

# 시스템 공학 기법에 의한 전기안전시스템 체계 개선에 관한 연구

신 흥 식\* · 이 재 천\*\* · 이 병 길\*\*

\*전기안전연구원 · \*\*아주대학교 시스템공학과

## On Improving the Electrical Safety Systems based on the Systems Engineering Method

Heung Sik Shin\* · Jae Chon Lee\*\* · Byoung Gil Lee\*\*

\*Korea Electrical Safety Research Institute

\*\*Dept. of Systems Engineering, Ajou University

### Abstract

In this paper we discuss the problems related with the existing electrical safety system that is influenced by all the socio-technical factors including the electrical safety law, government organizations, and their practicing rules and regulations. Sometimes intangible practices also affect the safety issues. It is our intention to incorporate all those factors effectively and systematically in improving the electrical safety system. Since, the problem in nature is so complex, an approach based on the systems engineering (SE) method could be a good candidate. Specifically, as a first step of the SE process we performed the requirements analysis of all the factors mentioned above and some recommendations from the experts in the field. In the work environment utilizing a computer-aided SE tool, the requirements are verified and managed efficiently although the data base is complicated in general in tracking the changes. Next, by analyzing the verified requirements, a functional architecture is developed to achieve an improved electrical safety system.

We also did the reverse engineering of the existing electrical safety system to explore potential problems there. The result can also help improve the existing one. Overall, a systematic approach to constructing electrical safety system based on SE is proposed for the first time in this paper. Note that the method described here can be adopted in the study of other safety systems.

Keywords : Electrical Safety Systems, Systems Engineering, Requirements Analysis and Management, Functional Architecture

### 1. 서 론

최근 삼성전자 기흥 반도체 공장에서 정전으로 6개 라인이 동시에 가동 중단되는 초유의 사태가 벌어지고, 현대자동차 울산 엔진 공장 옥상에서는 화재가 발생했다. 안전을 제1의 가치로 여기는 우리에게 시사하는 바가 적지 않다.

이들 사고를 타산지석으로 삼아 유사 사고가 재발하지 않도록 사전 점검 등에 만전을 기해야 할 것이다.

사후약방문보다는 사전예방이 귀중한 인명과 재산을 보호하는 데 가장 효과적임은 아무리 강조해도 지나치지 않다. 국민기업으로 불리는 삼성전자와 현대차 공장에서 각각 정전과 화재가 발생했다는 것은 참으로 충격적이지 않을 수 없다.

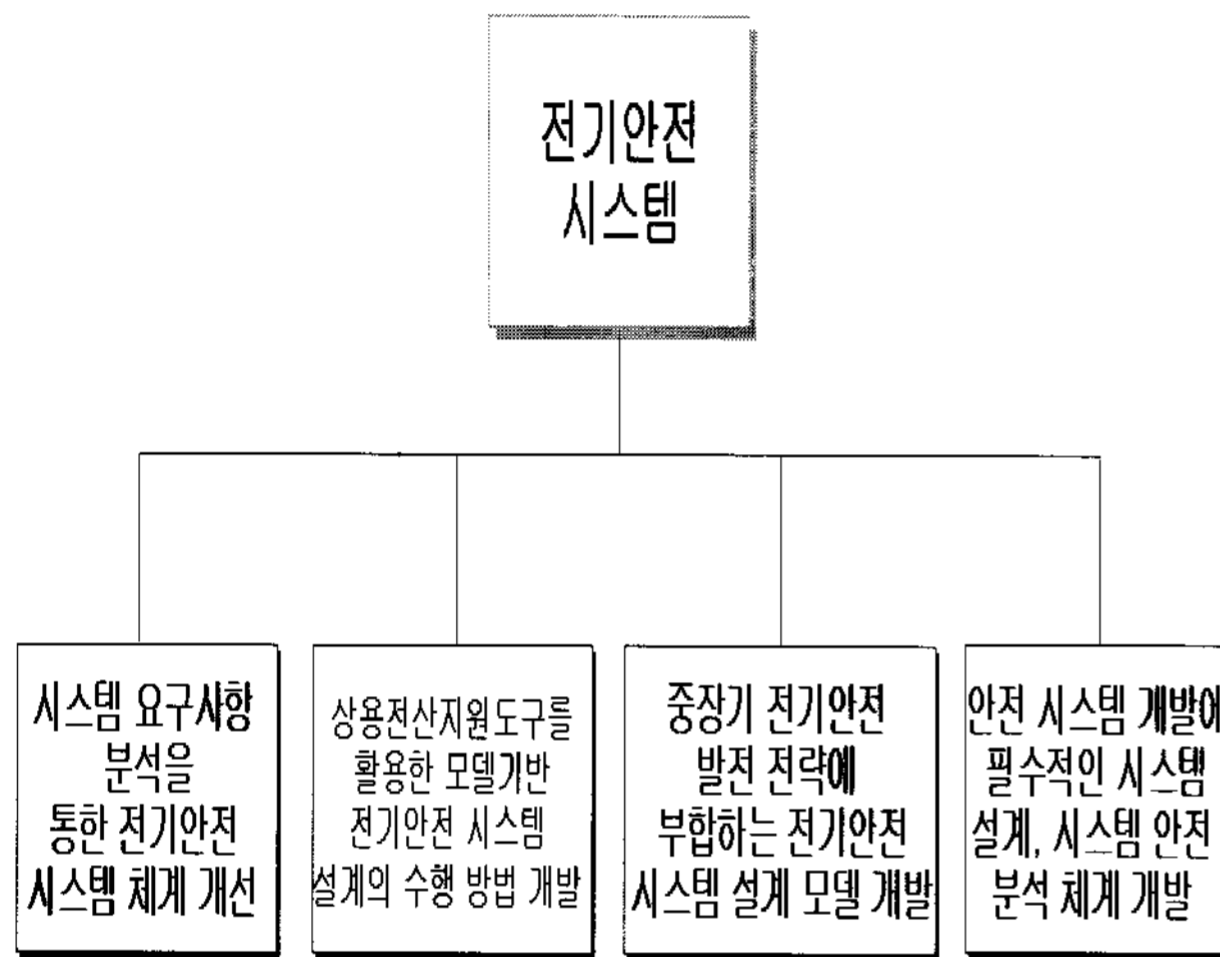
세계 유수의 기업들과 어깨를 나란히 하는 두 기업에서 이런 사고가 일어난 것은 해당 기업의 막대한 손실뿐 아니라 국가 경제에도 상당한 충격을 준다.[1~3]

최근 우리나라에서 자주 발생하고 있는 대형 참사들을 지켜보면서 이들 사고의 발생을 방지하기 위해 안전한 시스템 개발을 위한 시스템엔지니어링의 도입이 절실하다는 사실을 깨닫게 되었다. 시스템엔지니어링의 수많은 분야 중에서 특히 안전과 관련된 요구사항을 적절히 도출해내고 요구사항에 적합한 시스템이 개발되었는지 검증하는 구체적 방법을 모색해야 할 필요성이 대두된 것이다.

본 논문의 목표를 정리하면 다음과 같다.

선행 연구결과물을 통한 전기안전시스템의 요구사항 정리.  
 전기안전시스템의 수명주기와 관련된 이해 당사자 식별.  
 표준을 통한 시스템 생명주기를 고려, 개념, 설계, 구현의 부분을 상세화.  
 안전과 관련된 표준을 정리, 전기안전에 고려 항목 개발.  
 표준 절차를 따라 전기안전시스템이 가져야 하는 요구사항 분석.  
 전기안전시스템 전문가와 운영요구사항 개발.  
 시스템 생명주기 전기안전시스템을 개선하는 프로세스 개발.  
 개선 프로세스의 시뮬레이션을 통하여 운용상 누락된 부분이 없는지를 확인.  
 안전시스템이 가져야 하는 속성을 표로 정리.

