

DES를 이용한 가압경수로의 비상노심냉각계통 고장진단

김희표*, 박준효, 김칠수(부산대 대학원 지능기계공학과), 이석(부산대 기계공학과)

Failure Diagnosis of PWR-ECCS using Discrete Event System

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

ABSTRACT

As many industrial systems become more complex, they become extremely difficult to diagnose the cause of failures. The subject of this paper is ECCS(Emergency Core Cooling System) part of PWR (Pressurized Water Reactor). This paper presents modeling and diagnoser construction of ECCS based on discrete event system theory. Also, this paper presents that the ECCS system is diagnosable in our approach.

Key Words · Discrete Event System, PWR-ECCS, Failure Diagnosis

1. 서론

산업시스템의 고장진단은 지난 몇십년 동안 많은 관심을 받아온 연구분야였다. 특히 반도체 생산시스템, 화학공정 시스템, HVAC(Heating Ventilation and Air Conditioning) 시스템, 발전소 등과 같이 대규모이고 복잡한 시스템의 고장진단을 위한 보다 조직적이고 체계적인 방법이 필요하게 되었다. 그래서 fault tree, analytical redundancy, expert system, model-based reasoning, Discrete Event System(DES) 등을 이용한 많은 접근론들이 연구되고 있다. 이런 접근론들에는 각각 다음과 같은 제약이 있다. 먼저 fault tree는 기본적으로 그것을 구성하기가 지나치게 어려워서 실질적인 사례에 적용하기가 쉽지 않다. 그리고 analytical redundancy는 계산복잡도가 크고, 모델링 오차와 계측 노이즈로 인한 민감도(sensitivity)문제를 야기시킬 수 있다. 전문가 시스템은 전문가의 지식을 추출하는 것이 어려워 개발기간이 길어질 수 있는 단점이 있다. 마지막으로 model-based reasoning은 많은 연구가 이루어지고 있지만 아직까지 동적시스템에 대한 적용이 어렵다는 단점이 있다. 그렇지만 DES 접근법은 일반적으로 고장진단 할 대부분의 산업시스템이 DES로 생각될 수 있어 시스템을 모델링하기가 비교적 쉽고 고장진단을 위한 보다 체계적인 방법을 제시하므로 고장진단을 위한 좋은 방법이 될 수

있다.

본 논문에서는 복잡한 가압경수로 시스템 중 하나인 비상노심냉각계통을 DES 접근법을 이용하여 모델링하고 고장 진단기를 구성하는 방법을 제시한다. 가압경수로의 안전계통중 하나인 비상노심냉각계통의 고장진단은 실제적으로 대형사고를 막아주는 중요한 부분을 차지할 것이다.

2 Background

2.1 Notation^[2]

Finite State Automaton(FSA)를

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

X 는 state set, Σ 는 event set, δ 는 $\delta : X \times \Sigma^* \rightarrow X$ 인 transition function, x_0 는 초기 state이다. Transition function δ 에서 Σ^* 는 null event ϵ 를 포함하는 event의 sequence(string)를 나타낸다. 이렇게 구성된 FSA가 생성해내는 language를 $L(G)$ 로 나타낸다.

$$s \in L(G) \Leftrightarrow s \in \Sigma^*, \delta(x_0, s)!$$

여기서 $\delta(x_0, s)!$ 는 x_0 에서 string s 가 일어난 다음의 state가 정의됨을 나타낸다. $\overline{L(G)}$, $L_m(G)$ 는 $L(G)$ 의 prefix closure, marked language를 의미한다. 그리고 $G_1 \times G_2$, $G_1 \wedge G_2$ 은 각각 FSA G_1, G_2 의 synchronous

product, meet product를 나타낸다

2.2 Diagnoser^[1]

Event set에서는 관측 가능한 것(observable) 관측하지 못하는(unobservable) event가 있다. 이 두 가지 event set은 다음과 같이 나타내어진다.

$$\Sigma = \Sigma_o \cup \Sigma_{uo}$$

진단되어야 할 event set(failure event set)을 Σ_f 이리 하고 본 논문에서 다루고자 하는 고장은 $\Sigma_f \subseteq \Sigma_{uo}$ 이라고 할 것이다. 왜냐하면 관측가능한 것은 쉽게 진단이 가능하기 때문이다.

failure label의 집합 $\Delta_f = \{F_1, F_2, \dots, F_m\}$ 이라고 정의를 내리고 $|\Pi_f| = m$. 가능한 label들의 완전한 집합은 다음과 같이 표현되어질 수 있다.

