논문 2013-08-30

동적 Fault Tree 분석을 이용한 시스템 신뢰도 평가

(System Reliability Evaluation using Dynamic Fault Tree Analysis)

변 성 일, 이 동 익*
(Sungil Byun, Dongik Lee)

Abstract : Reliability evaluation is important task in embedded system. It can avoid potential failures and manage the vulnerable components of embedded system effectively. Dynamic fault tree analysis is one of the reliability evaluation methods. It can represent dynamic characteristics of a system such as fault & error recovery, sequence-dependent failures. In this paper, the steering system, which is embedded system in vehicles, is represented using dynamic fault tree. We evaluate the steering system using approximation algorithm based on Simpson's rule. A set of simulation results shows that proposed method overcomes the low accuracy of classic approximation method without requiring no excessive calculation time of the Markov chain method.

Keywords : Embedded system, Reliability, Evaluation, Fault tree analysis, Dynamic FTA

Ⅰ. 서론

최근 전자기술이 비약적으로 발전함에 따라 임베디드 시스템(embedded system)에 사용되는 부품들의 수가 매우 증가하고 있다. 시스템을 구성하는 전자 부품들은 시스템의 안전성에 영향을 미치는데, 이러한 부품들의 영향력은 각각에 따라 다양한 형태를 가지게 된다. 그러므로 시스템 설계자는 설계 과정에서부터 각각의 부품들이 미치는 영향을 분석하고 잠재적인 고장의 가능성을 미리 평가하여 대비하여야 한다. 이를 위해 시스템의 안전성을 분석하는 방법 중에 대표적으로 fault tree 분석(fault tree analysis, FTA) 방법이 있다. Fault tree 분석 방법은 시스템에서 발생할 수 있는 고장들을 진단하고 시스템의 신뢰성을 판단할 수 있는 기법이다. 즉, fault tree 분석 방법은 시스템에서 발생할 수 있는 고장들의 인과관계를 논리 게이트로 나타내고 각 부품들의 고장확률을 분석하여 시스템의 신뢰도를 평가하고 개선한다[1]. Fault tree 분석 방법은 일반적인 선형 시스템에만 적용이 가능하기 때문에 시간이나 고장 순서에 따라 변하는 동적인 특성을 가진 시스템을 표현하기에는 한계가 있다. 이러한 한계점을 극복하기 위하여 이전에는 마르코프 체인(markov chain)을 이용하였다. 정적인 부분은 fault tree로 표현하고 동적인 부분은 마르코프 체인으로 표현하여 시스템을 나타내었다. 그러나 마르코프 체인으로도 표현하기 어려운 특성들이 생겨나면서 동적 fault tree 분석(dynamic FTA) 방법이 개발되었다[2]. 동적 fault tree 분석 방법은 기존의 마르코프 체인으로 표현하였던 동적 특성들을 하나의 게이트로 나타내어 기존의 fault tree 분석 방법처럼 동적 특성을 지닌 시스템을 논리 게이트로 구성된 나무 형태로 표현할 수 있게 하였다.

이러한 fault tree 분석을 통해 시스템을 분석한 이후에 시스템의 신뢰성을 계산하기 위해 fault tree를 평가하게 된다. 일반적으로 동적 fault tree를 평가할 때에는 동적 fault tree 내의 정적 게이트(static gate)들을 먼저 평가하고, 동적 게이트(dynamic gate)들을 마르코프 체인으로 변환하여

*Corresponding Author (dilee@ee.knu.ac.kr)
Received: 16 Apr. 2013, Revised: 14 June 2013. Accepted 22 July 2013.
S. Byun, D. Lee: Kyungpook National University
※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 IT융합 고급인력과정 지원사업의 연구결과로 수행되었음 (NIPA-2013-H0401-13-1005)

