The Transactions of the Korean Institute of Electrical Engineers Vol. 63P, No. 4, pp. 226~235, 2014
http://dx.doi.org/10.5370/KIEEP.2014.63.4.226

철도 시스템 기능 안전(Functional Safety) 및 인증

Railway System Functional Safety and Certification

김 유 호† · 이 수 환* · 박 강 훈** · 고 태 국***
(You-Ho Kim · Soo-Hwan Lee · Kang- Hun Park · Tae-kuk Ko)

Abstract - Nowadays, railroads are considered the most efficient form of mass transportation. Furthermore, it is necessary that railroads be paired with state-of-the-art safety equipment. Unfortunately, it is impossible to prevent 100% of accidents that may be caused by system or human errors. In order to prevent future accidents, RAMS activity and Functional Safety Certification are required for new systems that are under development. In this paper we evaluate the necessity of the application of RAMS and the performance of RAMS in the system development process. We also explore the Safety Evaluation Procedure required for RAMS certification.

Key Words : RAMS(Reliability, Availability, Maintainability and Safety), SIL(Safety Integrity Level), HTC(Hybrid Track Circuit), V&V(Verification, and Validation), ISA(Independent Safety Assessment)

1. 서 론

과거에는 시스템 개발 또는 구축에 있어 해당 기업의 노하우와 기준이 시스템 개발에 많은 영향을 끼쳤다면 근래에는 산업의 급속한 발전과 함께 엄격한 국가의 표준과 더 나아가 국제 표준규격 기준을 준수한 시스템으로 개발되고 있다. 특히 철도는 특수한 교통수단으로 신속한 이동과 안전한 교통수단이지만 사고발생시 자칫 대형사고로 많은 인명사상에 이를 수 있어 안전에 대한 요구가 대단히 높으며, 안전성을 높이기 위하여 각종 열차제어시스템이 반영된 첨단 교통수단 이다. 하지만 시스템오류 및 기관사의 실수는 언제든지 발생할 수 있기 때문에 사고의 위험으로부터 완전히 자유로울 수 없는 것이 사실이다. 따라서 더욱더 안전에 대한 요구사항이 높아지면서 시스템 개발시 발생할 수 있는 위험원(Risk)을 줄이기 위하여 RAMS (Reliability, Availability, Maintainability and Safety) 활동과 기능 안전에 대한 인증이 점차 필수 사항으로 자리를 잡아가고 있다.

RAMS는 개발 대상 시스템의 개념 단계부터 폐기 단계에 이르는 전체 수명주기 단계 동안에 시스템 개발 단계와 맞물려서 수행되며, RAMS는 어떤 시스템을 장기간 운용하거나 그 시스템의 전반적인 수명주기동안 수립된 공학적 개념, 방법, 도구 및 기법의 적용에 의해 성취되는 특성을 갖는다. 시스템의 RAMS는 시스템 또는 시스템을 구성하는 하위시스템 및 컴포넌트들이 명시된 기능을 정상적으로 수행하고 있고, 안전하게 정상 운용되고 있는 정도를 정성적이거나 정량적인 척도로 명시된다. 따라서 본 논문에서는 시스템 개발에 있어 시스템 기능안전 및 안전에 대한 인증 절차와 실제적용 사례를 설명하고자 한다.

철도 시스템의 목표는 정해진 수준의 철도 수송을 안전하게 달성하는 것이다. 철도 RAMS는 철도 시스템의 목표를 달성할 수 있다는 확신을 기술하고 있는 것으로 고객에게 제공되는 서비스의 품질에 분명하게 영향을 미치며, 서비스의 품질은 기능성이나 운용 성과와 관련된 특성에 영향을 받는다. Neil Storey (1996)는 컴퓨터 시스템 안전성을 세 가지 측면으로 분류하고 있다. 첫 번째는 시스템 자체의 '1차 안전성(Primary safety)'으로 감전이나 전기적인 충격, 화상이나 화재로 인한 위험 등이 해당된다. 두 번째는 '기능안전(Functional safety)'으로 컴퓨터에 의해 직접적으로 제어되는 기기와 관련되는 것으로 컴퓨터 하드웨어와 소프트웨어의 올바른 기능과 연관된다. 세 번째는 '간접적인 안전성(Indirect safety)'으로 컴퓨터 고장이나 부정확한 정보 생성으로 인한 간접적인 결과와 관련된다.
철도 기능 안전 규격의 모태가 되는 IEC 61508은 위 세 가지 안전성 측면 중 두 번째, 즉 기능 안전을 다루고 있다. 유럽의 인증 기관이 철도시스템 분야에 대한 안전성 평가를 수행할 때 설계, 제조 및 운영에 관련된 시스템 사양서와 국제 규격, 유럽연합(EU) 규격뿐만 아니라 해당 국가의 규정이나 법령을 기준으로 하고 있다. 철도 신호 분야의 안전성 평가는 CENELEC 규격인 EN 50126, EN 50128, EN 50129를 기반으로 하고 있으며 그 외에 통신 규격인 EN 50159와 각종 환경 조건에 대한 규격인 EN 50125-3 등을 기반으로 하고 있다.

2. 철도 시스템 기능안전 규격

철도 신호 애플리케이션의 기능 안전에 관련된 주요 CENELEC 규격 범위 및 관계는 그림 1과 같다. 그림 1의

† 교신저자 : 연세대학교 전기전자공학과 박사재학
E-mail : asa812@korea.com
* (주)에이알텍 기술연구소 소장
** (주)에이알텍 기술연구소 부장
*** 연세대학교 전기전자공학과 교수
접수일자 : 2014년 7월 8일
수정일자 : 2014년 9월 23일
최종완료 : 2014년 10월 15일

규격은 모든 안전 관련 철도 신호 시스템, 하부시스템 및 기기에 적용될 수 있다.

EN 50126(1999)은 RAMS 규격으로 철도 기관과 철도 관련 산업을 위해 신뢰성, 가용성, 정비성 및 안전성 관리를 지속적으로 수행할 수 있도록 하기 위한 절차를 제공한다. 이 규격은 철도 애플리케이션의 전체 수명주기 단계별로 세부적인 RAMS 활동에 대해 정의하고 있으며 철도 기관과 철도 관련 산업체가 RAMS 요구사항을 개발하고, 이행하기 위한 기준을 제공한다. EN 50128(2011)은 철도 시스템에 대한 소프트웨어 규격으로 철도 분야의 제어용 안전 관련 소프트웨어의 개발, 배치 및 유지보수와 보호 시스템이 준수해야 할 일련의 요구사항들을 제공한다. 이 규격은 소프트웨어의 개발 수명주기 단계별 활동에 연관된 조직 구조, 조직 간의 관계 및 책임을 정의하고 있으며, 인력의 자격과 전문성에 대한 기준을 제공한다. EN 50129(2010)는 철도 신호분야에서 안전 관련 전자 시스템의 승인을 위한 요구사항을 정의한 규격이다. 신호용 안전 관련 전자 시스템은 하드웨어와 소프트웨어 측면을 포함한다. 전체 안전 관련 시스템을 설치하기 위해서 시스템의 전체 수명주기 동안 하드웨어와 소프트웨어 측면이 모두 고려되어야 한다. 이 규격은 안전 관련 하드웨어와 전체 시스템에 대하 요구사항을 정의하고 있으며 다른 요구사항은 연관된 CENELEC 규격에 정의되어 있다.

