첨단 경량전철 열차제어시스템 안전엔지니어링 기술동향
Basic Requirements for the Application of Risk Concept on Railway Safety Improvements

조연옥* 왕종배*** 김상암****
Cho, Yun-Ok Wang, Jong-Bae Kim Sang-Ahm

ABSTRACT

It requires different safety programs from those of the typical train control systems to develop AGT systems applying train control system based on communication technology. Especially Advanced LRT system involves the processes that have the various safety functions being conducted by softwares and also have characteristics that should have special interest in validation of interface specification. The core items for the safety engineering for LRT control systems are hardware & software engineering, safety-critical system safety engineering, application saftware validation & verification technologies. In this paper the trends of the technologies for the mentioned core-items are described.

1. 서 론

경량전철은 차량규모나 수송인원이 기존의 지하철보다는 작으나 버스보다는 큰 새로운 개념의 도시철도라 할 수 있다. 경량전철은 거리에 배기가스를 배출하지 않는 점에서 환경 친화적이며, 자동차를 이용한 여행보다는 훨씬 안전하고 안락하며, 다른 교통수단과 분리되어 운영되기 때문에 교통혼잡의 영향을 받지 않는다는 장점을 가지고 있어서 선진국에서는 이미 대중교통의 중요한 수단으로 자리를 차지하고 있다.

경량전철시스템은 중량전철시스템과 마찬가지로, 궤도, 역사, 차량기지로 구성된 구조물 시스템과, 운전 및 유지보수 센터, 급전설비, 신호 및 통신 등으로 구성된 고정설비시스템과 차량시스템으로 이루어져 있다.

일반적으로 첨단 경량전철시스템이라 함은 완전 자동 무인운전을 지원하는 AGT시스템을 말하는 것으로서, 철제차륜, 고무차륜 및 LIM 방식으로 대별할 수 있으며, 우리나라에서도 도시철도법에 표준화되어 있는 방식이기도 하다.

또한 경량전철시스템도 주요한 대중교통 수단이므로, 타 교통시스템과 마찬가지로 성공적인 경량전철시스템의 개발을 위해서는 승객의 안전보장이 가장 중요하며, 이를 위해서 경량전철시스템

* 한국철도기술연구원 수석연구원, 정회원
** 한국철도기술연구원 선임연구원, 정회원
*** 한국철도기술연구원 선임연구원, 정회원

의 설계에서부터 시운전까지의 안전 엔지니어링 기술 확보가 성공적인 경량전철시스템 개발에서 가장 핵심적인 기술이 된다.

철도시스템에서 고정된 선로 상에서 차량을 운행할 때 운전규칙을 철저하게 지켜 차량의 안전성을 보장하고 운행효율을 증대시키는 것은 매우 중요하다. 이러한 목적을 달성하기 위해서 철도시스템은 열차제어시스템을 사용하게 되는데, 열차제어시스템의 기본적인 목적은 다른 열차와 충돌하지 않는 것과 열차가 안전하게 운행하는 것은 가장 기본적인 것이다.

열차제어시스템은 열차의 운행을 감시하면서 진로를 자동으로 설정하여 제어하는 열차운행제어관리장치, 열차의 위치를 검지하여 열차의 충돌, 추돌, 탈선 등을 방지하고 열차의 안전운행을 보장하는 자동열차제어장치 및 이를 연결하는 통신장치로 구성된다.

현재, 각 국의 열차제어시스템 제작 회사들은 무선 통신을 이용한 통신기반열차제어(CBTC; Communication-Based Train Control) 시스템을 개발하거나 개발 중에 있고, 이를 이용해 이동폐색 시스템을 구현하고 있다. 이동폐색 방식은 고정폐색 방식의 개념을 초월하여 무선 신호 전송매체를 이용한 선행 열차와 후속 열차 신호간의 위치 및 속도를 파악하고 열차 간격을 조정하는 방식이다.