ISSN : 1975-5066
http://dx.doi.org/10.14372/IEMEK.2013.8.5.243

평가한다[3, 4]. 하지만 동적 게이트를 마르코프 체인으로 변환할 때에 몇 가지 문제점들이 발생한다. 마르코프 체인 변환 방법은 먼저 정확한 문법과 의미가 정해진 형식이 없고, 모듈 방식으로 분석하는데 있어서의 한계점으로 인해 상태-공간 폭발 문제에 취약하다. 상태-공간 폭발 문제는 동적 fault tree를 마르코프 체인으로 변환할 때 발생하는 문제로, 특정한 경우 마르코프 체인을 구성하는 시스템의 상태들이 무한정 늘어나게 되어 시스템을 제대로 표현할 수 없는 문제이다. 따라서 동적 fault tree를 마르코프 체인으로 변환하지 않고 계산하는 사다리꼴 공식 기반의 근사 알고리즘 방법이 제안되었다. 하지만 이 방법은 빠른 시간 내에 계산이 가능하지만 큰 오차를 가지고 있다[5].

본 논문에서는 사다리꼴 공식 기반의 근사 알고리즘을 Simpson의 법칙 기반의 근사 알고리즘으로 수정하여 시스템의 정확한 신뢰도를 구할 수 있는 방법을 제안한다. 이를 검증하기 위하여 자동차 내의 조향시스템을 동적 fault tree로 표현하고 기존의 동적 fault tree 평가 방법들과 제안한 방법으로 계산하고 비교 분석한다.

Ⅱ. 본 론

본 논문에서는 동적 fault tree 분석 방법의 평가 신뢰도의 향상을 검증하기 위하여 자동차 내의 임베디드 시스템 중의 하나인 조향시스템을 대상으로 동적 fault tree 분석을 수행한다. 기존의 평가 방법과 제안한 평가 방법을 통하여 시스템의 신뢰도를 구하여 비교 분석하고자 한다.

1. 조향시스템

본 논문에서의 조향시스템은 그림 1과 같이 크게 핸드 휠 시스템(hand wheel system)과 로드 휠 시스템(road wheel system)으로 나뉠 수 있다. 각각의 시스템에는 제어기와 센서, 액추에이터가 하나씩 있고 각각의 부품들 중에 하나만 고장이 나더라도 전체 조향시스템이 고장 난다.

1.1 제어기

제어기의 경우에는 두 개의 작은 제어기들로 구성되어 있다. 이 두 개의 제어기의 경우 우선순위가 있어 특정한 순서로 고장이 나야 전체 제어기의 고장이 발생하게 된다고 가정하였다. 이 경우 로드 휠 시스템의 제어기가 고장 난 다음에 핸드 휠 시스템의

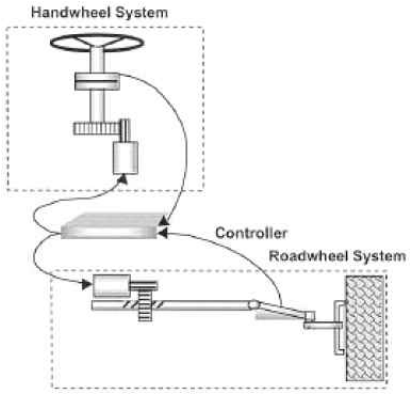

그림 1. 조향시스템 개념도[6]
Fig. 1 A conceptual design of steering system[6]

제어기가 고장 나야 제어기 전체가 고장 난 것이라고 시스템이 인지하게 된다. 이러한 경우에는 특정한 두 개의 순서를 나타낼 수 있는 Priority AND게이트를 사용하여 나타낼 수 있다.

1.2 센서

센서의 경우에는 두 개의 서브시스템들에 각각 하나씩 동작하고 있고 그 이외에 하나씩의 센서들이 여분으로 장착되어 있다고 가정한다. 여분의 센서들은 동작하지 않고 정지 상태로 대기하고 있다. 기존의 센서가 동작하고 있으면 여분의 센서들은 정지 상태로 존재하기 때문에 여분의 센서가 기존의 센서보다 먼저 고장 날 수는 없다. 이 경우 기존의 센서들이 고장 나면 여분의 센서들이 동작하게 되고 여분의 센서들까지 고장 나게 되면 시스템이 전체 센서가 고장 난다고 인식한다. 이러한 센서들은 여분의 장치를 표현할 수 있는 Cold-Spare 게이트를 사용하여 나타낼 수 있다.

