하향식 모델링 기법을 적용한 위험 분석 사례 연구

Studies of Case on Hazard Analysis Applying Top-Down Modelling Technique

홍선호* **홍순흠****

Hong, Seon-Ho **Hong, Sun-Hum**

ABSTRACT

A technology for inevitable integration as well as an ability of development of technology according to professional fields is needed and supported for securing technology in the era of international competition. In other words, advanced business technique and technology applied for streamlining of management are required and the relations between operations and systems could be clarified. This paper reviews the course for development of process used in the systems engineering and business administration and tries to seek the way of training professionals in a variety of fields for elevating domestic technologies in different fields to the international level. Particularly, it tries to get the way of overcome the present technical restriction that depends on imports through matching a hazard analysis method with the method above mentioned.

Especially, it tries to present the way of contributing to securing software safety on the basis of the importance of development of process model that takes the lfe cycle into consideration.

1. 서 론

국제 경쟁 시대에 요구되는 기술 확보를 위해서는 전문분야별 기술개발 능력과 더불어, 필수적으로 통합에 요구되는 기술 또한 반드시 뒷받침이 되어야 한다. 즉 경영의 합리성을 도모하기 위하여 적용하고 있는 선진 경영기법과 기술이 요구되어지며, 이를 기반으로 운영과 시스템간의 관계를 명확하게 할 수 있다. 본 논문에서는 시스템엔지니어링 또는 경영학 과정에서 사용되어지는 프로세스 개발과정을 검토하고, 국내 분야별 기술을 국제적인 수준으로 높이기 위한 다양한 분야의 전문가 인력의 양성 방안을 모색해보고자 한다. 특히, 최근 이슈화 되어지고 있는 위험분석방법을 상기 방법론과 매칭시키므로서 수입에 의존하고 있는 현재의 기술 제약사항을 극복할 수 있는 방안을 도출하고자 한다.

특히 생명주기를 고려한 프로세스모델 개발의 중요성과 이를 기반으로 하는 소프트웨어 안전성 확보에 기여할 수 있도록 하는 방안을 제시하고자 한다.

* 한국철도기술연구원, 철도종합안전기술개발사업단, 선임연구원
E-mail : shhong@krri.re.kr
TEL : (031)460-5542 FAX : (031)460-5509
** 한국철도기술연구원, 철도운영연구팀, 책임연구원

2. 시스템 모델과 위험분석

2.1 시스템에 대한 공학적 개념 정의

자동화된 시스템이나 사람의 입력은 물질계의 에너지의 파동을 아나로그로 받아 디지털로 전환한다. 컴퓨터나 사람의 뇌는 논리적인 판단을 한다. 컴퓨터나 사람의 출력은 디지털을 아나로그로 변환하여 물질계의 에너지 파동으로 변환시킨다. 즉, 에너지의 파동을 관찰하는 업무가 일의 시작이며, 에너지의 파동을 제어하는 업무가 일의 종료이다. 즉 제어 대상 에너지를 먼저 분류하면 자연현상의 종속관계의 업무가 드러나게 된다. 어떤 에너지를 제어해서 또는 다른 에너지와의 조화를 통해 고객이 원하는 업무를 제공할 것인가가 시스템엔지니어의 역할이라고 할 수 있다.

즉, 존재하는 지구와 우주는 상기 에너지를 일부 가지고 있으며, 인간은 이를 관측하여, 에너지의 성질 로부터 크기 변환을 이해, 상태로 판정하므로서, 다른 연계된 에너지 기능 과의 인터페이스 관계를 통해 효율적으로 해당 물건을 제어하며, 결과적으로 이익을 창출되어질 수 있다.

에너지는 6가지의 기계, 열 , 빛, 화학, 전기, 원자에너지 등과 같은 기본형태를 가지고 있다. 이 중에서 기계, 열, 전기, 화학에너지는 다이빙 도중에 흔히 접하게 되는 에너지의 유형들이다. 그밖에도 일상생활에서 날씨 변화조차, 소리, 추위, 열 등의 여러 가지 현상으로 에너지를 인식할 수 있다.