경량전철시스템에서 열차제어시스템은 열차운행이 효율적으로 이루어지도록 하고 열차운행의 안전성을 확보하기 위한 가장 핵심적인 장치로서 선행열차와의 안전거리를 유지하고 효율적인 운전시격을 단축시키기 위해서 사용된다. 열차제어시스템은 지상과 차상에 설치되며 상호간의 지속적인 통신을 통하여 열차운행의 안전성을 확보한다. 집적회로, 마이크로프로세서 및 소프트웨어의 도입으로, 하드웨어 부품의 고장 또는 소프트웨어 에러가 발생한 경우에 안전한 시스템 운전을 입증할 수 있는 방법으로 전통적인 분석기법을 사용할 수 없을 만큼 안전핵심 시스템은 복잡해지고 있다.

통신을 기반으로 하는 열차제어시스템을 적용하는 AGT시스템을 개발하기 위해서는 전통적인 열차제어시스템의 개발과 관련된 것과 상이한 안전 프로그램을 요구한다. 특히 첨단 경량전철시스템은 아래와 같은 안전상의 특징을 가지고 있다:

- AGT시스템은 소프트웨어에서 수행되는 많은 안전기능을 가진 프로세서를 포함하고 있다.
- AGT시스템의 안전 유효화를 위해서는 인터페이스 사양의 안전 요소의 유효화에 특별한 관심을 가져야 한다.

통신기반열차제어시스템은 크게는 지상장치, 차상장치 및 이들 하드웨어를 지원하는 소프트웨어로 구성되어 있고, 세부적으로는 다양한 제어장치, 송수신장치, 적용 소프트웨어 등이 복합적으로 조합된 복합시스템이다. 또한, 기술적 측면에서는 통신기반열차제어시스템은 위치탐지기술, 열차차상간 통신기술, 열차제어기술, 이들 하부 기술을 조합하는 시스템 엔지니어링 기술 등의 다양한 요소기술을 조합한 시스템이다.

통신기반열차제어시스템은 기존 열차신호제어시스템에 비해서 적용 소프트웨어에 훨씬 더 의존하고 있기 때문에 소프트웨어의 안전성 검증 및 유효화가 시스템 적용의 성공요건이 된다. 또한, 열차의 제어를 지역별로 구분하여 한 개의 제어구간에서 제어하는 열차의 수가 기존시스템에 비해 훨씬 많기 때문에 바이탈 지상 프로세서의 고장은 넓은 지역의 철도에 대한 주 제어손실을 야기할 수 있다. 그러므로, 이러한 문제들을 해결하기 위하여 바이탈 시스템 안전 설계기술, 소프트웨어 안전성 검증 및 인증기술의 확보가 시스템 적용에 필수적이다.

2. 기술 동향

2.1 AGT시스템의 안전엔지니어링 개요

안전보장은 시스템 수명주기에서 절대 필요한 부분이다. 안전 프로세스 활동은 모든 시스템, 바이탈 소프트웨어, 바이탈 하드웨어 수명주기 활동과 병행하여 수행되어야 한다.

시스템의 안전 수명주기는 두 가지의 핵심 프로세스 요소로 확립된다:

· 안전 엔지니어링: 요구조건, 설계, 개발, 실현 및 종합

· 안전 관리: 계획, 전개, 제작, 시운전, 개선, 유지보수 및 폐기

첨단 경량전철 시스템에서 적용되는 안전설계 개념은 아래와 같다:

· 안전측 고장 설계
  - 하드웨어 설계 통제
  - FMECA 분석
  - 고장을 밝혀내기 위해 안전측 고장 설계
  - EMI/EMC 인증
  - 제작 및 유지보수 사양

· 덧붙임 검사
  - 프로세서의 주기적인 자기검사
  - 바이탈 하드웨어 검사
  - 바이탈 소프트웨어 설계 및 시험 프로세스
  - 공통모드 고장 완화

· 기능 다양성 및 자기 검사
  - 덧붙임 검사는 검사프로세스가 자체적으로 페일-세이프 또는 덧붙임 검사이라는 것을 검증하여야 한다.
  - 비슷한 또는 동일한 오류 또는 고장이 검사 동안에 여분의 장치에서 일어날 수 없을 정도로 충분히 자주 검사 프로세스를 수행하여야 한다.
  - 검사 프로세스는 단일 장치의 모든 의미 있는 오류를 탐지하기에 충분히 민감하여야 한다.
  - 검사 실패는 안전을 유지하는 시기 적절한 대응동작이 일어나게 해야 한다.

