Journal of the Society of Korea Industrial and Systems Engineering
Vol, 29, No. 3, pp.1－6, September 2006.

페트리 네트에 기반한 제품의 안전분석 방법 : 하드웨어와 인간행태를 통합하여 분석하는 방법에 관하여

임창주* · 고봉기**

*한국산업기술대학교 게임공학과
**삼성전자 CS 경영센터

Petri-nets based Product Safety Analysis : A Way of Integrated Method of Hardware and Human Behavior

Chang-Joo Lim* · Bong-Ki Koh**

*Dept. of Game and Multimedia Engineering, Korea Polytechnic University
**CS Management Center, Samsung Electronics

In this paper, we described the existing methodology of product safety analysis and proposed a Petri-nets based method to analyze product safety systematically. The proposed method can be used to find the defects of hardware/software and the error of human behavior. We also discussed the differences between the Fault Tree Analysis and Petri-nets based method by giving an example.

Keywords : Safety Analysis, Petri-nets, Human Behavior, Fault Tree Analysis

1. 서 론

2002년 7월 1일부터 제조물 책임법(PL : Product Liability)이 시행되었다. 이에 대한 관심이 고조되면서 소비자 권리의 핵심 항목으로 제품 안전이 중요한 문제로 부각되고 있다. 제조물 책임법은 제조물의 결함에 의해 소비자의 생명, 신체 또는 재산상에 손해가 발생한 경우 제조자 등이 과실여부와 상관없이 손해배상책임을 지도록 하고 있다(한국표준협회 A, 2001). 즉, 제품으로 인한 소비자 피해가 발생할 경우 기업이 스스로 제조물의 무결함을 규명해야 손해배상책임에서 벗어날 수 있다. 따라서, 기업은 사용자가 요구하는 기능과 디자인을 최대로 반영하여 제품의 구매욕구를 최대화시켜 매출증대를 기대하는 동시에 한편으로는 제품이 갖는 고유의 위험성으로부터 야기될 수도 있는 손실을 최소화해야 한다(한국표준협회 B, 2001). 결국 기업은 제품이 갖는 잠재위험으로부터 파생할 수 있는 소비자 손실을 줄이기 위해 제품안전 확보에 특별한 관심을 갖고 노력을 기울여야 한다.

"리스크(risk)"란 위험요인(risk factor) 혹은 위험성(riskiness)에 의하여 손실(loss)과 같은 바람직하지 않은 결과를 초래할 가능성을 의미하는 것으로, 결과의 크기와 그 발생확률의 결합으로 정의된다. 따라서, 제품의 리스크는 제품이 원래 의도하던 목표 효용의 달성에 영향을 줄 수 있는 의도하지 않은, 동시에 바람직하지 않은 사건의 발생가능성과 그 결과적인 피해에 의해 표현된다. 위험요인이란 제품사고를 발생시키는 근본적인 원인이다. 위험요인은 제품의 고장(failure)이나 오기능(malfunction) 등 제품의 기능적 결함(functional defect)과 사용자의 예측 가능한 사용(foreseeable use) 및 오용(misuse)으로 인해 발생가능한 사용자 오류(foreseeable user negligence) 등 두 가지로 분류될 수 있다. 제품의 안전성을 평가하기 위한 리스크 평가의 기본원칙으로 제품 수명

주기(life-cycle)에 걸쳐 각 단계별로 요구되는 리스크 구명, 리스크 분석, 리스크 평가 등을 포함하여 관련된 업무 내용 및 요건이 제시된 바 있다(이용희, 2002). 제품의 안전성은 설계와 개발단계에서 60% 이상이 결정된다고 해도 과언이 아니며, 특히 안전하게 사용될 수 있는 제품 설계를 위해 사용자의 물리적, 인지적, 감성적 특성을 고려하여 제품과 사용자 간의 원활한 상호작용이 가능한 사용자 인터페이스를 디자인하는 것이 중요하다(정광태, 2002). 제품의 인터페이스를 디자인하기 위해서는 사용자가 제품을 사용하기 위한 조작과정이나 조작결과에 대한 사용자의 행동을 고려할 필요가 있다. 상대적으로 시스템의 기계적, 전자적인 하드웨어의 신뢰도와 수명은 높아지고 있는 반면, 복잡한 시스템의 운용을 맡고 있는 운용자는 그 역할의 인지적 어려움으로 인해 오작동을 유발할 수 있는 가능성이 더욱 커지고 있기 때문이다(Cacciabue, 2000). 이러한 행동은 감각-운동 기능(sensory-motor skill)뿐 아니라 인지적 추론능력(cognitive-reasoning abilities)도 포함하여야 한다(Cacciabue, 2000). 실제 제품을 사용하는 과정에 대한 고려 없이는 사용자에게 적합한 인터페이스를 제공할 수 없고 적합하지 못한 인터페이스 설계는 제품의 안정성을 저해하는 요인이 될 수 있다.