$\Delta = \{N\} \cup 2^{\Delta_f}$ 여기서 N은 정상상태를 나타내고 F_i 는 failure의 type이라고 정의를 내린다.

$Q_d = 2^{X_d \times \Delta_d}$ 라고 정의를 내리고 G에 대한 diagnoser를 FSA으로 표현하면 다음과 같이 나타내어진다.

$G_d = (Q_d, \Sigma_o, \delta_d, q_0)$ 여기서 Q_d 는 diagnoser의 state 이고 q_0 는 초기의 상태로 $\{(x_0, \{N\})\}$ 라고 나타낸다 또한 $Q_d \subseteq Q_o$ 이므로 G_d 의 q_d 는 $x_i \in X_o, i_i \in \Delta$ 인 $q_d = \{(x_1, i_1), \dots, (x_n, i_n)\}$ 라고 나타낸다

진단가능성(Diagnosability)의 정의를 정의 1에 나타내었고, diagnoser가 진단가능(diagnosable)하기 위한 필요충분조건을 정리 1에 나타내었다.

정의 1 : 다음의 조건이 만족되어질 때 prefix-closed 이고 live language L은 projection P와 Σ_f 의 partition Π_f 에 대해 진단가능(diagnosable)하다고 한다.

$$(\forall i \in \Pi_f)(\exists n_i \in N)(\forall s \in \Phi(\Sigma_f^*))(\forall t \in L/s) \\ (||t|| \geq n_i \Rightarrow D)$$

여기서 진단가능성 조건 (diagnosability condition) D는 아래와 같다

$$(\forall \omega \in P^{-1}(P(st))(\Sigma_f \in \omega))$$

정리 1 : Diagnoser에 F_i -indeterminate cycle이 존재하지 않는다는 것은 diagnoser가 F_i -diagnosable하기 위한 필요충분조건이다.

diagnoser를 구성하는 방법은 다음과 같이 요약될 수 있다 우선 시스템의 각 요소를 FSM으로 나타낸 다음 각각의 요소를 하나의 FSM으로 합치고(synchronous

product), 마지막으로 Label Propagation Function, Range Function, Label Correction Function^[11]을 차례로 적용시켜 diagnoser를 구성한다.

2.3 비상노심냉각계통(ECCS) 개요^[12]

비상노심냉각계통(Emergency Core Cooling System; ECCS)은 냉각제 상실사고(LOCA)가 발생할 때 노심에 비상 냉각수를 공급하여 핵연료봉을 안전하게 냉각시키기 위한 계통으로서, 원자력 발전소의 대표적인 안전계통이다. 비상노심냉각계통은 크게 주입 모드(Injection Mode)와 재순환 모드(Recirculation Mode)로 구성된다. 냉각제 상실사고의 발생시 비상노심냉각계통의 고장은 대형사고를 가져올 것이다. 이러한 이유로 본논문에서는 비상노심냉각계통을 고장진단 대상으로 선정하였고, 그 중에서도 주 부분을 차지하는 주입모드에 대한 고장 진단을 제시한다.

3. 비상노심냉각계통(ECCS)

3.1 시스템 구성

비상노심냉각계통 주입모드의 시스템과 그것의 구성 요소를 그림1과 표1에서 나타내었다.

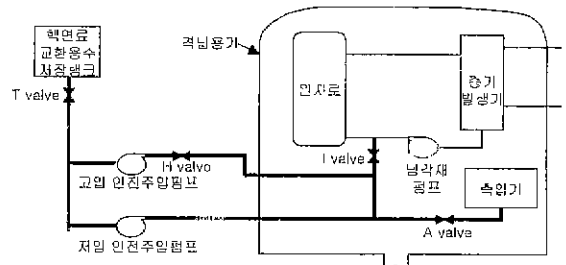


Fig.1 ECCS Injection Mode

3.2 DES Modeling

위의 비상노심냉각계통의 주입모드의 시스템은 펌프 2개(HP, LP)와 VALVE 4개(I-V, A-V, H-V, T-V) 그리고 Table 1 System Component

H-P	고압 안전주입펌프
L-P	저압 안전주입펌프
I-V	안전주입계통과 원자로 냉각제 계통을 격리하고 있는 밸브
A-V	축압기에 있는 밸브
H-V	고압 안전주입에 있는 밸브
T-V	핵연료 교환용수 저장탱크에 연결된 밸브
ACC	축압기(Accumulator)

축압기(ACC)로 구성되어 있다. 그리고 계측센서로는 고장이 발생시 가장 치명적인 부분이 될 수 있는 I-V와 TV 두 개의 밸브에 설치된 유량센서(flowmeter)가 사용된다고 가정하자. 각각의 flowmeter의 값은 noflow를 나타내는 NF와 flow를 나타내는 F 두개가 있다고 하자. 따라서 sensor output set $Y_1 = \{NF1-V, FI-V\}$,

$Y_2 = \{NFT-V, FT-V\}$ 이다. 시스템에서 펌프는 고장이 발생하지 않고, 두 개의 밸브(IV, TV)에서만 고장이 일어난다고 가정한다. 그리고 밸브에서 중요하게 여겨져야 할 Stuck_closed의 고장이 일어난다고 가정한다.

