 대한 방정식을 나타낸다.

$$C^S = \frac{\sum_{i=1}^{n} \lambda_i^{SD}}{\sum_{i=1}^{n} \lambda_i^{SD} + \sum_{i=1}^{n} \lambda_i^{SU}}$$

λ_i^{SD} : 부품 i의 안전성 탐지가능 고장률

λ_i^{SU} : 부품 i의 안전성 탐지불능 고장률

마찬가지로 위험성 유효범위(C^D)를 구할 수 있다. 다음은 위험성 유효범위에 대한 방정식을 나타낸다.

$$C^D = \frac{\sum_{i=1}^{n} \lambda_i^{DD}}{\sum_{i=1}^{n} \lambda_i^{DD} + \sum_{i=1}^{n} \lambda_i^{DU}}$$

λ_i^{DD} : 부품 i의 위험성 탐지가능 고장률

λ_i^{DU} : 부품 i의 위험성 탐지불능 고장률

<표 2> 디지털 신호 처리기의 FMEDA

1 부품	2 고장모드	3 영향	4 고장률	5 탐지 유무 (detect ability)	6 모 드	7 SD	8 SU	9 DD	10 DU
TMS320C40GFL60	Input Open	No Operating	0.783	1	0			0.783	
	Output Open	Wrong Operating	0.783	0	0				0.783
	Supply Open	No Operating	0.261	1	0			0.261	
	Output Stuck Low	Wrong Operating	0.196	0	0				0.196
	Output Stuck High	Wrong Operating	0.174	0	0				0.174
EPM7128STC-100-15	Output Stuck High	Wrong Operating	0.187	0	0				0.187
	Output Stuck Low	Wrong Operating	0.187	0	0				0.187
	Input Open	No Operating	0.147	1	0			0.147	
	Output Open	Wrong Operating	0.147	0	0				0.147
SCV64(CA91C078A-33-EG)	Supply Open	Wrong Operating	0.484	0	0				0.484
	Output Open	Wrong Operating	0.134	0	0				0.134
	Input Open	No Operating	0.134	1	0			0.134	
	Supply Open	No Operating	0.084	1	0			0.084	
DS1232N	Improper Output	Wrong Operating	0.063	0	0				0.063
74F04	Output Stuck High	Wrong Operating	0.012	0	0				0.012
	Output Stuck Low	Wrong Operating	0.012	1	0				0.012
	Input Open	No Operating	0.009	0	0			0.009	
	Output Open	Wrong Operating	0.009	0	0				0.009
74F245D	Output Stuck High	Wrong Operating	0.127	0	0				0.127
	Output Stuck Low	Wrong Operating	0.127	0	0				0.127
	Input Open	No Operating	0.100	1	0			0.100	
	Output Open	Wrong Operating	0.100	1	0				0.100

1 부품	2 고장모드	3 영향	4 고장률	5 탐지 유무 (detect ability)	6 모 드	7 SD	8 SU	9 DD	10 DU
K6R4016C1 D-TC10	Data Bit Loss	Wrong Operating	1.294	1	0				1.294
	Short	Wrong Operating	0.990	1	0				0.990
	Open	No Operating	0.876	1	0			0.876	
	Slow Transfer of Data	Operating Delay	0.647	1	0			0.647	
M27C256B -12F1	Data Bit Loss	Wrong Operating	0.003	0	0				0.003
	Short	Wrong Operating	0.003	0	0				0.003
	Open	No Operating	0.002	1	0			0.002	
	Slow Transfer of Data	Operating Delay	0.002	1	0			0.002	
KX0-110 (60Mhz)	No Output	No Operating	0.027	1	0			0.027	
	Untunned Frequency	Wrong Operating	0.003	0	0				0.003
	Reduced Power	Potential Failure	0.003	1	0			0.003	
0.1UF	Short	No Operating	0.109	1	0			0.109	
	Change in Value	Wrong Operating	0.064	0	0				0.064
	Open	No Operating	0.049	0	0			0.049	
10K	Open	No Operating	0.107	0	0			0.107	
	Parameter Change	Wrong Operating	0.065	1	0				0.065
	Short	Wrong Operating	0.049	1	0				0.049

3.3 결과 분석

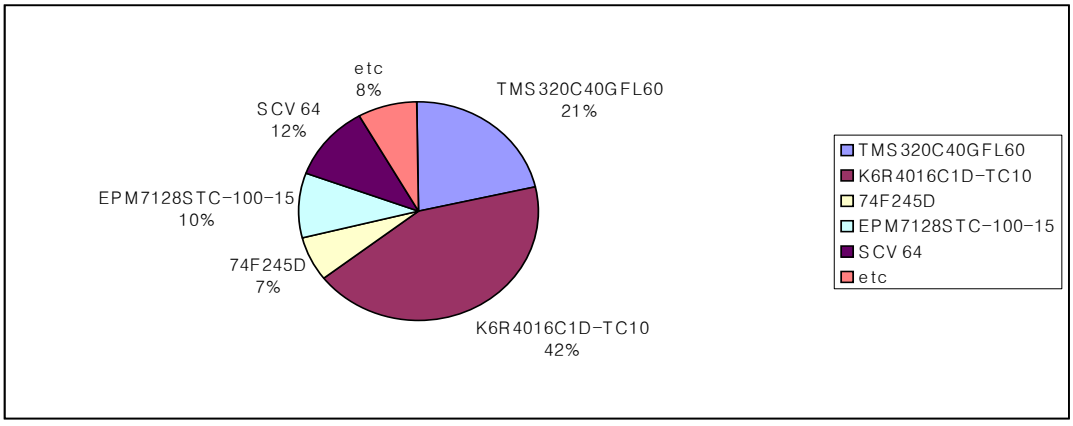
디지털 신호 처리기의 FMEDA 결과 안전성 고장모드와 안전성 고장 관련 부품은 발견되지 않았다. 부품 LED(R)과 부품 LED(G)는 “일부가 아님”에 해당하는 부품들이며, 안전기능 구현의 일부가 아니기 때문에 FMEDA 분석에 포함되지 않았다.