1.3 액추에이터

핸드 휠 시스템의 액추에이터의 고장은 전체 조향 시스템에 미치는 영향이 아주 미비하기 때문에 무시하고 로드 휠 시스템의 액추에이터의 고장은 곧바로 조향 시스템의 고장으로 볼 수 있으므로 fault tree 내에 표현하여야 한다.

1.4 동적 Fault Tree 분석

위에서 언급한 조향시스템의 특성을 고려하여 동적 fault tree 분석 수행 결과를 그림 2와 같이 나타낼 수 있다.

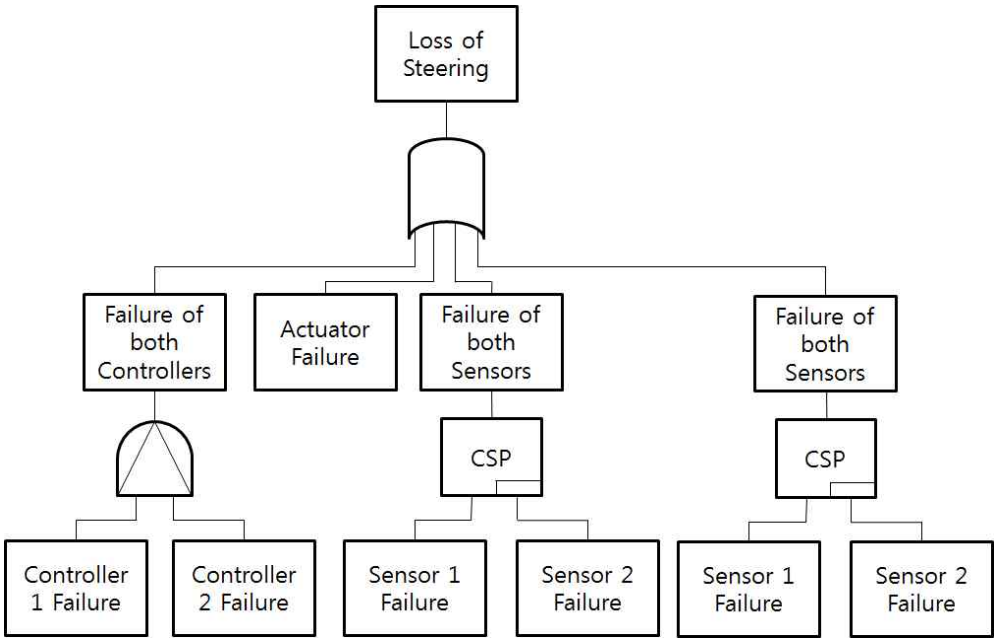

그림 2. 조향 시스템의 동적 Fault Tree
Fig. 2 The dynamic fault tree of the steering system

Ⅲ. 신뢰도 평가 기법

동적 fault tree의 신뢰도 평가 기법은 여러 가지 수학적 도구들을 사용하여 구성된 fault tree를 기반으로 하여 시스템의 신뢰도를 구하는 것이다. 신뢰도를 구하는 방법은 크게 두 가지로 나눌 수 있는데 하나는 동적 fault tree를 마르코프 체인으로 변환하여 신뢰도를 구하는 방법이고 또 다른 하나는 변환하지 않고 수학적 도구들을 사용하여 신뢰도를 구할 수 있는 방법이 있다.

1. 마르코프 체인 변환

마르코프 체인 변환 방법은 가장 일반적인 방법으로 여러 가지 평가 기법들 중에서 가장 정확한 방법이다. 하지만 동적 fault tree를 마르코프 체인으로 변환할 때에 시간적 비용과 일반적인 형식이 없다는 문제점 때문에 비효율적인 방법으로 알려져 있다. 동적 fault tree를 평가할 때에는 먼저 정적 fault tree와 동적 fault tree로 분리하여 신뢰도를 계산한다. 정적 fault tree의 경우, 부울대수 식을 이용해 fault tree를 간략하게 정리하고 확률론적 식을 사용해 시스템의 신뢰도를 구한다. 반면에 동적 fault tree의 경우, 동적 게이트들을 마르코프

