2002년도 대한전기학회 하계학술대회 논문집 2002.7.10-12

철도시스템의 안전성 요구사양 작성을 사전 절차 연구

정의진*°, 이종우*, 김양모**
*한국철도기술연구원, **충남대학교

A Study on the Pre-process for Developing Railway Safety Requirement

Eui-Jin, Joung*°, Jong-Woo, Lee* Yang-Mo, Kim**
*KRRI(Korea Railroad Research Institute), **Chungnam National University

Abstract - It is very important to ensure system safety during the process of developing a system. Railway system is also devoting a great portion for the safety. Nowadays many countries leading railway industry have their own system assessment process according to the situation of their train control system. In this paper, a preprocess to establish system safety requirement is represented in the railway signalling system. We also adopt electronic interlocking system for an example.

1. 서 론

철도시스템은 신속, 정확, 안전이라는 세 가지 사항에 중점을 두고 운영되고 있다. 특성상 대량 인원 및 물자를 실어 나른다는 점에서 안전성이 특히 중요시되고 있다. 이러한 철도시스템의 안전성을 확보하기 위해서 시스템의 안전성 요구사양을 마련하는 것은 대단히 중요하다. 시스템의 안전성 요구사양을 마련하기 위해서는 시스템의 안전성 분석이 필수적인데 이를 단계적으로 살펴보면 먼저 시스템 개발에 중점을 두는지, 시스템 설치시의 안전성 확보에 중점을 두는지를 명확히 하는 안전성 확보 대상을 선정하고, 둘째, 안전성 평가의 비교 단위가 인명손실인지 열차지연인지 혹은 장치손상인지를 정하는 평가 기준을 정하여야 한다. 셋째로 선정한 평가기준에 영향을 미치는 위험요인을 선정하고, 넷째 Failure Mode Effect Analysis(FMEA), Fault Tree Analysis(FTA), Event Tree Analysis(ETA) 등의 기법을 적용하여 관련 위험요인의 심각성 및 발생빈도를 정량적으로 분석하는 위험도 분석을 한다. 이를 토대로 안전성을 확보하기 위한 시스템 안전성 요구사양을 도출할 수 있다. 본 논문에서는 안전성 요구사양을 도출을 위한 정량적이고, 과학적인 안전성 분석방법에 대하여 논하고자 한다.

2. 철도시스템의 안전성 인증체계

철도시스템의 안전성을 확보하기 위하여 철도 선진국에서는 자국내 실정에 맞추어 안전성 인증 체계를 마련하여 운영하고 있다. 국내에서도 이에 발맞추어 철도시스템의 안전성을 확보하기 위하여 안전성 인증 체계에 대한 연구가 이루어지고 있는 중이며, Fig.1은 현재 제안중인 철도시스템의 안전성 인증 체계를 나타낸 것이다.

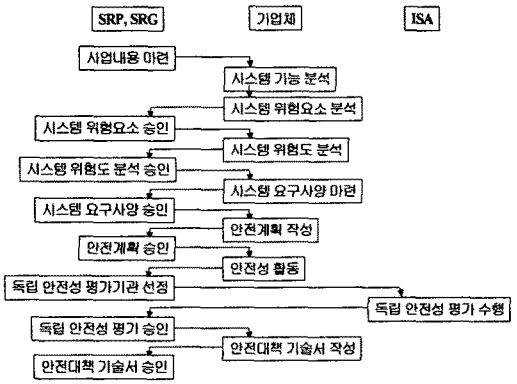

Fig. 1 철도시스템의 안전성 인증체계

① 사업내용 마련
- 안전성 목적 설정 : 장치개발이 목적인지 장비설치가 목적인지 선정, 장치개발을 목적으로 하는 경우 개발하고자 하는 장치의 정의
- 위험결과의 범위 지정 : 인명손실에 관련하는지, 열차지연에 관련하는지, 장치손상에 해당하는지 범위 선정

② 시스템 기능 분석
개발시스템의 특성 및 정의 등을 고려하여 기능을 분석한다.