밸브와 펌프 그리고 축압기에 대한 FSA는 다음 그림과 같다

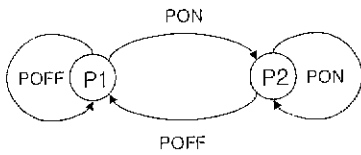


Fig. 2 FSA of H-Pump, L-Pump

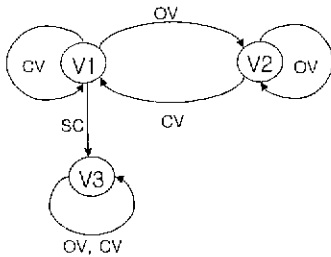


Fig. 3 FSA of I-Valve, T-Valve

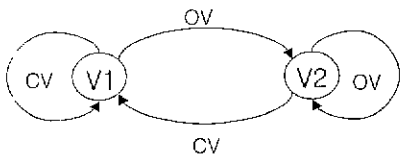


Fig 4 FSA of A-Valve, H-Valve

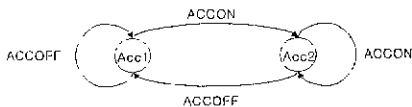


Fig 5 FSA of Accumulator

비상노심냉각계통의 주입 모드에 대한 Controller를 구성하기 위해서 대략적인 작동과정을 나타내면 다음과

같다.

㉞ 비상노심냉각계통 주입모드의 작동과정

- 1) 대규모 냉각제 상실사고(LOCA) 발생
- 2) 원자로 정지신호와 안전주입 기동신호(SIAS)가 발생
- 3) 안전 주입계통과 원자로 냉각제 계통을 격리하고 있는 밸브를 연다.
- 4) 고압 안전주입 펌프 가동
- 5) 축압기에 있는 밸브가 열려 축압기의 용산수가 노심으로 주입
- 6) 저압 안전주입 펌프가 가동
- 7) 저장탱크의 수위가 낮아져 주입모드가 끝나니고 계순환 모드로 넘어감

위의 1)~7)까지의 작동순서를 토대로 주입모드의 Controller를 구성하면 다음과 같다.

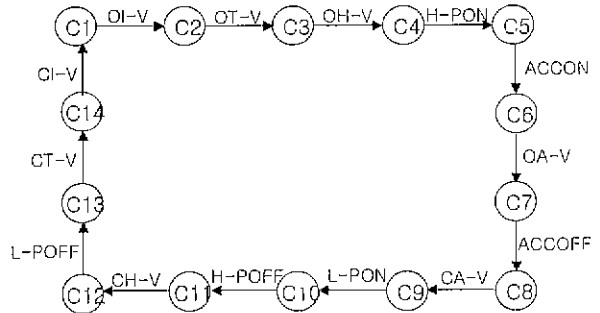


Fig. 6 FSA of Controller

앞의 펌프 2개, 밸브 4개, 축압기의 FSA와 위의 Controller의 FSA를 synchronous product를 하면 시스템의 전체 플랜트가 나온다. 본 논문에서는 결과로 나온 플랜트의 state 수가 총 56개가 나왔다. 이에 대한 그림은 지면 관계상 생략한다.

3.2 Diagnoser

본 논문에서는 diagnoser를 구성하기 위해 UMDES Software를 사용하였다. 앞에서 구성한 DES에 대해서 I-Valve의 Stuck-closed event를 failure mode F1, T-Valve의 Stuck-closed event를 failure mode F2로 두자. 그리고 이 시스템에 대한 global sensor map을 표2에서 제시한다.

