고속전철 기술개발 안전 확보 계획
System Safety Program Plan for The Development of KHSR

황희수* 최강윤**
Hwang, Hee-Soo Choi, Kang-Yoon

ABSTRACT

In this paper the system safety program plan(SSPP) for the development of Korea high speed railway system was presented. The plan for the design phase built up base upon MIL-STD 882C, manual for the development of rail transit system safety program plans by American Public Transit Association, and SSPP for Seoul-Pusan High Speed Rail project, should be modified and then applied to the phases of manufacturing, test and commissioning. The plan deals with the safety program, the reference standards, the management and responsibility for the safety related activities, the methods to be used for early identifying safety critical items and functions and eliminating or controlling all hazards in a timely and cost-effective manner, and the documentation generated for safety assessment.

1. 서 론

시스템 안전 확보 계획(SSPP: System Safety Program Plan)은 다음과 같은 두가지 목적을 가진다. 첫째, 정부와 국민에게 고속전철 기술개발 프로젝트가 안전하게 승객을 수송할 수 있도록 설계되고 제조/시험 되었음을 입증(문서를 통해)하고 둘째, 고속전철 시스템에 적용된 RAMS 요구조건을 달성할 수 있음을 입증한다. 이를 위해 본 계획에서는 고속전철 기술개발 과제에서 수행되어야 할 안전 관련 활동과 규약을 정의하고 제시한다. 이런 계획에는 국민의 안전을 위해 중요하고 잠재적인 안전 관련 모든 위험, 법규 및 규정을 찾아내서 위험을 제거하거나 제어할수 있는 안전 조치를 설계에 반영하도록 하고 모든 찾아진 위험에 대해 적절한 통제가 이루어졌고 관련 법규, 규정 및 설계 조치대로 생산/시험 되었음을 검증하기 위한 방법론을 포함한다. 모든 개발 참여자가 주어진 RAMS(Reliability, Availability, Maintainability, Safety) 목표 달성을 위해 노력해야 하며 전체 시스템 통합 측면에서 RAMS는 이 목표가 전체 개발 프로젝트에 걸쳐 적절히 분배, 통합되고 프로젝트 각각이 상호 협력할 수 있도록 하는 것이다. 이 계획은 또한 개발 과제에서 RAMS를 담당하는 사람들로 구성된 안전성 관리 팀이 향후 구성되고 시스템 엔지니어링 과정을 통해 이들의 의견을 반영하여 최종 확정되어야 하며 개발과제의 체계, 개발 범위 및 개발 단계 등에 부합해야 한다. 이 계획은 전체 개발 시스템의 안전을 보증하기 위해 필요한 활동 및 과업과 관련하여 안전 프로그램, 참고 규격, 안전 관련 활동에 대한 관리 및 책임, 안전에 치명적인 기능 및 장비를 찾아내고 위험을 제거하거나 절적한 시기에 효율적인 방법으로 위험을 제어하는데 사용되는 방법과 안전성 평가를 위해 작성된 문서 등을 다룬다.

* 한국철도기술연구원 고속철도기술개발사업단 시스템개발팀 선임연구원, 정회원
** 한국철도기술연구원 고속철도기술개발사업단 시험설비시스템팀 책임연구원, 정회원

2. 안전 계획 범위 및 관리

2.1 범위

이 문서는 고속전철 기술개발 전체 시스템의 안전 확보 계획을 다룬다. 전체 시스템은 크게 차량, 열차제어 및 전차선 시스템으로 구성된다. 전체 시스템의 안전은 각 시스템 별로의 안전을 의미하는 것은 아니고 통합된 시스템의 안전을 의미한다. 전체 시스템의 안전 분석을 통해 안전에 중요한 장비를 찾고 이들의 안전 임무 수행 능력과 이들의 안전 확보 수준을 결정한다. 그러나 작업 및 시험 현장에서의 건강 및 안전 문제, 폭력 및 테러에 대한 안전 문제, 안전 확보 관련 교육 문제와 안전 관련 운영 규칙 등은 이 계획의 과업 법위에 포함하지 않는다.