바이탈 소프트웨어에 실현된 안전기능을 나타내고 분석하는데 사용되는 주요한 기술은 아래와 같다:

· 사양을 상세히 기술하고 동적행위결함(dynamic behavior flaw)을 규명하기 위해서 세부적인 바이탈 소프트웨어 요구조건을 모델화

· 실현된 안전 핵심 결정을 나타내기 위한 논리 다이어그램

· 코드에서 모델 및 논리 다이어그램 기능, 안전 요구조건, 위험 완화까지 추적성

· 안전 요구조건에의 적합성 및 위험 완화를 평가하기 위한 모델, 논리 다이어그램 및 코드의 검토, 정적 워크스루(Walkthrough) 및 분석

· 엔지니어링 변경 통보서(ECN)에 문서화된 변경/결과의 분석 및 검토

안전 검증 및 유효화:

· 시스템의 성능 및 기능성을 검증하기 위한 시운전 시험 외에 안전시험은 규명된 안전 위험의 완화를 광범위하게 검증한다.

· 현장시험 이전에 소프트웨어 종합 및 공장 인수시험을 시뮬레이터에서 수행한다 - 현장에서 재현될 수 없는 하위수준의 안전설계 유효화 시나리오를 포함하여

· 현장에 장치를 설치한 후에, 정확한 설치 및 기능적 성능을 확인하기 위하여 정적 및 동적 설

치 전 및 확인시험을 수행한다.
· 시험은 열차를 상용 궤도 또는 매우 대표적인 시험궤도에 올려놓고 최대한으로 가능한 설계 상황에서 시험을 진행한다.
· 새로운 장치에 대해서는 장치를 완전하게 시운전하고 안전 인증 이전에 사고 또는 피해 위험도를 제한할 수 있는 점진적인 시운전 전략을 사용하여야 한다.

2.2 AGT 시스템 요구조건

전형적으로, AGT운전은 완전 자동, 무인운전 시스템이다. 자동 진입, 진로결정 및 스케줄 변경 기능을 제공하는 중앙제어소에서 열차의 스케줄을 결정한다.
AGT시스템의 일차적인 목적은 다음과 같다:
· 열차충돌, 열차탈선, 예기치 않은 차량 또는 승강장 도어 개방, 화재 및 기타 위험 등과 같은 모든 위험 조건의 발생을 방지
· 자동 무인운전 열차운전을 제공
· 운전계획을 최적화하고 교통수요의 변화에 대응할 수 있는 성능을 제공
상기 요구조건을 만족하기 위해서, AGT시스템은 자동열차보호장치(ATP), 자동열차운전장치(ATO) 및 자동열차감시장치(ATS) 등과 같은 전통적인 요소로 분할할 수 있다.

2.3 AGT시스템 안전기능 실현

모든 ATP, ATO 및 ATS 기능은 최소한의 지상 및 차상 하드웨어 세트를 사용하여 수행된다. 차상, 지상 제어 위치 및 원격 연동장치에 있는 바이탈 컴퓨터 시스템을 사용하여 안전 열차이격, 연동제어 및 열차속도 제한을 수행한다. AGT시스템의 설계 및 개발 단계에서 하드웨어 및 소프트웨어에서 바이탈 원리를 준수한다. 시스템 설계의 한 부분으로서의 안전분석은 설계가 이들 원리를 성공적으로 준수한다는 것을 증명한다.

2.4 AGT 제어수준

모든 안전기능을 실현하기 위해서는, 완전한 AGT 운전구조는 관리수준, 운전수준 및 동작수준의 3단계 계층으로 정리되어야 한다. 전반적인 시스템 수준은 표 1과 같이 정의된다.

