

철도 시스템 안전성 평가

한국과학기술정보연구원
전문연구위원 정현갑
(99102@reseat.re.kr)

1. 철도의 총합 시스템과 안전 확보

- 철도의 보안제어는 ATC나 ATS를 기본으로 하는 열차제어로 그의 기본인 신호장치도 안전한 열차수송을 목적으로 하고 있다. 그러나 철도의 안전은 신호보안만으로 끝나는 것은 아니다. 근래의 사고를 보아도 궤도 시스템이나 방재 시스템, 운전에 관여하는 것 등 그의 원인은 여러 가지이다. 철도를 구성하는 차량, 궤도, 전차선, 신호, 역과 플랫폼 품의 시설 등 인프라는 무엇보다도 운전 관여하며 여러 소프트웨어를 포함하며 안전에 관여하지 않는 것은 없다.
- 미국 샌프란시스코 만안고속철도의 자동운전제어에 종래 열차제어 기술이 아닌 항공우주의 침단기술을 도입 주목을 받았지만 개업 초기부터 사고를 일으켜 구식 열차제어로 운영을 바꿨다. 이는 철도와 같은 대규모에 복잡한 시스템을 전혀 제로로부터 구축하는 것은 용이하지 않다는 것을 뜻한다. 복잡 다양한 시스템을 제로의 상태에서부터 만족할 수 있는 수준으로 창조해내는 시스템 공학기술은 아직 확보하고 있지 못하다.
- 현재의 고밀도 고속수송은 초기 단순한 시스템으로 시작하였으나 긴 세월 동안에 축적된 경험이나 노하우들이 오늘날 복잡한 시스템의 신뢰성, 안전수준을 지탱하고 있다. 오늘날의 철도시스템이 안전하게 유지되고 있는 것은 시스템 공학적 입장에서 모든 서브시스템이 안전성이나 신뢰성에 대하여 대략 동등수준을 가지고 있다는 것 즉 신뢰도 협조와 안전성협조가 중요시 되고 있기 때문이다. 일부의 취약함이 전체의 신뢰성이나 안전성을 저하시키는 것은 경험을 통하여도 명확하며 일부만이 극단으로 높은 수준을 갖고 있어도 그것은 코스트의 상승을 가져올 뿐이다.
- 신호분야는 고장 시에도 안전성을 유지 하도록 이론회로 설계가 경험

적으로 구축되었고 폐색이나 연동장치의 페일세이프(fail safe: 안전기능)를 지탱하였다. 예를 들면 일단 구성된 진로 상을 열차가 주행 중에 스위칭이 만일 전환을 시작해버리면 탈선이나 전복의 사고로 이어진다. 대책으로 계전연동 장치에는 쇄정회로가 삽입되어 있으며 열차통과가 끝날 때 까지는 스위칭의 모터회전에 전기가 들어가지 않도록 되어 있다. 이 쇄정회로는 계전기의 비대칭인 에러 특성을 이용한 페어세이프 이론회로로 되어 있다.

2. 안전성에 대한 수량평가의 시도

- 안전도의 수량평가: 안전정도를 보안도라는 용어를 사용하는 것도 특수한 철도 계에서의 검토라는 감이 들지만 보안도라는 용어는 극히 정성적인 평가로서 쓰이고 있다. 일본 보안도위원회에서 확인하는 보안도인식은, 보안도는 부품 또는 단일장치 개개에는 문제되지 않고 어떤 시스템 전체에 대하여 파악된 양이며 시스템에는 사람이 개재, 개재여지가 적은 것일수록 보안도가 높고 사람이 쓰기 어렵거나 오인하기 쉬운 시스템은 보안도가 낮다. 신뢰도가 높은 설비는 보안도가 높으며 페일 세이프의 환경이 큰 것은 보안도도 높다. 시스템의 기능이 정지하는 시간이 긴 것일수록 보안도가 낮고 설비에 고장이 일어났어도 운전이 지장을 줄 환경이 적은 시스템은 보안도가 높다는 것을 확인하고 있다.
- 시스템에서 위험 측 고장율의 계산: 안전성평가가 논의된 것은 신호시스템에 컴퓨터를 도입하려는 시기였다. 다양한 고장모드나 에러모드를 컴퓨터 신호보안장치에 이용하는 데에는 다양한 모든 고장에 대한 안전성 확보와 종래 장치와 동등 이상의 안전성에 대한 정량적 입증 여부이다. 설계단계에서 치명적 고장모드와 그 원인의 철저한 추출 및 대책을 과거의 안전성기술에 의거 적합 시키는 일과 그리고서 그의 타당성을 발주자 측에 인증을 받도록 하는 것이 중요하다.

