韓國精密工學會 2001年度 春季學術大會論文集 pp.570~573 KSPE 01S124

DES를 이용한 SIR의 주급수계통의 고장진단

박준효*, 김희표, 김철수(부산대 대학원 지능기계공학과), 이석(부산대 기계공학부)

Failure Diagnosis of Main Feedwater System for SIR using DES

J. H Park, H. P. Kim, C. S. Kim(Intelli. Mech. Eng. Dept., PNU), S. Lee(Mech. Eng. School., PNU)

ABSTRACT

Safety is very important to operate nuclear power plant. To have the safety, nuclear power plant should be run without trouble. This paper presents the application of a failure diagnosis approach based on discrete event system theory to the Main Feedwater System for Safe Integral Reactor.

Key Words Discrete Event Systems (이산사건시스템), Failure diagnosis (고장진단), Safe Integral Reactor (SIR), Main Feedwater System (주급수계통)

1. 서론

1979년 미국에서 발생한 TMI(Three Mile Island) 사고와 1986년 구 소련의 체르노빌 원전 사고는 원전의 안전성에 대한 일반인들의 의구심을 크게 확산시켰다 안전성에 대한 우려는 산업화에 따른 환경파괴를 우려하는 최근의 경향과 맞물려서 원자력 산업의 성장을 둔화시키는 가장 큰 원인이 되고 있다. 이는 또한 원자력 산업에 대한 안전요건들을 더욱 강화시켜서 원자력 발전 원가를 상승시키는 원인이 되기도 한다

이에 원자력의 이용에 있어서는 안전성의 확보를 위하여 고장이 발생하였을 때 빠른 시간내에 어떤 부분에서 문제가 생겼는지 알아내는 것이 중요하다. 실제로 발전소에서 고장이 발생하면 매전반의 수많은 알람 중에 어떤 것이 문제가 되었는지 알아내는 것은 작업자에게는 너무나 힘든 일이다. 이러한 점 때문에 여러 가지 고장기법들이 원전에 적용되었고 전문가 시스템이나 이와 비슷한 기법을 개발하여 사용중이다

전문가시스템은 가장 일반적으로 사용되고 있고, 복잡하고 미묘한 시스템에의 적용도 가능하다. 그러나 이 기법은 다음과 같은 단점이 있다. 일단 충분한 정보와 지식을 얻으려면 시간이 많이 들어간다는 점과 정당성을 입증하기가 매우 힘들다 [1]

이에 반해 본 논문에서는 최근에 각광을 받고 있는 Discrete Event Systems(DES)를 이용하여 고장진단 시스템을 구성하겠다. DES 접근법은 일반적으로 고장진단 할 대부분의 산업시스템이 DES로 생각될 수 있고 또한 시스템을 모델링하기가 비교적 쉽고 고장진단을 위한 보다 체계적인 방법을 제시하므로 고장진단을 위한 좋은 방법이 될 수 있다.

2. 고장진단기 구성방법

2.1 Automata and Formal Language

연속변수 시스템으로는 다양한 인공시스템들의 제어와 자동화에 있어서는 시스템의 동적인 특성 자체에 근본적으로 기존의 연속변수 시스템과는 다른 점이 있기 때문에 모델링이 어렵다 이에 "이산사건 시스템(Discrete Event Dynamic System), DES'이라는 시스템 부류가 부각되었다 DES의 모델링 및 분석 도구로는 두 가지 중 Petri net보다 모델링하기가 쉬운 Automata에 의한 DES의 방법을 사용하기로 하겠다.

2.1.1 Notation

Finite State Automaton(FSA)은 다음과 같은 4개의 구성요소를 가지고 있다

$$G=\{X,\ \Sigma,\ \delta,\ x_0\}$$

X는 state set, Σ는 event set, δ는 $\delta : X\times\Sigma^*\rightarrow X$ 인 transition function x_0는 초기 state 이다 Transition function δ에서 Σ^*은 null event ε을 포함하는 event의 string를 나타낸다. 이렇게 구성된 FSA가 생성해 내는 language를 $L(G)$로 나타낸다 Event set에서는 관측 가능한 것과(observable) 관측하지 못하는(unobservable) event가 있다 이 두 가지 event set은

$\Sigma = \Sigma_o \bigcup \Sigma_{uo}$로 나타내어진다. 진단되어져야 할 event set(failure event set)을 Σ_f이라 하고 본 논문에서 다루고자 하는 고장은 $\Sigma_f \subseteq \Sigma_{uo}$이라고 할 것이다 왜냐하면 관측가능한 것은 쉽게 진단이 가능하기 때문이다. 본 논문에서는 system이 다음과 같은 가정아래에서 고장진단이 이루어진다고 한다.