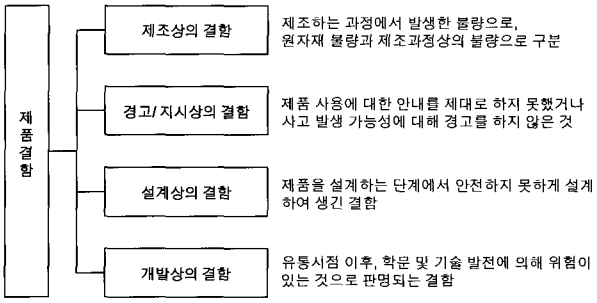
본 논문은 사용자와 제품의 상호작용을 고려한 위험요인 분석방법에 관한 연구결과이다. 2장에서는 제품결함의 유형들을 정리하였고, 3장에서 기존의 위험요인 분석방법에 관해 기술을 하였다. 4장에서는 페트리 네트를 이용하여 하드웨어나 소프트웨어뿐만 아니라 인간 행동까지도 고려한 위험요인 분석방법을 제안하였으며, 실례를 들어 그 효용성을 검증하였다.

2. 제품결함

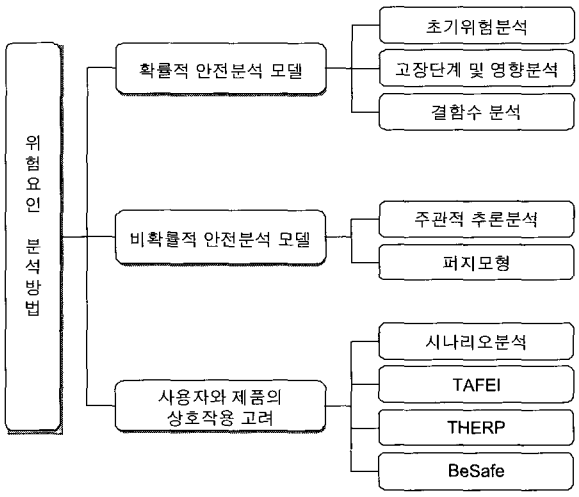
제품의 결함은 품질의 결여(lack of quality)가 아니라 생명, 신체, 재산상의 손실을 야기할 수 있는 안전의 결여(lack of safety)를 의미하며, 좁은 의미로 보면, 제품의 성격, 일반적으로 예측 가능한 사용방법, 제품이 인도된 시점 등을 고려하여 제품이 갖추어야 할 안전의 결여를 말한다. 이러한 제품의 결함은 <그림 1>과 같이 크게 제조상의 결함, 경고지시상의 결함, 설계상의 결함, 개발상의 결함 등으로 구분할 수 있다(김유창 외, 2002).

3. 위험분석 방법

위험분석은 기본적으로 제조업자에 의해 수집되는 소비자 고발과 제품사고보고서, 클레임(claims)과 제조물 책임소송 등과 같은 소비자 피해사례 분석을 통하여 수행된다. 또한 필요에 따라 확률적 안전분석 모델(probabilistic safety analysis model)이나 비확률적 안전분석 모델(non-probabilistic safety analysis model)과 같은 공학적 기법을 이용하기도 한다. 아울러 사용자와 제품의 상호작용을 고려한 위험요인 분석에 관한 연구도 활발히 진행되고 있다. 일반적으로 빈번하게 적용되고 있는 위험요인 분석방법을 정리하면 <그림 2>와 같다.