3. 안전성 평가의 일반화

- 독자적 안전성 기술의 주장: 개개의 산업영역에서 안전성 기술론은 배경으로 하는 시스템의 다양성에 의거 독자성이 강하고 어느 것이 우위에 또 어느 것이 열등인가의 비교에는 익숙하지 못할 뿐 아니라 공통

의 방법론도 확립될 수 없는 상태가 이어지고 있다. 고장 시 정지시키는 것으로 안전을 유지하려는 철도와 공작기계의 안전장치에 대한 기술은 양상을 달리하고 있다. 이와 같이 기본으로 하는 안전성의 개념이나 안전성기술도 서로 다른 상태에서는 안전성을 수량적으로 평가하는 것에 합의가 이루어지기 어렵다.

- 안전성의 척도로서 리스크의 등장: 안전성 개념과 기술평가에 결정적인 영향을 준 것은 리스크라는 개념의 안전성 평가이다. 리스크는 안전성 기술의 평가가 아니고 치명적 요인의 발생확률과 그의 치명도로부터 이루어지는 평가 치이다. 산업계의 조건차이에 관계없이 공통으로 이용될 수 있다. 리스크가 안전성에 대한 공통의 지표로서 인식되도록 된 배경에는 각 산업계에서 성숙되어진 독자적 기술이 점차 컴퓨터를 이용한 것으로 이행 해 가고 있으며 기술 그 자체에도 공통요소가 증가하였다는 상황의 변화도 있기 때문이다.

4. 국제규격의 정비와 통일적 안전성 평가수법

- 안전성에 관한 국제규격: 안전성 확보를 위한 국제규격으로 ISO12100 (기계류안전성, 설계를 위한 기본개념, 일반원칙)이나 컴퓨터를 사용한 안전관련 장치를 대상으로 한 기능안전규격 IEC61508이 있다. 리스크 해석으로 대상시스템이 요구하는 리스크 수준과의 분리 분위기로 안전성수준 SIL(Safety Integrity Level)을 정하고 제품의 라이프 사이클을 통하여 그의 SIL수준에 맞는 작업을 실행하는 것과 그의 실행 프로세스의 타당성을 제 3자가 인증하는 것이다.
- 통일적 안전성 해석수법: 통일적 안전성 해석수법이 요망하는 요건으로 시스템의 위험 측 장애 발생률을 산출할 수 있고 안전성 기술을 삽입할 때 위험 측 장애발생률의 저감효과가 산출될 수 있다. 개개의 안전성기술효과가 산출, RISK나 SIL이라고 하는 국제규격에 있어 척도가 산출될 수 있어 위의 요건에 맞는 것이 개발될 수 있다.
- 리스크, 위험 측 장애발생확률의 평가: 해석대상 시스템에 모든 장애를 열거하고 시스템 구성요소 각각에 대하여 고장모드를 열거, 그의 고장률로 이루어지는 고장확률 벡터 A를 생성한다. 이 고장확률 벡터 A와

상기 장애의 관계를 상관행렬 PM으로 표시, 양자의 적을 취함으로써 각 장애의 빈도벡터(기능장애빈도 벡터 $P(g)$)가 계산된다. 이 단계에서 위험 측에 있는 것인지 아닌지의 필터링을 하면 시스템이 갖는 위험 측장애 발생확률이 산출 될 수 있으며 치명도를 정상적으로 수준을 부여함으로써 각 기능장애 리스크나 시스템 리스크도 산출할 수 있다.

- 안전성 기술의 효과와 시스템의 안전성 평가: 안전성 기술의 효과에 대한 해석을 설명한다. 우선 리스크저감책으로 추진된 각종 안전성 기술을 열거하고 각개 기술을 대상으로 고장확률 벡터 A의 각 요소마다 정도효과가 있는 것인가를 1부터 0까지의 수치로 표현한 억지효과 벡터를 생성한다. 1은 전혀 효과가 없고 0은 완전히 마스크 될 수 있는 것을 의미한다. 또 억지효과 벡터로부터 대각 행렬을 만들어 고장확률 벡터 A와의 적을 취함으로써 그의 기술을 추진한 결과 어느 정도 효과가 나왔는가가 산출될 수 있다.

5. 철도 시스템의 안전성 평가

- 안전성 평가는 개개의 시스템이나 장치를 대상으로 하였다. 장치나 시스템 개발평가에 유효하게 이용될 수 있다. 그러나 철도를 구성하는 궤도나 신호보안, 전차선 등 각 기술계통 내에 봉입된 서브 시스템이나 장치의 평가는 가능하여도 이대로 철도 시스템의 안전성수준이 어떻게 될 것인지를 중요한 문의에는 답할 수 없다. 이용자가 바라는 평가는 개개의 장치나 시스템의 안전성만이 아니라 그들이 유기적으로 기능하고 있는 상태 하에서의 철도 시스템 전체에 대한 안전성을 기대한다.
- 사고 리스크에 의한 철도의 안전성 평가: 일본의 열차사고는 운전사고가 전체의 1%정도이고 사고발생 빈도와 사고 리스크를 분석하였다. 분석결과 사고 리스크는 3.3×10^2 [사람 수/년]이며 이 중에서 주로 승객 등의 피해사고인 열차사고의 사고 리스크는 4.6[사람 수/년]이다. 이를 기준으로 운전사고에 의한 한사람 당 사고 리스크 허용수준 10^{-5} [1/년]을 또 넓게 수용 가능한 수준으로 10^{-6} [1/년]의 값을 얻었다. 같은 방법으로 열차사고인 경우 한사람 당 사고 리스크 허용수준 10^{-7} [1/년], 넓게 수용 가능한 수준으로 10^{-8} [1/년]이라는 값을 얻었다. 자동차의 사고 리스크는 3×10^{-5} [1/년], 일본 국내 항공기는 1×10^{-6} [1/년]이다. 앞서 구한 철