③ 시스템 위험요소 분석
기능 구현의 오류로 인한 영향 분석 : 장치의 해저드 분석, Preliminary Hazard Identification 수행

④ 시스템 위험도 분석
오류의 심각성 및 발생빈도를 살펴 장치 위험도 산정
FTA, ETA, FMEA 등의 방법 적용
정량적으로 위험도 산정, 사고데이터 등 체계적인 데이터 확보 필요
FTA : 기능 오류를 큰 사상으로 잡고 하위 사상 분류 - 하위 사상의 발생 확률 산정에 중요
ETA : 기능오류로 인해 발생할 수 있는 위험요인 분류 - 위험요인 발생확률 산정에 중요

⑤ 시스템 요구사양 마련
- 기능별, 장치별 Safety Integrity Level(SIL) 정의 : 장치 자체의 SIL 선정, 도달하여야 할 SIL과 현재 기술수준의 차이를 고려하여 SIL 선정
- 안전성 요구사양 정립 : 장치의 기능 구현시의 안전성 기능 요구사양 정립

⑥ 안전 계획 수립
제시된 SIL을 만족하기 위한 구체적인 기능구현 방법 및 계획 선정
기능구현을 위한 방법으로 제시된 SIL에 따라 IEC 61508에서 제시된 방법 중 적당한 방법 선정

⑦ 안전성 활동
선정한 방법의 실제적인 구현방법 서술, 구현방법의 정량적, 정성적인 분석 수행, FMEA, FTA, 환경시험 등을 통해 입증

⑧ 독립 안전성 평가 수행
제시한 분석결과를 토대로 안전성 활동이 기술적, 체계적으로 맞게 수행되었는지 확인

⑨ 안전대책기술서 작성
안전성 평가에 따라 안전성 승인 및 인도

3. 안전성 요구사양 도출

안전성 확보 대상으로 전자연동장치를 선정하였는데 기존의 장기간의 실적으로 안전성이 입증된 릴레이 구동 연동장치를 대신할 목적으로 하드웨어로는 마이크로일렉트로닉스 기술을 소프트웨어 기술로 안전성을 입증하기 위한 여러 기법을 적용한 시스템이다. 본 전자연동장치의 안전성 요구사양을 마련하기까지의 절차에 대하여 아래에 기술하고자 한다.

3.1 기능요구사양 조사 및 분석

기업체에서는 발주처의 사업목적에 따라 제품을 제작하게 되는데 사업목적은 경우에 따라서 개괄적이거나 개략적일 수 있다. 이러한 상황에서 기업체는 발주처의 사업목적 및 규격을 참조하여 안전성 확보를 위한 작업을 진행해야만 한다. 여기에서는 전자연동장치의 개발을 대상으로 하여 발주처중 하나인 철도청의 개발규격을 참조하여 분석하는 방법에 대하여 알아보고자 한다.

3.1.1 일반적 시스템 요구사항 분석

가. 전자연동장치의 기능
- 연동기능 : 진로선별기능, 신호기제어기능, 진로복위기능, 차량추적, 보수용차 진로제어, 선로폐쇄제어, 신호기사용정지, 신호기 이상감시
- 표시반의 입력기능 : 정보표시, 정보입력, 조작방법
- 구내관리기능 : 진로의 자동설정, 진로설정의 자동판단, 열차번호의 관리
- 유지보수정보관리기능 : 동작기억·기록, 고장표시·기록
- CTC 결합기능
- 시스템관리기능