<그림 1> 제품결함 구분



<그림 2> 위험요인 분석방법

3.1 확률적 안전분석 모델(probabilistic safety analysis model)

확률적 안전분석 모델은 사고원인 및 결과, 사고발생 빈도와 같은 자료를 이용하여 정성적(qualitative) 또는 정량적(quantitative) 안전분석을 통해 발생가능한 사고원인을 추적하고 적합한 예방책을 도출하는 기법이다. 이 확률적 안전분석모델은 우리가 흔히 사용하는 소비재 상품(consumer product) 설계에 널리 응용된다. 대표적인 기법으로는 초기위험 분석(PHA : Preliminary Hazard Analy-

sis), 고장단계 및 영향 분석(FMEA : Failure Mode and Effect Analysis), 결함수 분석(FTA : Fault Tree Analysis), 인간신뢰도 분석(HRA : Human Reliability Analysis) 등이 있다.

3.2 비확률적 안전분석모델(non-probabilistic safety analysis model)

비확률적 안전분석 모델은 분석 대상 자료의 신뢰성이 부족하여 확률적 안전분석 모델의 수행이 어려울 때 적용한다. 이 모델은 일반적으로 퍼지모형(fuzzy modelling)이나 매우좋음(very good), 매우낮음(very low) 등의 용어를 사용한 주관적 평가치(subjective measurement)를 이용하기 때문에 주관적 추론분석(subjective reasoning analysis)이라고도 불린다. 이 모델은 일반 소비제품보다는 장치산업과 같이 주로 규모가 크고 복잡한 시스템에 대한 분석에 많이 이용된다.

3.3 사용자와 제품의 상호작용을 고려한 위험요인 분석

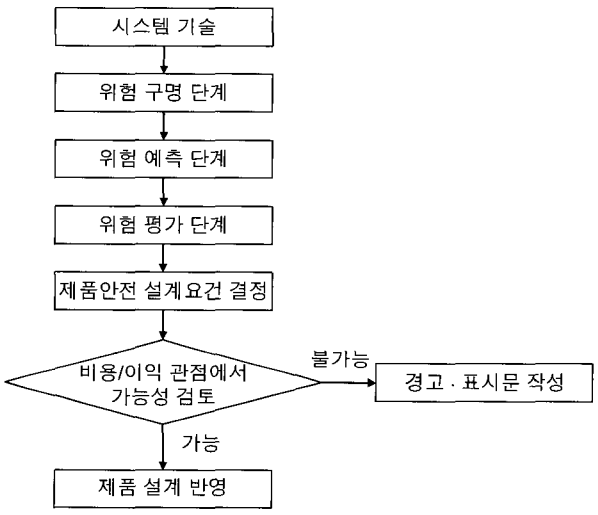
이상의 분석기법들은 현재 널리 활용되고 있지만 제품의 기능적 결함 및 사용자의 오류에 의해 발생 가능한 위험요인을 종합적으로 분석하는 데는 한계가 있다. 제품사고는 제품의 기능적 결함뿐만 아니라 사용자 특성, 사용행위, 사용 환경 등과 같은 사용자관련 요소와 밀접하게 연관되어 발생하기 때문이다(Harmsen, 1990).

사용자와 제품의 상호작용(HPI : Human/Product Interaction)을 고려한 위험요인 분석은 인간공학 관련 분야에서 활발히 진행되고 있으며 대표적인 기법은 시나리오 분석(Scenario Analysis), TAFEI(Task Analysis For Error Identification), THERP(Technique for Human Error Rate Prediction), BeSafe(Behavior Safe method) 등이 있다.

4. 페트리 네트를 이용한 위험분석 방법

<그림 3>의 위험분석 과정에서 핵심은 시스템 기술(system description) 단계이다. 앞에서 살펴본 바와 같이 사용자를 시스템 혹은 제품과 독립적인 요소로 간주하여 위험요인을 분석한다는 것은 무의미하다. 제품의 기능(machine function)과 사용자의 조작(human task) 사이에서 생기는 상호작용(interaction)을 포함하여 분석하기 위해 사용자를 전체시스템의 일부로 간주하여 기술하는 것이 바람직하다(Felix Redmil and Jane Rajan, 1997).