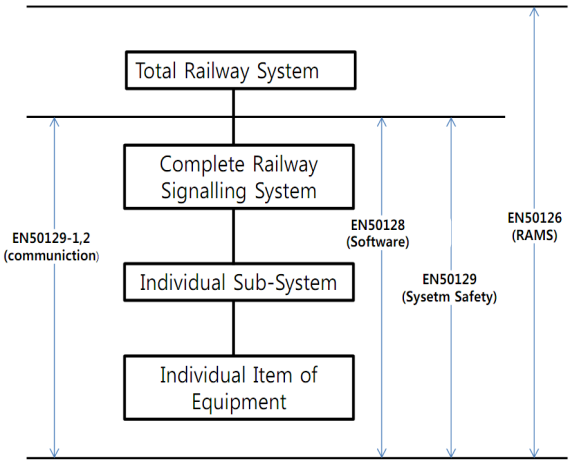

그림 1 CENELEC 기능안전 규격 범위
Fig. 1 Range of functional safety standards CENELEC

EN 50159(2010)는 통신 규격으로 전송 시스템의 안전 관련 통신에 대해 고려해야 할 요구사항을 제공한다. 안전 관련 전자 시스템이 다른 장소 간의 정보를 전송할 경우 전송 시스템은 안전 관련 시스템의 필수 부분이 되고 EN 50129에 의하면 종단 간 통신이 안전하다는 것을 증명해야 한다. 안전성 요구사항은 전송 시스템의 특성에 따라 다르다. 그 시스템의 안전성을 입증하는 방법의 복잡성을 감소시키기 위해 전송 시스템은 세 개의 범주로 분류하고 있다. 첫 번째는 시스템 수명주기 동안 설계자가 통제할 수 있고 기기의 수나 특성이 고정된 시스템이다. 두 번째는 기기의 수나 특성을 부분적으로 알 수 없거나 고정되지 않지만 권한이 없는 접속을 배제할 수 있는 시스템이다. 세 번째는 설계자가 통제할 수 없고 권한이 없는 접속을 고려해야 하는 시스템이다.

3. 시스템 개발 내용 및 RAMS 적용대상

하이브리드궤도회로 시스템 개발에 철도시스템 기능안전과 관련하여 적용하고자 한다. 하이브리드 궤도회로(Hybrid Track Circuit : 이하 HTC) 개발목적은 RFID를 이용한 열차를 검지하는 방식으로 현재에도 RFID를 이용한 열차제어 및 검지하는 방법은 이미 오래전부터 상용되어 왔다 그러나 본 연구에서 개발하는 목적의 초점은 열차검지시스템의 해외 의존도 탈피와 고가의 외산 설비를 국산화시켜 국내 철도기술을 세계화 하는데 있다. 그림 2는 연구에서 개발하고 있는 RFID기술을 차량에 탑재한 시스템 구성도이며, 크게 2가지의 핵심설비로 분류된다. 지상의 침목에 설치된 태그(Tag)는 차상의 리더기에서 송출된 전력파를 수신하여 자신의 고유 정보를 차상리더기에 송신한다. 이때 차상과 지상태그간의 정보전송은 900MHz의주파수로 이뤄진다. 차상 리더기에서 수신된 정보는 차상의 제어장치에서 태그와의 거리를 분석하고 궤도회로를 생성하여 열차의 위치를 검지한다.

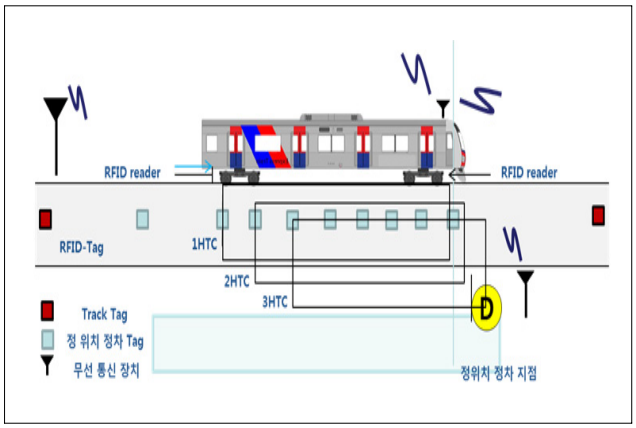

그림 2 하이브리드 궤도회로 시스템 구성도
Fig. 2 Hybrid track circuit system configuration

4. 시스템 개발 단계별 RAMS 활동

4.1 철도 RAMS 구성 요소

철도 RAMS의 요소인 신뢰성, 가용성, 정비성 및 안전성 사이의 상호작용을 고려하는 것이 중요하다. 안전성과 가용성은 경우에 따라 상호 상충될 수 있는 요소이다. 즉, 상황에 따라 안전성을 높이면 가용성이 낮아지고, 반대로 가용성을 높이면 안전성이 낮아질 수 있다. 그러므로 이들 두 요소 간에 상충되는 것을 잘 관리해야 한다. 시스템을 운용하면서 두 요소의 목표를 달성하기 위해서는 신뢰성과 정비성의 모든 요구사항을 만족해야만 하며, 장기간의 지속적인 운용 및 정비 활동과 시스템의 환경을 관리해야만 한다. 철도 RAMS 요소의 내부 관계는 그림 3과 같다.

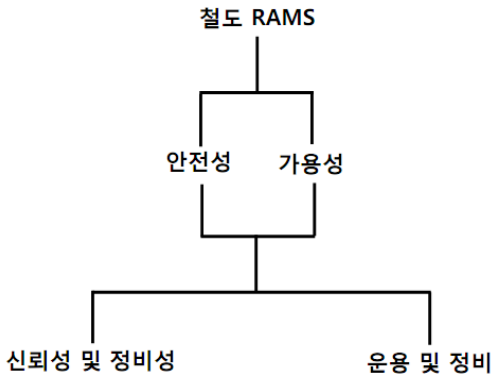

그림 3 철도 RAMS 요소의 내부 관계
Fig. 3 Railway RAMS elements of internal relations

가용성에 대한 기술적인 개념은 다음의 신뢰성, 정비성, 운용 및 정비에 관한 사항을 기반으로 한다.

① 신뢰성
- 특정 애플리케이션과 환경에서 모든 가능한 시스템 고장 모드
- 각 고장의 발생확률 또는 발생빈도
- 시스템의 기능성에 관한 고장의 영향

② 정비성
- 계획된 정비를 수행하는데 걸리는 시간
- 결함의 감지, 규명 및 위치 파악에 걸리는 시간
- 고장 난 시스템을 복구하는데 걸리는 시간

③ 운용 및 정비
- 시스템 수명주기에 관련된 모든 가능한 운용 형태와 필요한 정비 활동
- 인적 요인 문제

안전성에 대한 기술적 개념은 다음의 5가지 사항을 기반으로 한다.

