시스템 이론 기반의 안전사고 모델의 해석과 응용사례 소개

박 철 호*1), 박 영 원2)
아주대학교 시스템공학과

An Introduction to Systems Theory Approach to Accident Modeling and Its Applications

C. H. Park* and Y. W. Park**
1) 2) *Institute For Advanced Engineering, Systems Engineering Lab, 633-2 Koan-Li Baekam-Myon Youngin Kyunggi-Do 449863 South Korea*

Abstract : This paper presents the general system theory and its applications to the safety analysis method that is a recent trend over the traditional event-driven model. This new model is known as STAMP(Systems Theory Accident Modeling and Process) proposed by Nancy G. Leveson in MIT. The new model has benefits of systemic approaches concerning the system safety as a whole including the context it is in, its stimulants and outcomes, and its parts as well as the relationships among them in a holistic manner. The method consists of a hierarchical control structure, a process model, and the safety constraints governing the control. This paper demonstrates an example that contrasts the differences between the approaches of STAMP and the traditional safety models.

Key Words : STAMP, Systems Theory, System Safety, Safety Model

1. 서 론

시스템 안전모델은 오랜 기간동안 산업적인 기반을 두고 산업의 요구에 따라 발달해 왔다. 그러나 빠른 기술 변화, 디지털 기술로 인한 사고의 양상 변화, 항공 교통 제어와 같이 새로운 형태의 위험(hazard) 대두, 시스템의 복잡성 및 연계성(coupling)증가, 복잡해진 인간과 자동화 기술과의 관계 등으로 인해 기존의 이벤트 기반 안전 모델들의 한계가 두드러지기 시작했다.

기존의 시스템 안전분석 기법은 시스템의 개념설계 단계에서 정성적이고 포괄적인 개념을 통해 이루어지는 분석 기법과 주어진 재해를 이벤트 기반의 모델로 추적하는 분석 기법으로 크게 나눌 수 있다. 전자의 안전분석 기법은 예비 위험분석(Preliminary Hazard Analysis)이나 고장형태 영향분석(Failure Mode and Effect Analysis) 등이 대표적이다. 이러한 안전분석 기법은 주로 시스템 개발 초기 가능한 위험요소들을 판단하기 위해 중요하나 하부수준 계층과의 연관성을 보기 위해 구체적인 분석 기법이 필요하다. 따라서 필요한 것이 모델 기반의 안전분석 기법인데 이것은 이벤트 수목 분석(ETA), 고장수목 분석법(FTA), 시스템 안전성 위험분석(SSHA) 등이 있다.

* eastblotting@paran.com

2. 안전모델의 개선

2.1 기존 안전모델들의 한계

전통적으로 모델 기반의 안전분석 기법들은 이벤트 기반의 모델들이 대부분이었다.(Fig.1)

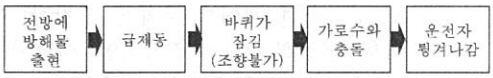

Fig.1 이벤트 모델 예제

이러한 이벤트 모델 작성 후 각 이벤트에 대해 이벤트를 억제할 수 있는 방안을 모색한다. 이벤트 기반 모델은 하나 이상의 물리적 컴포넌트의 오작동으로 인해 전체 시스템의 실패나 위험이 초래되는 경우에 좋은 효과를 볼 수 있다.

그러나 이러한 모델들은 시스템의 가장 낮은 수준의 거동에 관심을 두기 때문에 시스템적인 접근이 제대로 이루어지지 않는다는 단점이 있다.

이러한 단점을 극복하고 시스템적인 접근을 이루기 위한 개선책이 다양하게 연구되고 있다. 고장수목 분석법(FTA)에 운영/관리적인 요소를 결합하려는 Johnson's Model이나 이벤트 모델에서 각 이벤트가 일어나게 되는 조건(condition)을 분석하여 중간 모델을 만들고 그러한 조건을 가능케 하는 시스템 요소를 찾는 Leveson's Three-Level Model 등이 그것이다. 그러나 이러한 노력들은 이벤트 기반의 모델의 한계를 크게 벗어나지 못했다.