<그림 2> 전기안전 프로세스 정립



<그림 1> 전기안전시스템 목표

논문의 목표를 달성하기위한 연구절차는 현행 전기안전시스템의 개선안을 시스템엔지니어링 기법으로 리엔지니어링하여 전기안전시스템 개선안과 시스템엔지니어링 기법을 안전 규격인 MIL-STD-882C와 FAA Safety HandBook의 안전 목표로 정리하여 비교하였다.

리엔지니어링 하기위해 선행 연구 결과인 전기안전시스템 개선안 도출 방법을 시간순서로 정리하고, 시스템엔지니어링 절차와 비교하여, 선행 연구 결과에 누락된 부분을 찾았다.

선행연구결과에서 누락된 부분은 아래와 같다.

- (1) 시스템의 수명주기의 고려가 부족하다.
- (2) 표준 프로세스의 고려가 이루어지지 않았다.
- (3) 개선안 도출에서 시스템을 지원하는 환경에 대한 고려가 이루어지지 않았다.

선행 결과물을 활용하기위해 아래와 같은 절차를 통해 프로세스를 재정립하였다.

논문의 구성을 보면, 본론에서는 개념적인 배경으로 적용 프로세스, 시스템 안전, 요구사항 수집, 요구사항 분석, SE 도구 적용, 운영시나리오, 통합시나리오 개발, 시뮬레이션 구현의 절차로 구성하였고, 결론에서는 안전 표준 규격인 MIL-STD-882C, FAA Safety Handbook의 안전시스템이 가져야하는 속성을 정리하여, 현행 결과물과 SE 방법론을 적용한 결과물을 비교하였다. 또한 각 단계별 타당성을 검증하기위해 SE 지원하는 시뮬레이션을 활용하여, 누락된 운용시나리오는 없는지를 확인하였다.[4]

## 2. 본 론

### 2.1 관련 연구 사례 조사

<표 1> 국내 · 외 선행 연구

국내 선행 연구	해외 선행 연구
전기설비 검사(점검)제도 개선방향에 관한 연구	National Electrical Safety Code(NESC) Handbook
전력산업구조개편에 따른 중장기 전기안전정책방향 연구 II (전기안전 규제방향 중심)	Managing Electrical Safety
전기재해 통계분석	Electrical Inspections Designing to the Wiring rule
외국의 전기안전관리제도 연구	IEE Wiring Regulations Inspection Testing & Certification

전기안전 제도 개선에 관한 연구가 국내 · 외에서 활발히 진행되고 있다. 선행 연구사례를 보면 선진국에 전기안전 제도의 분석을 통해 우리나라의 부족한 제도

보완에 대한 연구와 해외의 경우 전기 안전에 관하여 관리하는 방법에 대해 다루고 있다.

하지만 아직까지 SE 표준에 의한 시스템 수준의 전기안전에 관한 접근은 우리나라에서 최초로 시도되었다. 또한 해외의 경우 국방 산업과 철도 산업에서 SE 기법을 활용하여 연구를 하고 있으나, 전기 안전에 대한 사례는 찾기 힘들다.

## 2.2 적용 프로세스

적용프로세스는 크게 시스템엔지니어링 적용에 활용되는 ISO/IEC 15288과 EIA 632 프로세스와 안전관련 표준인 MIL-STD-882C와 미항공안전인 FAA Safety Handbook을 고려하였다.

시스템엔지니어링 프로세스로 전기안전시스템을 개발하는데 전체 수명주기를 고려할 수 있도록 활용하였고, 개념, 설계 단계에서 안전시스템 개발의 각 단계를 고려할 수 있도록 FAA Safety Handbook의 예방적인 안전 계획의 절차를 적용하여, 전기안전 개선안을 도출하였다.[5]

### 2.2.1 시스템엔지니어링 표준

시스템의 수명주기를 고려하기위해 국가 표준인 ISO/IEC 15288의 내용을 고려하여 각 단계별의 항목을 정리하였다. 각 표준의 상세 수준을 보면 ISO/IEC 15288은 시스템의 생명주기 전체를 포함하고, 이해당사자 요구사항 정의 프로세스부터 폐기 프로세스까지의 11단계로 분류하여 정의하고 있다.

EIA 632 프로세스는 개념, 설계, 구현의 단계를 상세하게 구현하고 있다. EIA 632 프로세스의 특징은 ISO/IEC 15288보다 개념, 설계, 구현에서 고려해야하는 기술관리, 획득과 공급, 시스템 설계, 제품 구현, 기술평가의 5가지의 범위로 정리하여, 각각의 요구사항을 상세하게 정리하고 있다.[6]

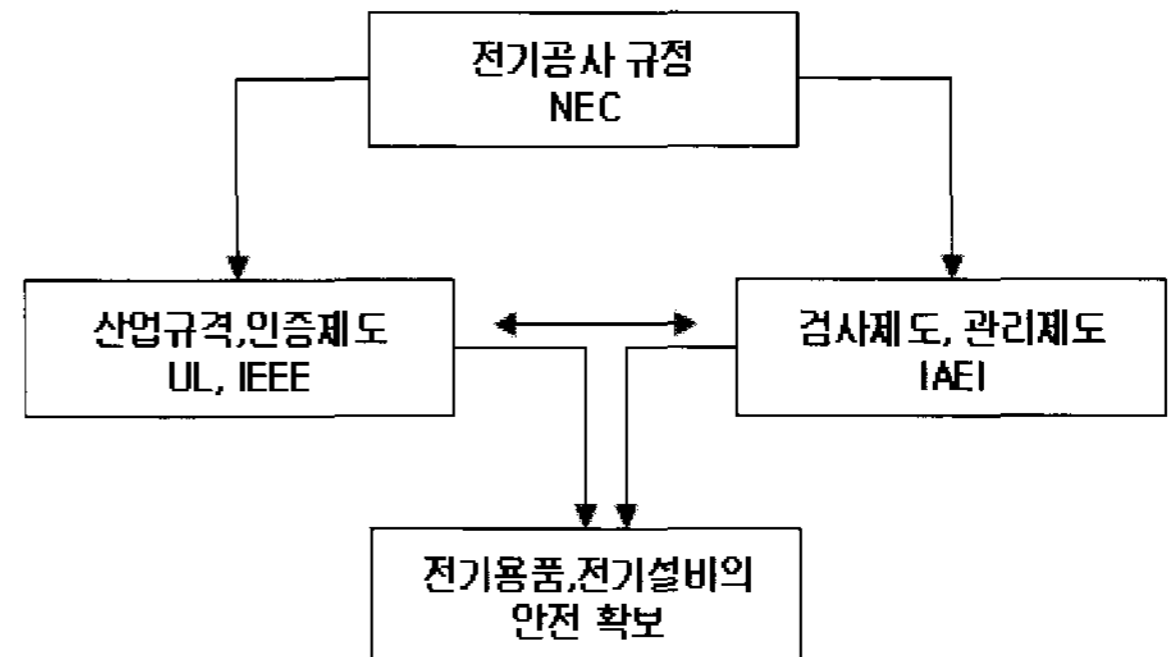
### 2.2.2 시스템 안전 프로세스

안전관련 표준인 MIL-STD-882C에서는 안전시스템이 가져야하는 목표와 활동을 정리하고, FAA Safety Hand Book에서는 예방활동으로서 안전 계획에 대한 각 단계를 기술하고 있다. [7]

## 2.3 시스템 안전

시스템 안전은 그 시스템, 직원, 환경, 디자인 개발에 직면한 건강 재난 위험도, 시험, 생산, 사용, 시스템의 제거, 하부시스템, 장비, 재료 그리고 설비들을 관리하

는 프로세스(공정)이다. 전기안전 시스템이 가져야하는 시스템의 구성요소는 아래의 <그림 3>과 같다.



