건널목장치에서의 안전성확보 방안 고찰

정의진*°, 김양모**
*한국철도기술연구원, **충남대학교

A Study on the Process to Establish Safety of Level Crossing

E.J.Joung*°, Y.M.Kim**
*KRRI(Korea Railroad Research Institute), **Chungnam National University

Abstract - In this paper, the relationship between system engineering lifecycle and safety lifecycle is investigated. V diagram and IEC 61508 model are represented in the lifecycle model. V diagram easily shows the flow of information between phases. But it does not show the amount of work involved in each stage. IEC 61508 model describes the activities to be performed during each phase of the lifecycle. And also the causal-consequence analysis for the level crossing is presented. Representing this analysis procedure, we are try to establish safety of level crossing.

1. 서 론

안전과 관련된 시스템에서 컴퓨터의 사용은 많은 장·단점이 있다. 컴퓨터를 이용한 기능 구현방법이 모든 경우에 있어서 항상 이상적이지만은 않다는 것 또한 잘 알려져 있다. 그러나 많은 경우 컴퓨터를 이용할 때의 장점이 단점보다 더 부각되기 때문에 컴퓨터를 이용한 방법이 채택되어 온 것은 사실이다. 열차제어시스템 또한 컴퓨터화 된 시스템으로 고도의 안전성과 신뢰성이 요구되고 있으며, 이를 위해 국내·외에서 철도 신호제품의 설계, 제작, 검증, 사후관리 등 품질보증을 위한 신뢰도와 안전성 판단근거를 마련하고자 부단히 노력하고 있으며, Lifecycle 전체를 대상으로 결함, 고장, 장애 등 모든 위험요소를 미연에 방지하고자 하고 있다. 본 논문에서는 열차제어시스템에서 사용되는 다양한 lifecycle 모델을 조사하여 각 단계의 시스템 분석 방법에 대하여 살펴보았다. 여기에서는 V diagram과 IEC 61508 모델을 분석하였다. 또한 건널목 장치를 대상으로 원인-결과 분석 절차를 살펴봄으로써 시스템의 안전성 확보방법을 고찰하였다.

2. 안전시스템의 lifecycle 모델

안전과 관련된 시스템의 개발은 기술하는 수단으로서 lifecycle 모델을 이용할 수 있다. 안전성 lifecycle은 위험요인 및 위험도 분석을 고려한다는 점을 빼고는 시스템 lifecycle과 매우 유사하다. 여기에서는 V diagram과 IEC 61508 model을 비교하여 그 장·단점을 살펴보았다.

2.1 V diagram

널리 사용되는 lifecycle 모델로는 V diagram이 있다. 그림 1에 V diagram을 나타내었다. V diagram 모델은 각각의 개발 단계의 출력을 명확히 나타내며, 또한 각 단계간의 정보 흐름을 잘 나타낸다. 하지만 언제 작업이 필요한 지 또는 각 단계에 포함되는 작업량이 어느 정도인지를 명확히 나타내지는 못한다. 이 모델은 그림 왼편에 있는 top-down 방식의 설계를 위한 접근법과 그림 오른편에 있는 buttom-up방식의 시험을 위한 접근법을 강조한 것이다.