2.2 개선이 필요한 사항

(1) 사회, 조직적인 요소를 고려

이벤트 기반 모델은 조직/기관의 구조적이거나 관리적인 측면의 결여, 또는 안전 의식이나 문화 관습적 결점 등과 같은 숨겨진 시스템 주변정황 요소들의 발견에 부적합하다.

(2) 시스템 사고의 표현

시스템 사고(System Accident)는 2차 세계대전 이후에 새로이 부각된 사고의 형태로서 개개의 컴포넌트 오작동이 아닌 컴포넌트 간의 상호작용에 의해 발생하는 형태의 사고이다. 화성탐사선, MPL 실종 사건과 같은 경우, 개개의 컴포넌트들은 설계자가 의도한대로 정확히 작동하였으나 상호작용의 불일치로 인해 발생한 사고이다. 시스템 사고에서 에러는 개개 컴포넌트의 문제가 아닌 컴포넌트의 상호작용에 의해 나타나는 창발성(emergent property)의 결과이므로 이러한 문제는 시스템적 접근방법으로 해결할 수 있다.

(3) 인간 과오의 반영

인간 과오는 "미리 결정되고 구체화된 일련의 행위 수준에서 발생하는 편차"로 정의된다. 이러한 인간 과오는 단순한 실수뿐만 아니라 특정 상황에서의 잘못된 의사결정을 포함한다. 대구 지하철 참사에서 화재가 전선의 합선을 통해 확산되리라는 추측 하에 전원 공급을 끊어버린 것이 더 엄청난 결과를 초래한 잘못된 의사결정의 예이다.

2.3 시스템적인 접근

일반 시스템 이론은 초기 이론생물학에서 발생하였고 30~40년대 복잡한 시스템의 개발이 증가함에 따라 전통적인 분석 기법의 한계에 부딪히면서 주목받기 시작했다.

시스템은 복잡성과 무작위성을 기준으로 생각할 때 Fig.3에서와 같이 3가지 영역으로 나누어 생각할 수 있다.

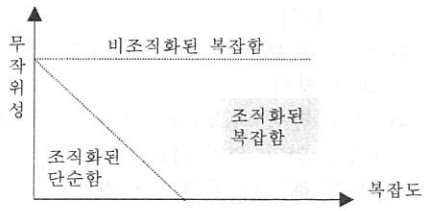

Fig.3 시스템의 3가지 영역

"조직화된 단순함"은 무작위성이 매우 낮고 상호작용이 적은 형태의 시스템이다. 이와 같은 형태의 시스템은 분석적인 접근이 필요하다. 이에 반해 "비조직화된 복잡함"은 무작위성이 매우 높고 상호작용도 많은 경우이며, 이러한 경우는 거시적인 관점의 통계학적인 접근

이 유용할 때가 많다.

문제는 "조직화된 복잡함"의 성격을 가지는 시스템으로서 이러한 시스템은 분석적인 접근을 취하기에는 너무 복잡하고 통계적인 접근을 취하기에는 너무 조직화되어 있다. 이러한 형태의 시스템을 위해 일반 시스템 이론이 제안되었다.

일반 시스템 이론에 따르면 모든 인위적 시스템은 "계층적 구조와 창발성(Emergent Property)", "의사소통(communication)과 제어(control)" 특성들이 쌍을 이루며 발생되어 개발된다. 즉 계층적 구조가 존재하면 그에 따르는 창발성이 항상 나타나야 하고, 제어가 이루어지기 위해 되먹임(feedback)에 의한 의사소통이 뒤따라야 한다는 특성이 일반 시스템의 공통적인 특성이라는 이해이다.

따라서 이러한 시스템의 특성에 기반한 "시스템적인 접근 원칙들"은 다음과 같다.