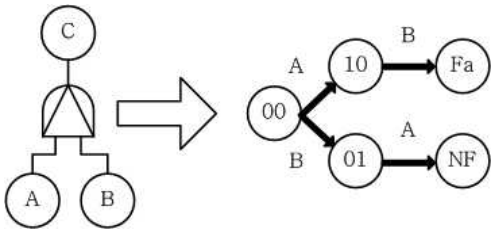

그림 3. Priority-AND 게이트의 마르고프 체인 변환
Fig. 3 Markov chain for Priority-AND gate

체인으로 변환하여 시스템이 신뢰도를 구한다. 아래 그림 3은 동적 fault tree에 사용되는 동적 게이트 중의 하나인 Priority-AND 게이트를 마르코프 체인으로 변환하는 과정이다. Priority-AND 게이트는 입력 A 이벤트가 발생한 이후에 입력 B 이벤트가 발생할 경우, 고장이라는 출력 C를 발생하게 되는데 이를 마르코프 체인으로 변환하면 그림 3과 같이 나타낼 수 있다. 마르코프 체인에서 Fa는 시스템의 고장(failure), NF는 시스템의 정상상태(non-failure)를 나타낸다.

마르코프 체인에서 시스템의 상태 변화를 전이라고 하는데, 이 전이의 횟수에 따라 시스템의 신

뢰도를 계산하는 식이 결정된다. 전이 횟수 n에 다른 신뢰도(전체 시스템의 고장 확률) 계산식은 다음과 같다.

$$P_n(t)=p_{0n}(t)=\prod_{i=1}^{n}\lambda_{i-1,i}\left[\prod_{i=1}^{n}\frac{1}{\lambda_{i-1,i}+\lambda_{i-1,NF}}-\sum_{i=1}^{n}\frac{e^{(\lambda_{i-1}+\lambda_{i-1,NF})t}}{(\lambda_{i-1,i}+\lambda_{i-1,NF})}\times\frac{1}{\prod_{j=1,j\neq i}^{n}(-\lambda_{i-1,i}-\lambda_{i-1,NF}+\lambda_{j-1,j}+\lambda_{j-1,NF})}\right] \quad (1)$$

여기서 $\lambda_{i-1,i}$는 $i-1$ 번째 상태에서 i 번째 상태로 천이할 확률을 나타내고 0 보다 큰 값을 가진다. $\lambda_{i-1,NF}$는 $i-1$ 번째 상태에서 정상상태(non-failure state)로 천이할 확률을 나타내고 0 이상의 값을 가진다.

2. 근사 알고리즘

마르코프 체인 변환 기법은 시간적 비용으로 인해 잘 사용되지 않는다. 이러한 마르코프 체인 변환 기법을 사용하지 않고 동적 fault tree를 평가하는 방법은 여러 가지가 있다. 그 중에서 계산 속도를 매우 빠르게 향상 시킨 방법이 근사 알고리즘을 이용한 기법이다. 이 근사 알고리즘은 식 (2)와 같이 동적 게이트를 적분 식으로 표현하고, 식 (3)과 같이 적분 식을 사다리꼴 공식을 이용해 근사한다. 여기서, 식 (2)에서의 $P(t)$는 t 시간에 안에 동적 게이트 하위 단의 모든 입력 이벤트들이 발생하여 게이트의 고장 출력이 날 확률이다.

$$P(t)=p\{T_1\le T_2\le\cdots\le T_m\le t\}=\int_0^t\int_{x_2=x_1}^{t}\cdots\int_{x_m=x_{m-1}}^{t}dP_m(x_m)\cdots dP_2(x_2)dP_1(x_1) \quad (2)$$

$$P(t)\approx\sum_{t_1=1}^{M}\left[P_1(i_1h)-P_1((i_1-1)h)\right]\times\left[\sum_{i_2=i_1}^{M}\left(P_2(i_2)-P_2((i_{2-1})h)\cdots(P_m(t)-P_m(i_{m-1}h))\right)\right] \quad (3)$$

여기서 m은 기본 이벤트의 수, M은 시간 간격의 수, $h=t/M$는 스텝의 수를 나타낸다.