① 모든 운용, 정비 및 환경 조건에서 시스템의 모든 가능한 위험 요소

② 결과의 심각도에 대한 각 위험의 특성

③ 안전성 및 안전 관련 고장
- 어떤 위험(안전성 관련 고장 모드)을 초래하는 모든 시스템 고장 모드
- 각 안전 관련 시스템 고장 모드의 발생확률
- 사고로 귀결될 수 있는 순차적이거나 동시에 발생하는 사건, 고장, 작동상태, 환경 조건
- 각 사건, 고장, 작동상태, 환경조건 등의 발생확률

④ 안전 관련 부분의 정비성
- 위험 요소나 안전 관련 고장 모드와 관련된 시스템, 구성요소에 대한 정비의 수행
- 안전 관련 부분에 대한 정비 활동 중에 발생하는 오류의 확률
- 시스템을 안전 상태로 복구하는데 걸리는 시간

⑤ 시스템 안전 관련 부분의 시스템 운용 및 정비
- 시스템의 모든 안전 관련 부분에 대한 효과적인 정비 및 시스템의 안전 운용에 영향을 미치는 인적 요인
- 시스템의 안전 관련 부분에 대한 효과적인 정비 및 안전 운용을 위한 도구, 시설 및 절차
- 위험 요소를 처리하고 그 결과를 경감하기 위한 효과적 관리 및 수단

4.2 철도 RAMS 관리

시스템 수명주기 동안에 철도 애플리케이션에 대한 RAMS 요소의 효율적인 관리를 위해서는 다음과 같은 관리 절차를 수립해야 한다.
- RAMS 요구사항의 정의
- RAMS에 저해되는 징후의 평가 및 관리
- RAMS 업무의 계획 및 이행
- RAMS 요구사항의 성취 여부
- 수명주기 동안 적합 여부의 지속적인 감시

이 절차는 철도의 RAMS에 초점을 맞추고 있기는 하지만 이는 전반적인 철도 시스템의 많은 분야 중의 하나이며, 이 절차는 전 철도 시스템의 모든 측면에 대해 기술하고 있는 종합 관리 방법의 한 요소인 RAMS 관리를 위한 계통적인 절차를 기술하고 있다. 어떤 철도기관의 철도 시스템에 대한 안전성의 허용 위험도에 대한 기준은 국가 안전규제기관이나 안전규제기관에서 인정한 철도기관이 정한 안전성 기준을 따라야 한다. 위험도를 평가하고, 관리하고, 저감시켜야 하는 일에 대한 일차적인 책임은 철도기관에 있다. 어떠한 경우에는 시스템이 안전하다는 것을 실증하는 공식적인 증빙 자료의 제출을 요하는 법령의 제정이 필요하다.

시스템 수명주기는 초기의 개념 설계부터 폐기 및 처분에 이르기까지 시스템의 전체 수명주기뿐만 아니라 각 단계별 해당 업무를 포함하는 일련의 과정을 의미한다. 수명주기 내용에는 협의한 시간 내에 적정한 가격에 적정한 제품을 공급할 수 있도록 시스템이 각 단계별로 업무를 진행함에 따라 RAMS를 포함한 시스템의 모든 측면을 계획, 운용, 관리 및 감시를 위한 체계를 제공해야 한다.

4.3 시스템 수명주기 단계별 활동

철도 애플리케이션의 관계에 있어서 적합한 시스템 수명주기는 그림 4와 같다. RAMS 업무는 각 수명주기 단계별 일반적인 프로젝트 업무에 영향을 준다. 각 수명주기 단계별 일반 업무와 RAMS 업무는 다음과 같다.

1단계 개념에서 수행하여야 할 일반 업무로는 HTC프로젝트의 범위와 목적 수립, 재정 분석 및 실용성연구의 착수, 관리절차 수립 등이 해당된다. RAM 업무로는 이전에 달성된 RAM 성과의 검토와 프로젝트의 RAM 관련성을 고려하는 일이다. 안전성 업무는 이전에 달성한 안전성 성과 검토, 프로젝트 관련 안전성 관련 사항 검토, 안전성 정책과 목표 검토 등이 해당된다.

2단계 시스템 정의 및 적용 조건에서의 일반 업무로는 HTC 시스템 임무 프로파일 수립과 시스템 기술서 준비, 운용과 정비 전략의 규명, 그리고 운용 조건의 규명, 정비 조건의 규명, 기존 기반시설의 제약조건의 영향을 확인 및 분석 등이 해당된다. RAM 업무로는 RAM에 대한 과거경험 데이터 평가, 예비 RAM분석 수행, RAM 정책수립, 장기 운용 및 정비 조건의 확인, 그리고 기존 기반시설의 제약조건이 RAM에 미치는 영향 규명 등이 해당된다. 안전성 업무로는 과거의 경험 데이터를 통하여 안전성에 대한 데이터 평가와 예비 위험분석 수행, 그리고 전반적인 안전성 계획을 수립하고, 허용 위험도 기준을 정하고, 기존 기반시설의 제

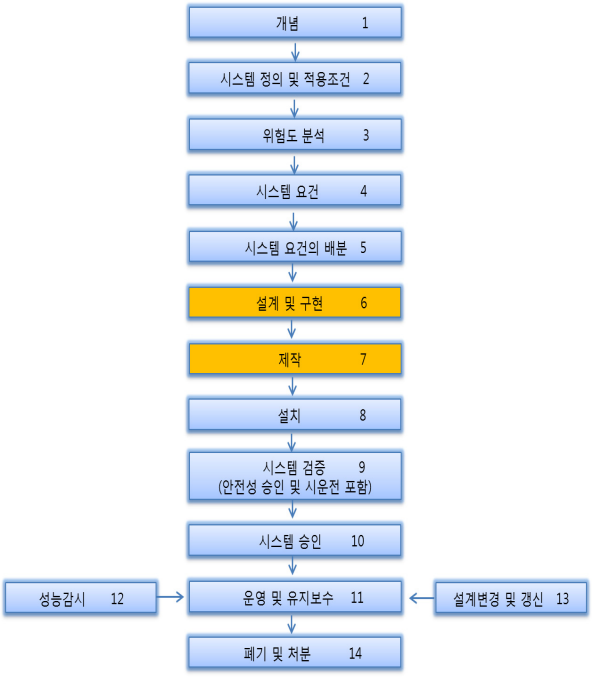

그림 4 시스템 수명주기 단계
Fig. 4 System life-cycle stages

약조건이 안전성에 미치는 영향을 규명하는 일 등이 포함된다.

3단계 위험도 분석 단계에서의 일반 업무로는 HTC 프로젝트 관련 위험도 분석을 수행하는 일이다. RAM 관련 업무는 없으며, 안전성 업무로는 시스템 위험 요소와 위험도 분석을 수행하고, Hazard Log 요구사항 수립 및 위험도 분석을 수행하는 일이 해당된다.

4단계 시스템 요구사항 단계에서의 일반 업무로는 요구사항 분석, 시스템 요구사항 명시, 환경 요구사항 명시, 시스템 실증 및 허용 기준 정의, 검증 계획 수립, 관리, 품질 및 조직 요구사항의 수립과 변동 사항 관리 절차의 수립 등이 해당된다. RAM 업무로는 전반적인 시스템 요구사항 수립, 전반적인 RAM 허용 기준의 정의와 시스템의 기능적 구조의 정의, RAM 프로그램의 수립, RAM 관리 체계의 수립 등이 해당된다. 안전성 업무에는 전반적인 시스템 안전성 요구사항 수립, 안전성 허용 기준의 정의, 안전성에 관련된 기능적인 요구사항 정의, 안전성 관리 체계 수립 등이 해당된다.

5단계 시스템 요구사항의 배분 단계에서의 일반 업무는 시스템 요구사항의 배분이고, RAM 업무는 시스템 RAM 요구사항의 배분이고, 안전성 업무는 시스템 안전성 목표와 요구사항의 배분, 시스템 안전성 계획을 개정하는 일이 해당된다.