(1) 전체를 보고 접근하는 사고 체계
(2) 컴포넌트보다 상호의존 관계를 보는 생각
(3) 시간의 단편보다 수명주기 상의 변화 양상을 보는 생각

이상의 기본적 접근원칙 들을 통해 얻어진 시스템엔지니어링 엔진 프로세스는 시스템안전 확보 시스템의 정의를 위해 다음과 같은 활동을 요구한다.

(1) 안전 확보 시스템의 요구사항 및 제약사항 해석
(2) 안전 확보 시스템의 기능 아키텍처와 거동분석
(3) 안전 확보 시스템의 물리적 아키텍처 대안 정의
(4) 안전 확보 시스템의 전 수명주기에 걸친 효과성을 얻기 위한 (1)~(3) 단계별 정량적 또는 정성적 해석과 아키텍처 최적화

3. STAMP 이론

3.1 STAMP 소개

위와 같은 시스템적인 접근을 위해 MIT 공과대학의 Nancy G. Leveson에 의해 제안된 기법이 STAMP이다. 이 기법에서 사고는 부적절한 제어나 안전 관련 제약사항들이 존재하거나 필요한 제약사항을 미 이행 함 으로서 발생한다고 이해된다. 제약사항의 이행 여부 역시 제어의 문제이다. 이벤트 기반의 안전분석은 사고 발생에 대한 현상을 쫓는데 반해 사고와 관련된 제어 구조를 추적하는 STAMP 기법은 시스템적인 원인을 찾는데 주력하는 것이다.

그리고 이러한 제어의 문제를 고찰할 때에는 앞에서 언급한 "사회/조직적인 맥락의 요소"를 고려하기 위해 주목하는 시스템과 관련된 계층적인 제어 구조를 전체적으로 파악해야 한다.

또한 시스템적 접근에서 요구하는 "변화의 양상"을 파악하고 이와 "시스템의 제어"가 부합되는지를 파악하기 위해 STAMP 기법에서 강조하는 것이 프로세스 모델이다.

따라서 STAMP 기법에서 요구하는 3가지 필수요소는 다음의 3가지로 요약될 수 있다.

(1) 제약사항
(2) 계층적 제어 구조
(3) 프로세스 모델

위의 안전 관련 제약사항은 전체적으로 파악된 계층적 제어 구조의 모든 컴포넌트에서 기술되어야 하며 또한 모든 수준의 계층에서 프로세스 모델이 작성되어야 한다.

첫 번째 단계로 물리적인 프로세스 과오와 그러한 과오를 초래하게 된 역기능들을 분석한다. 그 다음 낮은 수준의 컴포넌트부터 Table.1의 분석을 행한다. 이 분석 항목들은 사고 또는 부적절한 제어에 대한 시스템적인 분석을 행하기 위해 선정되었다. 특히 "감성 모델의 오류 식별"은 인간 과오를 분석에 반영하기 위한 항목이다.

	분 석 항 목
1	문제가 되었던 안전 관련 제약사항을 식별
2	부적절한 의사결정 및 제어행위 식별
3	감성 모델 오류 식별(부주의, 미인지, 등)
4	역기능적 상호작용 식별
5	정황 / 그리고 조정(coordination)의 오류

Table.1 분석항목

3.2 안전확보 시스템 설계와 STAMP 비교 해석

안전 확보 시스템의 개념은 대상 시스템의 안전 확보를 위해 부가적 시스템을 추가하여 개발하므로서 정의 된다. 이때 수행하는 개발 프로세스가 시스템엔지니어링 프로세스를 따른다면 대상 시스템의 설계와 개발 시에 누락된 요구사항 또는 제약사항들을 요구사항 분석 시에 식별한다. 대상시스템이 여러 정황 속에서 운용하면서 발생하는 위협요소, 고장영향 등이 사고의 위험요인으로 작용하지 않도록 안전 확보 시스템의 설계가 식별된 요구사항들과 제약사항들을 만족하도록 수행되어야 한다.