표 1. AGT 제어 수준

계층	하부시스템	안전수준
관리수준	자동열차감시시스템	논-바이탈
운전수준	제어 지상제어장치	바이탈
동작수준	차량 제어장치	바이탈
	인덕티브 루프	바이탈
	정거장 제어장치	바이탈

2.5 AGT시스템 안전원칙 실현

AGT시스템 아키텍처를 설계하는데는 운전 안전을 고려하는 것이 첫 번째이며 가장 앞서는 일이다. 열차를 운전하는데 안전을 약속하는 것은 다음 기능으로 나누어져 있다:
· 강제적인 열차이격
· 열차 위치에 대한 스위치 체결

· 강제적인 열차속도 제한
· 승강장 및 열차 도어 제어

이들 기능들은 열차 차상, 각 선로변 제어 위치, 각 원격 스위치 연동 위치 및 중앙에서 바이탈(덧붙임 검사) 컴퓨터 하부시스템에 의해서 실현된다.

AGT시스템을 설계하고 개발하는데, 덧붙임 검사, 안전측 고장(fail-safe) 원칙을 엄격하게 따른다. 시스템의 어떤 수준에서의 고장도 보다 덜 허용되는 상태로 시스템이 복귀되도록 한다.

2.6 AGT시스템 안전분석 프로세스

AGT시스템의 일생주기는 아래 단계로 정의된다:

· AGT시스템 개념
· AGT시스템 정의
· AGT시스템 개발
· AGT시스템 제작
· AGT시스템 운전

AGT시스템 수명주기 동안에, AGT시스템 안전분석 프로세스를 실현한다. 이 프로세스는 그림 1에 설명된 것과 같다. 이 안전 프로세스의 목적은 아래와 같다:

· AGT시스템이 통제하여야 하는 일차적인 위험을 규명
· 한 개 이상의 일차적인 위험에 기여할 수 있는 근원을 규명
· 각 위험을 통제하는 책임이 있는 AGT 하부시스템 또는 기능을 규명
· AGT 하부시스템 안전기능 요구조건을 유도하고 각 위험을 완화할 수 있는 기술을 협의(설계 및 운전 절차)
· 각 위험 완화방법에 대한 검증방법을 규명(시험 및 설계검토)
· 안전분석으로 안전 요구조건을 규명하고 해석하고, 허용할 수 있는 수준으로 완화하고 시험절차 또는 유지보수/운전절차로 시험하고 실현한다는 것을 입증

3. 전망

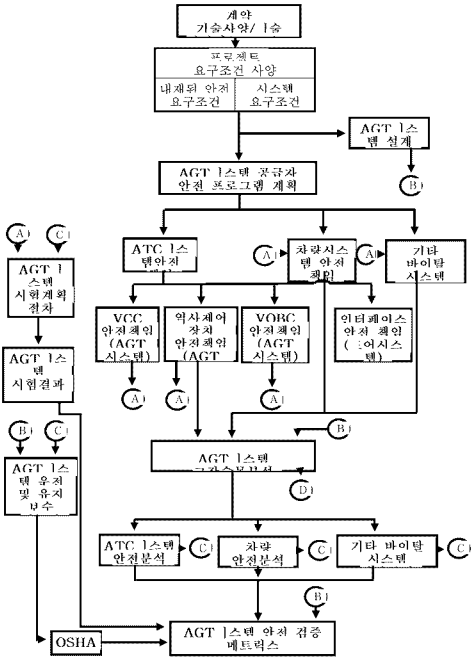
AGT시스템의 안전성에서 가장 핵심적인 것은 컴퓨터를 집중적으로 사용하는 열차제어시스템과 같은 안전핵심시스템의 안전성 확보이다. 이를 위해서 경량전철 개발 선진국에서는 시스템의 안전성 향상을 위해서 안전핵심시스템에 대한 기술개발을 꾸준하게 추진하고 있는 것이다

안전핵심시스템은 시스템 안전엔지니어링의 가장 핵심적인 주제이다. 안전에 관련된 보다 오래된 분야는 신뢰성공학이라고 불린다. 이 분야는 컴퓨터의 적용이 널리 확대됨에 따라서 컴퓨터에 대해서 점진적으로 관심을 증가시키고 있다. 전통적인 분야의 입증된 기술을 소프트웨어에 대해서 반복적으로 채택하여 왔기 때문에 소프트웨어 안전을 연구할 때 시스템 안전엔지니어링 기술은 상관이 있을 수 있다.