6단계 설계 및 구현 단계에서의 일반 업무는 계획의 수행, 설계와 개발 수행, 설계 분석과 시험의 수행, 설계 확인의 수행, 구현과 검증 수행, 물류 지원계획의 수행 등이다. RAM 업무는 신뢰성과 가용성, 정비와 정비성, 최적 정비 정책, 물류지원 등을 포함하여 검토, 분석, 시험, 데이터 평가에 의한 RAM 프로그램의 구현 등이 해당된다. 또한 RAM 프로그램 관리, 하청업체 및 공급자의 관리 업무도 포함된다. 안전성 업무는 Hazard Log, 위험 분석 및 위험도 평가를 포함하여 검토, 분석, 시험, 데이터 평가에 의한 안전성 계획을 이행하는 일이다. 또한 안전성 관리, 하청업체 및 공급자의 관리, Generic Safety Case 준비 등이 해당된다.

7단계 제작 단계에서의 일반 업무로는 생산계획 수행과 제조, 하위시스템이나 컴포넌트의 제조 및 시험, 관련 문서 준비 그리고 교육훈련 수행 등이 해당된다. RAM 업무로는 환경 스트레스 스크리닝(ESS) 수행, RAM 성장 시험 수행 그리고 고장보고, 분석 및 시정조치 시스템 착수 등이 해당된다. 안전성 업무로는 안전성 계획의 이행, Hazard Log 활용하는 일이 해당된다.

8단계 설치단계에서의 일반 업무로는 시스템 조립과 설치가 주요 업무이고, RAM 업무로는 정비 담당자 교육훈련 시작과 예비품의 공급계획 수립 등이며, 안전성 업무로는 설치 프로그램 수립과 이행 등이 해당된다.

9단계 시스템 검증 단계로서 현재 HTC시스템이 적용되어 시험단계에 있다면 일반 업무로는 시운전, 시험운용 수행과 교육훈련 수행 등이 해당되며, RAM 업무로는 RAM 실증평가가 주된 업무이며, 안전성 업무로는 시운전 프로그램 수립 및 이행 그리고 Application Specific Safety Case를 준비하는 일이 해당된다.

10단계 시스템 승인 단계에서의 일반 업무로는 승인 기준에 기초한 승인 절차 수행, 인수를 위한 증빙자료의 수집, 운행 시작 및 시범 운용기간 의 지속 등이 해당되며, RAM 업무는 RAM 실증 평가 주요 업무이고, 안전성 업무는 Application Specific Safety Case 평가가 주요 업무이다.

11단계 운용 및 정비 단계에서의 일반 업무로는 장기간의 시스템 운용, 지속적인 정비수행, 지속적인 교육 및 훈련 수행 등이 해당된다. RAM 업무로는 예비품과 도구의 지속적인 조달, 지속적인 신뢰성 중심정비(RCM)를 위한 물류 지원 수행이 해당되며, 안전성 업무로는 지속적인 안전성 중심의 정비 수행, 지속적인 안전성 성능 감시 및 Hazard Log의 기록 및 관리 등이 해당된다.

12단계의 성능 감시 단계에서의 일반 업무로는 운용상의 성과에 대한 통계자료 수집, 자료의 수집, 분석 및 평가 등이 해당되며, RAMS 업무로는 자료 수집, 분석 및 평가, 운용성과 및 RAMS 통계량이 해당된다.

13단계 설계 변경 및 갱신 단계에서의 일반 업무로는 설계 변경 요구 절차 이행, 설계 변경과 갱신절차의 이행 등이 해당되며, RAMS 업무로는 설계 변경과 갱신을 위한 RAMS 관련 사항을 고려하는 일이 해당된다.

14단계 폐기 및 처분의 단계에서는 폐기되고자 하는 설비 또는 제품에 대하여 폐기 및 처분 계획과 사용중지 이행, 폐

기 이행 순으로 진행되며, RAM 업무는 특별히 필요치 않다. 다만 안전성 업무로는 안전성 계획 수행, 위험 분석 및 위험도 평가 수행과 안전성 계획 이행 절차에 따라 진행되어야 한다.

5. 독립안전성 평가(ISA)절차

5.1 ISA활동 기관의 관계

ISA(Independence Safety Assessment)는 시스템이 RAMS 요구 사항을 충족하고 제품의 달성 여부를 확인하며 시스템의 의도 된 목적에 적합 되는지 여부를 판단 하기 위해 분석하는 과정이다. ISA활동은 다음과 같은 고리로서 고객의 요청에 따라 컨설팅을 하게 되는데 조작자(Operator)는 시스템에 대한 수명주기 단계별 문서를 최초 작성하여 검토자를 통하여 고객(Client)또는 컨설팅업체에 검증을 받는다. 컨설팅 업체는 안전성에 필요한 요구문서를 조작자나 권한이 있는 관리자에게 시스템에 대한 LOP(List of Open Points) 작성하고 적합성 여부를 판단하여 시스템에 대한 문서를 지속적으로 관리한다.

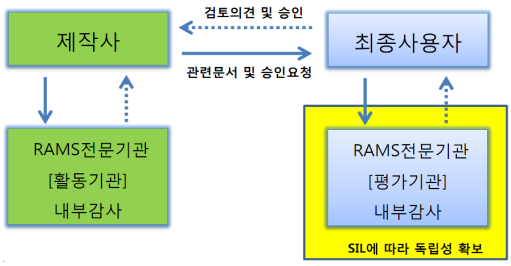

그림 5 ISA활동 기관의 관계
Fig. 5 ISA activity relationship of agency

5.2 문서 갱신 및 처리절차

HTC프로젝트 또한 수명주기 단계별 절차에 의해 작성된 문서는 인증 및 평가기관에 검증을 받아야 한다. 검증기관은 각각 단계별 수명주기에서 생성되어져야 하는 출력물의 내용을 검토하여 EN50126에서 요구하는 내용이 수록되어 있는지 검토하고 누락된 부분에 대하여 내용을 추가하도록 요구하거나 오류로 인한 부분을 수정할 수 있도록 요청을 하면, 시스템 개발사에서는 검증기관의 요청내용이 문서에 수록되어 있는지 혹은 누락되어 있다면 조치결과를 LOP(List of open points)를 작성하여 문제가 클리어(Clear)되도록 한다. 그림 6은 HTC개발에 있어 생성되는 문서 중에서 시스템 품질관리계획서 작성시 검증기관이 요청하는 LOP의 작성 예시를 보여주는 것으로 검증기관이 문서에 대한 이의를 제기하면 조치결과를 수록하여 재 검토를 받는 형식으로 진행되며, 검증기관의 최종 승인이 있기까지 버전(Version)관리를 하여야 한다.