그러나 근사 알고리즘은 12% 정도의 오차율을 가지고 있다. 이러한 단점을 보완하기 위해 본 논문에서는 근사 알고리즘을 수정하여 더 정확한 값을 구하는 기법을 제안한다.

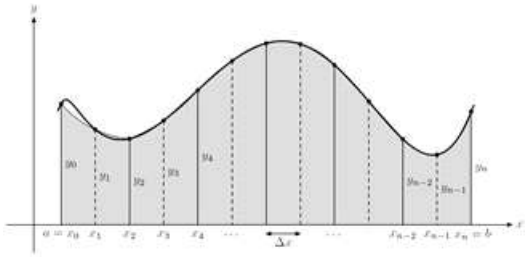

그림 4. 곡선 그래프 예시
Fig. 4 Example of curve graph

3. Simpson's rule 기반의 근사 알고리즘

이 알고리즘은 기존의 근사 알고리즘의 적분 식을 높은 정확성을 지닌 Simpson's rule을 통해 근사하여 시스템의 신뢰도를 계산한다. Simpson's rule은 그림 4와 같은 일반적인 곡선의 그래프를 근사 적분하여 그 값을 구한다. 근사하고자 하는 일반적인 곡선을 나타내는 함수식을 $f(x)$라고 할 때 식 (4)와 같이 근사할 수 있다.

$$\int_a^b f(x)dx\approx\frac{\Delta x}{3}(y_0+2y_1+4y_3+2y_4+\cdots+4y_{n-1}+y_n) \quad (4)$$

일반적으로 근사는 누적 오차를 지니는데 이러한 오차를 보상하여 더 정확한 값을 얻기 위해서 Simpson's rule의 표준 오차를 다음 식 (5)와 같이 수정하여 사용한다. 수정된 표준 오차를 사용하여 식 (4)를 식 (6)과 같이 수정하여 근사를 수행한다.

$$C=f(\zeta)\frac{e^{-1.1622\times10^{-3}t}}{\left|f\left(\frac{b-a}{2}\right)\right|}\left(\frac{b-a}{2}\right)^5\left|f^{(4)}\left(\frac{b-a}{2}\right)\right| \quad (5)$$

여기서 a, b는 적분 구간의 양 끝점이고, ζ는 a와 b 사이의 임의의 수이다.

$$\int_a^b f(x)dx\approx\frac{\Delta x}{3}(y_0+4y_1+2y_2+4y_3+2y_4+\cdots+4y_{n-1}+y_n-C) \quad (6)$$

Ⅳ. 시뮬레이션

1. 시뮬레이션 셋업

시뮬레이션에 사용되는 조향시스템은 두 개의 제어기와 네 개의 센서, 그리고 한 개의 액추에이터로 구성되어 있다. 각각에 해당하는 고장 확률은 표 1과 같다.

표 1. 각 부품의 고장 확률
Table 1. Failure Probabilities of Each Component

부품	고장확률
Controller 1	6.28E-06
Controller 2	2.60E-06
Actuator	7.90E-07
Sensor 1	6.06E-04
Spare Sensor 1	8.76E-05
Sensor 2	6.06E-04
Spare Sensor 2	8.76E-05

표 2. 조향 시스템의 비 신뢰도
Table 2. Unreliabilities of steering system.

Hour(h)	MC	Existing Alg.	Proposed Alg.
500	3.3581E-04	2.951E-04	3.3010E-04
1000	1.2111E-03	1.0801E-03	1.1796E-03
1500	2.4655E-03	2.2123E-03	2.3891E-03
2000	3.9821E-03	3.5285E-03	3.9303E-03
2500	5.6748E-03	4.9589E-03	5.6237E-03
3000	7.4806E-03	6.6151E-03	7.3160E-03
3500	9.3529E-03	8.2231E-03	9.2033E-03
4000	1.1259E-02	1.0025E-02	1.1135E-02
4500	1.3174E-02	1.1662E-02	1.2858E-02
5000	1.5081E-02	1.3413E-02	1.4764E-02
5500	1.6967E-02	1.4807E-02	1.6662E-02

