

고속철도시스템의 안전 요구사항 적용을 위한 통합 아키텍처 구축 사례

An Application of Building an Integrated Architecture to Apply Safety Requirements of the High Speed Railway System

윤재한*, 김찬목, 장재덕, 이재천(아주대학교 시스템공학과),
최요철, 왕종배(한국철도기술연구원)

1. 서 론

고속철도시스템은 선로, 차량, 열차 등의 운영, 제어 및 유지보수 같은 다양한 기술 분야로 구성된 대형복합시스템이다. 분야들의 유기적인 결합이 이루어지지 않을 경우 탈선, 충돌 등으로 인해 치명적인 인명, 재산 손실을 야기한다. 대구 지하철 참사를 계기로 국내에서도 안전에 관한 인식이 점점 높아지고 있다. 기존의 시스템은 안전을 시스템 개발 후 보조 구축물에만 의존하려는 경향이 있었다. 하지만 최근에는 시스템 개발 단계부터 시스템 안전을 고려하여 설계하려는 노력들이 생겨나고 있다. 이는 시스템 개발 단계부터 안전을 고려하여 설계하지 않고서는 목적하는 안전 지수를 가질 수 없음을 인식하게 되었다고 볼 수 있을 것이다.

시스템이 궁극적인 안전 목표 값에 도달하기 위해서는 개발 초기에 각 분야별로 위험요소를 정의하고 시스템 인터페이스 위험요소를 사전에 명확히 정의함으로써 고속철도시스템 전체의 안전대책을 수립해야 한다. 이를 이용해 시스템의 설계 시 요구사항단계부터 안전에 관련된 요구사항들을 수집하고, 안전 요구사항으로부터 시스템 기능을 생성하여 실제 물리적 구성품(Component)에 할당해야 한다. 또 그렇게 개발한 시스템의 체계적인 성능 및 안전 시험&평가가 필요하다.

이와 같은 작업을 기존의 고속철도시스템에 적용하였다. 기존의 고속철도시스템을 모델링하고 안전 요구사항을 적용시킨 통합 아키텍처를 구축하였다. 또한 통합 아키텍처를 통해 시험 및 평가 계획을 위한 안전 및 성능 시험&평가 기준을 정리하였다.

앞으로 본 논문에서는 통합 아키텍처의 구축 목적과 정의를 설명하고 구축 프로세스와 그에 따른 구축 내용에 대해서 구축 프로세스 순서를 기반으로 설명하겠다. 마지막으로 본 연구의 의의와 한계, 앞으로 연구방향을 설명하면서 논문을 마치겠다.

2. 통합 아키텍처의 목적과 정의

시스템의 개발의 초기 즉, 요구사항을 정의할 때부

터 성능, 기능, 제약사항에 대한 요구사항 뿐만 아니라 위험 분석을 통해 안전에 대한 요구사항을 정의해야 한다. 또한 각 기능 및 물리적 구성품을 구성할 경우에도 각 종 안전 사항들에 대한 대책 기능 및 구성품(사용자 오작동에 대한 예방 및 대책에 관한 기능과 구성품, 기계 오작동에 대한 예방 및 대책에 관한 기능과 구성품, 승객 안전 확보를 위한 기능 및 구성품 등)을 고려해야 한다. 즉, 시스템을 구축할 때 안전 사항과 기능, 성능, 제약사항은 동시에 고려되어야만 한다. 그리고 그러한 요구사항으로부터 어떻게 개발되었는지 추적성을 명확하게 만들어야 하고 안전 요구사항이 시스템에 어떤 영향을 미치는지 파악할 수 있어야 한다. 또 결국 시스템의 어떤 구성품을 왜, 어떻게, 무엇으로 시험&평가해야 하는지를 알 수 있어야 한다.

이러한 일을 수행하기 위한 방법을 연구하기 위한 하나의 예로 고속철도시스템에 안전 요구사항을 적용한 통합 아키텍처를 구축하였고 본 논문에서 말하는 통합 아키텍처의 정의는 다음과 같다.

- 통합 아키텍처:

기존의 고속철도시스템에 안전 요구사항을 적용하여 모델링하고 성능 및 안전 시험&평가를 위한 기준을 정리하여 모델에 통합한 고속철도시스템 아키텍처

3. 통합 아키텍처의 구축 프로세스와 구성

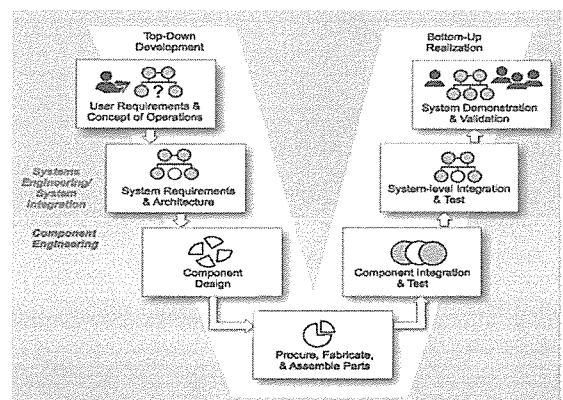


그림 1. Systems Engineering Vee Model

며 다음과 같이 수행하였다.