No	Topic	Question				Severity	Answer			Status		
		Initial	Date	Chapter or Page	Text		Initial	Date	Text	Initial	Date	Text
1	RMSP	SMO	2012-06-13	General	본 문서를 작성하는 목적이 기술되어야 합니다.	Minor	KHP	2013.01.29	1. 목적에 기술되어 있습니다.	SMO	2013-01-23	pending
2	RMSP	SMO	2012-06-13	Ch1	적용 범위가 함께 기술되어 있습니다.	Minor	KHP	2013.01.29	3.4 개발 및 RAMS 활동범위에 기술되어 있습니다.	SMO	2013-01-24	pending
3	RMSP	SMO	2012-06-13	Ch2	EN 규격과 IEC 규격이 혼재되어 있습니다. 본 프로젝트와 관련한 적용규격을 명확히 기술하시길 바랍니다.	Major	KHP	2013.01.29	4.1 적용규격에 기술되어 있습니다.	SMO	2013-01-25	pending
4	RMSP	SMO	2012-06-13	General	참조문서 (input documents)가 존재하지 않습니다.	Minor	KHP	2013.01.29	1.3 참고문서에 기술되어 있습니다.	SMO	2013-01-26	pending
5	RMSP	SMO	2012-06-13	General	RAMS 활동의 대상 시스템에 대한 설명이 존재하지 않습니다. (3.3.2절에서 대상 시스템은 확인 하였습니다.)	Major	KHP	2013.01.29	3.2 시스템정의 3.3 시스템 구성에 기술되어 있습니다.	SMO	2013-01-27	pending
6	RMSP	SMO	2012-06-13	Ch 3	본 문서 상에 사용된 약어 및 용어가 모두 정의되어야 하며, 사용되지 않은 약어 및 용어는 제거되어야 합니다.	Minor	KHP	2013.01.29	2.2 약어에 기술되어 있습니다. 사용하지 않는 약어는 제거 되었습니다.	SMO	2013-01-28	pending
7	RMSP	SMO	2012-06-13	Ch 4 4.1	조직도가 명확하지 않습니다. EN 50129 or IEC 62425 상의 5.3.3 safety organisation을 기반으로, RAMS 조직이 구성되어야 합니다.	Major	KHP	2013.01.29	5.1 프로젝트 수행조직에 기술되어 있습니다.	SMO	2013-01-29	pending
8	RMSP	SMO	2012-06-13	Ch 4 4.2	RAMS 조직의 구성원에 대한 설명과 각 구성원의 책임 및 역할, 경험, 자격, 적절한 교육 등의 내용이 상세히 기술되어야 합니다.	Major	KHP	2013.01.29	5.1 프로젝트 수행조직 5.2 RAMS 활동조직구성에 기술되어 있습니다.	SMO	2013-01-30	pending
9	RMSP	SMO	2012-06-13	Ch 5	시스템 개발 수명 주기를 기반으로, 각 단계별 RAM 활동에 대한 상세한 내용이 기술되어야 합니다.	Major	KHP	2013.01.29	6. 시스템 수명주기별 RAMS활동에 기술되어 있습니다.	SMO	2013-01-31	pending
10	RMSP	SMO	2012-06-13	Ch 5	RAM 활동 절차에 대하여 개괄토가 이루어져야 하며, RAM 분석을 위해 적용되는 모든 기법이 소개되어야 합니다.	Major	KHP	2013.01.29	7. RAMS활동 절차 및 분석 방법에 기술되어 있습니다.	SMO	2013-02-01	pending
11	RMSP	SMO	2012-06-13	Ch 5 5.2.2	시스템 개발 수명 주기를 기반으로, 각 단계별 안전성 활동에 대한 상세한 내용이 기술되어야 합니다. (EEC 6227)를 기반으로 한 소프트웨어 포함)	Major	KHP	2013.01.29	6.시스템 수명주기별 RAMS활동에 기술되어 있습니다.	SMO	2013-02-02	pending
12	RMSP	SMO	2012-06-13	Ch 5	안전성 활동 절차에 대하여 개괄토가 이루어져야 하며, 안전성 분석을 위해 적용되는 모든 기법이 소개되어야 합니다.	Major	KHP	2013.01.29	Answer 10번과 동일한 답변입니다.	SMO	2013-02-03	pending

그림 6 LOP 작성 및 조치결과
Fig. 6 LOP and actions create resultsl

6. 기능 안전 및 안전성 승인 조건

6.1 SIL 개념

IEC 61508-5에 의하면 안전 무결성(Safety Integrity)은 안전 관련 시스템이 일정 기간 내에 모든 일정 조건에서 요구되는 안전 기능을 성공적으로 수행할 확률로 정의하고 있다. 안전 무결성은 안전기능을 수행할 때 안전 관련 시스템의 성능과 관련된다.

안전 무결성은 다음 두 가지 요소를 포함하고 있다.

- 하드웨어 안전 무결성(Hardware safety integrity): 위험한 고장 유형으로 하드웨어의 임의 고장과 관련된 안전 무결성의 일부분
- 계통 안전 무결성(Systematic safety integrity): 위험한 고장 유형으로 계통 고장과 관련된 안전 무결성의 일부분

안전 무결성 수준(SIL, Safety Integrity Level)은 안전 무결성 값의 범위에 해당하는 이산적인 수준을 의미한다. SIL은 어떤 시스템, 하부시스템 요소나 컴포넌트의 속성이 아니다. 'SIL n 안전 관련 시스템'(여기서 n은 1, 2, 3 또는 4)이란 그 시스템이 SIL n까지로 안전 기능(Safety functions)을 잠재적으로 지원할 수 있다는 것을 의미한다.

6.2 작동 유형과 SIL 등급

작동 유형은 안전 기능이 사용될 방식과 관련되며 작동 요구 빈도에 따라 다음 세 가지로 분류된다.

- 낮은 요구 모드(Low demand mode): 안전 기능에 대한 작동 요구 빈도가 1년에 한 번보다 크지 않은 경우
- 높은 요구 모드(High demand mode): 안전 기능에 대한 작동 요구 빈도가 1년에 한 번보다 큰 경우
- 연속 모드(Continuous mode): 안전 기능에 대한 작동 요구 빈도가 연속적인 경우

낮은 동작 요구 모드의 경우 안전 기능에 대한 요구 시 위험 고장의 평균 확률(PFDavg) 범위별 SIL은 표 1과 같으며, 높은 동작 요구 모드 또는 연속 동작 모드의 경우 안전 기능의 위험 고장에 대한 평균 빈도(PFH) 범위별 SIL은 표 2와 같다.

표 1과 표 2는 안전 관련 시스템에 의해 수행되는 안전 기능에 SIL을 할당되듯이 고장에 대한 조치 목표와 관련된다. 안전 관련 시스템의 모든 측면에 대해 정량적으로 안전 무결성을 예측할 수는 없을 것이다. 고장 조치 목표를 달성하는 것을 보장하기 위해 고려해야 하는 예방책에 관한 정

표 1 낮은 요구 모드의 SIL
Table 1 Low demand mode SIL

SIL	PFDavg
4	≥1E-05 to <1E-04
3	≥1E-04 to <1E-03
2	≥1E-03 to <1E-02
1	≥1E-02 to <1E-01

표 2 높은 동작 요구 모드 또는 연속 동작 모드의 SIL
Table 2 High demand mode or continuous mode of operation of operation SIL

SIL	PFH(/h)
4	≥1E-09 to <1E-08
3	≥1E-08 to <1E-07
2	≥1E-07 to <1E-06
1	≥1E-06 to <1E-05

성적인 기법을 적용해야 한다.

6.3 SIL 요구사항 결정 방법

SIL 요구사항을 결정하는 데 사용될 수 기법에는 여러 가지가 있다. 예를 들면, ALARP(As low as reasonably practicable) 방법, 정량적인 방법, Risk Graph 방법, LOPA(Layer of protection analysis), Risk Matrix 등이 있다. 이러한 방법 중에서 적용되는 분야에 따라 적절한 방법을 선택해야 한다. SIL 요구사항을 결정하는 방법 중에서 Risk Graph 방법을 예로 들면 다음과 같다. 이 방법은 정성적 또는 정량적인 기준으로 사용될 수 있으며 다음 수식을 기반으로 한다.

R= (f) of a specified (C)

여기서
- R: 위험도
- f: 위험한 사건의 빈도
- C: 위험한 사건의 결과

Risk Graph 도식에 대한 예는 그림 7과 같다.