결함수 분석(Fault Tree Analysis)은 의도되지 않은 사건의 결과에서 비롯된 시스템의 구성요소 간의 관계를 표현할 수 있는 논리 기반(logic-based)의 모델링 기법이다. 결함수 분석은 시스템 설계, 개발, 수정 및 검증하는데 적용될 수 있으며, 제안된 디자인의 고장 행태를 정량적 또는 정성적으로 평가하는데 사용된다. 결함수(fault tree)는 정상사상(top event)이라고 부르는 바람직하지 않은 사상을 시작으로 그 발생원인이나 거기에 기여하는 조건들이나 원인들을 찾아 시간적 흐름을 거슬러 분석해 가는 연역적 구조이며(한국표준협회 B, 2001), 여러 가지 하부 시스템으로 구성된 복잡한 제품을 분석하는데 적합하다. 또 부품뿐만 아니라 인간 오류(human error), 소프트웨어 오류, 환경 스트레스에 의한 고장 등 다중고장의 해석이 가능하다. 그러나, 논리적인 부분에 있어 부울 대수(boolean algebra)나 최소절단집합(minimal cut sets), 또는 중요도 지수를 이용하므로 일반인이 이해하기 어려운 부분들이 있으며, 시간적 연쇄를 취급하거나 공통원인고장 등을 고려한 역동적인 분석(dynamic analysis)은 곤란하다(한국표준협회 B, 2001). 또한 제품의 기능적 결함 및 사용자의 오류에 의해 발생가능한 위험요인을 종합적으로 분석하는 데에는 한계가 있다.



<그림 3> 일반적인 위험분석 과정

따라서 본 연구에서는 이에 대한 보완책으로 페트리 네트(Petri-nets)를 이용하여 제품의 위험분석을 수행해 보았다. 페트리 네트는 동시성(concurrency)과 병렬성(parallelism)측면에서 효과적인 시스템 모델링 방법으로 하드웨어나 소프트웨어뿐만 아니라 인간 행동(human behavior)에 대해서도 모델링이 가능하다고 알려져 있다(Peterson, 1981). 제조자가 예측학 어려운 인간의 오작동 행위를 고려할 수 있도록 인간행위의 분석단위를 개발한다면 페트리 네트를 이용하여 시스템 안전을 체계적으

로 모델링하고 분석할 수 있다. 또한, 페트리 네트는 부품 수준(component level)의 에러/고장 회복 과정에 제약이 있는 시스템의 고장행태를 모델링하는데 사용되기도 하였다. 최근에는 신뢰도 분야에서 신뢰도 계산, 고장내구분석(fault-tolerant analysis), 안전성/위험분석(safety/risk analysis), 마아코프 과정(markov process) 및 추계적 과정(stochastic process) 등에 적용되고 있다. 특히, 소프트웨어 안전성 분석, 고장 진단, logic flow graph methodology, 논리 연산의 상태방정식 표현 등에서는 페트리 네트와 결함수 분석이 결합되어 적용되기도 한다.

본 연구에서는 제품을 사용하는 사용자의 행동과 사용자의 조작결과에 따른 제품의 기능 동작상황을 페트리 네트를 이용해 모델링 및 분석을 수행해보고 그 결과를 결함수 분석 방법과 비교하여 그 장단점을 논의하고자 한다.

4.1 페트리 네트(Petri-nets) 개요

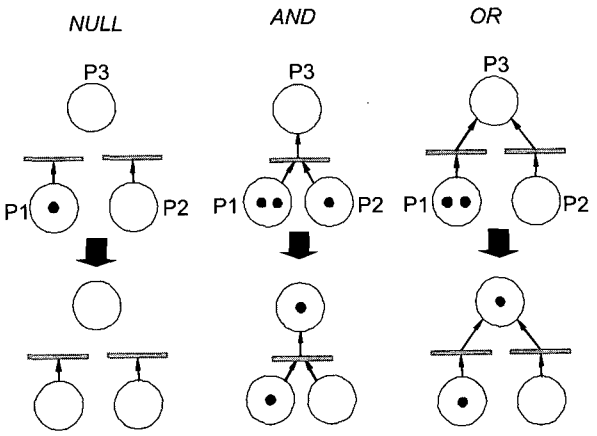
1962년 Petri에 의해 처음 제안된 페트리 네트는 조건과 사상 간의 관계를 나타내기 위하여 간단한 기호(symbol)를 사용하여 그림으로 나타나는 방법이다(Peterson, 1981). 이는 시스템의 동적인 행적을 나타내고 분석할 수 있게 해준다. 페트리 네트는 place(P)와 transition(T)의 두 가지 모양의 node를 가지고 있다. 이 node들은 transition을 place에, 또는 place를 transition에 연결하는 arc (A)에 의해 연결되며, 각 place는 하나 또는 그 이상의 token을 가질 수 있다. 이 기호들은 다음과 같이 정의된다.