<그림 3> 전기안전 관련 시스템 구성 요소

## 3. SE 표준 적용

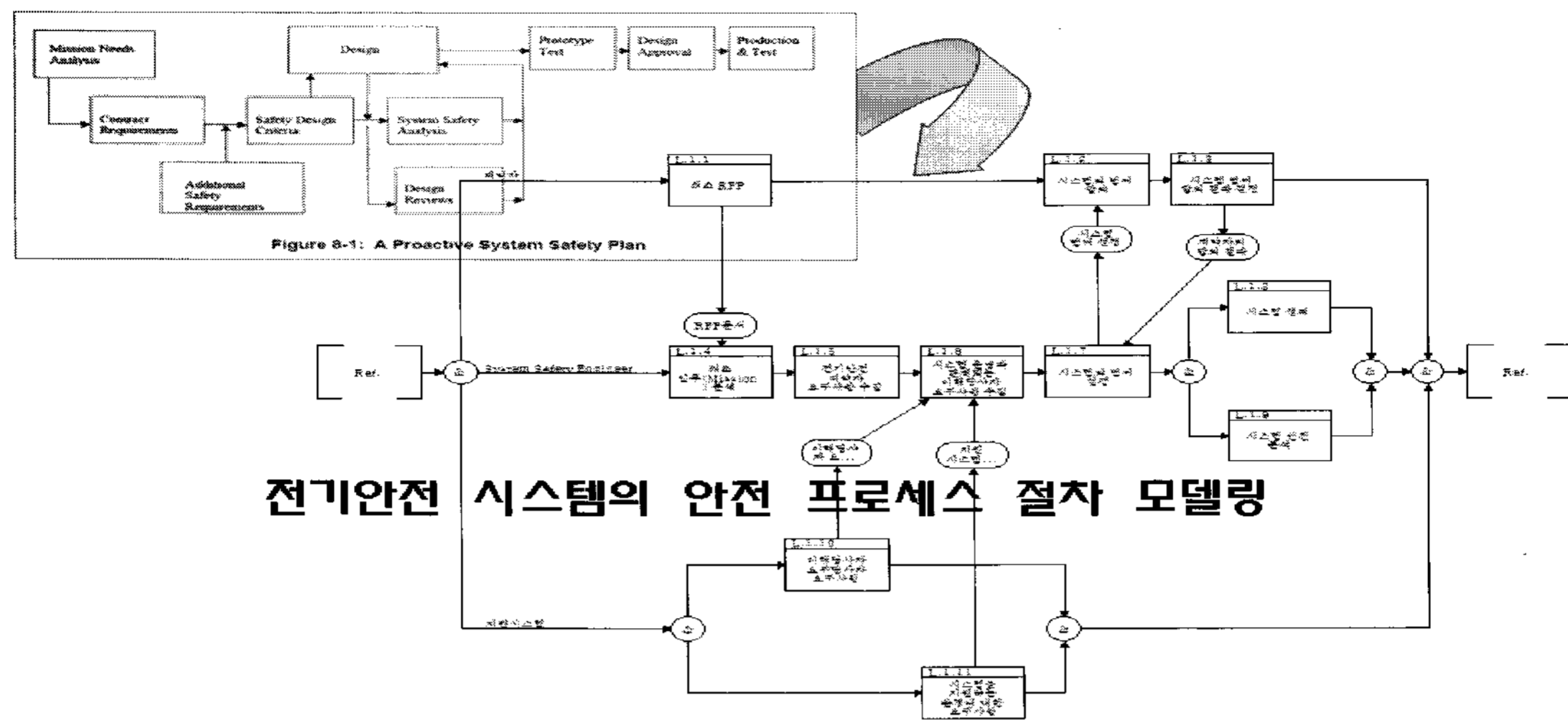
### 3.1 이해당사자 요구사항 수집

프로세스 요구사항	주요 내용	수행 업무	결과물
획득자 요구사항	개발자는 시스템 또는 시스템 일부에 대해 확인된 획득자 요구사항을 정의해야 한다.	획득자의 시스템 요구사항 식별, 수집, 우선 순위 결정 수집된 획득자 요구사항의 완전성과 일관성 확인 획득자 요구사항 기록	정의된 획득자 요구사항 확인된 획득자 요구사항
기타 이해관계자 요구사항	개발자는 시스템 또는 시스템 일부에 대해 확인된 기타 이해 관계자 요구사항을 정의해야 한다.	기타 이해당사자의 최종 제품 및 지원제품에 대한 요구사항 및 제약사항 식별 및 수집 요구사항의 완전성 및 일관성 확인 요구사항 기록	시스템 최종제품의 엔지니어링하는 것을 제약할 수 있는 기타 이해당사자의 요구사항
시스템 기술 요구사항	개발자는 확인된 시스템 기술 요구사항을 정의해야 한다.	필요한 전환 규칙, 우선 순위, 입력, 출력, 상태, 모드 및 형상의 확립 운용 요구사항의 정의 성능 요구사항의 정의 획득자 및 기타 이해당사자 요구사항의 분석	시스템 기술 요구사항에 영향을 미칠 전환 규칙, 우선 순위, 입력, 출력, 상태, 모드 및 형상이 각 시스템 제품별 식별/정의됨