2. 시뮬레이션 결과

각 부품들의 확률을 기반으로 하여 이전에 언급한 세 가지의 평가 기법으로 조향 시스템의 비 신뢰성을 계산한 결과는 표 2와 같다. 각 방법의 정확도를 살펴보기 위하여 500 시간에서 500 시간 단위로 5500 시간까지 시뮬레이션을 수행하였다. 동일한 동적 fault tree를 대상으로 가장 기본적인 마르코프 체인 변환을 통한 방법과 근사 알고리즘 그리고 제안된 방법으로 평가를 수행한 후 마르코프 체인 변환 방법을 기준으로 근사 알고리즘을 이용한 방법과 제안된 방법의 오차 크기를 비교하였다. 그림 5를 통해 결과 값을 확인해보면, 제안된 방법이 기존의 근사 알고리즘을 이용하여 계산한 값보다 오차가 10%정도 더 낮음을 확인할 수 있다.

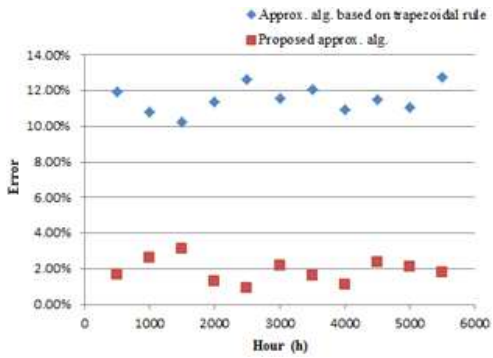

그림 5. 평가 결과의 오차 그래프
Fig. 5 The graph of error of evaluation results

V. 결론

본 논문에서는 자동차 내의 임베디드 시스템 중의 하나인 조향 시스템을 대상으로 동적 fault tree 분석을 수행하였다. 조향 시스템을 동적 fault tree로 표현하고, 세 가지의 동적 fault tree 분석 기법들을 통해 조향 시스템의 비 신뢰도를 계산하였다. 이를 통해 기존의 근사 알고리즘의 단점인 정확성을 개선시킬 수 있는 방법인 Simpson's rule 기반의 근사 알고리즘 방법을 제안하고 검증하였다.

References

[1] Limnios, Nikoaos, Fault Trees, ISTE LTD, 2007.

[2] J.B. Dugan, S.J. Bavuso, M.A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," IEEE Transactions on Reliability, Vol. 41, No. 3, pp.363-377, 1922.

[3] J.B. Dugan, B. Venkataraman, R. Gulati, "DIFTree: a software package for the analysis of dynamic fault tree models," Proceedings on Annual Reliability and Maintainability Symposium, pp.64-70, 1997.

[4] H. Boudali, J.B. Dugan, "A new bayesian network approach to solve dynamic fault trees," Proceedings on Reliability and Maintainability Symposium, 2005.

[5] W. Han, W. Guo, Z. Hou, "Research on the method of dynamic fault tree analysis," Proceedings on International Conference of

Reliability, Maintainability and Safety, 2011.
[6] S. Amberkar, J.G. d' Ambrosio. B.T. Murray, J. Wysocki, B.J. Czerny, "A system-safety process for by-wire automotive systems," Proceedings on SAE World Congress, 2000.

저 자 소 개

변 성 일

2011년 경북대학교 IT대학 전자공학부 학사.
2013년 경북대학교 대학원 전자전기컴퓨터 석사.
현재 경북대학교 IT대학 전자공학부 박사과정.
관심분야: 신뢰도 평가, 시스템 설계
Email: bsi880705@naver.com

이 동 익

1987년 경북대학교 전자공학과(이학사).
1990년 경북대학교 전자공학과(공학석사).
1990년~1997년 국방과학연구소 연구원.
2002년 영국 셰필드대학교 자동제어시스템공학과(공학박사).
2002년 1월~2005년 3월 영국 DRTS Ltd 공동설립 및 CTO.
2005년~현재, 경북대학교 IT대학 전자공학부 부교수.
관심분야: 고장진단, 고장대처, 시스템 안전, 산업용 네트워크, 풍력발전기, 지능형 자동차, 무인잠수정
Email: dilee@ee.knu.ac.kr