- 고속전철 기술개발 시스템은 한국철도(KNR) 환경하에서 운영 및 유지되는 것으로 가정.
- 안전 확보 계획의 과업 범위는 개발로 인한 고장에 한정하며 운영 및 유지보수 오류에 의한 고장은 포함하지 않음.

2.2 관리, 책임 및 조직

안전 확보를 위한 관리 조직(이후 안전 관리 조직으로 부름)은 독립성을 유지해야 하며 시스템별 조직과 이들의 대표자들을 통합한 시스템 안전 관리 팀으로 구성될 수 있다. 향후 개발 과제 내용별로 팀의 구성, 시스템 및 전체 시스템을 위한 안전 관리 조직의 구성이 필요하다. 안전 관리 조직 구성원이 전체 시스템의 안전에 책임이 있으며 각 조직의 책임자가 안전 계획의 구현, 감시 및 보완을 책임지고 시스템 및 전체 시스템 안전 관리 조직의 책임자는 인터페이스를 포함한 시스템 및 전체 시스템의 안전을 책임지며 이를 위해 필요한 조정 작업을 수행한다. 또한 이들은 담당 시스템의 안전성 평가를 수행하며 필요할 경우 적절한 조치를 요구할 수 있다. 전체 시스템의 안전 확보 계획에 준해서 시스템과 개발 과제별 안전 확보 계획을 작성하고 이것이 승인되어야 하며 승인된 계획에 따라 모든 개발 작업이 이루어져야 한다. 승인된 계획은 프로젝트 진행 과정에서 적정 절차를 거쳐 변경될 수 있으며 문서 번호를 통해 관리되어야 한다.

3. 안전 요구 조건

고속전철 기술개발 프로젝트의 모든 단계에서 안전 확보를 위해 시스템 설계 기준과 운영 절차를 파악해야 하며 안전성 분석을 통해 파악한 잠재적 또는 실제적 위험을 제거할 수 있거나 다음과 같은 우선 순위에 따라 제어할 수 있어야 한다: 위험을 최소화하는 설계, 경고 장비의 사용, 기타 특수한 절차의 사용. 기존에 안전성이 입증된 장비, 하위 시스템과 시스템을 재사용하는 경우 별도의 안전성 분석을 수행하지 않아도 되며 다만 다른 장비나 시스템과의 인터페이스와 관련된 최소한의 분석은 수행되어야 한다.

3.1. 위험 분류

위험 수준과 위험 영향을 평가하는데 다음과 같은 위험 분류를 사용한다.

- 분류 I 파국(catastrophic): 설계 결함, 하위 시스템이나 컴포넌트의 결함 또는 절차상의 결함이 사망이나 심각한 상해 또는 주요 시스템의 손실을 발생하는 경우
- 분류 II 치명(critical): 설계 결함, 하위 시스템이나 컴포넌트의 결함 또는 절차상의 결함이 인적 상해나 주요 시스템의 손상을 초래하여 즉각적인 복구 조치를 필요로 하는 경우
- 분류 III 경미(marginal): 설계 결함, 하위 시스템이나 컴포넌트의 결함 또는 절차상의 결함이 인적 상해나 주요 시스템의 손상을 발생하지 않거나 발생하지 않도록 제어되는 경우

3.2 정성적 요구 조건

정성적 요구 조건에는 다음과 같은 것이 있다.