<그림 4> EIA 632 요구사항 분석

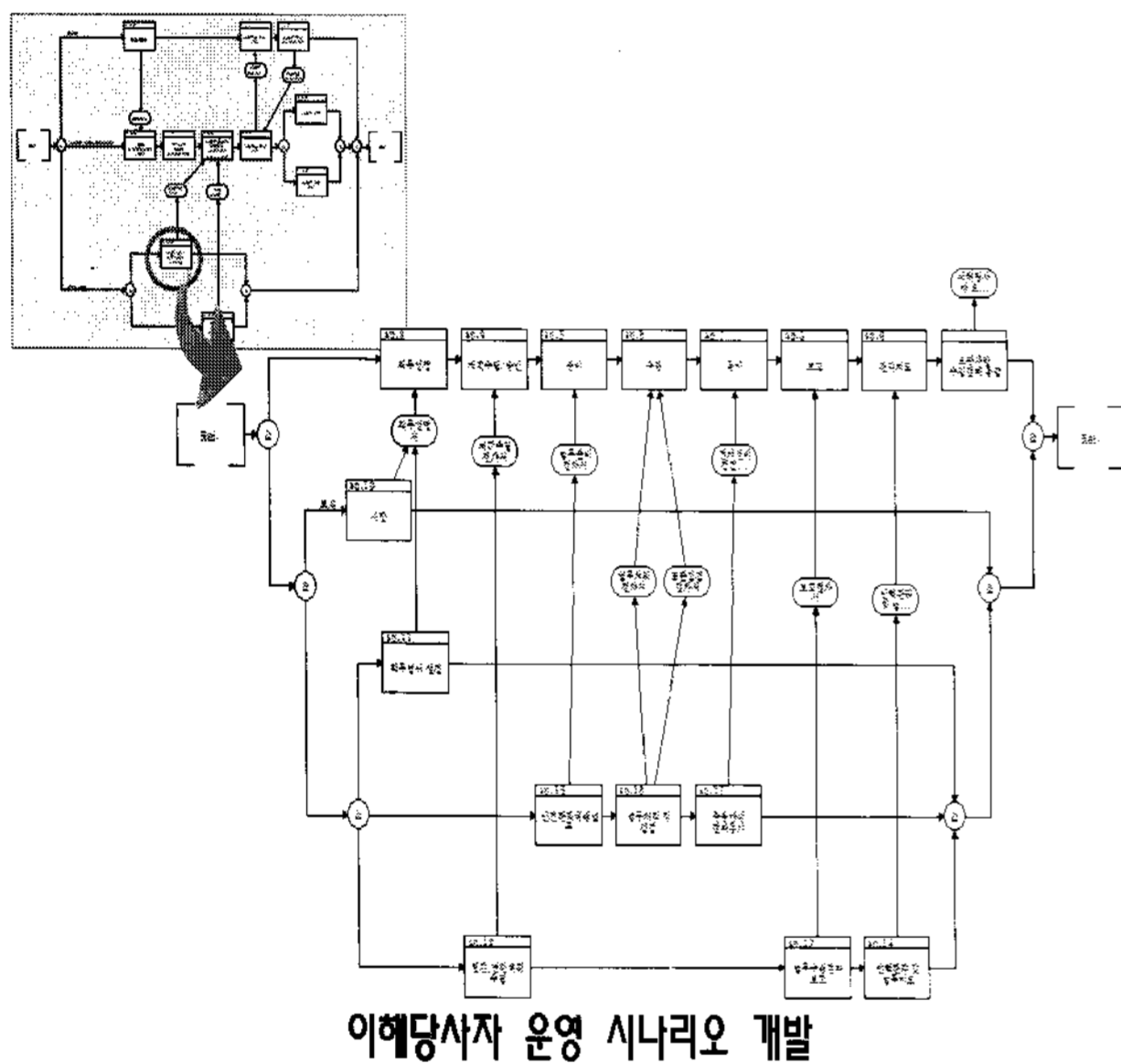
시스템은 시스템의 목표와 부합하는 최종 시스템과 지원시스템으로 이루어진다고 EIA 632에서 기술하고 있다. 사용자가 원하는 시스템을 개발하기위해서는 각 수명주기와 관련된 이해당사자의 요구사항과 지원 시스템의 요구사항이 수집되어 시스템 개발 요구사항에 반영되어야 한다. 각 단계별 요구사항이 가져야하는 주요내용, 수행업무, 각 단계 결과물을 <그림 4>와 같이 정리한다.





전기안전 시스템의 안전 프로세스 절차 모델링

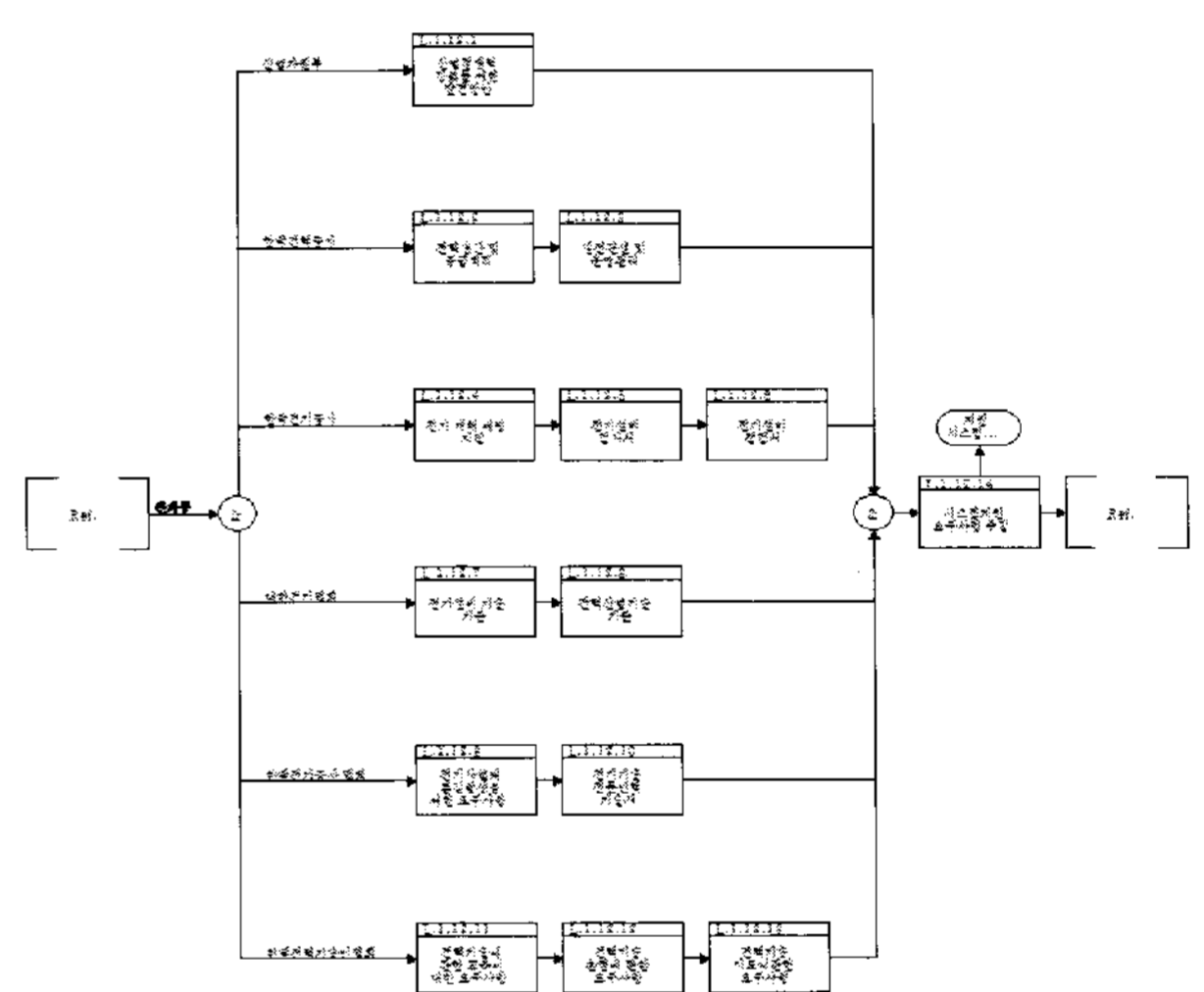
<그림 10> FAA 시스템 안전 예방 계획 기반 전기안전 시스템 프로세스 모델



<그림 11> 이해당사자 운영시나리오 개발

전산지원도구를 통해 요구사항 분석 절차를 DB화한 결과 <그림 9>와 같은 요구사항의 중복성이 나타나게 된다. 이러한 경우 전기안전시스템의 전문과와 합의를 통해 중복성을 제거하게 된다. 중복성이 제거되지 않는다면 하부에 시스템 복잡성이 증가하여, 개발에 어려움을 가중시킨다.

<그림 10>의 전체 프로세스 모델을 기반으로 각 단계의 상세 운영시나리오 개발하였다. 상세 운영시나리오 개발을 위해 전기 안전 전문가와 함께 <그림 11>과 같은 식별된 이해당사자의 요구사항을 수집하는 운영시나리오를 개발하였다. 운영시나리오 개발 시 전문가와의 합의를 통해 개발해야 한다.