디지털 신호 처리기의 고장모드인 ‘No Operating′, ″Operating Delay′ 및 ’Potential Delay′는 위험성 탐지가능 고장모드로 분류하였으며, ‘Wrong Operating′은 위험성 탐지불능 고장모드로 분류하였다.

<표 3> 디지털 신호 처리기 고장모드별 분포

고장모드	고장률 $(10^{-6}/h)$	고장모드 분포
No Operating	2.83540005	32.05279 %
Wrong Operating	5.35548782	**60.54114 %**
Operating Delay	0.64892485	7.335774 %
Potential Failure	0.00621850	0.070297 %
합	8.84603122	100 %

FMEDA 결과는 디지털 신호 처리기의 고장모드는 위험성 탐지가능 고장모드의 분포가 39.46%, 위험성 탐지불능 고장모드의 분포가 60.54%로 나타났다. 위험성 진단 유효범위는 39.46으로 나타났다. 위험성 탐지불능 고장모드의 비율(그림 2 참조)은 K6R4016C1D-TC10 (RAM)이 42%, TMS320C40GFL60 (마이크로프로세서)이 21%, SCV64(CMOS)가 12%, EPM7128STC-100-15가 10%, 74F245D가 7%, 기타가 8%를 차지했다.



<그림 2> 각 부품이 차지하는 위험성 탐지불능 고장모드의 비율

또한 FMEDA는 고장주입 시험 케이스(test cases)를 선정할 때 지침으로 사용될 수 있다. 100%의 시험이 불가능할 경우, 가장 높은 고장률을 가진 부품에 시험의 우선순위가 주어질 수 있다. 왜냐하면, 대부분 이러한 부품들이 유효범위에 기여하기 때문이다.

4. 결 론

부품의 고장모드 및 고장모드 분포 정보는 유효범위를 계산하는데 필수적이다. 이들 정보를 기반으로 디지털 신호 처리기에 대한 FMEDA를 수행하여 위험성 진단 유효범위를 계산하였다. 위험성 탐지 불능 고장률에 가장 크게 기여하는 부품은 램이었으며, 그 다음으로 마이크로프로세서, CMOS 등이 그 뒤를 이었다. 위험성 유효범위의 값을 개선하기 위해서 이들 부품들에 대한 위험성 탐지불능 고장률을 줄이는 방법을 강구해야 할 것이다.

아키텍처에 관계없이 진단 유효범위는 안전성과 시스템 불가용도에 영향을 미치는 주요 변수 중의 하나이다. 디지털 신호 처리기 보드의 FMEDA를 통해 안전성 및 불가용도를 증진시키기 위한 디지털 신호 처리기의 설계는 높은 수준의 진단 유효범위를 달성하기 위해 최적화되어야 함을 알 수 있다. 완벽한 진단이 달성되기 어려울 경우, 우선순위가 잠재적인 위험성 고장에 주어질 수 있다. 제한된 범위 안에서 FMEDA는 유효범위를 분석할 수 있다. 이러한 분석은 고장주입시험을 통해 검증할 수 있다. 또한 FMEDA는 고장주입시험의 우선순위를 결정하는데 유용한 도구가 될 것이다.

참 고 문 헌

[1] 강현국, 성태용, 이기영, 디지털 안전계통에 대한 확률론적 안전성 평가의 주요인자 및 정량분석, 한국원자력학회, 춘계학술대회, 2001

[2] 한국원자력연구원, 디지털 계측제어 계통의 확률론적 안전성 평가를 위한 주요 인자 선정 및 민감도 분석, KAERI/TR-2026/2002, 2002

[3] John C. Grebe, William M. Goble, "FMEDA - Accurate Product Failure Metrics", exida, Sellersville, PA 18960 USA, February 2007

[4] CEI International Standard IEC 61508 Part 4, 1998-2000

[5] W.M. Goble, A.C. Brombacher, "Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems", Reliability Engineering and System Safety, Volume 66, Issue 3, April 1999, Pages 145-148

[6] A.C. Brombacher, I.W.R.J. van Beurden, "RIFIT: analyzing hardware and software in safeguarding systems", Reliability Engineering and System Safety, Volume 66,

Issue 3, February 1999, Pages 149-156

[7] Hsueh, Mei-Chen, Tsai, T.K., Iyer, R.K., Fault Injection Techniques and Tools, IEEE Computer 30 (4), 1997, Pages 75-82

[8] Riccardo Mariani, Gabriele Boschi, "A Systematic approach for Failure Modes and Effects Analysis of System-On-Chips", Proceeding of 13th IEEE International On-Line Testing Symposium IOLTS, 2007, Pisa, Italy