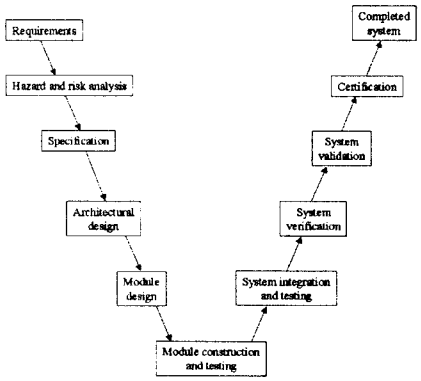

그림 1. V diagram

처음의 작업은 시스템 요구사양을 작성하는 것으로 결정된다. 일반적으로 요구사양이라는 것은 시스템이 해야만 하는 사항을 관념적으로 정의한 것이다. 이러한 관념적인 요구사양은 기능 요구사양 기술문서로 유형전환을 하여야만 한다. 일단 시스템의 기능 요구사양이 확립되면, 시스템에서의 잠재적인 위험을 규정하고, 전체 안전무결성 정도를 할당하기 위하여 위험요인 분석 및 위험도 분석을 수행한다. 시스템의 안전성 요구사양은 위험요인 분석 및 위험도 분석으로부터 도출된다. 안전성을 확보하기 위하여 안전성 요구사양은 시스템이 해야만 하는 것과 하지 말아야 하는 것을 정의한다. 일단 사양이 만들어지면 시스템의 구조를 정의한 최상위 레벨의 설계에 대하여 근거자료로 사용한다. 이러한 절차의 주요 양상 중 하나는 시스템을 하드웨어 및 소프트웨어 각각의 범위를 나눈다는 것이다. 하드웨어와 소프트웨어의 균형을 맞추는 것은 설계 상 vital한 부분에서 이루어지며, 다각도로 고려해야만 한다. 설계단계에서는 프로젝트의 설계 및 시험 절차를 단순화하기 위하여 많은 관리 가능한 모듈들로 분리한다. 그런 다음 세부적으로 각각의 모듈에 대하여 하드웨어 및 소프트웨어 설계가 이루어진다. 설계를 마치면, 모듈들을 제조하고 개별적으로 시험하게 된다. 이러한 시험은 각각의 모듈들이 각기 요구사양을 만족하는지를 확인하는 단계인 검증 단계의 일부분으로 사용될 수 있다. 검증작업은 lifecycle 전반에 걸쳐서 계속되어야만 하고 각각의 단계에 있어서 중요한 부분을 차지한다. 일단 다양한 모듈들이 완성되고 검증되면, 시스템 통합 절차가 이루어진다. 시스템이 완성되고 정확하게 기능을 수행한다면 전체 시스템에 대한 입증작업이 수행된다. 최종 단계는 시스템이 안전성을 외

부 평가 기구에 의해 확인을 받는 단계이다. 안전과 관련된 시스템에 있어서는 프로젝트에 대하여 적절한 건전도 레벨을 결정하기 위하여 좀더 자세한 위험요인 분석 및 위험도 분석이 필요하다.

2.2 IEC 61508 Model

또 하나 널리 사용되는 lifecycle 모델은 그림 2에 나타낸 IEC 61508 모델이다. 이 모델은 시스템을 전기/전자/프로그램, 기타 기술, 외부 장치의 3부분으로 나누어 실현하고 있다. IEC 61508 모델은 시스템 수명기간중의 변경사항으로 인한 영향을 고려하며, 이 모델에서는 lifecycle 각 단계 중에 수행되는 활동 및 각 단계에서의 개략적인 입출력 내용을 자세히 기술하고 있다.

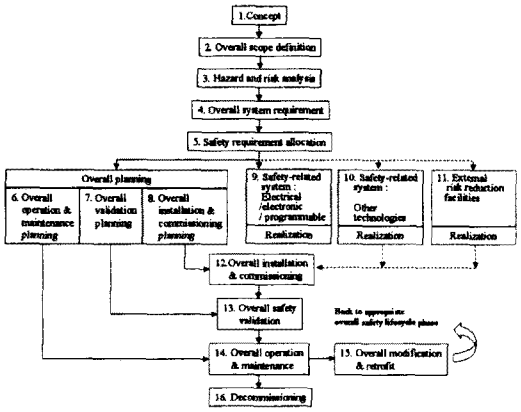

그림 2. IEC 61508 model

그림 2의 단계 1-4는 시스템의 전체 성격에 대한 결정사항 및 안전성 적용사항에 대하여 기술하고 있다. 사전 위험요소 및 안전성 분석 결과를 이용하여 해당 기법들을 결정한다. 개념적으로 단계 3과 관련되어 있는 위험요인 및 위험도 분석은 시스템에 대한 적절한 무결성 레벨을 결정하기 위해서 단계 4에서 사용된다. 단계 5에서는 단계 4에서 정의된 다양한 안전성 요구사양들을 적절한 안전 관련 시스템으로 할당한다. 시스템 구성시 복잡한 사항은 가능한 한 피해야만 한다. 시스템의 안전성은 설계 및 개발에서 뿐만이 아니라 어떻게 설치되고, 사용되며, 유지보수 되었는가에 의해서 결정된다. 그렇기 때문에 시운전, 운영, 유지보수에 대한 전체 정책은 개발 초기 단계에 확립되어야 한다. 안전성 lifecycle에서 9, 10, 11단계는 다양한 안전 관련 시스템의 설계 및 실현과 관련되어 있다. 다양한 안전성 관련 시스템을 실현한 연후에 단계 12의 설치단계동안 통합되고, 그런 다음 전체 시스템은 검증 단계에 들어간다. 만약 필요하다면 단계 13의 인증단계로 들어간다. 시스템 수명기간 중에서 운영 및 유지보수 단계는 14단계에서 수행되고 단계 15에서 수정 또는 갱신작업이 이루어진다. 시스템의 폐기는 단계 16에서 언급된다.