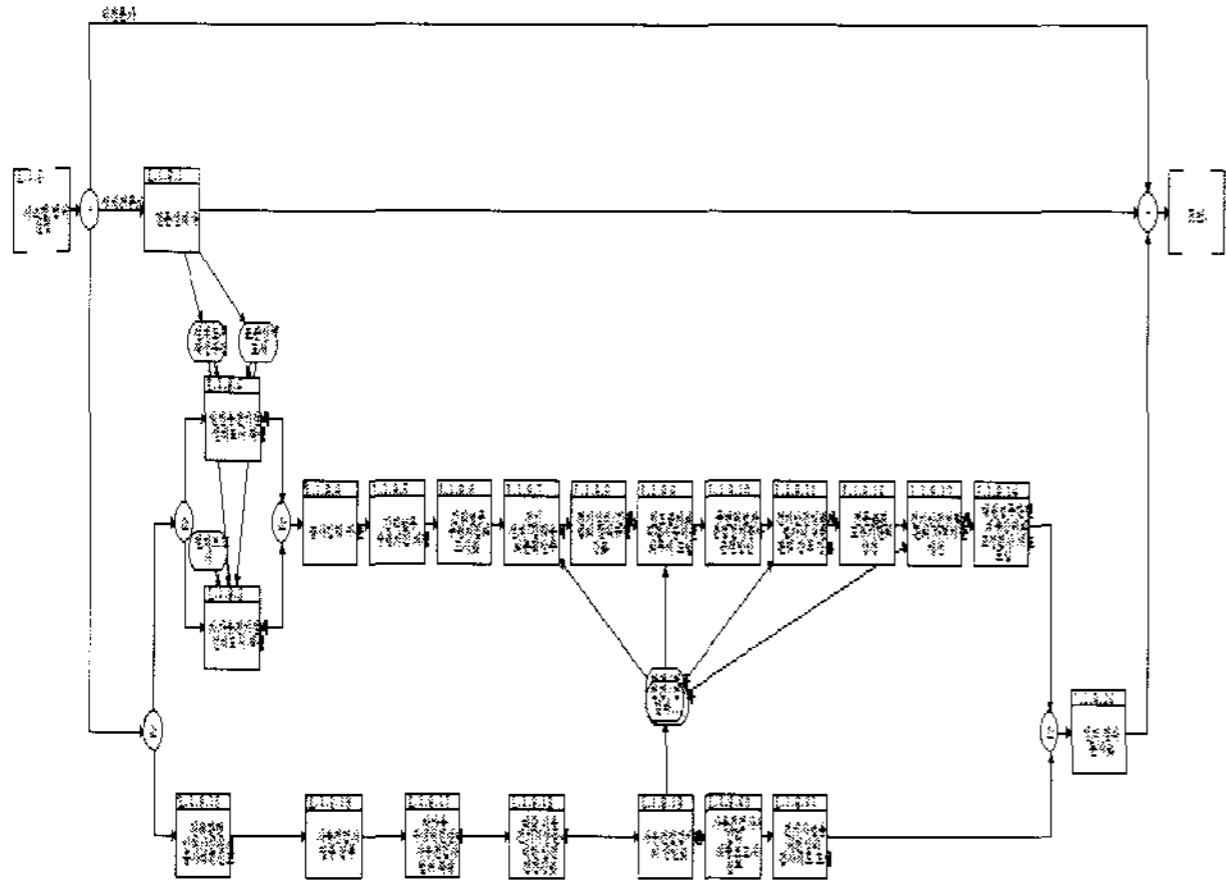


<그림 12> 시스템을 지원하는 환경에 대한 운영시나리오 개발

합의를 통하면 향후 결과물의 변경을 줄일 수 있고, 각 단계마다 고려해야 할 고려사항을 모델에 반영할 수 있다. 개발자가 없을 경우 각 단계별 검토를 통하여, 다음 단계로 넘어가는 것이 중요하다.

시스템 개발 초기에 시스템과 직접적으로 관련된 이해당사자 요구사항과 시스템을 지원하는 환경에 대한 고려를 통하여, 운영과 유지보수 등의 변경을 최소화할 수 있다. <그림 11>은 시스템의 수명주기에 영향을 주는 이해당사자의 요구사항을 수집하는 운영시나리오이고, <그림 12>는 시스템을 지원하는 산업자원부, 한국전력공사, 한국전기공사, 대한전기협회, 한국전기공사협회, 한국전력기술인협회 등의 요구사항을 수집하여 요구사항을 분석하는 단계의 운영시나리오이다.





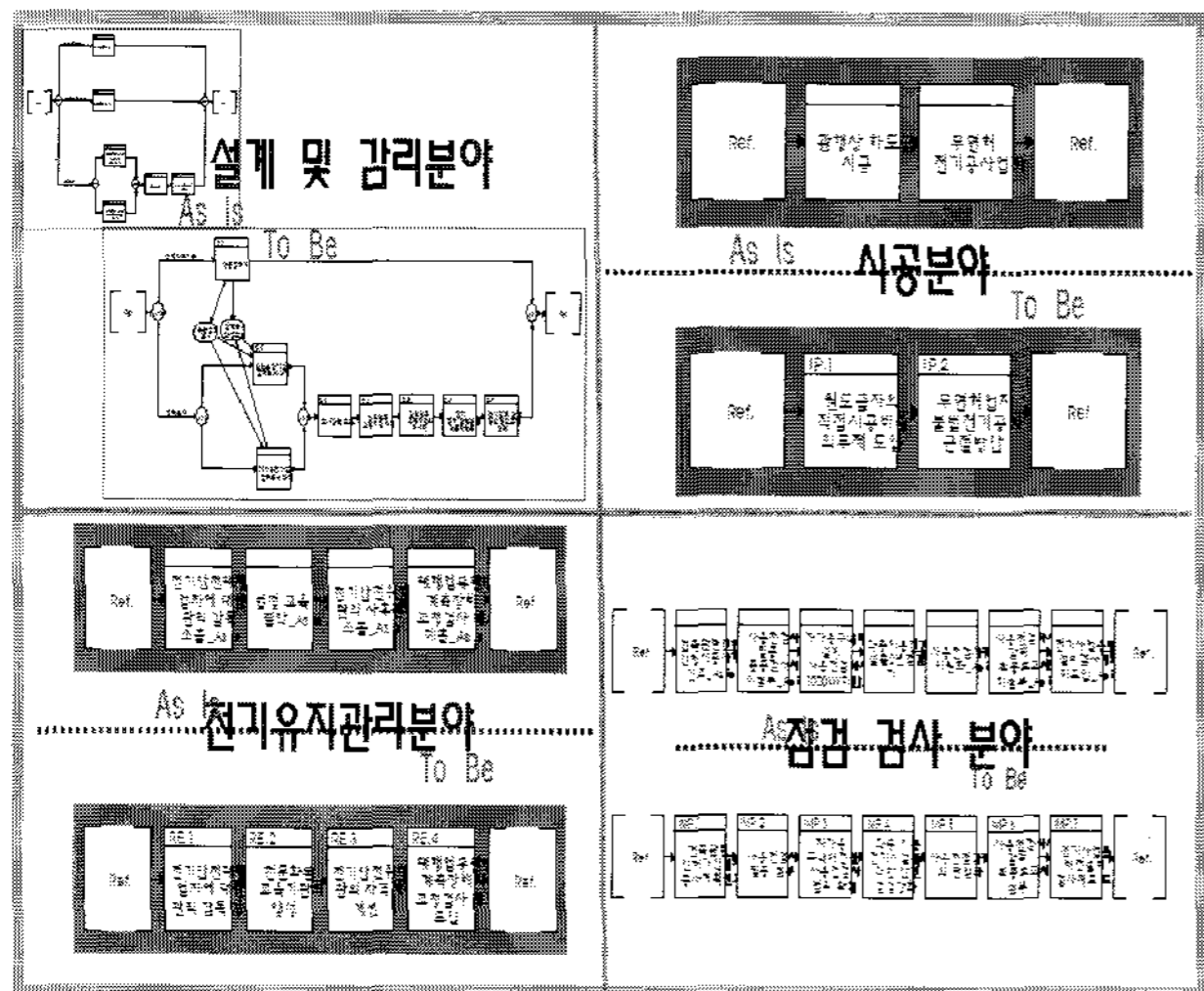
<그림 13> 전기안전시스템 설계 운영시나리오 개발

<그림 13>은 전기안전시스템을 시스템 설계의 운영 시나리오이다. 개발초기부터 도입까지의 시나리오를 포함하고 있다.