- 바이탈 시스템에서의 고장 또는 고장 결합이 안전 치명 장비에 파국 위험이나 예기치 못한 동작을 발생해서는 안됨. 이러한 치명적 시스템은 안전측으로 동작해야 함. 즉, 어떠한 고장이나 오동작이 안전하지 않은 상황을 발생해서는 안됨.
- 고장이 인적 상해나 주요 시스템의 손상을 발생하는 경우 적절한 곳은 어디든 여분 원리를 설계에 적용해야 함.
- 정해진 순차를 이탈하는 동작이 위험을 야기하는 경우 장비들이 상호 연동하여 동작하도록 설계해야 함.
- 일반 시민을 위한 비상 장비/도구는 식별하기 쉽고 접근하기 용이해야 함. 연동 장비나 절체 장비들은 파괴나 방해 행위를 최소화할 수 있도록 접근 패널을 통해 접근이 가능하도록 함.
- 안전 중요 영역에서는 checked redundancy가 기존의 안전측 설계를 대체할 수 있음. 그러나 한 지점에서의 고장이 안전 보호 장치의 손실을 초래해서는 안되며 여분의 경로에 공통의 고장 모드가 있어서도 안됨. 여분 시스템에서의 고장은 감지되고 기록되어야 함.
- 단일 콤포넌트 고장이나 입력 신호의 손실이 안전하지 않은 결과를 발생해서는 안됨.
- 동일한 원인이나 연관된 원인에 의한 콤포넌트들의 동시 고장이 안전하지 않은 결과를 발생해서는 안됨.
- 승객이 머무르는 지역내에서 파국 위험을 막기 위해 가능한 곳이면 어디든 차량이 점진적 고장 특성을 보이도록 해야 함.
- 모든 감지 가능한 고장은 조작자에게 보고 되고 또는 진단 시스템에 의해 기록되고 또는 주기적인 검사에서 감지되어야 한다.
- 여자시나 전력공급 차단시 반응하지 못하는 릴레이가 안전하지 않은 상황을 발생해서는 안됨.
- 바이탈 회로에 사용된 릴레이는 UIC code 736, Type N 또는 동등한 규정을 만족해야 함.
- 전자회로의 안전측 동작 기준을 설정할 때 콤포넌트는 개폐 조건에서 고장이 있는 것으로 고려되며 증폭기가 NFF 01-510에 규정된 특정 주파수에서 진동하는 경우에 대한 보호 조치가 마련되어야 함.

3.3 정량적 요구 조건

정량적 안전도 요구 조건이 있으면 안전도 분석을 통해 정량적 요구 조건을 만족시킴을 보여야 한다.

4. 안전 구현

일반적인 안전 확보 방법은 정량적/정성적 평가와 점진적으로 위험을 줄이기 위한 반복적인 과정을 통해 구현된다. 이 과정에는 다음과 같은 일이 포함된다: 위험의 식별, 위험의 제거 또는 제어(적용 우선 순서: 위험을 최소화하도록 설계, 경고 장비의 사용, 특수 절차의 사용), 잔류 위험의 평가와 위험 수락 및 관리. 하위 시스템, 시스템과 전체 시스템의 안전 관리 조직 책임자는 안전 관련 모든 문서의 검토 및 분석을 책임지며 수행된 과업이 안전 요구 조건을 만족시킬 수 있는지 보이고 이를 문서화하기 위하여 분석 내용을 파일로 만든다.

고속전철 시스템에 사용되는 장비의 안전성 평가는 크게 다음의 4 가지 수준으로 구분하여 실행한다.

- 수준 A: 이전에 설계된 장비로 유사 환경하에서 사용되고 있는 경우
- 수준 B: 이전에 설계된 장비로 상이한 환경하에서 사용되고 있는 경우
- 수준 C: 수정된 장비
- 수준 D: 완전히 새로이 설계된 장비

수준 A와 B에 해당하는 장비에 대해서는 이전에 수행된 안전성 분석 자료를 제시하거나 이에 상응하는 근거를 제시하면 되고 수준 C의 경우에는 수정된 내용에 대해서 안전성을 분석하고 그리

고 수준 D에 대해서는 전적으로 안전 확보를 위한 절차 및 과정을 적용한다. 소프트웨어의 경우 수준을 SA, SB, SC, SD로 정의한다. 기능 및 장비의 안전성 영향 분류를 위해 다음 표1과 같은 정의를 사용한다.

표 1. 안전성 영향 분류 및 정의

분류	정의	표시
안전 중요 항목/기능 (Safety critical item/function)	장비/기능의 고장이 직접적으로 재난적 위험(분류 I)을 발생	C
안전 요주 항목/기능(Safety essential item/function)	장비/기능의 고장이 직접적으로 재난적 위험(분류 I)을 발생하지는 않지만 직접적으로 치명적 위험(분류 II)을 발생.	E
안전 무관 항목/기능 (Non-safety item/function)	장비/기능의 고장이 재난적 위험(분류 I)과 치명적 위험(분류 II)을 발생하지 않음.	N