3. 건널목장치에서의 안전성 확보 방안

3.1 개요

다음 내용은 안전성 평가 절차에 대하여 알아보기 위하여 작성한 것이다. 적용 데이터는 외국 데이터를 이용하였으며, 국내 상황보다 가혹하기 때문에 큰 문제점은 없을 것으로 생각된다. 다만 절차의 진행을 위하여 몇가지 사항에 대하여는 적절하게 가정하였다.

해석 대상은 건널목장치로 하였으며 시스템에서 개선점을 도출하고 이에 대해 분석하였다.

표 1에서는 각각의 위험요소에 대한 발생빈도와 심각성을 분류하여 위험도를 산정하였다.

표 1. 위험요인의 위험도

위험도 (빈도×심각성)			참재적인 상해와 손실의 심각성				
			2인이상 사망	1인 사망	2인이상 중상	중상	경상
			5	4	3	2	1
발생빈도	1일 ~ 1개월	5	25	20	15	10	5
	1개월 ~1년	4	20	16	12	8	4
	1년 ~ 10년	3	15	12	9	6	3
	10년 ~ 100년	2	10	8	6	4	2
	100년 이상	1	5	4	3	2	1

표 2는 건널목에서 발생할 수 있는 위험요인을 도출하고 위험도를 나타낸 것이다.

* 도출한 위험요인의 위험도 = 발생빈도×심각성

표 2. 위험요인과 위험도

위험요인 참조	위험 요인 설명	예측 주기	예측 심각성	위험요인 순위	비교/근거
1	인가를 받지 않은 건널목이 사용되는 경우 (작업용)	N/A	N/A	N/A	해석 중인 건널목은 작업용 건널목이 아니므로 이 위험요인은 관련이 없다.
2	열차로부터 사람들을 보호하기 위한 건널목의 고장	2	4	8	건널목을 지나는 교통량이 낮음으로 해서 위험요인의 심각성을 간과할 수 있다.
3	차단기가 열차가 없는데도 작동	3	4	12	이 형태의 고장은 주로 서비스 장애로 귀결된다. 고장으로 인하여 차단기를 수동 조작할 경우 사고로 이어질 가능성이 있다.
4	보행자가 건널목을 잘못 사용	4	2	8	이 형태의 사고는 대부분 차단기가 내려오는데 갑자기 끼어들어 발생하고, 대표적인 영향은 기반 시설에 충격을 주고 그 결과 중상으로 귀결될 수 있다.
5	초기 설계 범위를 벗어난 건널목 사용	N/A	N/A	N/A	사용중인 건널목은 초기 설계 범위 내에서 사용하고 있다.
6	건널목의 좋지 못한 시야	5	4	20	건널목의 시야가 좋지 못한데서 기인되는 위험은 보행자가 건널목에 다가갈 때마다 기차가 접근하여 건널목차단이 있을 때마다 발생한다.

3.1 원인분석 (Causal Analysis)

표 2중에서 두 번째 위험요인 (열차로부터 사람들을 보호하기 위한 건널목의 고장)을 대상으로 원인 분석을 하여 보았다. 그림 3은 위험요인의 발생주기를 예측하기 위하여 나타낸 고장나무분석(Fault Tree Analysis)을 나타낸 것이다.

고장나무분석을 위한 데이터는 다음과 같이 가정하였으며, 해석결과를 정량화 할 수 있었다.

① 한시간에 평균 4대의 열차가 건널목을 지나가고, 각 열차에 대하여 약 90초 동안 건널목이 작동한다고 가정하면, 열차가 건널목에 있거나 혹은 근처에 있을 경우의 수는 다음과 같다.

$$probability = \frac{90 \times 4}{3600} = 0.1$$

② 외국의 경우 선로를 열차가 점유했는데도 선로에 아무 것도 없다고 제어기가 표시할 사건 발생 가능성은 연간 5×10^{-3}이었다.

③ 또한 선로회로의 고장 가능성은 2.5×10^{-3}이었다.

④ 통신 시스템 고장의 경우는 1.5×10^{-3}이었다.