그 다음단계는 sensor map과 plant의 reachable state를 통합하여 state/sensor map을 생성시킨다.

diagnoser를 구성하기 전에 먼저 전체 plant의 관측불가능한 사건들을 생성시킨 다음 전체 plant와 Table 2 The global sensor map

$h(I-V1, T-V1, \cdot) = \setminus NFI-V, \setminus NFT-V$
$h(I-V2, T-V1, ACC1, \cdot) = \setminus NFI-V, \setminus NFT-V$
$h(I-V3, T-V3, \cdot) = \setminus NFI-V, \setminus NFT-V$
$h(I-V3, T-V1, \cdot) = \setminus NFI-V, \setminus NFT-V$
$h(I-V1, T-V3, \cdot) = \setminus NFI-V, \setminus NFT-V$
$h(I-V2, T-V3, ACC1, \cdot) = \setminus NFI-V, \setminus NFT-V$
$h(H-P1, L-P1, I-V2, T-V2, ACC1, \cdot) = \setminus NFI-V, \setminus FT-V$
$h(I-V3, T-V2, \cdot) = \setminus NFI-V, \setminus FT-V$
$h(H-P2, I-V2, H-V2, T-V2, \cdot) = \setminus FI-V, \setminus FT-V$
$h(I-V2, A-V1, T-V3, \cdot) = \setminus NFI-V, \setminus NFT-V$
$h(I-V2, A-V2, T-V3, ACC2, \cdot) = \setminus FI-V, \setminus NFT-V$
$h(L-P2, I-V2, T-V2, \cdot) = \setminus FI-V, \setminus FT-V$
$h(H-P1, L-P1, T-V1, ACC1, \cdot) = \setminus NFI-V, \setminus NFT-V$

state/sensor map을 결합시킨다. 위에서 논의된 failure partition에 따라 비상노심냉각계통 주입모드의 diagnoser를 생성시킨다. 마지막으로 정리 1에서 제시된 것처럼 진단가능하지를 알아보기 위해서 indeterminate cycle이 존재하는지를 확인한다.

그림 7에 Diagnoser를 나타내었다. 시스템 구성요소의 수와 사건(event)의 수가 많아서 기면관계상 이 그림에는 Failure Label만 나타냄으로써 indeterminate cycle이 존재하는지, 즉 진단가능하지를 확인하는데 목적을 두었다. 그림 7을 보면 failure mode F_1, F_2 각각에 대해서 indeterminate cycle이 존재하지 않음을 알 수 있다. 이것은 정리 1에 의해서 diagnoser가 진단 가능하다는 것을 말해준다

4. 결론

본 논문에서는 가압경수로의 비상노심냉각계통 주입모드의 고장진단을 위하여 event-based 접근법을 적용하였다 그리고 이 시스템이 진단가능하다는 것을 보였다

추후 연구과제로는 상태(state)수를 줄일 수 있는

state-based 접근법을 적용시키는 것과 고장진단이 가능하지 않은 시스템을 진단가능하게 하는 active

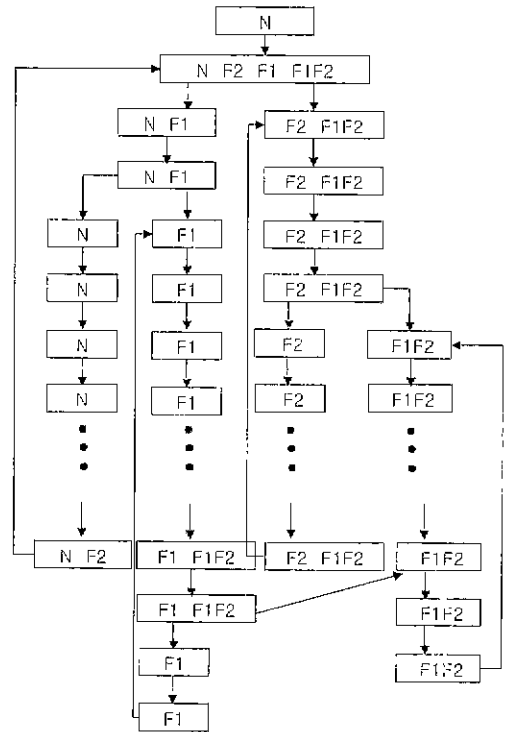


Fig 7 Diagnoser

diagnosis 문제를 다루는 것을 들 수 있다. 그리고 시스템이 진단가능하기 위한 최적의 센서 개수와 위치를 찾는 것도 앞으로 다루어야 할 문제이다.

참고문헌

- [1] Mcera Sampath, "A Discrete Event Systems Approach to Failure Diagnosis", Ph.D Thesis, The University of Michigan, December, 1995
- [2] W. M Wonham, "Notes on Control of Discrete Event Systems". Department of Electrical and Computer Engineering, University of Toronto, 1998
- [3] 장순홍, 백원필, 원자력 안전. 청문각, 1998
- [4] 손형일, 김기용, 이석, "이산사건 시스템의 Failure Diagnosis", 제어계측, 로봇틱스 및 자동화 연구회 합동 학술 발표회 논문집, pp298-303, 2000