2.2 기능과 가치 사슬

기능은 구조, 즉 형태와 밀접한 연관이 있다. 부분의 기계적 집합으로서의 구조 전체에 대해서는 부분의 활동은 전체의 상태에 대응하며, 수학에서 한 변수(變數)와 다른 변수 사이에 성립하는 함수관계의 뜻으로 통한다. 반대로 구조 전체가 부분의 목적이 될 때에는 유기적 구조에 대한 부분, 곧 “기관(器官)의 합목적적인 활동이라는 뜻”이 된다.

유기적인 전체의 요구와의 대응관계에 있어서 구성요소의 활동이라는 의미에서는 생물체에 대한 기능분화와 기능전환, 의식활동에 대한 심적 기능, 사회구성에 대한 기능사회나 기능적 체계 등을 말한다. 19세기 이래, 과학적인 사고방식은 형태로서의 정적 구조보다는 동적 기능을 존중하는 기능주의적 경향을 택하였다. E.카시러는 이를 '실체개념(實體槪念)에서 기능개념으로의 전향'이라고 하였다.

기업경영의 경쟁력 강화를 위한 PI(Process Innovation)에서 그 시발점을 찾을 수 있다. 21세기 기업의 생존력을 보장받기 위한 다양한 노력 중에 하나로 원가절감, 프로세스효율화 그리고 고객만족 극대화를 목적으로 한다. 가치사슬(value chain)이란, 기업 활동에서 부가가치가 생성되는 과정을 의미한다. 1985년 미국 하버드대학교의 마이클 포터(M. Porter)가 모델로 정립한 이후 광범위하게 활용되고 있는 이론 틀이다. 부가가치 창출에 직접 또는 간접적으로 관련된 일련의 활동·기능·프로세스의 연계를 의미하고 있다. 가치라는 것은 수행성과 대비 비용을 의미한다. 즉, 같은 성과를 내더라도 비용이 덜 투입된 쪽이 보다 가치가 있는 것이다. 이는 미국 생산재고 관리협회에서 제시하고 있는 가치에 대한 제조관점의 개념이다. 기업은 가치사슬에 대한 분석을 통하여 가치 활동 각 단계에 있어서 부가가치 창출과 관련된 핵심활동이 무엇인가를 규명할 수 있다. 또한, 각 단계 및 핵심활동들의 강점이나 약점 및 차별화 요인을 분석하고, 나아가 각 활동단계별 원가동인을 분석하여 경쟁우위 구축을 위한 도구로 활용할 수 있다

2.3 안전성 분석과 기능의 관계

Argyris는 조직이 필요로 하는 투입 자원으로는 기계적 에너지(mechanical energy), 인간 생리적 에너지(human physiological energy; 의식주 욕구), 인간심리적 에너지(human psychological energy)의 3가지 가 있으며 심리적 에너지는 개인의 심리적 성공(psychological success)의 경험이 많을수록 증가하는데, 전통적 조직은 심리적 성공의 경험과 역행하는 작업환경을 조성한다고 주장한다. 즉 조직 목표의 성취를 위해 지시·통제·처벌의 수단을 동원하는 관리방식은 심리적 성공의 경험 을 추구하는 구성원의 욕구와 배치되며, 이러한 전통적 조직관리 풍토 속에서 구성원은 상부지 시에의 의존·생산량의 고의적 하향 조정·작업진도의 지연·결근·이석 등 수동적 적응행동 (adaptive behavior)을 나타냄으로써 생산성의 저하를 초래한다는 것이다. 이러한 과정이 시간 이 흐르면서 반복되고 강화되는 현상을 악순환이라 부른다.

3. 철도교통 분야 안전성 활동 적용 방안

상기에서 정의한 바와 같이 기능 즉, 합목적적인 활동을 적용하기 위해서는 대상 철도기관의 목적으로부터 규명하여야 한다. 이 경우 가치사슬의 대표적인 분류 방법인 Inbound , Operation , Outbound, 마케팅, 서비스의 임의의 활동 경계가 요구되어지며, 하위 기능은 에너지 또는 재료를 경계로 하여 전개시 중복되지 않는 기능 전개가 가능해진다.