기능 및 장비와 안전성과의 관계를 정의하기 위해 표2와 같은 양식을 사용한다. 분석 대상 시스템의 기능을 세부 항목화하여 왼쪽 첫 열에 기술하고 안전성 항목란에 세부 항목의 안전 영향 분류를 표시하고 그 옆에 하위 시스템 장비와의 연계성을 표시하는데 안전 관련 기능을 갖는 장비에 대해서는 Y 표시로 관련이 없는 장비는 X로 표기한다. 맨 우측에는 인터페이스되는 외부 시스템이 있으면 이를 적는다. 표2의 세부 기능 및 장비와의 연계성을 잘 파악하기 위해서는 기능 모델 문서를 작성하면 도움이 되는데 이 문서에는 다음과 같은 내용을 포함할 수 있다.

- 기능간의 정보 흐름(어떤 기능의 출력이 다른 기능의 입력으로 사용)을 추적할 수 있는 방법론
- 계층구조를 통한 기능을 기본 단위로 분류 세분화
- 기능 분류를 통해 각 기본 기능들을 그룹화
- 이전에 외부 규약이 정의된 것이 있으면 이를 활용
- 장비 구조에 독립적인 모델링
- 유지보수와 관련된 기능은 무시

표3에 기능 세분화에 사용되는 양식이 제시된다.

표 2. 기능/장비와 안전성과의 관계

기능	안전성	하위 시스템 1			하위 시스템 2				외부 시스템
		세부 항목 1-1	세부 항목 1-2		세부 항목 2-1	세부 항목 2-2	세부 항목 2-3		
주요기능 1									
세부기능 1-1	C	X	X		X	X	Y		
세부기능 1-2	E	X	X		X	X	Y		
주요기능 2									
세부기능 2-1	N	X	X		X	X	X		

표 3. 기능 세분화를 위한 양식

단계별 기능 모듈(상위 모듈->하위 모듈)						해당 모듈의 기능 설명
M						
	M1					
		M11				
		M12				
			M121			
				M1211		
					M12111	

이런 기능의 하향식 세분화를 통해 모델 선도(모듈과 각 모듈의 정보 입출력 관계를 표시)를 작성하면 정보의 흐름을 추적할 수 있으며 가장 하위 수준의 기능들을 시스템별로 그룹화할 수 있으며(표3에서 왼쪽에는 하위 기능 모듈 열만을 두고 오른쪽에는 시스템 열을 두고 해당 기능에 관련이 있는 시스템칸에 'x'를 표기한후 시스템별로 'x' 표기된 모듈 기능들을 모음. 이를 좀더 확장하면 시스템을 구성하고 있는 장비와 하위 기능과의 관계를 정의하는 기능과 장비간의 관계 표를 구성할 수도 있음). 또한 하위 기능과 외부 규약과의 관계를 정의하는 표를 구성할 수도 있다.

5. 안전성 분석

안전에 대한 정량적 요구 조건이 있다면 이를 하위 시스템에 할당하고 하위 시스템의 안전도 분석 결과를 통합하여 전체 시스템이 달성한 안전도 수준이 요구 조건을 만족시켜야 한다. 안전성 분석은 위험을 찾아내고 제어하며 안전 요구 조건을 만족시키는지 예측하고 필요하다면 이 조건을 만족시키기 위해 설계 변경에 사용된다. 안전성 분석에는 다음과 같은 내용이 포함된다.

(1) 예비적 위험 분석(PHA): 모든 장비에 대해 실행하여 파국 사고(분류 I, II)를 야기할 수 있는 고장을 찾음(분석 및 문서화).

(2) 시스템 위험 분석(SHA): 최종 시스템 구조가 결정되기전인 기본 설계 단계에서 수행. PHA 결과를 입력 자료로 FTA를 통합(분석 및 문서화). 시스템의 잠재적 사고를 찾음. 시스템에 관련된 안전하지 못한 사건을 찾고 위험 분류에 따라 결과 평가. 안전하지 못한 사건에 관계된 시스템 항목 결정(외부 요인에 의한 것 포함). 위험을 제거하거나 통제할 수 있는 설계 요구 조건과 절차를 찾음. 안전과 관련하여 취해진 조치의 정당성을 보이기 위해 FTA 분석 수행(참고 그림1). SHA의 최종 결과를 아래 표4와 같은 양식으로 종합할 수 있다. 이 표에는 위험 영향 분류에 따라 해당 항목을 분류 종합한다.