그림 7에서 S는 결과의 심각도로 세부 인자의 정의는 다음과 같다.
- S1: 경미한 부상
- S2: 한 명 또는 여러 명의 돌이킬 수 없는 심각한 부상 또는 한 명 사망
- S3: 여러 명 사망
- S4: 파국적인 영향, 매우 많은 사망자

A는 위험의 노출정도로 세부 인자의 정의는 다음과 같다.
- A1: 위험에 거의 노출되지 않거나 드물게 노출
- A2: 위험에 빈번한 또는 지속적인 노출

G는 위험/결과에 대한 방어로 세부 인자의 정의는 다음

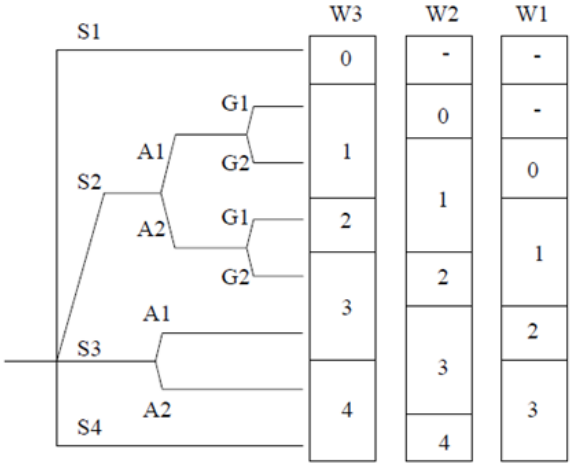

그림 7 Risk Graph 예
Fig. 7 Risk Graph Example

과 같다.
- G1: 가능한 인자
- G2: 불가능한 인자

W는 위험 발생 가능성으로 세부 인자의 정의는 다음과 같다.
- W1:매우 낮음 (두 개의 방호벽(barrier))
- W2:낮음(한 개의 방호벽)
- W3:상대적으로 높음(추가적인 방호벽 없음)

6.4 안전성 승인 조건

1) 종합안전성보고서(Safety Case)

종합안전성보고서는 명시된 안전성 요건을 만족한다는 것을 증빙하는 서류이다. 안전에 관련된 시스템이 대상 애플리케이션에 대해 충분히 안전하다는 것을 승인할 목적으로 요구되는 조건은 크게 다음 세 가지 측면에 대한 증거 자료이다.
- 품질 관리 증거
- 안전성 관리 증거
- 기능 및 기술 안전성 증거

안전에 관련된 시스템이 충분히 안전하다는 것으로 승인받기 전에 장치, 하부시스템 및 시스템 수준에서 위 세 가지 측면의 모든 조건들을 만족해야 한다. 이러한 조건을 만족한다는 내용의 증거를 구조화된 안전성 입증 문서에 포함해야 하는데 이를 종합안전성보고서(Safety Case)라고 한다. 종합안전성보고서는 일반제품, 응용분야 또는 특정 응용분야에 대한 안전성 승인을 얻기 위해서 안전성 인증기관에 제출할 전반적인 서류로 이루어진 근거 자료이다.

2) 품질관리 증거

안전성 승인을 위해 만족해야 할 첫 번째 조건은 시스템/하부시스템/장치의 품질이 수명주기 동안 효과적인 품질관리체계에 의해 관리되고, 지속적으로 관리되어야 한다는 것이다. 이를 입증하는 문서로 이루어진 증거를 품질관리 보고서에 제시해야 한다. 품질관리체계의 목적은 수명주기의

각 단계에서 인적 오류의 발생을 최소화하고, 시스템, 하부 시스템 혹은 장치에서 계통 결함으로 인한 위험도를 저감시키기 위한 것이다. 품질관리에 대한 요구사항의 준수는 SIL 1에서 SIL4까지 필수이다.

3) 안전성 관리 증거

안전성 승인을 위한 만족해야 할 두 번째 조건은 시스템, 하부시스템 및 장치의 안전성이 효과적인 안전성 관리 절차에 의해 관리되고 지속적으로 관리되어야 한다는 것이다. 이 절차의 목적은 수명주기 동안 안전 관련 인적오류의 발생을 저감시키기 위한 것이고, 안전과 관련된 계통 결함으로 인한 잔여 위험도를 최소화하기 위한 것이다. 이를 입증하는 문서로 이루어진 증거를 안전성관리 보고서에 제시해야 한다. 안전성 관리 절차의 적용은 SIL 1에서 SIL4까지 필수이다.

4) 기능 및 기술 안전성 증거

안전성 승인을 위한 만족해야 할 세 번째 조건은 시스템, 하부시스템 및 장치가 설계의 안전성에 대한 기술적인 증거이다. 기술 안전성 보고서에는 다음과 같은 내용을 포함해야 한다.

가) 서론

시스템, 하부시스템 및 장치의 안전성 범위와 기술적인 안전성 원리를 포함하여 설계에 대한 전반적인 설명을 제공해야 한다. 또한 설계의 기술적인 안전성에 대한 기준으로 사용한 규격이나 조건 등을 언급해야 한다.

나) 올바른 기능의 작동 보증

명시한 운영 및 안전성 요구사항에 따라 결함이 없는 정상적인 조건에서 시스템, 하부시스템 및 장치가 올바른 작동을 실증하는데 필요한 모든 증거를 포함해야 한다.

다) 결함의 영향

시스템, 하부시스템 및 장치가 하드웨어의 랜덤 결함의 경우에 정량적인 안전성 목표를 포함하여 명시한 안전성 요구사항을 만족하는 지를 실증해야 한다. 게다가 기능 결함은 품질 및 안전성 관리를 수행하더라도 여전히 존재할 수 있다. 결과적으로 나온 위험도를 허용 가능한 수준으로 저감하기 위해 기술적으로 취한 조치를 실증해야 한다. 또한 전체 시스템의 SIL보다 낮은 SIL을 갖는 어떤 시스템, 하부시스템 및 장치 내에 결함은 전체 시스템의 안전성을 저감시킬 수 없다는 것을 실증해야 한다.

라) 외부 영향을 갖는 작동

시스템 요구사항 명세서에 정의한 외부의 영향을 받을 때 시스템, 하부시스템 및 장치는 명시한 운영 요구사항을 계속 수행해야 하며, 안전성 요구사항을 계속 수행해야 한다.

마) 안전 관련 애플리케이션 조건

시스템, 하부시스템 및 장치의 애플리케이션에서 관측해야 할 규칙, 조건 및 제약사항을 명시해야 한다. 또한 관련된 하부시스템이나 장치의 종합안전성보고서에 포함된 적용 조건을 포함해야 한다.

바) 안전성 자격증명 시험

운영 조건하에서 안전성 자격증명 시험의 성공적인 완료를 실증하는 증거를 포함해야 한다.

7. 안전성 평가 절차

TUV SUD나 로히드와 같이 유럽의 대표 인증기관이 안전성을 평가할 때 특정 시스템이 안전하기 위해서는 하드웨어의 고장에 대해서도 안전 무결성을 가져야 하고, 기능(또는 계통)고장에 대해서도 안전 무결성을 가져야 한다는 관점으로 접근하게 된다. 인증기관의 안전성 평가 절차를 간단히 소개하면 요구사항 단계와 구현단계로 나눌 수 있으며, 각 단계의 주요 사항은 다음과 같다.

1) 요구사항 단계 (개념 단계)

가) 평가 계획서 작성

CENELEC 규격을 기반으로 다음과 같은 내용을 고려하여 평가 계획서를 작성한다.

- 평가 대상 시스템 범위
- 평가 목적과 범위
- 평가 방법 및 절차
- 평가 내용

나) 기술 및 기능에 대한 안전성 원리 평가

기술 및 기능 안전성 평가 이전에 시스템의 원리가 CENELEC 규격과 고객의 요구사항에 적합한지를 평가한다.