3.1 기능 기반의 안전성 분석 프로세스

3.1.1 분해

분해는 상위 기능에 요구되는 하위 기능을 도출하는 과정이다. 3-6개의 하위 기능으로 분해되어 질 수 있으며, 원자성 활동이 정의되어질 때 까지 계속적으로 분해되어야 한다.

3.1.2 기능들의 관계의 규명

상위 기능으로부터의 전개시 명령과 제어의 관계를 명확히 하여야 한다. 이는 각 객체의 종속관계와 더불어 거래관계를 정의 하므로서 개념 데이터모델의 개발에 활용되어지기 때문이다.

3.1.3 프로세스 시나리오의 전개

상기 분해와 관계의 규명으로부터 정의된 모델은 작성자의 생각을 정적으로 표현한 것이다. 따라서, 이를 동적으로 표현하는 시나리오 전개가 필요하다. 이때 패터리넷, 상태전이 모형 등과 같은 순차적인 흐름을 도출할 수 있는 모델이어야 한다.

3.1.4 위험분석

시나리오 모델로부터 높은 리스크가 발생가능한 이벤트 분기점들을 찾아내어 크리티컬한 지점을 식별하여야 한다. 이때 리스크 매트릭스가 적용되어질 수 있다.

3.1.5 프로세스 시나리오의 개선

상기 절차에 따라 도출된 높은 위험이 분기되는 조건을 기반으로 대안이 도출되어질 수 있으며, 이

대안으로부터 시나리오의 개선으로 해당 위험에 대한 전략이 결정되어질 수 있다.

상기 처리절차는 전형적인 시나리오의 개발절차이며, 특히 분산처리시스템의 경우, 기능과 기능간 다양한 조건들의 관계가 도출되어진다.

3.1.6 피드백

피드백은 상기 이벤트 정의 과정을 기반으로 하는 전형적인 절차에 따른 문제를 식별할 수 있는 교정활동이다. 이는 단순히 개념분석 단계에서 이루어지는 활동은 아니며, 현실과의 만남을 통해 더 높은 품질을 공급자로부터 제공받을 수 있기 때문이다.

3.2 안전성 활동과 현실의 접목

현실에서 안전성 활동을 적용하기 위해서는 사건(Event)에 대한 개념이 등장하게 된다. 사건이란 실세계에서 발생하는 시간과 공간을 점유하는 의미 있는 일로서 정의되어질 수 있으며, 상태머신의 문맥에서는 사건을 이용하여 자극이 상태전이를 발생시키는 행위를 모델로 작성된다.

사건의 종료는 시스템 내부의 오브젝트 간 발생하는 사건을 내부사건으로 정의하며, 시스템과 수행자간 발생하는 사건을 외부사건으로 정의할 수 있다.

이렇게 역할 과 활동에 근거하여, 어떤 역할이 특정 활동을 수행한다는 것을 규정할 수 있다. 또한 이러한 활동은 상호작용으로서 활동 및 상호작용의 순서가 표현될 수 있으며, 사건을 정의하므로서 안전 요건이 도출되어진다.

안전 요건이란 변경을 통하여 야기된 안전 리스크가 수용할 만한 수준으로 감소되었다는 것을 확인하기 위해 충족되어야 하는 요건을 뜻한다. 안전 요건은 다음 사함을 지정할 수 있다.