표 4. SHA 종합

분류 C에 관련된 항목	분류 E에 관련된 항목	분류 N에 관련된 항목

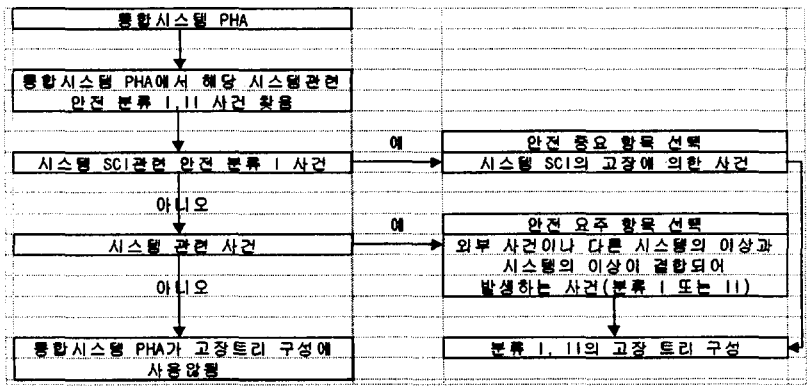

그림 1. 고장 트리 구성 방법

(3) 인터페이스 위험 분석(IHA): 장비의 인터페이스 규약이 설정될 때 수행. 각 시스템간에 교환되는 정보의 기능적 분석(FA)에 기초하여 각 인터페이스의 중요도와 중요 정보의 교환을 위한 기술적 선택 사항을 검증(분석 및 문서화). 시스템의 특성에 따라 분석 내용 및 그에 따른 작성 양식이 상이할 것으로 판단됨.

(4) 안전 중요 항목 목록(SCIL): 안전에 중요한 장비의 목록 작성(문서화). SCIL은 PHA와 IHA에 기초해서 FMECA를 통해 얻어진 안전성 영향 결과로부터 구성. FMECA(참고 그림2)는 기능적

고장의 모드를 찾아내고 고장 영향을 분류(Critical(C), Essential(E), Non safety(N))하고 고장에 기인한 불안전한 사건을 찾아 위험을 제거하거나 제어할 수 있는 수단을 찾기 위함이다.

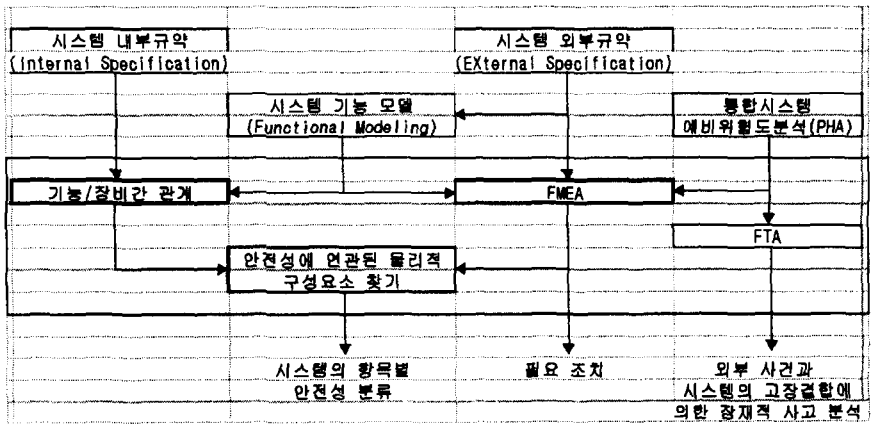

그림 2. FMECA의 입출력 관련 문서

(5) 안전도 할당: 안전 요구 조건을 하위 시스템에 할당(할당 및 문서화). 이상의 분석 결과를 토대로 하위 시스템에 대한 안전 요구 조건을 할당하고 이것이 결과적으로 하위 시스템의 안전도 목표치가 됨. 안전 요구 조건의 할당은 시스템 장비에 대한 정량적 요구치 할당과 시스템 장비가 접하는 외부 조건과 인간의 오류에 대한 정의를 포함한다.