가정 1 : FSA G에 의해 형성된 L은 live이다 이것이 의미하는 바는 blocking state(dead state)가 없다는 말이다.

가정 2 : unobservable event로 이루어진 cycle은 G에는 존재하지 않는다

정의 1 : 다음의 조건이 만족되어질 때 prefix -closed이고 live language L은 projection P와 Σ_f의 partition Π_f에 대해 진단가능(diagnosable)하다고 한다 $(\forall i \in \Pi_f)(\exists n_i \in N)(\forall s \in \Psi(\Sigma_{fi}))(\forall t \in L/s)$

$(|t| \geq n_i \Rightarrow D)$,

여기에서 $\Psi(\Sigma_{fi}) = \{s \in L : s_f \in \Sigma_{fi}\}$이고 string s의 마지막 event를 s_f로 나타내며 L에 속하는 s의 postlanguage를 $L/s = \{t \in \Sigma^* \mid st \in L\}$, |t|는 string의 길이를 나타낸다. 끝으로 $P : \Sigma^* \rightarrow \Sigma_o^*$인 projection P를

$$P(\varepsilon) = \varepsilon$$
$$P(\sigma) = \begin{cases} \varepsilon & \text{if } \sigma \in \Sigma_{uo} \\ \sigma & \text{if } \sigma \in \Sigma_o \end{cases}$$
$$P(s\sigma) = P(s)P(\sigma), \forall s \in \Sigma^*, \forall \sigma \in \Sigma$$

과 같이 정의하고 $P_L^{-1}(y) = \{s \in L : P(s) = y\}$이다.

진단가능성 조건 (diagnosability condition) D는 다음과 같다 $(\forall \omega \in P_L^{-1}(P(st)))(\Sigma_{fi} \in \omega)$

2.2 Diagnoser(진단기)

failure label의 집합 $\Delta_f = \{F_1, F_2, \ldots, F_m\}$이라고 정의를 내리고 $|\Pi_f| = m$, 가능한 label들의 완전한 집합은 $\Delta = \{N\} \bigcup 2^{\Delta_f}$ 같이 표현되어질 수 있다. N은 정상상태를 나타내고 F_i는 failure의 type이라고 정의를 내린다

진단기를 FSA으로 표현하면 다음과 같이 나타내어진다 $G_d = (Q_d, \Sigma_o, \delta_d, q_0)$, 여기서 Q_d는 고장진단기의 state이고, q_0는 초기의 상태로서 집합의 원소의 형태로는 $\{(x_0, \{N\})\}$라고 나타낸다.

정리 1 : 진단기에 F_i-indeterminate cycle이 존재하지 않는다는 것은 진단기가 F_i-diagnosable하기 위한 필요충분조건이다

증명 : [1]의 Chapter 3의 Theorem 2 참조 ■

◎Diagnoser를 구성하는 순서는 다음과 같다.

1) 시스템의 각 부분을 FSA로 나타낸다.
2) FSA들을 합친다. (Synchronize)
3) 합쳐진 시스템의 모델을 [1]의 논문에서 Label Propagation Function Range Function Label Correction Function의 순서로 진행시킨다 그리고 순서대로 고장진단기를 구성하여 정리1를 적용시키면 구성한 진단기가 고장진단이 가능한지 알 수가 있다.[1]

3. SIR에서 전력공급계통의 고장진단기

3.1 Safe Integral Reactor

ABB-CE, AEA Technology등이 공동으로 개발중인 SIR(Safe Integral Reactor)는 320MWe의 일체형 원자로이다. SIR는 안전성을 높이고, 운전자의 조작을 쉽게 하며, 신뢰성을 높이고, 보수 및 유지를 쉽게 하고, 가능한 한 입증된 기술을 사용하여 개발비용을 줄이는 것을 설계 목표로 하고 있다.