### 3.3 통합시나리오 모델 개발

<그림 10>의 프로세스 모델을 기반으로 상세한 운영 프로세스를 개발하고, 이를 통합하여 시스템의 통합 시나리오 모델을 개발하였다. 통합시나리오 모델은 각 단계별 조직이 무엇을 해야 하는지와 다른 조직에 어떤 결과물을 전달해야 하는지를 나타낸다.

또한 자신이 하는 일 이전에 선행기관으로부터 어떤 결과물을 가져야 하는지를 알 수 있다. 이를 통하여, 시스템이 가져야 하는 역할을 정확하게 알 수 있다. 이 단계에서는 기존의 결과물과 통합시나리오의 결과물을 전산지원도구를 통해 비교하였다.



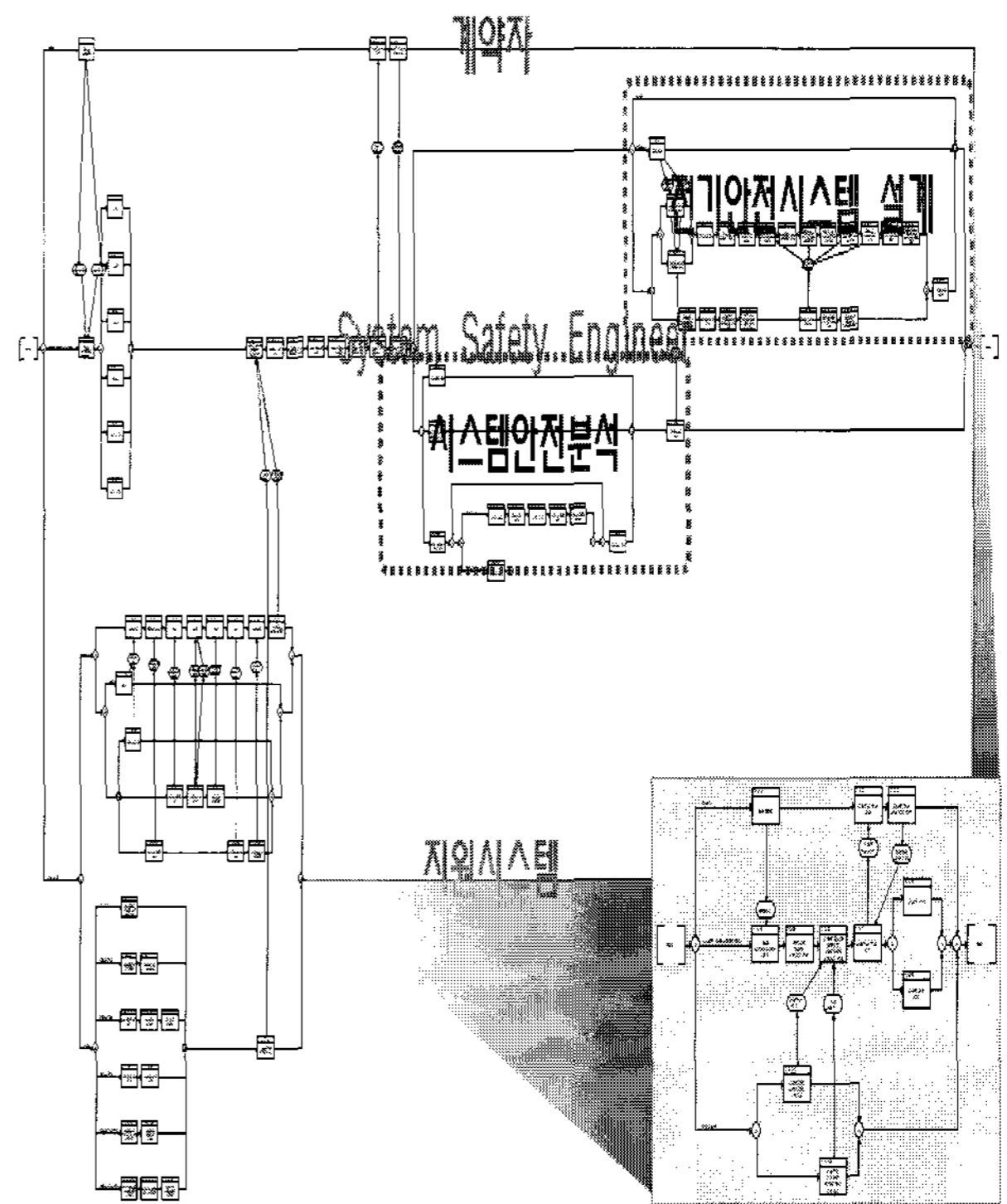
<그림 14> 현행 전기안전 시스템 개선안

<그림 14>와 같이 현행 전기안전시스템에 관한 모델의 통합은 어렵다. 전기안전시스템의 4분야(설계 및 감리분야, 시공분야, 전기유지 관리 분야, 점검분야)를 현행 모델과 향후 개선 모델로 비교하고 있다.

<그림 15>는 제안된 전기안전시스템의 개선모델로 크게 계약자와 시스템 안전 엔지니어, 지원시스템의 관계를 수명주기 관점에서 통합한 모델이다.

### 3.4 연구결과

연구결과는 안전 표준인 MIL-STD-882C와 FAA System Safety Program Plan을 기반으로 평가항목을 만들어 안전시스템이 가져야 하는 목표를 통해 비교하였다. 또한 제안된 시스템의 통합시나리오 모델을 전산 지원도구의 도움을 받아 누락된 부분은 없는지를 확인하는 시뮬레이션을 실시하였다. 시뮬레이션을 통해 각 단계의 전후관계의 순서를 확인할 수 있다.