(6) 하위 시스템 위험 분석(SSHA): 신뢰도 분석시 사용된 것을 이용하여 식별된 위험에 대해 FMECA를 수행(분석 및 문서화).

(7) 안전성 시험 및 검증 프로그램(문서화). 안전을 위한 조치, 기준과 권고 사항등이 구현되었음을 입증하기 위해 시험 및 검증 프로그램이(중간 과정에서 수정 및 보완될 수 있음) 작성 수행된다. 이 프로그램에는 수행된 동작이 연대순으로 기술되며 통상적 시험과 특수 시험으로 구성됨.

(8) 안전성 평가(필요하다면 분석, 문서화). 안전성 분석 결과를 평가하는 것으로 하위 시스템의 평가를 시스템별로 그리고 전체 시스템으로 종합한다.

이상에서 설명한 안전 확보를 위한 활동은 아래 그림3에서와 같이 계획 단계에서부터 시운전 시험까지 연계되어 있으며 동시에 RAM 관련 활동과도 연계되어 있다.

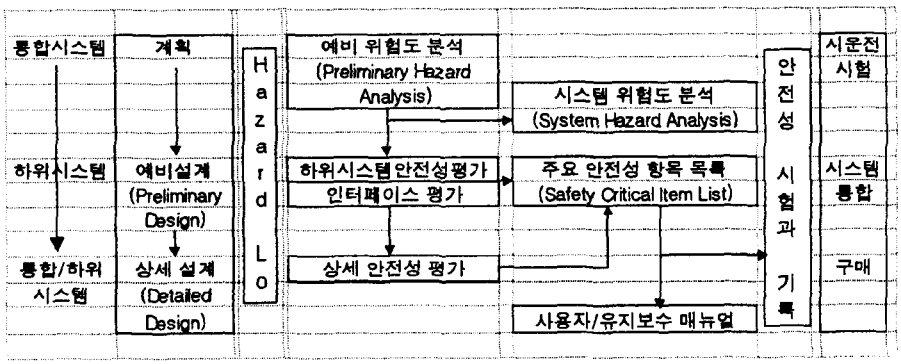

그림 3. 안전성 관련 활동

안전 확보 활동은 기본적으로 V-cycle에 기초하여 제품의 설계(예비 설계 -> 상세 설계)단계에서부터 제품의 제작/통합 및 시험 단계까지 그 안전성을 확인하는 과정을 포함한다.

6. 문서화

앞 단원에서 논의된 안전성 분석 내용은 문서로 작성되며 여기에 추가로 다음의 3개 문서가 작성된다. 프로젝트 기간 동안: Event Sheet, Hazard Log. 프로젝트 종료시: 안전성 종합 보고서

1) Event Sheet

잘못된 사건이 발생할 때 이 문서가 작성된다. 이 문서는 개발자의 안전 관리 조직의 내부 절차에 따라 작성, 배포된다. 이 문서에 따라 Hazard Log를 갱신한다.

2) Hazard Log

이 문서의 목적은 프로젝트 기간 동안 발생한 모든 안전에 관한 문제를 기록, 추적하는 것이다. 프로젝트 종료시 모든 감지된 문제가 해결되었음을 보여야 한다. 안전 관리 조직의 관리자가 작업의 시점에서 HL을 열고 안전 관리 문제가 발견될 때 마다 이 기록을 갱신한다. 이 기록에는 식별 번호, 날짜, 문제에 대한 서술, 관련 문서와 문제의 현재 상태를 기술한다.

3) 안전 종합 보고서

이 보고서는 달성된 안전 수준을 종합적이고 포괄적으로 제시해야 한다. 이 보고서는 이전에 수행 작성된 보고서, SHA, SCIL, IHA, HL, 안전성 평가, 안전성 검증 및 확인 내용을 포함해서 위험을 찾아내고 제거/제어하는데 상용된 방법론 요약하고 수행된 분석을 목록화하고 안전을 확보하기 위해 어떤 예비 조치나 권고 사항이 필요하다면 잔류 위험을 제시하고 동시에 다음 사실을 제시해야한다.