3.1.1 SIR의 주급수계통

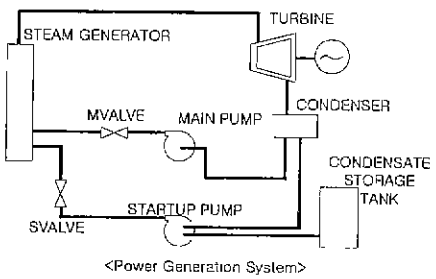

Fig. 1 Power generation system

주급수계통은 증기발생기(steam generator)에서 발생된 수증기를 터빈으로 우회하여 복수기(condenser)에서 응축된 후 다시 급수로 공급된다.

3.2 DES Modeling

3.2.1 Valve

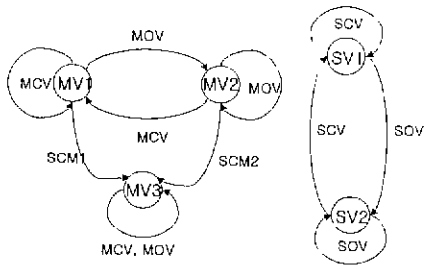

Fig 2 FSA of MVALVE and SVALVE

1) 2장의 모든 내용은 참고문헌 [1]를 참조

주급수계통에 관심이 있기 때문에 Main Pump와 관련이 있는 밸브에서 닫혀있는 경우를 심각하게 생각하여 MVAVLE에서만 고장이 있다고 가정하였다.

3.2.2 Pump

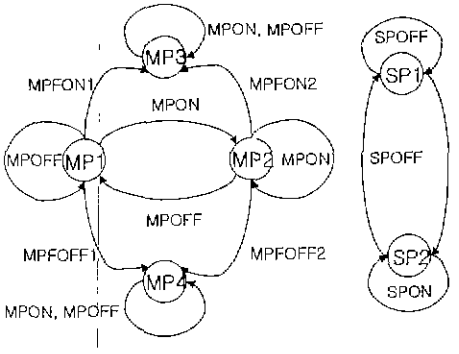

Fig 3 FSA of Main pump and Startup Pump

펌프에서도 역시 밸브와 마찬가지로 주급수계통에 초점을 맞춰 Main Pump만 고장이 있다고 하였다.

3.2.3 Condenser, Turbine and Controller

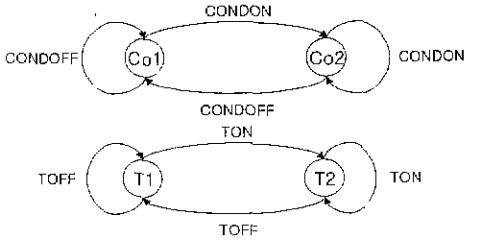

Fig. 4 FSA of Condenser and Turbine

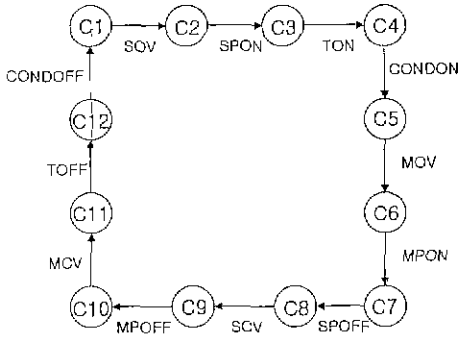

Fig 5 FSA of Controller

복수기와 터빈은 고장이 없다고 보고, controller (제어기)는 전체적인 작업 순서라고 보면 된다. SIR에 대한 자료가 거의 없기 때문에 [2]에 나와있는 그림들과 설명으로 구성하였다

3.2.4 Event List

이때까지의 모든 모델링에서 사건들의 표시와 의미는 아래의 표와 같다.

Table 1 Event List

MCV	MVALVE Close (c)(o)	SPOFF	Startup Pump Off (c)(o)
MOV	MVALVE Open (c)(o)	SPON	Startup Pump On (c)(o)
SCM1,2	Stuck Closed (uc)(uo)	CONDOFF	Condenser Off (c)(o)
SCV	SVALVE Close (c)(o)	CONDON	Condenser On (c)(o)
SOV	SVALVE Open (c)(o)	TON	Turbine Off (c)(o)
MPOFF	Main Pump Off (c)(o)	TOFF	Turbine On (c)(o)
MPON	Main Pump On (c)(o)		
MPFOFF1,2	Main Pump Failed Off (uc)(uo)		
MPFON1,2	Main Pump Failed On (uc)(uo)		

위의 표에서 (c)의 의미는 제어가능한 사건을 의미하며 (o)는 관측가능한 사건을 의미한다 (uc)(uo)는 반대의미의 사건이라는 뜻이다

3.3 Diagnoser

2.2 절에서 고장진단기를 구성하는 순서를 따르면, 첫 번째 부분은 앞의 3.2절에서 두 번째 절차부터 마지막까지는 미시건대학에서 개발한 UMDES-LIB를 사용하여 구현하였다

합성하여 구한 전체 상태(state)의 수는 72개이고, 아래의 전체적인 센서의 출력값을 나타낸 표 2를 사용하여 진단기를 구성하면 총 76개 상태의 수가 나타내어졌다.