다) 요구사항 및 계획 문서 평가

개념 단계에서 중요한 평가 내용 중 하나로 각종 요구사항 명세서와 계획서(프로젝트 계획, 품질보증계획, 안전성 관리 계획 등)를 평가한다.

라) 안전성 심사

안전성 원리, 요구사항 및 계획 문서를 평가한 후 제작사에 대한 사전 심사를 수행하게 되는데 품질관리와 안전성 관리 측면의 세부 내용을 확인하고 심사한다.

마) 상태 평가 보고서

요구사항 단계에서 수행한 심사 활동에서 발견한 사항에 대한 평가 보고서를 작성한다. 이 보고서를 기반으로 다음 단계에서 수행할 평가 활동에 대한 방향을 세부적으로 정한다.

2) 구현 단계 (세부 단계)

가) 세부 기술 평가

안전성 평가는 CENELEC 규격에 따라 다음 세 가지 측면으로 수행한다. 이는 종합안전성보고서의 핵심 내용에 해당한다.

- 품질 관리
- 안전성 관리
- 기능 및 기술 안전성

나) 심사

세부 설계 단계에서 작성된 문서에 대해 심사하고 현장 심사를 수행한다. 심사 항목으로는 형상관리, 품질관리, 안전성 관리, 각종 설계 관련 위험도 분석 자료 심사 및 공장심사 등이 포함된다.

다) 고장 주입 시험 및 기능시험

현장에서 주로 수행하는 심사 활동으로 고장 주입 시험은 시스템에 고장이 발생할 경우 시스템이 의도한 대로 동작하는지를 검사하기 위해 수행한다. 기능시험은 복잡한 동작 상황을 갖는 요구사항에 대해 주요 안전 기능을 선택해서 수행한다.

라) 최종 평가 보고서
구현 단계에서 최종 평가를 수행한 후 작성하는 평가 보고서이다.

8. HTC프로젝트 RAMS활동 및 인증절차

8.1 HTC프로젝트 단계별 RAMS 활동 절차

현재 하이브리드궤도회로(이하 HTC)개발은 EN50128의 기준에 따라 단계별 절차에 따라 개발 진행 중에 있으며, 연구개발에 참여한 에이알텍, 외 2개 기관이 맡은 업무에 대하여 RAMS에 근거하여 ISA활동을 하고 외부 인증기관인 TUV가 시스템 수명주기에서 요구하는 항목대로 진행되어 가고 있는지를 확인하기 위한 독립적 안전성평가(ISA)를 하는 방식으로 추진되고 있다. 아래 그림 8은 HTC프로젝트의 RAMS를 진행하는 절차를 도식화한 것이다.

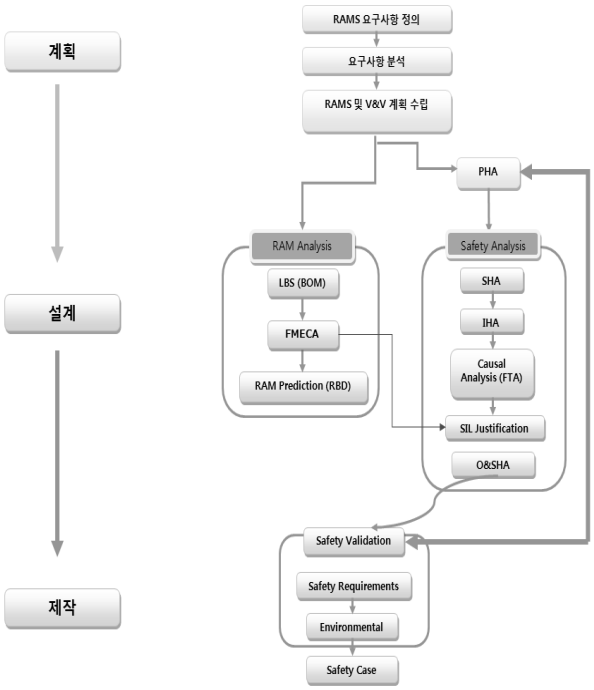

그림 8 HTC프로젝트 단계별 RAMS 활동
Fig. 8 RAMS activities of HTC Project in each steps

8.2 HTC 시스템 생성문서

다음 표 3과 4는 연구개발 시작단계에서 시스템의 H/W와 S/W에 대한 RAMS문서 생성에 대하여 각 기관에서 생성되어야 할 문서를 나눈 것이다.

8.3 HTC프로젝트 RAMS활동 절차 세부내용 정리

8.3.1 계획단계

표 3과 4의 H/W와 S/W의 업무분장 내용과 같이 1차년도 개발시점이 계획단계에서는 국제기술규격(IEC62278, IEC62279, EN50126~50129)참고문서를 근거로 RAMS측면의 요구사항 검토 및 분석 그리고 예비위험도 분석을 수행하였으며, HTC의 설계 및 제작을 위해 V&V계획을 수립하였다.

표 3 시스템 H/W 개발문서
Table 3 System H / W development documents

No	System Lifecycle Phase	System Documents(or Activities)
1	Concept	HTC System RAMS Plan
		HTC System Quality Management Plan
		HTC System Configuration Management Plan
2	System Definition and Application Conditions	HTC System Verification Plan
		HTC System Validation Plan
		HTC System Hazard Identification: PHA
3	Risk Analysis	Risk Analysis Report (Including hazard analysis)
4	System Requirements	HTC System Requirements Specification
		HTC System Safety Requirements Specification
		HTC System Architecture Specification
		HTC System Test Plan
5	Design and Implementation	HTC System Hardware Design Specification
		HTC System FMEA
		HTC System FTA
		HTC System Hazard Log
		HTC System RAM Prediction Report
		HTC System Verification Report on SRS, SAS, HWDS
6	Manufacture	HTC System Manufacturing Instruction
7	Installation	HTC System Installation Manual
8	System validation	HTC System Environment Test Report
		HTC System Validation Report
		HTC System Generic Application Safety Case

표 4 시스템 S/W 개발문서
Table 4 System S / W development documents

No	Software Lifecycle Phase	Software Documents(or Activities)
1	Planning	HTC SW Quality Assurance Plan
		~~HTC SW Quality Assurance Verification Report~~
		HTC SW Configuration Management Plan
		HTC SW Verification Plan
		HTC SW Validation Plan
2	Requirements	HTC SW Requirements Specification
		HTC SW Requirements Test Specification
		HTC SW Requirements Verification Report
3	Architecture & Design	HTC SW Architecture Specification
		HTC SW Design Specification
		HTC SW Interface Specification
		HTC SW Integration Test Specification
		HTC SW/HW Integration Test Specification
		HTC SW Architecture and Design Verification Report
4	Module Design	HTC SW Module Design Specification
		HTC SW Module Test Specification
		HTC SW Module Design Verification Report
5	Module Implementation and Testing	HTC SW Source Code
		HTC SW Source Code Verification Report
		HTC SW Module Test Report
6	Integration	HTC SW Integration Test Report
		HTC SW/HW Integration Test Report

HTC System | HTC Software | 버전

8.3.2 설계 및 제작단계

계획단계에서 정의된 위험원 분석 및 RAM분석, 안전성 분석 활동과 동시에 각각 구성 부품들의 고장유형, 원인, 영향, 치명도분석(FMECA)를 수행하고 이를 통한 SIL입증활동을 실시하였다. 설계 및 제작단계는 시스템생명주기 6,7의 시행단계 업무로서 계획과 설계단계를 통해 제시된 요구사항을 바탕으로 설계 및 구현 제작 즉, 개발품의 생산계획, 제조, 하위시스템이나 컴포넌트 제조 및 시험에 대한 문서를 작성하였다.