시스템 안전 및 컴퓨터 신뢰성과 별도의 연구주제로서의 안전핵심 디지털 컴퓨터 시스템에 대한 연구는 매우 최근의 일이다. 이 연구분야는 안전핵심 시스템에서 컴퓨터의 사용이 급격하게 증가함에 따라서 지난 5 - 10년 사이에 급격하게 확대되고 있는 경향이다.

명확하게 소프트웨어는 자체적으로 사고를 야기할 수는 없다. 소프트웨어를 잠정적으로 위험한 시스템을 제어하기 위해서 사용하였을 때만 소프트웨어는 안전핵심 문제가 된다. 안전은 시스템 특성이며 소프트웨어의 안전성 또는 비안전성은 그것을 전체 시스템의 한 부분으로 간주하였을 때만 평가할 수 있다. 실제로, 소프트웨어공학의 현재 기술 상태로서 소프트웨어를 안전핵심 시스

그림. 1 AGT시스템 분석 프로세스



템에 적용할 수 있느냐는 논란거리이다.

안전은 인적인자와 인간-기계 인터페이스를 통한 상호작용에 강한 의존성을 가지고 있을 수 있다. 특히, 인적요인에 의한 사고가 철도사고의 상당한 부분을 차지하고 있고, 열차제어시스템과 같은 안전핵심시스템에서 인적요인에 의한 사고는 대형사고를 야기할 수 있으므로 이에 대한 많은 연구가 진행되고 있다.

IEEE(미국 전기전자 엔지니어 학회)는 CBTC시스템 표준화의 일환으로 1999년에 CBTC 성능 및 기능 요구조건에 대한 표준을 완료하였다. 이 표준에서는 안전프로그램 요구조건, 위험규명 및 위험평가 프로세스, 안전프로그램계획, 바이탈 기능, 정량적 안전성능기준, 안전프로그램, 안전설계 등 시스템 안전요구조건을 제시하고 있다. 그러나, 이 요구조건은 기본적으로 시스템 개발에 따르는 안전관리에 초점을 맞춘 것으로서, 세부적인 열차제어시스템의 안전엔지니어링 기술 자체는 제시하지 못하고 있다. 더구나, AGT시스템의 열차제어시스템은 소프트웨어를 집중적으로 사용하는 안전핵심시스템인데도 불구하고, 안전핵심시스템의 안전과 연계한 개발절차와 소프트웨어의 안전성 검증 및 인증에 대한 세부적인 절차를 다루고 있지 않고 있다.

현재는, AGT시스템의 발주기관이 열차제어시스템과 같은 안전핵심시스템과 같은 대해서는 시스템의 안전성에 대해서 수학적이고 엄밀한 검증을 요구하는 추세이므로, 안전핵심시스템의 소프트웨어 개발에서 수학적인 안전검증기술의 확보가 필요하다.

참고문헌

1. 김병석, 나승훈, (1998), "시스템 안전공학", 형설출판사
2. Ken Wong, (1998), " safety Verification Condition for Software-Intensive Critical Systems", Thesis, University of British Columbia
3. Jack W. Boorse, E.L. Tennyson, John W. Schumann,(2000), "This is the light rail transit", 8th Joint Conference on Light Rail Transit
4. Simon Ginn, (1998), "An Overview of Light Rail Technology and Its Potential Within an Australian Environment", Western Australian Planning Commission
5. 최 규형, (2000), "경량전철시스템 기술개발사업 2차년도 연구개발보고서", 건설교통부
6. Transportation Research Board, (2000), "This is Light Rail Transit"
7. 한국철도기술연구원, (2001), "경량전철기술"
8. 건설교통부, (2001), "지능형 열차제어시스템 국내적용방안 검토"
9. IEEE P1474.1/D8.0, (1999), "Communications-Based Train Control(CBTC) Performance and Functional Requirements"
10. Alcatel 내부자료, (2001), "System Safety Engineering"