나. 전자연동장치의 구성
- 중앙처리장치
- 표시제어반
- 모니터설비
- 데이터전송장치
- 감시장치
- 유지보수장치
- 전원장치
- 릴레이

다. 시스템 경계 및 인터페이스
- 제전기 랙
- 광통신 부

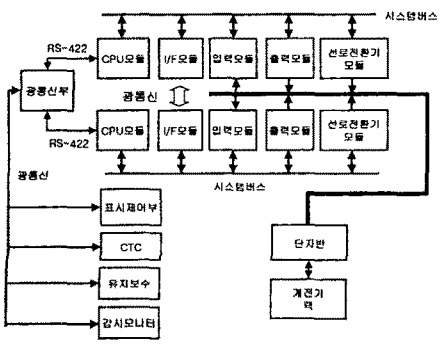

Fig. 2 시스템 경계 및 인터페이스

라. 시스템의 특징
- 마이크로프로세서를 이용한 분산 시스템
- S/W를 이용한 시스템
- 광통신을 이용한 시스템

3.1.2 안전성 확보를 위한 시스템 요구사양 분석

가. 일반요구사양
- 계층적구조
- 바이탈 기능
- 논바이탈 기능
- 네트워크 연결
- 전원장치의 이중화

나. 하드웨어의 일반적인 구조
- 안전 측 동작(Fail-safe) 확보
- 이중화
- 모듈화
- 고장분리
- 자기진단

다. 소프트웨어의 일반적인 구조
- 특별한 언급은 없음

3.2 시스템 위험도 분석

신호시스템의 위험도를 산출하기 위해서는 일련의 과정을 밟아야만 한다. 먼저 위험요소를 산출하고 도출된 위험요소의 발생확률 및 위험요소로 인해 야기된 사고의 심각도를 곱함으로써 위험도를 정량적으로 도출할 수 있다. 도출한 위험요소에 대해서는 Safety Review Group (SRG) 및 Safety Review Panel (SRP)의 승인을 받아야만 한다. 이렇게 도출 승인된 위험요소에 대하여 정성, 정량적인 위험도 분석을 수행하게 된다. 위험도 분석 또한 SRG 및 SRP의 승인을 받아야만 한다.

3.2.1 위험요소 도출

여기에서는 전자연동장치에서 사고의 원인이 될 위험요소들 중 대표적인 몇 가지에 대해서 살펴보고자 한다.
- 한 구역에 두 열차가 동시에 존재
- 비 보호된 고압 전력공급 고가선
- 기본시설 점유이후 비안전 상태로 복귀
- 선로전환기가 열차아래서 움직임
- 선로전환기 불일치
- 접지고장
- 부적절한 신호 중복

3.2.2 위험요소 목록 작성

Table 1 전자연동장치 위험요소 목록

번호	위험요소	승객피해	철도원 피해	주변피해
1	한 구역에 두 열차가 동시에 존재	○		
2	선로전환기가 열차아래서 움직임	○		
3	부적절한 신호 중복	○		
4	선로전환기 불일치	○		
5	접지고장		○	
6	기본시설 점유이후 비안전 상태로 복귀		○	
7	비 보호된 고압 전력공급 고가선		○	○
8	EMC의 영향	○		

3.2.3 위험도 분석

다음의 표를 작성하여 각각의 위험요소에 대한 발생빈도, 심각성을 정량적으로 산정한다.
안전성 분석 기법에는 FMEA, FTA, ETA 등을 거론할 수 있다. 물론 이러한 분석기법을 적용하기에는 관련 데이터 확보가 최우선이다.

Table 2 전자연동장치 위험도 분류

번호	위험요소	발생빈도	심각도	위험도
1	한 구역에 두 열차가 동시에 존재			
2	선로전환기가 열차아래서 움직임			
3	부적절한 신호 중복			
4	선로전환기 불일치			
5	접지고장			
6	기본시설 정유이후 비안전 상태로 복귀			
7	비 보호된 고압 전력공급 고가선			
8	EMC의 영향			

3.3 안전성 요구사양 도출

요구사양 도출 과정에서 주된 작업은 시스템의 SIL을 할당하는 것이다. SIL 할당에는 몇 단계의 작업이 요구되는데 아래에 간략히 나타내었다. 도출한 위험요인들과 전자연동장치와의 관계를 연결하면 Table 3과 같다. 즉 도출한 위험요인에 대하여 전자연동장치의 어느 기능의 오류나 잘못이 사고로 이어지게 되는 가를 결정한다. 이러한 과정을 거침으로써 각각의 기능에 대하여 위험도를 선정할 수가 있으며, 각각의 기능을 구현하기 위한 하드웨어 및 소프트웨어의 위험도 목표치가 결정된다. Table 4는 연동장치의 기능 구현을 위한 모듈 분류와, 각각의 모듈에 대한 SIL 할당 예를 나타낸 것이다.

Table 3 위험요인 대비 전자연동장치의 기능 할당

번호	위험요소	전자연동장치 관련 기능
1	한 구역에 두 열차가 동시에 존재	연동기능, 표시반 입력기능, 구내 관리기능, CTC결합기능
2	선로전환기가 열차아래서 움직임	연동기능, 구내 관리기능
3	부적절한 신호 중복	연동기능, 구내 관리기능
4	선로전환기 불일치	연동기능, 구내 관리기능
5	접지고장	시스템 관리기능
6	기본시설 정유이후 비안전 상태로 복귀	연동기능
7	비 보호된 고압 전력공급 고가선	시스템 관리기능
8	EMC의 영향	환경요인