도 열차 사고의 사고리스크 허용수준 10^{-7} [1/년]보다 큰 값을 갖는다.

- 진정 안전철도를 위한 안전성 평가: 사고 리스크는 이제까지의 철도에서 발생한 사고데이터에 의거한 시스템의 평가이기 때문에 이용자나 국민의 시점에 가까운 평가 척도라고 말할 수 있다. 또 평가의 대상도 신호 시스템이나 궤도인 기술영역 개별의 평가가 아니라 총체로서의 평가로 다른 교통기관이나 산업 시스템과의 상대적 비교가 가능하다. 최근에 발생한 중대 사고의 원인을 보면 보통은 상정도 하지 않은 곳에서 발생하고 있는 것에 주목해야 한다.
- 안전문화의 양성: 안전문화가 모든 것에 우위를 가지며 그 중요성에 걸맞게 주위가 확실히 반영 작용되는 기관의 기능과 개인태도의 집적이라 할 수 있다. 구체적으로는 무엇인가를 할 경우는 우선 그에 의하여 어떠한 리스크가 생길 것인가를 생각하는 습관을 가지며 그 결과에 대하여는 확실한 대응을 해야 한다.

6. 결 론



- 철도는 많은 기술영역 계통이 조합되어 성립된 총합 시스템이다. 이제까지는 기술영역이 독자적으로 안전성이나 신뢰성을 달성함으로써 토털로서 철도의 품질이 확보되어 왔다. 그러나 기술의 진보는 시스템을 거대화 시킴과 동시에 영역이 복잡하게 얽히는 상황을 산출하고 있다. 이제까지의 안전성 평가에 멈추지 말고 유기적, 총합적 관계가 해석될 수 있는 새로운 안전성, 신뢰성 평가의 패러다임을 만들어 나가야 할 필요가 있다.

출처 : 中村 英夫, “鐵道システムの安全性評價の取組み”, 「計測と制御(日本)」, 45(9), 2006, pp.821~826

◁ 전문가 제언 ▷

- 교통 시스템에서 친환경적으로 가광을 받고 있는 철도 시스템은 대량 운송 시스템이다. 세계 각 국은 도심의 지하철을 비롯하여 교외선 등 철도 노선을 증설해가고 있는 것이 현실이다. 철도 시스템은 1회의 운행으로 다량의 화물과 사람을 운송하게 됨으로 무엇보다도 보안 시스템의 신뢰성은 중요하다고 하겠다. 따라서 사용자가 신뢰할 수 있는 안전성 평가는 중요한 요소이다.
- 최근 우리나라 철도 시스템은 사고로 운행정지로 인한 시민들의 불평이 크다. 고속철인 KTX의 집전선로 고장으로 장시간 정체라든지 서울 지하철의 빈번한 사고로 운행정지로 시민의 출퇴근에 많은 지장을 초래하고 있다. 이것은 철도운행의 총체적 운영 시스템의 신뢰성과 안전성이 확보되어 있지 못하기 때문으로 사료된다.
- 고장과 사고를 줄이기 위하여 서울지하철인 경우는 승차 역 플레이트 홈에는 승객과 열차간의 안전 분리를 위한 보호막을 설치하거나 또는 고속철에서는 사람이 선로에 접근 못하도록 차폐 벽을 설치하고 있다. 이런 시설물의 설치도 지정된 안전도 기준에 준하여 평가된 후 이루어졌기를 기대한다.
- 우리나라에서는 아직 보고되고 있지 않은 내용이지만 일본의 경우는 신간선 선로위에(레일 상면) 까마귀가 장난으로 자갈을 올려놓아 고속으로 주행하는 차량에 심한 진동을 유발시키는 사례가 있었다. 처음에는 사람에 의한 장난으로 여겼으나 조사결과 사람은 선로에 들어 갈 수 없도록 되어 있어 사람에 의한 행위는 아닌 것으로 결론지었다. 며칠을 지켜본 결과 까마귀의 행위였음이 밝혀졌다. 이는 사고원인이 예측하기 어려운 곳으로부터 유발되고 있음을 시사해주는 내용이다.
- 예기치 못한 불가사의한 내용에 대한 안전성의 신뢰를 구축하기 위하여는 폭넓은 고찰과 많은 경우에 관한 연구가 뒤따르지 않으면 안 된다.