표2의 센서값을 나타내는 순서대로 압력센서, 유량센서, 온도센서 총 3개의 센서를 사용하였다 온도센서는 MVALVE와 MPUMP의 사이에 있는 것이라고 가정하였다 LP는 Lower Pressure, NP는 Normal Pressure, UP는 Upper pressure, NF는 Non Flow, F는 Flow, NT는 No change Temperature, CT는 Changer Temperature.

구성한 진단기를 고장진단가능한 것인지 확인을 해보려면 진단기내에 F_i-indeterminate cycle이 존재하지 않아야 한다. UMDES-LIB를 사용하면 그러한 사이클이 존재하지 않는 것을 알 수가 있다. 따라서 본 논문에서 구성한 시스템에서의 진단기는 고장진

단가능하다.

Table 2 Global Sensor Map

State	Sensor Value
MV1 MP1	LP,NF,NT
MV1 MP3	UP,NF,NT
MV1,MP4	LP,NF,NT
MV2,MP1	LP,NF,CT
MV2,MP2	NP,F,CT
MV2,MP3	NP,F,CT
MV2,MP4	LP,NF,CT
MV3,MP1	LP,NF,NT
MV3,MP2	UP,NF,NT
MV3,MP3	UP,NF,NT
MV3,MP4	LP,NF,NT

지면관계상 모든 진단기의 내용을 보여줄 수가 없기에 그림 6에 부분만 나타내었다.

그림 6은 왼쪽 사이클이 정상상태로 움직일 때의 여러 가지 고장가능성을 가진 채 움직이고 있는 것을 보여주며 오른쪽의 사이클은 밸브가 계속 닫혀있는 경우의 사이클을 보여준다.

이 사이클은 F_t-indeterminate cycle이 존재하지 않는다 N은 정상상태를 나타내며 나머지 고장의 기호는 다음의 표와 같다.

Table 3 Fault Type

scm1,2	F1
mpfon1,2	F2
mpfoff1,2	F3

4. 결론

본 논문에서는 주급수계통의 펌프-밸브에 중점을 두어 DES접근법으로 고장진단기를 구성하였다.

이 방법(Event based)은 [3]과 [4]의 방법보다 진단기의 상태의 수가 많은데 [3],[4]의 방법으로 하려면 상태의 수가 많아지는 경우 해석해 낼 프로그램이 없어 아직 시도를 하지 못하고 있다 따라서 프로그램의 개발이 필요하다

추후연구과제로 센서의 개수를 정의하는데 있어서 아직까지 이렇다할 방법이 없기 때문에 센서의 최적화 기법이 있다.

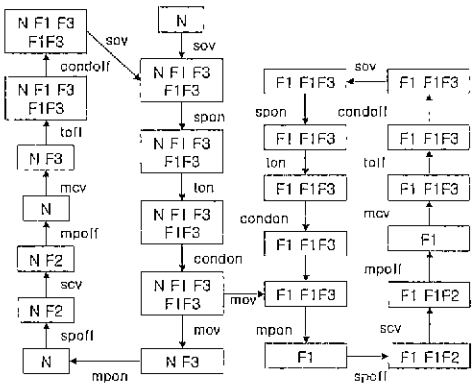

Fig. 6 Part of Dignoser

참고문헌

1 Meera Sampath, "A Discrete Event Systems Approach to Failure Diagnosis" Ph D Thesis. The University of Michigan. December, 1995.

2 배윤영 외, "신형원자로 기술개발 신형원자로 계통개념연구, 최종보고서" 한국원자력연구소, 과학기술처 1997 7.

3. Shahin Hashtrudi Zad, "Fault Diagnosis in Discrete Event and Hybrid Systems", Ph.D. Thesis, The University of Toronto. 1999.

4. 손형일, 김가웅, 이석, "이산사건 시스템의 Failure Diagnosis", 제어계측, 로보틱스 및 자동화 연구회 합동 학술 발표회 논문집, pp.298- 303, 2000.