○ : Place, '원'으로 표시
— : Transition, '바'로 표시
↖ : Arc, 'place'와 'transition' 간에 화살표로 표시
• : Token, place 안에 점으로 표시

또한 Peterson은 P, T, A를 다음과 같이 수리적으로 정의하였다(Peterson, 1981) (I는 자연수).

$P = \{P_i \mid P_i = \text{place}, 1 \le i \le I\}$
$T = \{T_i \mid T_i = \text{transition}, 1 \le i \le I\}$
$A \subseteq (P \times T) \cup (T \times P)$

페트리 네트에서 state는 각 place P_i에 포함되어 marking이라 불리는, 토큰의 수 m_i로 표시된다. <그림 4>는 결함수 분석과 유사한 방법으로 사상(event)간의 인과관계(Null, AND, OR 등)를 페트리 네트를 이용해 도식적인 방법으로 나타낸 것이다.



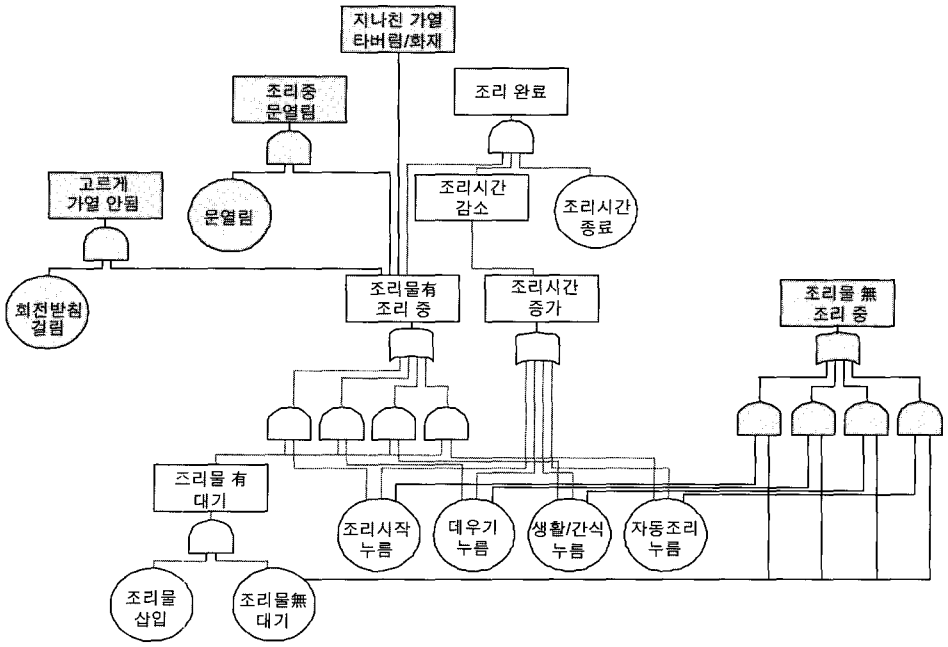
<그림 4> 페트리 네트를 이용한 논리 연산

<그림 4>의 AND 연산의 경우를 보면 각 input palce P_1과 P_2에는 토큰이 있으나 output place P_3에는 없다. 따라서 이 페트리 네트 Marking은 M = (2, 1, 0)이다. 해당 페트리 네트의 모든 input place가 하나 이상의 토큰을 포함하고 있을 때 transition이 가능해지며, transition이 이루어지면, 모든 input place에 있는 토큰이 제거되고 모든 output place에 토큰이 놓여진다. 이렇게 됨으로써 marking의 변화 즉 state의 변화가 끝나게 된다. <그림 4>의 AND 연산을 보면 2개의 input place P_1과 P_2가 하나 이상의 토큰을 포함하고 있기 때문에 transition이 가능하다. AND 연산의 경우에서 transition이 이루어지고 나면, 토큰을 P_1과 P_2로부터 각 output place P_3로 옮긴다. <그림 4>의 AND 연산의 경우 place P_1은 원래 2개의 토큰을 가지고 있고, transition이 이루어지면 각 input place로부터 하나의 토큰만을 빼오기 때문에 P_1에 토큰이 하나 남게 된다. <그림 4>에 NULL, OR 연산에 대해서도 transition이 이루어지는 과정을 나타내었다.