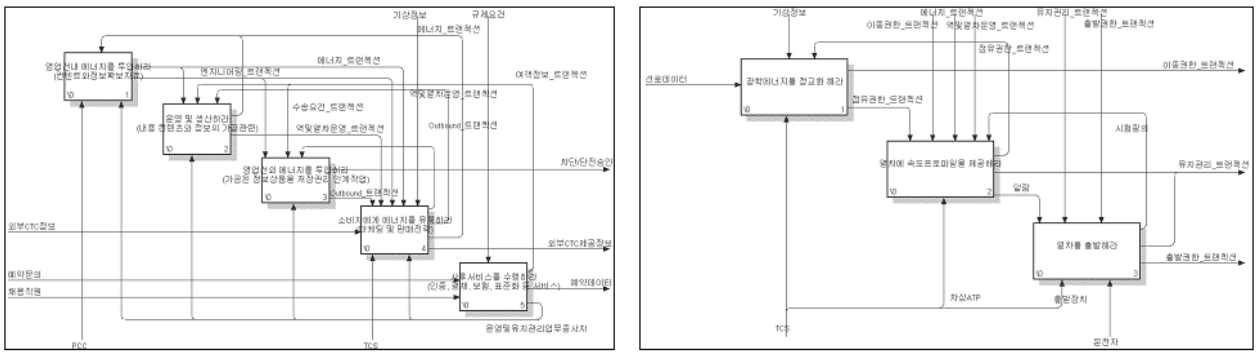
- 사람들의 위험한 실수를 방지하는 데 도움이 되는 변경의 특징 및 기능
- 안전성을 위해 변경 사항이 해당되어서는 안 되는 사항
- 변경 사항이 안전하게 진행될 수 있는 환경적 조건
- 기능을 신뢰성 있게, 또는 위험한 상황을 피하면서 신뢰성 있게 수행하려는 목표
- 설계 특성 및 공정
- 운영 절차 및 제약 사항

즉, 이러한 피드백 활동이 지속적으로 이루어지며 다시 시스템에 해당 요구사항이 반영되어지는 체계의 구축이 필요하다고 할 수 있다.

4. 기능 분해 사례

철도시스템의 기능은 역 공학 과정을 수행하여 정의할 수 있다. 즉, 기존 기능을 모델링 하여 현실에서의 사건과의 관계를 설정하므로서 위험에 대한 근거를 식별할 수 있으며, 이를 기반으로 Systematic 한 접근이 가능해진다. 따라서, 이러한 기능분석기술은 선진국으로 도입할 수 있는 초석이라고 할 수 있다.

따라서, 철도운영과 관계된 사례모델을 소개하고자 한다.



<a> 철도를 운영 기능모델 <b> 열차를 운영 기능모델

<그림 1> 철도 기능 모델 사례

상기 모델은 상위 단계의 모델로서, 마지막 단계의 모델 전개까지의 진행이 요구되어지며 이를 기반으로 다음 단계인 프로세스 시나리오의 작성이 가능해진다. 이들 프로세스 모델은 해당 분야의 전문가 간의 의사소통의 수단으로서 사용되어지며, 결국 개선되어지는 모델의 품질은 시스템의 가용성과 안전성 수준의 판정시 사용되어질 수 있다.

더불어 소프트웨어의 핵심인 운영의 규칙을 설명하므로서, 소프트웨어 엔지니어의 디자인 단계에서 기인되는 오류를 예방할 수 있을것으로 판단되어진다.

5. 결 론

이상과 같은 기능 및 프로세스, 그리고 피드백의 과정은 선진 경영시스템의 기본이 되며, 국가/운영자/공급자/연구자 의 관계를 명확히 함으로서 사용자를 위험으로부터 보호하고, 이를 기반으로 자연스러운 기술 육성이 접목되어지는 최적의 방안이라고 할 수 있다.

본 논문에서는 시스템엔지니어링 또는 경영학 과정에서 사용되어지는 프로세스 개발과정을 검토하고, 국내 분야별 기술을 국제적인 수준으로 높이기 위한 다양한 분야의 전문가 인력의 양성방안을 모색해보고자 하였다. 특히, 최근 이슈화 되어지고 있는 위험분석방법을 상기 방법론과 매칭시키므로서 수입에 의존하고 있는 현재의 기술 제약사항을 극복할 수 있는 방안을 도출하였다.

특히 생명주기를 고려한 프로세스모델 개발의 중요성과 이를 기반으로 하는 소프트웨어 안전성 확보에 기여할 수 있도록 하는 방안을 제시하였다.

감사의 글

이 연구는 국토해양부 지원으로 수행되고 있는 철도종합안전기술개발사업의 일환으로 수행되었습니다.

참고문헌

1. 홍선호,조연옥 외 (2007년), “철도안전성평가및분석프로그램개발에 관한 연구”, 한국철도기술연구원
2. 한국철도공사, CTC 운영매뉴얼
3. Railway Britich, Yellow book