<그림 15> 제안된 전기안전시스템 개선모델

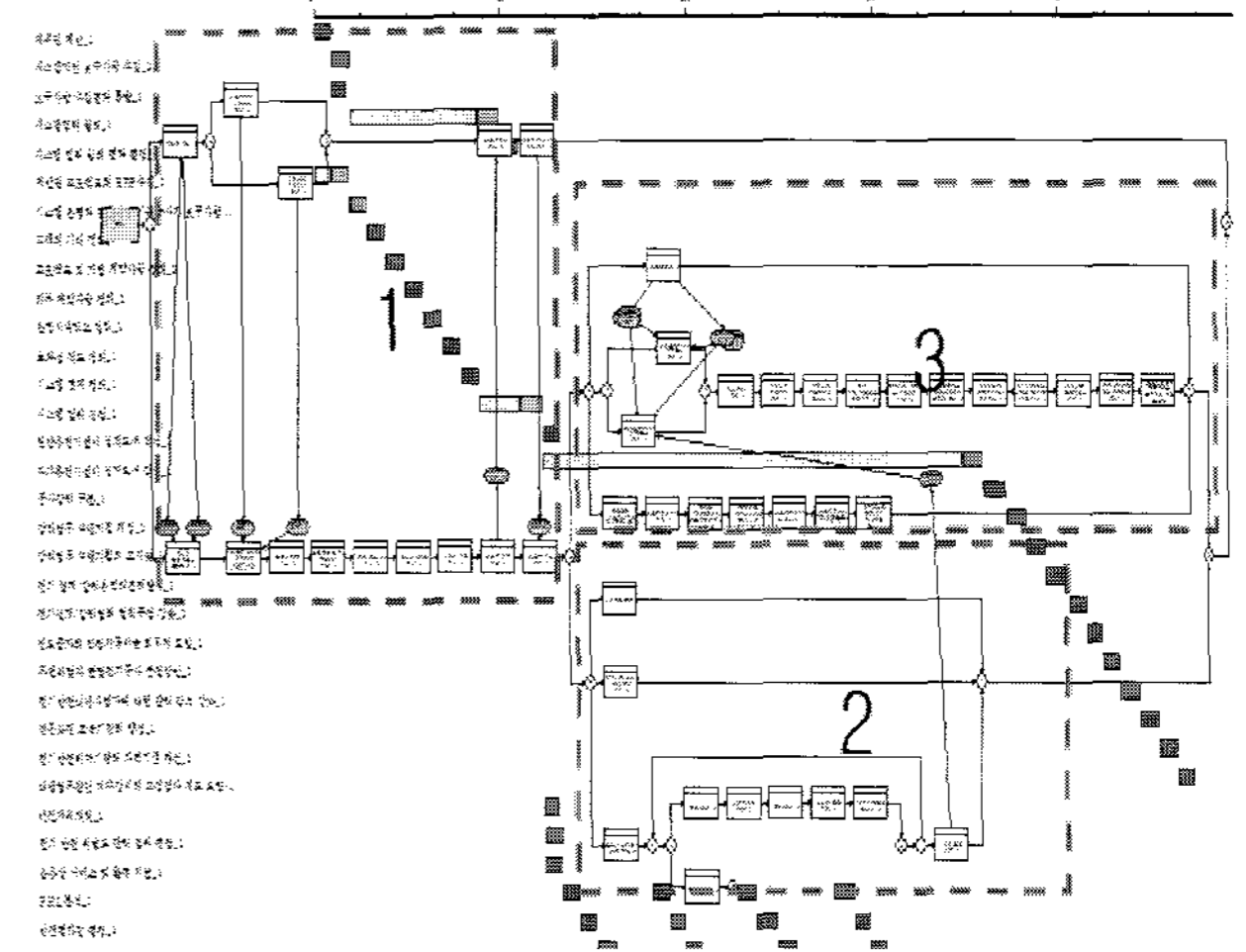
두 사례 비교 결과 기존의 전기안전시스템 개선안은 선진국의 안전 모델을 분석하고, 우리나라의 현재 모델을 분석하여 차이를 개선하는 모델을 제안하고 있다.

본 논문에서 제안된 모델을 표준평가항목에 의해서 기존 시스템과 비교 평가해본 결과 11개 항목에서 개선됨을 확인할 수 있었다.

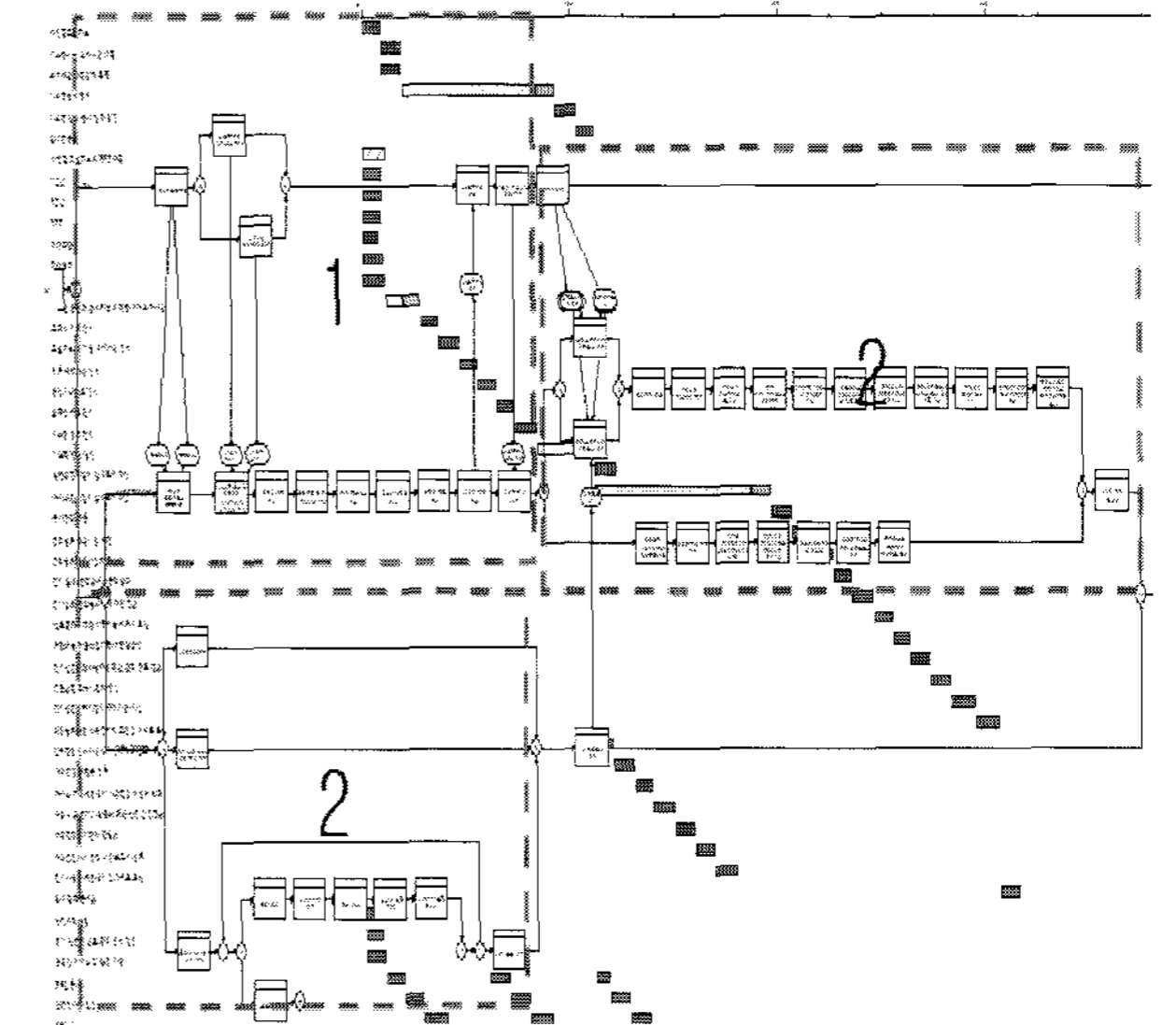
<표 2> 제안된 전기안전시스템 체계 비교

관련 자료	평가항목	기준	개선
FAA	Hazard Analysis를 식별하는 것과 사용되고 있는 Accident나 Assessment Processes 내용을 포함하였는가?		○
	FAA의 Integrated Product Development System과 Integrated Product Team 구조에 대한 통합된 System Safety방법을 포함해야 한다.		○
	Hazard와 Residual Risk에 대한 방법론적 정의는 프로그램 매니저가 의사소통을 해결하며, 프로그램 매니저는 수용하고, Hazard와 Residual Risk를 추적한다.		○
	범위, 조직, 마일스톤, 요구사항, 안전 데이터, 안전 검증, 사고 보고서, 안전 프로그램 인터페이스를 포함한다.		○
MIL-STD-882C	임무 요구사항과 일치되는 안전은 시스템에 시기적절하고 비용 효과적으로 설계되어야 한다.		○
	시스템에 관련된 위험이 식별, 추적, 평가, 제거되어야 한다.		○
	시스템 전체 수명주기를 고려해야 한다.		○
	다른 시스템으로부터 얻은 교훈/시행착오를 포함하여, 과거의 안전데이터가 고려되어 사용되어야 한다.		○
	위험을 제거하거나 위험도를 관리조직에서 수용 가능한 수준까지 줄이기 위해 취해지는 조치는 문서화된다.		○
	안전을 향상시키기 위해 필요한 새로운 조치는 시스템연구, 기술 개발과 그것을 조달하는 과정에 안전 특성을 포함해야 한다.		○
	설계, 형상 혹은 임무 요구사항의 변경은, 위험도 수준을 관리조직에서 수용 가능하게 유지하는 방식으로 달성한다.		○
	수명주기 초반에 안전과 폐기의 용이함과 시스템과 관련된 모든 위험물의 해체를 고려한다.		○
	위험물 사용을 최소화시킴으로 그 사용에 따른 위험도와 수명주기 비용을 최소화시키기 위한 조치가 취해져야한다.		○
	모든 결과는 데이터 보관하는 곳에 저장되어 관리되어야 한다.		○