Table 4 전자연동장치 기능별 모듈 구성 및 SIL 할당

기능 / 구성	연동기능	시스템 관리기능	표시반 입력기능	구내 관리기능	유지보수 관리기능	CTC 결합기능
CPU보드	SIL4		SIL3	SIL2	SIL2	SIL3
I/F		SIL4				
Output Board	SIL4					
Input Board	SIL4					
Pointer Output	SIL4					
Relay Rack	SIL4					
Comm. Module	SIL3					SIL3

실제로 각각의 위험요인에 대하여 위험발생 확률을 계산하고, 위험요인으로 인한 사고의 심각도를 산출하여 위험도를 산정함이 타당하나, 현재 축적된 데이터가 없기 때문에 선진 외국의 적용사례를 살펴보고자 하였다. Table 5는 신호시스템 각각의 기능에 대하여 각 국의 SIL 할당 사례를 나타낸 것이다. 표에서 보면 전자연동장치는 SIL 4에 해당함을 알 수 있다. 참고로 CENELEC 규격에서 제시하고 있는 SIL의 정도를 Table 6에 나타내었다.

3.4 전자연동장치 안전 계획 수립

위에서 도출한 전자연동장치의 H/W 및 S/W SIL 할당 값에 대하여 어떠한 기술을 이용하여 전자연동장치의 기능구현을 할 것인가를 정하는 작업이 안전 계획이다. 해당 SIL에 대하여 권장하는 기술은 이미 국제규격(IEC 61508)으로써 권고되고 있다.

Table 5 철도신호시스템에 대한 각 국의 SIL 할당 예

기 능	DB	BR	NMBS	SNCF	SBB	FS	LUL	OeBB	NS
연동장치	4	4	4	4	4	4	4	4	4
선로전환기	4	4	4	4	4	4	4	4	4
열차검지	4	4	4	4	4	4	4	4	4
열차제동시스템	2	2	4	4	2	4	4	2	4
자동폐색	4	4	4	4	4	4	4	4	4
건널목제어	4	4	4	4	4	4	NA	4	4
건널목 감시	4	4	2	NA	4	2/4	NA	4	NA
제어반	4	2	4	4	3	4	NA	4	NA
ATP	4	4	4	NA	NA	4	4	NA	4
자동진로설정	2	2	NA	NA	2	2	2	2	2

Table 6 Safety Integrity Level (SIL)

단계	안전성에 요구되는 무결성 단계	가혹도	사람 혹은 기기에 대한결과	서비스에 대한 결과	연속/고수요 운전 유형 (단위 요소별 단위 시간당 위험한 고장율)
4	매우 높음	Catastrophic	다수 사망, 기기의 매우 큰 손실	주요 시스템 상실	$< 10^{-10}$
3	높음	Critical	사망 및 부상 기기의 중대 손실	주요 시스템 상실	$\geq 10^{-10}$ to $< 0.3\times10^{-8}$
2	중간	Marginal	부상 및 기기에 대한 중대 손실	심한 시스템 손상	$\geq 0.3\times10^{-8}$ to $< 10^{-7}$
1	낮음	Insignificant	사소한 손상	사소한 시스템 손상	$\geq 10^{-7}$ to $< 0.3\times10^{-5}$
0	안전성 관련 되지 않음	negligible	손상 없음	사소한 고장	

4. 결 론

지금까지 전자연동장치를 대상으로 하여 안전성 요구사양 도출 과정을 살펴보았다. 정성·정량적인 위험도 분석에는 실제로 많은 노력 및 연구가 필요하며, 적절한 분석을 위해서는 다량의 양질의 데이터가 필요하다. 위험도 분석은 또한 경제성 분석 등의 기초가 되어 과도한 기술개발을 줄이거나 적정투자를 유도하는데 근거로서 활용할 수 있다. 국내 철도신호 산업환경을 고려하면 이러한 안전성 평가 및 위험도 분석작업이 어려운 작업일 수 있으나 세계적으로 요구되고 있는 사항이며, 국내 철도 산업의 발전 및 철도시스템의 안전성 확보를 위해서는 필요불가결한 작업이라고 생각된다. 기존의 실적 위주의 평가척도에서 벗어나 신제품 사용이나 국외 철도제품의 검증에도 도움이 될 것으로 기대된다. 이를 위해서는 앞으로도 지속적인 안전성 확보 및 평가 기술에 대한 연구가 필요하다고 하겠다.

[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 ENV50129, Railway application Safety related electronic systems for signalling

[4] Institution of Railway Signal Engineers(IRSE) report, Safety system validation with regard to cross acceptance of signalling systems by the railways, 1992.1