STAMP에서 요구되는 세 가지 필수요소들을 안전 확보 시스템 설계를 위한 시스템엔지니어링 프로세스 결과물 관점에서 관찰하면 다음과 같이 비교하여 해석 할 수 있다

	STAMP	안전확보 시스템
1	제약사항	총 순기 안전요구사항
2	계층적 제어구조	운용 상세설계 및 구축
3	프로세스 모델	운용, 정비 및 지원 프로세스

Table.2 Analysis for STAMP의 필수 요소 해석

STAMP 기법을 이상과 같이 안전확보 시스템 설계와 개발의 접근적 시각에서 해석 할 경우 더 완벽한 시스템적 접근을 시도 할 수 있다. 시스템엔지니어링의 모든 프로세스, 방법 및 도구들을 활용 한 안전확보 시스템의 설계 구축과 운용/정비/지원이 가능하며 부수적으로 STAMP 기법의 결과물 들이 얻어 진다.

3.3 STAMP 적용 사례 소개

3.3.1 배 경

걸프전 이후 북부 이라크의 산악지대로 피난한 수십만의 피난민들을 구제하기 위한 인도주의적 노력으로 창설된 OPC는 피난민 및 구제사업에 종사하는 외국 민간인들을 보호하고 군사 우세 확보를 위해 이라크 북위 36도 이상의 상공영역을 "비행금지구역(No-Fly-Zone)"으로 설정하고 미확인 항공기에 대한 감시를 실시했다. 따라서 통상 "비행금지구역"내의 인가된 항공기는 주로 초계임무를 맡는 미공군의 고정익기와 지원작전을 수행하는 미육군의 회전익기였다.

3.3.2 사 건

위와 같은 배경하에 작전 수행 후 약 3년째 되는 1994년 4월 15일 2대의 미육군 소속의 블랙호크 헬기가 2대의 미공군 소속의 F-15 전투기에 의해 격추되었다. 이 사고로 15명의 민간인과 11명의 다국적군 장교 등이 전원 사망하였다.

3.3.3 이벤트 기반 분석

이벤트 기반의 전통적인 안전분석 모델로 사건을 분석하여 보면 Fig.4와 같이 간략히 분석될 수 있다.

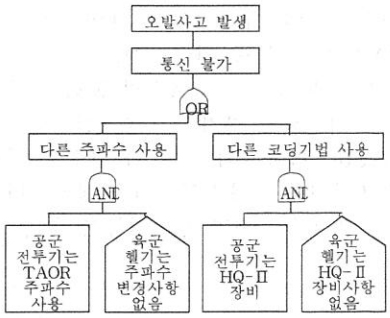

Fig.4 예제의 고장수목도(Fault Tree)

위의 분석을 보면 격추되는데 직접적인 원인을 제공한 "통신 불가"라는 이벤트가 발생하는데 필요한 이벤트들을 분석해 나가게 된다.

3.3.4 STAMP 적용

위의 예제를 보면 쉽게 오발사고의 원인을 알 수 있지만 좀 더 깊이 고찰하면 미공군과 육군의 통신제어에 대한 더 전체적이고 구조적인 수준의 사건 언급은 빠져있음을 알 수 있다.

STAMP를 따르기 위해 위 예제에 대한 제어 구조를 간략히 소개하면 Fig.5와 같다. 이와

같은 계층적 제어구조를 파악한 후에 이를 구성하는 각 컴포넌트들의 역할에 따른 안전 관련 제약사항과 그에 따른 제어활동을 분석한다.