3.4.1 통합 프로세스 모델 시뮬레이션



<그림 16> 개선 전 시나리오



<그림 17> 개선 후 시나리오

전산지원도구에서 지원하는 시뮬레이션은 각 흐름과 프로세스 수행시기의 논증을 통하여 오류를 수정하고, 잘못된 부분이 없는지를 확인 할 수 있다. 개선된 전기 안전시스템의 운영시나리오를 보면 최초 외부시스템으로 부터 요구사항단계에 최초 소스문서를 전달하여, 요구사항을 개발하고, 동시에 안전단계에 최초 소스문서를 기반으로 안전계획을 세우는 활동을 시작하여, 결과를 설계단계에 보내면 앞에 개발한 활동과 동일하게 모든 이벤트를 만족시키고, 시간은 줄이는 효과를 했다.

또한 요구사항 분석 단계와 시스템 안전 단계의 동시적인 활동으로 리소스의 활용성을 높이도록 개선시켰다.

## 4. 결론

전기안전을 확보하기 위하여 전기안전과 관련된 법령, 제도 및 이를 시행하기 위한 정부 조직, 기관 및 단체들 간에 이루어지는 유기적인 행정절차로서 정의할 수 기존 전기안전시스템 체계를 다음과 같은 관점에서 기존 체계를 개선하였다.

기존 전기안전시스템 체계 개선의 부족한 점은 최초 요구사항 수집단계에서 많은 노력을 하였으나, 개선안 도출 방법이 체계적이고 논리적이지 못하다. 이는 향후 유지보수, 확장, 개선 시 운용비용의 낭비를 초래하고, 전기안전 시스템과 관련된 다양한 이해당사자의 식별이 고려되지 않아 전체시스템 관점에서 파악하기 어려웠다.

본 논문에서 제안된 전기안전시스템 체계 개선 사항은 SE 표준을 기반으로 최초 요구사항을 수집하고, 표준 절차를 따라 요구사항 분석 절차를 수행하였고, SE 절차를 전산지원도구를 활용하여 데이터의 활용성을 높였다. 또한 현행 결과물과 SE방법론을 적용한 결과물을 비교하여, 향상된 절차를 제안하였으며 리엔지니어링 통한 기존 결과물의 부족한 부분을 보강하였다.

국내 최초로 전기안전시스템 체계에 시스템공학 개념을 적용하여 체계 개선 모델을 적용하여 표준 안전 모델 프로세스를 구축하고 향후 타 시스템의 안전 분야에 확장될 수 있는 모델을 제안했다는 것에 의의가 있다. 본 논문에서는 전기안전 분야의 SE 표준 프로세스 적용에 관한 연구로, 차후 각 단계의 검증 방법에 대한 연구가 진행되어야 한다. 또한 하부 시스템 설계에 필요한 인터페이스 설계에 대한 추가 연구가 필요하다.

## 5. 참고 문헌

- [1] 산업자원부, “전기설비 검사(점검)제도 개선방향에 관한 연구”, 2004. 10
- [2] 한국전기안전공사, “전기안전관리제도 연구”, 1992. 12
- [3] 한국전기안전공사, “전기해해통계분석”, 2005. 11
- [4] 한국전기안전공사, “외국의 전기안전관리제도 연구”, 1999. 3
- [5] 한국전기안전공사, “전력산업구조개편에 따른 중장기 전기안전정책방향연구 I(전기안전 점검·검사 중심)”, 2003. 2
- [6] 한국전기안전공사, “전력산업구조개편에 따른 중장기 전기안전정책방향 연구 II(전기안전 규제방향 중심)”, 2004. 10
- [7] 박중용, “안전중시 시스템을 위한 동시공학 설계 모델”, 박사학위논문, 아주대학교, pp. 139, 2003.

## 저 자 소 개

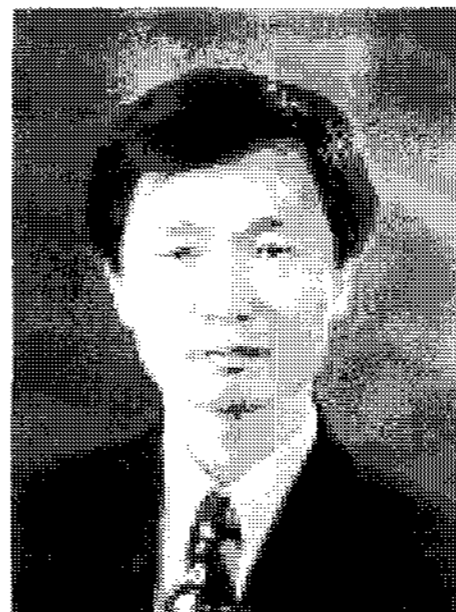
### 신흥식



현 한국전기안전공사 전기안전연구원 재직 중. 광운대학교 전기공학과에서 학사, 석사를 취득하고, 2004년 아주대학교 시스템공학과 박사과정을 수료 하였으며, 1997년 이탈리아 Alenia사 객원연구원, 1998 ~ 2003년 고등기술연구원 연구원 역임, 주요관심분야는 전기안전시스템, 통신시스템, 시스템엔지니어링이며, RF 및 위성통신분야에도 관심을 가지고 있음. Tel. (031) 580-3019, Fax. (031) 580-3111, e-mail : hsshin@kesco.or.kr

주소: 경기도 가평군 청평면 상천리 27 전기안전연구원 연구기획

### 이재천



현 아주대학교 시스템공학과 정교수 및 학과장. 서울대학교 전자공학과 공학사. KAIST 공학석사 및 박사 학위 취득 후 미국 MIT에서 Post-Doc 연구를 수행. 계속해서 미국 Univ. of California 에서 초빙연구원, 캐나다 Univ. of Victoria에서 초빙교수 등 역임. KIST 책임연구원 및 연세대학교 겸임교수 재직. 최근 Stanford Univ. 방문 교수 역임. 현재 연구 및 교육 관심분야는 Systems Engineering (SE) 및 Systems Safety에의 응용 등. SE 분야에서는 Model-based SE 및 CASE tools, Modeling & Simulation, Systems Architecting and System of Systems 등.

주소: 경기도 수원시 영통구 원천동 산5번지 용인우체국 사서함25호

### 이병길



현 아주대학교 시스템공학과 박사과정, 관심분야는 시스템 요구사항 분석, 시스템 아키텍처 설계, 시스템 통합 및 최적화이며 수행과제로는 철도안전 SE 표준 스키마 과제 P.M, 고속철도신뢰성분석 설계 과제, 철도안전연구지원요구사항 아키텍처 구축 과제 수행.

주소: 경기도 수원시 영통구 원천동 산5번지 용인우체국 사서함25호