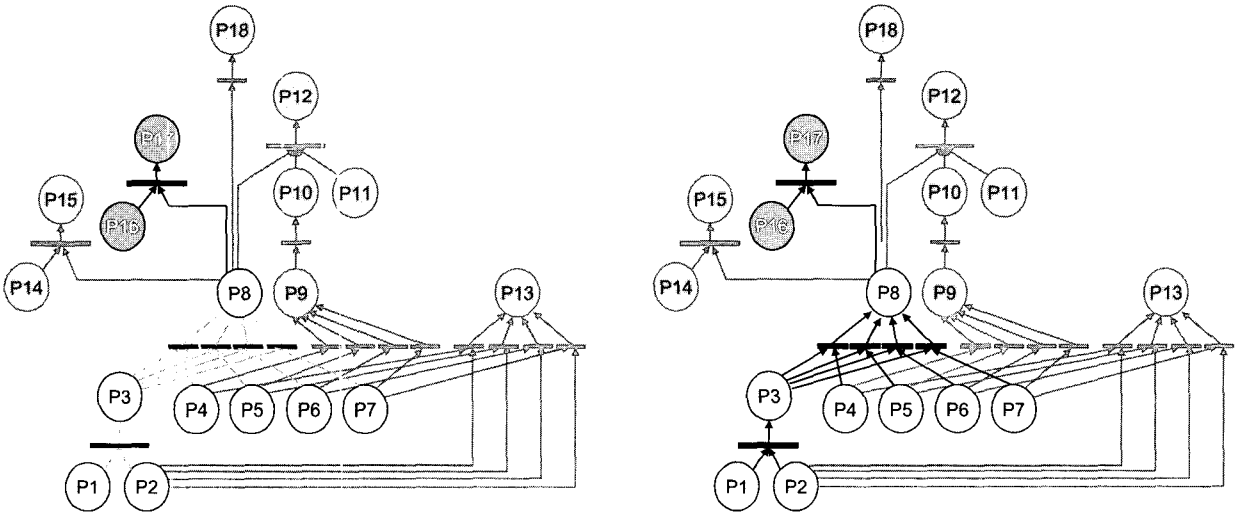
4.2 페트리 네트를 이용한 모델링(예)

<그림 5>는 제품을 사용하는 과정에서 발생할 수 있는 결함 상황(작동 중인 전자레인지의 문이 열리는 경우)을 결함수(Fault Tree)를 이용해 모델링한 예이다. 이는 전자레인지 사용자의 행동과 사용자의 조작결과에 따른 전자레인지의 동작상황을 포함한 것이다.

이를 페트리 네트로 전환시키면 <그림 6>(a)와 같고 각 Place의 토큰의 유/무를 통해 전체 상황을 쉽게 이해할 수 있으며, Transition의 조건이 충족된 경우 토큰의 이동이 일어나게 되므로, 결함 상황이 발생하기까지 어떠한 과정을 거치게 되는지 시뮬레이션 해 볼 수 있다. 이러한 시뮬레이션 과정은 이미 개발된 여러 페트리 네트 모델링 툴을 이용해 살펴볼 수 있다.



<그림 5> 정비작업 중 제품이 가동되는 결함(결함수 모델)



(a) 조리 중 문이 열리는 결함 (b) 번호를 다시 정함(Renumbering)

<그림 6> 정비작업 중 제품이 가동되는 결함(페트리 네트 모델)

결함을 발생시키는 minimal cut set과 정상 동작 상태를 나타내는 path set은 Liu와 Chiou(1997)이 제안한 절차를 따라 쉽게 구할 수 있다. <그림 5>에서 "조리 중 문이 열리는 결함"에 관한 시나리오를 생각해보면 <그림 6>(a)와 같이 페트리 네트로 표현할 수 있다. <그림 6>(a)의 페트리 네트에 번호를 다시 매겨서 <그림 6>(b)를 만들 수 있고 이는 Place와 Transition으로 이루어진 행렬을 구성할 때 편리하게 조작할 수 있도록 한다. 즉 제품의 작동상황을 그래픽하게 표현할 수 있도록 하는 기능이 있다. <그림 6>(b)의 경우 최소절단집합을 구해보면 [P1, P2, P4, P9], [P1, P2, P4, P10], [P1, P2, P5, P9], [P1, P2, P5, P10], [P1, P2, P6, P9], [P1, P2, P6, P10], [P1, P2, P7, P9], [P1, P2, P6, P10]이다. 분석방법은 일반적인 페트리 네트에서 절단집합(cut sets)과 경로집합(path sets)을 계산하는 알고리즘을 이용하거나 행렬을 이용한 방법을 사용하면 된다. 경로집합은 듀얼 페트리 네트(dual Petri-nets)를 이용하여 최소절단집합의 경우와 유사한 절차를 통해 구할 수 있다.