⑤ 시차고장의 경우는 차단기가 내려온 상황에서 보행

자 또는 자동차가 건널목에 있을 경우에 해당하며, 평균 일년에 두 번 정도 건널목에서의 보호가 제대로 이루어지지 않는다고 가정하면, 시차고장의 연간 2.0라고 할 수 있다.

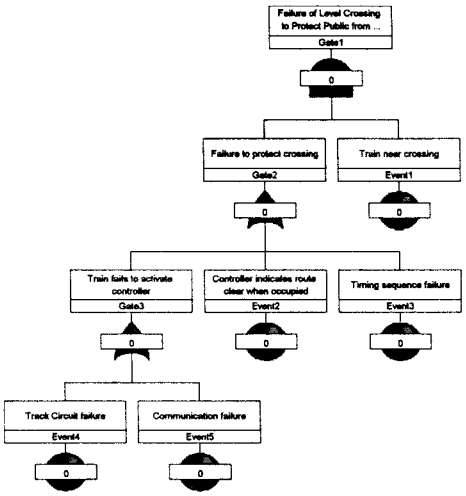

그림 3. 위험요인에 대한 고장나무분석

결합나무분석은 위에서 조사한 사건들의 발생가능성을 대입하여 나타낼 수 있다.

$$((2.5\times10^{-3+}+1.5\times10^{-3})+5\times10^{-3}+2.0)\times0.1 = 0.20$$

여기에 나타난 것처럼 시차고장이 큰 부분을 차지함을 알 수 있다.

3.2 결과분석 (Consequence Analysis)

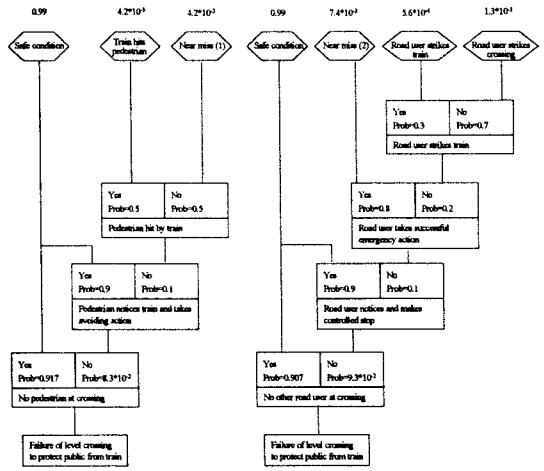

그림 4. 원인-결과 모델

결과분석은 각각의 위험요인으로부터 발생할 수 있는 사건들을 결정하는데 사용된다. 수행하는 해석방법은 각 위험요인의 원인분석과 유사한 방법으로 수행한다.

앞에서의 원인분석 대상에 대하여 결과분석을 하면 다음과 같다. 분석방법은 고려중인 위험요인이 Tree의 아래부분에 표시되도록 하는 귀납적인 방법을 택한다. 그 영향은 안전한 상태로부터 대형사고 또는 치명적인 사고에 이르기까지 범위가 다양하다. 대략적인 원인-결과 모델을 그림 4에 나타내었다.

4. 결 론

본 논문에서는 열차제어시스템에서 사용되는 다양한 lifecycle 모델을 조사하여 각 단계의 시스템 분석 방법에 대하여 살펴보았다. 여기에서는 V diagram과 IEC 61508 모델을 분석하였는데 V diagram은 각각의 개발 단계의 출력을 명확히 나타내고, 각 단계간의 정보 흐름을 명확히 나타낼 수 있지만 언제 작업이 필요한 지 또는 각 단계에 포함되는 작업량이 어느 정도인지를 명확히 나타내지는 못한다. IEC 61508에서는 lifecycle 각 단계 중에 수행되는 활동 및 각 단계 중의 개략적인 입출력 내용을 자세히 기술할 수 있다 또한 건널목 장치를 대상으로 원인-결과 분석을 살펴봄으로써 시스템의 안전성 확보를 위한 절차에 대하여 알아보았다. 앞으로의 연구내용으로는 위험요인으로 인한 손실분과 그 영향 감소 대책에 대해 검토하여 ALARP (As Low As Reasonably Practicable)의 적용방안에 대하여 검토할 예정이다.

[참 고 문 헌]

[1] International Electrotechnical Commission, IEC61508, Functional safety of electrical /electronic/programmable electronic safety-related system.

[2] CENELEC EN50126, Railway application The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)

[3] CENELEC EN50128, Railway application Software for railway control and protection system.

[4] CENELEC ENV50129, Railway application Safety related electronic systems for signaling, May 1998