8.3.3 신뢰성 확보

신뢰성 확보는 설계와 제작단계에서 병행하여 확보하여야 한다. 그러나 설계단계에서 완벽한 신뢰성을 확보하기는 매우 어려운게 현실이다. 따라서 신뢰성 블록 다이어그램(RBD: Reliability Block Diagram)은 시스템을 성공 관점으로 모든 요소들 간의 의존관계를 표현한 방법으로, 블록 다이어그램을 이용하여 시스템의 신뢰도, 가용도, 예상 고장수 등의 결과를 정량적으로 분석해서 신뢰성의 정량적인 분석을 위한 수학적 모델로 표현하는 것으로 하였다. RBD는 시스템을 구성하고 있는 여러 개의 부품 중 어느 하나라도 고장이 발생하면 시스템 전체가 기능을 상실하게 되도록 부품이 결합되어있는 직렬구조와, 하나의 구성 품으로 요구되는 기능을 수행할 수 있지만 여분의 추가 연결된 구조로 시스템의 전체 신뢰도가 향상하는 병렬구조로 이루어져 있다. 단일고장은 시스템 고장을 초래하는 블록들이 직렬구조로 구성되며, 단일고장이 단지 다른 고장과 함께 결합되어 결과적으로 시스템 고장을 초래하는 경우는 블록들이 병렬로 구성된다. HTC 시스템 개발품은 내부구조가 병렬구조로 구성되어 있어 부품이 고장이 나더라도 전체시스템에 영향을 주지 않도록 되어 있다. 목포 대불 시험선에서 1개월에 한번씩 현장 설치시험을 통해 검증작업이 진행 중에 있다. 현장테스트 결과가 기대이상 도달하지 못할 경우에는 개발품에 대하여 3단계인 위험도 분석단계의 고장 모델을 결정하고 4단계 시스템의 진단 기법 평가방법에 의하여 개발품의 유효성을 재검토하고 수정내용에 대하여 버전개정을 통해 개발품의 유효성을 인증기관인 TUV에 제출하여 재검토 승인을 받는다. 검증을 바탕으로 안전성을 입증하기 위해 EN50129에 근거하여 Safety Case를 작성하였다.

8.4 SIL 인증 절차

SIL 입증(Justification)은 SIL 입증에 관한 사항으로 유럽 및 국제적인 상호 안전성 수용을 위하여 HTC프로젝트에 대해 제시된 안전성 요구사항을 위해 우발고장 측면에서의 정량적인 SIL 입증 업무를 수행할 예정이다.

본 HTC 시스템은 특정 현장에 적용하지 않는 제작단계와 현장실험에 따른 성능입증 까지의 업무범위에 해당하므로, 일반제품(Generic Product) 수준에 해당하며 EN50129의 안전성 요구사항을 만족하는 HTC프로젝트 관련 주요 위험원에 할당된 THR을 FTA방법론을 활용하여 정량적으로 입증함으로써 EN 50129에 근거한 HTC프로젝트에 대한 SIL 레벨입증을 수행할 것이다. 해당 SIL 입증에 대한 결과는 HTC 안전성 분석 보고서 및 안전성 검증 보고서에서 기술하는 것으로 계획하고 있으며, 현재 진행중에 있다.

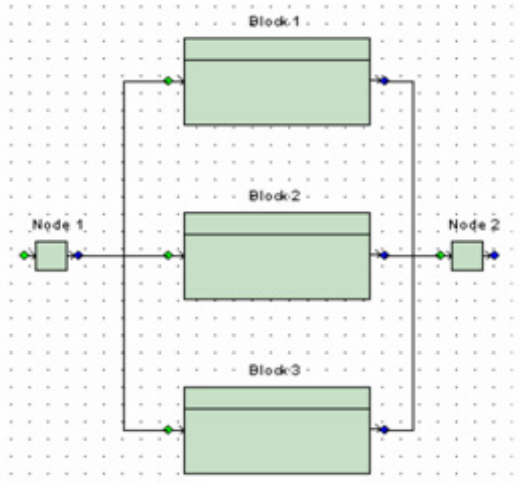

그림 9 HTC 시스템 병렬구조
Fig. 9 HTC parallel structure system

9. 결 론

앞에서 철도 시스템의 기능안전 규격, 시스템 수명주기 단계별 RAMS활동 그리고 기능 안전 개념과 안전성 승인 조건에 대해 설명하였다. 이러한 내용은 안전성 평가 또는 SIL 인증을 수행할 때 기반이 되는 개념이다. 안전 관련 시스템에 대한 SIL인증 절차는 개발된 제품의 안전성 적합 여부를 평가하는 것이 아니라 제품 개발의 개념 단계에서 구현 단계에 걸쳐 안전 관련 활동을 모두 심사하는 것이다. SIL 인증을 위해서는 시스템 개발 단계별로 많은 활동이 요구되므로 기술적인 검토뿐만 아니라 충분한 시간과 인력의 지원을 고려하는 것이 중요하다.

감사의 글

본 논문은 2014년도 국토교통과학기술진흥원의 재원으로 하이브리드 궤도회로 개발과 관련된 지원을 받아 수행된 ISA활동 연구비 지원에 의하여 이루어진 연구로서, 관계부에 감사드립니다.

References

[1] IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems, 2010.
[2] EN 50126, Railway Applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999.
[3] EN 50128, Railway Applications - Communication, signalling and processing systems - Software for railway control and protection systems, 2011.
[4] EN 50129, Railway Applications - Communication, signalling and processing systems - Safety related electronic systems for signalling, 2003.
[5] Safety-Critical Computer Systems, Neil Storey, 1996.

[6] Basic and applied for certification SIL RAMS 'books, TUV Korea Co., Ltd, 2013.
[7] Basic and applied for certification SIL RAMS 'books, T UV Korea Co., Ltd, 2013.
[8] IEC 61508, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety Related system,2010.
[9] Development of test method for H/W functional certification of hybrid track circuit, The Korean Society for Railway(Spring), 2013.
[10] RAMS basic and application of the SIL certification, TUV Korea Co., Ltd, 2012.
[11] Technical lecture of RAMS for railway signalling, Korea Railway Research and Institute, 2010. 09.
[12] IEC 62425 International Standard-Railway applications Communication, Signalling and Processing system

저 자 소 개

김 유 호 (金 侑 鎬)

1986년 건국대학교 전기공학과 졸업. 2006년 연세대학교전기전자공학 석사 졸업. 2006년~현재. 연세대학교전기전자공학 박사 재학. 2007년~현재 (주)에이알텍
Tel : 02-2083-5601
Fax : 02-2083-5650
E-mail : asa812@korea.com

고 태 국 (高 太 國)

1981년 연세대 전기공학과 졸업, 1983년 Case Western Reserve Univ. Dept. of EEAP 졸업(Ph.D), 1986년~1988년 Ohio Cleveland State Univ. 전기공학과 조교수, 2008~2010년 한국 초전도 저온공학회 회장
현재 연세대학교전기전자공학과 교수

이 수 환 (李 秀 桓)

현, (주)에이알텍 기술연구소 상무
2010년 우송대학교 철도대학원 철도전기공학 졸업(석사)
Tel : 02-2083-5631
Fax : 02-2083-5650
E-mail : ksjlsh1@naver.com

박 강 훈 (朴 降 勳)

현, (주)에이알텍 기술연구소 부장
2003년 유한대학 전기과 졸업
Tel : 02-2083-5632
Fax : 02-2083-5650
E-mail : kieng1976@hanmail.net