- 발견한 위험이 제거되었거나 이와 관련된 위험이 제어 됨
- 안전 관련 요구 조건이 있으면 이것이 만족됨
- 안전 관련 외부 요인에 대한 가정이 있으면 이를 제시
- 안전 관련 모든 시나리오가 고려되었음을 입증

안전성 평가에는 위험도 인식과 차량의 경우 탈선, 충돌, 화재/폭발, 탈출, 상해 등, 전차선의 경우 결빙, 이선, 낙뢰, 단선 등, 신호 시스템의 경우 충돌, 탈선 등에 대한 안전성 분석을 포함해야 함 (예비 위험도 분석, 시스템 위험 분석 등을 통해 찾아진 위험과 그 대책 기술). 위험도 분석에 기초하여 위험 요소에 대한 안전 확보 방안 및 그 처리 내용을 포함하고 개별 시스템의 안전성 종합 보고서에 기초하여 안전에 대한 종합적인 의견을 제시해야 한다. 위험도 분석에서 합의대로 구현된 안전성을 입증하는 문서에 대한 참고 목록 색인을 부록에 표시하고 안전성 검사 및 확인에서는 시스템별로 그리고 전체 시스템에 대해 검사 및 확인 내용을 기술하며 검사에는 문서 검사, 확인에는 설계와 안전성 중요 항목에 대한 확인 내용을 포함한다. 그림4에 계획에서 확인까지 안전성을 포함한 전체 RAMS에 필요한 문서를 표시하였다.

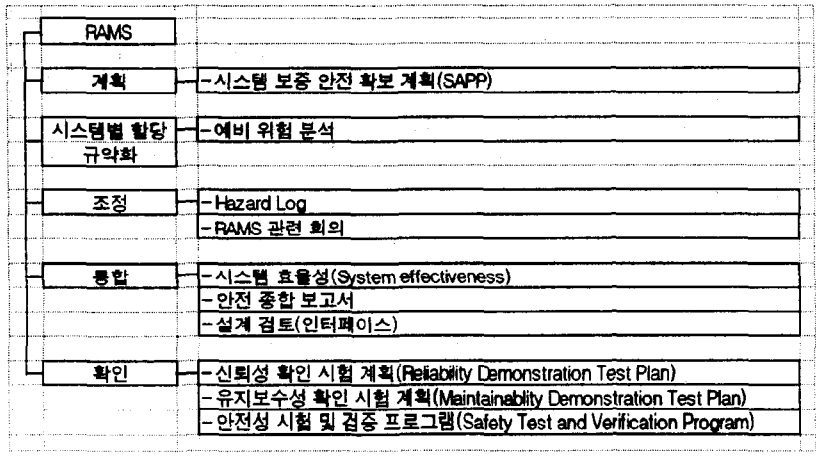

그림 4. RAMS 관련 문서

7. 결론

개발(설계/제조/시험) 단계에서의 문서는 품질 확보 계획에 준해서 작성될 것이며, 안전 관련 문서는 내부 절차에 따라 안전 관리 조직의 관리자에 의해 검사되어야 한다. 설계 마지막 단계에서 설계 검토가 이루어져야 하며 안전 관리자는 이 검토 과정에 참여하여 안전 관련 내용이 설계에 반영되었는지 검증해야 하고 그 결과를 안전 종합 보고서에 포함해야 한다. 프로젝트 진행 동안 시스템 엔지니어링 과정을 통해 안전 관련 회의가 정기적으로 그리고 특정 문제가 안전 관리자나 시스템 엔지니어링 관리자에 의해 제기되었을 때 열릴 수 있어야 하며 이를 통해 문제가 해결될 수 있어야 한다. 또한 안전 뿐만아니라 시스템의 신뢰성 보장을 위해 안전 관리를 포함한 RAMS를 관리하는 독립적인 조직이 개발 주체에 반드시 필요할 것이며 그 독립성 여부가 결과의 성패를 좌우할 것이다.

참고 문헌

1. USA MIL-STD 882C.
2. Manual for the development of rail transit system safety program plans, APTA(American Public Transit Association).
3. 경부고속철도 계약서 Exhibit D: System Assurance and Safety