- 시스템이 달성해야할 미션을 설정한다.
- 미션을 달성하기 위한 기능 시나리오로 작성한다.
- 시나리오를 상세화 하여 모델을 작성한다.
- 작성된 모델의 거동을 분석하여 논리적 오류를 없애고 모델의 성숙도를 높인다.

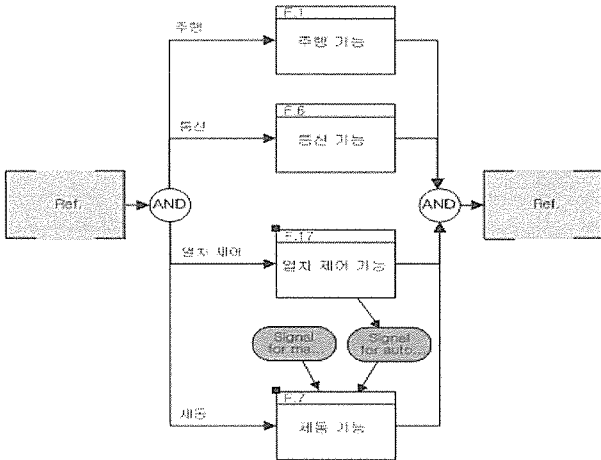


그림 5. 차량 시스템 수준의 기능 아키텍처

그림 5는 EFFBD를 이용하여 시나리오를 작성한 예이다. 기존 시스템을 구성하는 하부 시스템 수준에서 최초로 도출된 시나리오이다. 이렇게 시나리오를 상세해 나가면서 시스템의 기능 아키텍처를 수립했다.

시스템 수준의 기능 아키텍처에서 세부사항을 작성하려하니 문제가 발생하였다. 요구사항으로부터 도출되어야 할 기능, 성능, 제약사항들이 시스템 사양서 만으로는 실제 시스템과 상이하게 도출되었다. 하여 회피책으로 기능, 성능, 제약사항들을 기존에 존재하는 시험절차서를 이용하여 역으로도 도출하였다. 기존의 시험절차서인 경우 시스템에 존재하고 있는 기능, 성능, 제약사항들을 시험하기 때문이다. 허나 이러한 방법은 시스템엔지니어링에서 가장 중요시 하는 추적성이 약해지는 문제가 있다. 하여 요구사항과 기능, 성능, 제약사항과의 추적성을 다음과 같이 확보하였다.

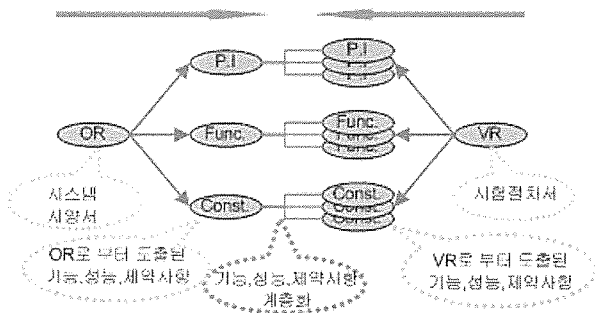


그림 6. 기능, 성능, 및 제약사항의 계층화 및 추적성 확보 방안

그림 6을 좀 더 자세히 설명하자면 다음과 같다.

- ① 최초요구사항(고속철도시스템의 기본 사양 분석 자료 기반)으로부터 도출된 시스템 수준의 기능/성능 및 제약사항을 최상위에 둔다.
- ② 시험절차서로부터 도출된 기능/성능 및 제약사항은 같은 수준의 유사항목으로 그룹화한다. 즉 시험절차서로부터 도출된 기능/성능 및 제약사항은 최초요구사항으로 도출된 기능 및 성능의 하부 기능 및 성능으로 묶어서 계층화를 한다.

기능 아키텍처를 수립하고 요구사항과 기능, 성능, 제약사항 간의 추적성이 확보되면 기능 아키텍처를 이용하여 물리적 아키텍처를 작성한다. 물리적 아키텍처를 작성할 때 또한 기존의 고속전철시스템의 물리적인 구조를 고려하였으며, 물리적 아키텍처에 기능 아키텍처의 기능들을 할당하게 된다. 기능 아키텍처가 시스템 하위 수준에서부터는 시험절차서를 이용하여 작성되었기 때문에 해당 기능이 실제 시스템의 어느 구성품에 해당하는지 좀더 쉽게 파악할 수 있었다.