4.3 페트리 네트를 이용한 제품 안전 분석 방법의 장단점

페트리 네트를 통해 제품의 안전성 분석을 실시하는 방법은 다음과 같은 장점이 있다. 첫째, 페트리 네트는 AND, OR, XOR, NAND 등 모든 종류의 논리 연산을 표현할 수 있으며, 단지 Transition과 Place만을 이용하여 간단하게 모델링할 수 있다. 둘째, 결함 및 오류 분석에 있어 결함수(Fault tree)를 이용하는 것보다 페트리 네트를 이용하는 것이 효율적으로 minimal cut set 및 minimal path set을 구할 수 있어 분석이 용이하다. 셋째, 페트리 네트는 토큰의 흐름을 통해 오류 분석 대상이 되는 시스템에 대해 명료한 시각적 모델링이 가능하고 오류검사의 중간과정을 각 Place에 할당된 토큰을 통하여 쉽게 알 수 있으며, 시스템 상태 변화를 시뮬레이션할 수 있다. 넷째, 제품을 사용하는 사용자의 행동과 사용자의 조작결과에 따른 제품의 동작상황을 모델링할 수 있고 효과적으로 분석할 수 있다.

5. 결론 및 토의

본 연구에서는 제품의 안전분석을 위해 리스크의 정의와 제품 결함에 관해 살펴보았고, 제품 안전분석을 위한 방법으로 페트리 네트를 이용한 방법을 제안하였다. 이는 시스템의 하드웨어나 소프트웨어의 결함 뿐 아니라 사용자의 조작상황을 모델링함으로써 인간에 의한 오작동 원인도 파악할 수 있는 가능성을 제시하였다. 페트리 네트를 이용한 제품 안전분석 방법은 Place와 Transition을 이용해 간단하게 시스템을 표현할 수 있고, minimal cut set과 path set을 비교적 간단한 절차를 통해 구할 수 있기 때문에 모델링 파워와 분석력에 있어서 결함수(Fault tree)보다 우수한 성능을 지니며 시스템의 상태변화를 시각적으로 시뮬레이션할 수 있어서 제품의 사용과정을 분석 및 평가하는 데 매우 유익하다.

본 연구의 발전시키기 위해서는 사용자의 행위를 구체적으로 모델링할 수 있는 시스템적 가이드라인(예 : 인간행위 분석지침)을 마련해야할 필요가 있다. 4.2절의 예에서 시스템적 사고로 하드웨어와 사용자의 행위가 복합적으로 모델링을 시도하였지만 이 결과를 일반화하고 구체화하기위한 이론적 배경이 뒷받침될 수 있어야 할 것이다.

참고문헌

[1] 김유창, 이창민, 문찬식, 최은진; "어린이 완구의 제조물 책임에 대한 연구", 대한인간공학회 춘계학술대회, 2002.

[2] 이용희; "제품안전을 위한 리스크 평가의 원칙과 체계", 대한인간공학회 춘계학술대회, 2002.

[3] 한국표준협회 A; PL대응 제품안전표준 세미나, 2001.

[4] 한국표준협회 B; 제품안전을 위한 리스크 평가기법 및 소프트웨어 활용 지침, 2001.

[5] 정광태; "제품 안전 측면에서 사용자 인터페이스의 설계 방향", 대한인간공학회 춘계학술대회, 2002.

[6] Cacciabue, P. C.; "Human factors impact on risk analysis of complex systems," *Journal of Hazadous Material*, 71 : 101-116, 2000.

[7] Felix Redmil and Jane Rajan; Human Factors in Safety-critical Systems, Reed Educational and Professional Publishing, pp. 120-141, 1997.

[8] Harmsen, M. S.; "A design method for prodct safety", *Ergonomics*, 33(4) : 431-437, 1990.

[9] Liu, T. S. and Chiou, S. B.; "The application of Petri nets to failure analysis", *Reliability Enginering and System Safety*, 57 : 129-142, 1997.

[10] Peterson, J. L.; *Petri Net Theory and the Modeling of Systems*, Prentice Hall, Inc., 1981.