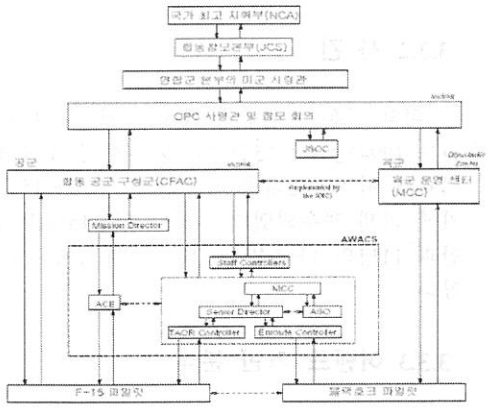

Fig.5 예제의 계층적 제어 구조

Fig.5를 보면 우리가 분석하고자 하는 시스템과 상호작용하는 최고 제어구조까지 고려하고 있다. 이와 같은 모든 제어구조의 파악이 STAMP의 특징 중 하나이다.

그 다음 사고 프로세스의 물리 수준에서 물리적 과오와 역기능 상호작용을 분석한다.(Fig.6) "미사일의 발사"가 가장 직접적인 상호작용이지만 의사소통분석을 통해 "미사일 발사"를 막지 못한 4가지 역기능을 찾을 수 있다.

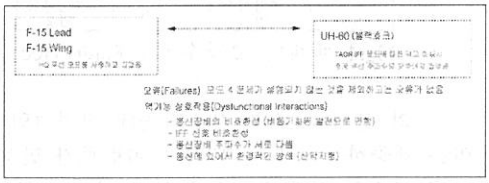

Fig.6 사고 프로세스의 분석

그리고 Fig.5에 나타난 사고에 관련된 전체 계층적 제어구조를 모든 수준에 대해서 Table.1의 분석 항목을 이용하여 분석한다.(Fig.7)

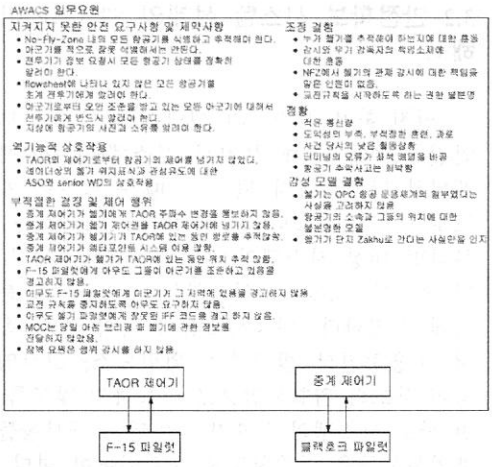

Fig.7 제어 레벨의 분석 예(AWACS↔파일럿)

4. 결 론

본 연구에서는 기존 안전분석 기법들의 한계점을 고찰하고 일반 시스템 이론에 근거한 새로운 시스템 안전 접근 방법인 STAMP방법을 소개하였다. 시스템 공학 및 일반 시스템 이론은 전에 없었던 새로운 과학적 법칙으로 구성된 것은 아니다. 그러나 우리 주변에 산재해 있고 느끼고 있으나 객관적이고 일관성있게 파악하지 못한 시스템의 공통적인 특성을 파악하여 막연히 더 잘하는 방식이 아닌 체계적인 접근을 시도할 수 있는 발판을 마련한다는 점에서 매우 유용하다. 본 연구는 시스템적 접근방법이 오랜응용을 통해 성숙되어 있는 시스템엔지니어링 기본 프로세스를 적용하여 안전확보 시스템을 개발 할 경우 STAMP 기법을 보다 성숙 시킬 수 있음을 암시 한다. 그리고 그런 시스템적인 접근방법에서 사고(accident)를 보는 시각을 새롭게 정의한다는 측면에서 STAMP 기법과 안전확보 시스템은 그 의미가 있다.

우리 사회의 시스템 안전 문제는 이미 여러 번 강조되어 왔다. 사회/과학, 군사 등의 대형 시스템에 안전분석 모델의 하나로서 도입되어 체계적이고 총괄적인 시스템 안전이 이루어져야 할 것이다.

참 고 문 헌

1. Nancy G. Leveson, "A New Approach To System Safety Engineering," 2002
2. 제무성, 정재희 공저, *시스템 안전공학 개론*, 신광문화사, 서울(1999)