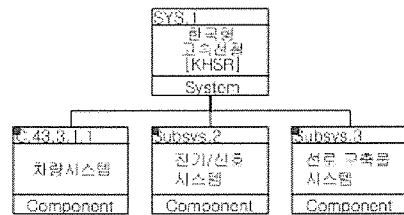


그림 7. 고속철도시스템의 물리적 아키텍처

그림 7은 작성된 고속철도시스템의 물리적 아키텍처이다. 시스템과 하위 시스템 수준의 아키텍처를 표현하고 있다.

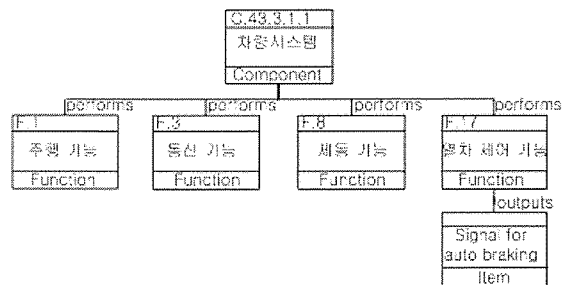


그림 8. 물리적 아키텍처에 할당된 기능 아키텍처

그림 8은 그림 7의 물리적 아키텍처 속에 있는 한 구성품에 기능 아키텍처의 기능들이 할당돼있는 모습이다.

실제 시스템 설계 시 물리적 아키텍처를 구축하면 시스템에 대해 통합 및 검증을 수행한다. 이를 위해

요구사항으로부터 검증요구사항을 도출하고 시스템을 통합하면서 검증 요구사항에 맞게 테스트를 계획 및 수행&평가해야 한다. 테스트를 올바르게 수행하기 위해 TEP(Test & Evaluation Plan)를 작성해야 한다. 즉, TEP를 올바르게 작성해야 시스템을 올바르게 수행&평가할 수 있고 이를 위해 시험절차서를 이용하여 성능 및 안전 시험&평가 기준을 정리하였다. TEP를 위해 고려된 항목들은 다음과 같다.

- 검증 요구사항(Verification Requirement)
- 검증 이벤트(Verification Event)
- 검증 책임조직(Responsible Organization)
- 시험 장비(Test Configuration)
- 시험 절차(Test Procedure)

이렇게 정리된 성능 및 안전 시험&평가 기준들을 이용해서 최종적으로 TEP를 작성하고 안전요구사항이 어떻게 시스템에 적용되었는지를 제시하였다.

5. 결 론

기존의 고속철도시스템을 모델링하고 안전 요소를 적용하여 체계적인 시험 및 평가 계획을 세울 수 있는 기본 골격을 다지는데 목표가 있었다. 이를 위해 고속철도시스템의 성능 및 안전 시험&평가 기준을 정리하고 고속철도시스템에 안전 요구사항 적용한 모습을 제시해 보았다. 이를 위해 수행한 내용들은 다음과 같다.

- 고속철도시스템의 시스템 수준 요구사항을 정리 및 추적성 확보
- 고속철도시스템의 요구사항 및 검증 요구사항을 위한 DB 개발
- 시스템 수준의 요구사항과 기능, 성능 및 제약사항과의 추적성 확보
- 고속철도시스템의 서브시스템 수준의 기능/물리적 아키텍처 개발
- 요구사항과 기능/물리적 아키텍처의 추적성 확보
- 기존 고속철도 시스템의 성능시험 절차 정리

현재 정리한 시험&평가 기준은 기존의 시험절차서를 정리한 수준이다. 이 때문에 이를 이용하여 작성한 TEP 역시 현재 시험절차서와 차이가 없다. 또한 시스템의 기능, 성능 및 제약사항은 시스템 수준의 기능, 성능 및 제약사항은 도출하였으나 이는 실제 고속철도 시스템을 구성하는 기능, 성능 및 제약사항들의 존재 근거를 명확히 설명하지 못 한다.

고속철도시스템이 더 나은 시험&평가를 수행하기 위해서는 정리된 기준들을 가지고 최적화된 TEP를 연

구할 필요가 있다. 또 현재 수준보다 분해된 하부 수준의 기능 시나리오들을 도출함으로써 하부의 기능 아키텍처를 연구하고 이를 이용해 하부의 물리적 아키텍처를 연구해야 할 것이다.

현재 구축한 통합 아키텍처를 더 세부적으로 다듬어 나간다면 차후에 현재 고속철도시스템을 개선하거나 또는 근간으로 새로운 시스템을 작성할 시 개선 또는 추가되는 미션들에 대한 기능들만을 파악하여 관련된 구성품들만을 개발함으로써 시간과 비용을 동시에 절감시켜 줄 것이다. 또한 현재 정리된 시험&평가 기준들을 보강시키고 이를 통해 좀 더 최적화된 TEP를 제시함으로써 고속철도시스템의 시험&평가를 강화시킬 것이다.

6. 참고 논문

- [1] <http://www.globalsecurity.org>
- [2] James N. Martin, Systems Engineering Guidebook, CRC Press, 1997