# 안전제어시스템의 사전 안전성 해석절차 연구

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

# A Study on the Prospective Safety Analysis Procedure for Safety Control System

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

**Abstract** - The train control system using radio is based on the radio communication between an on-board control system and a ground control system unlike other train control systems that rely on track circuit. To realize a new train control system based on a new principle, it is important to analyze safety in a systematic manner at an early stage, and identify important factors for the system. For this reason, we think a procedure that select hazards and identify their causes and allocate safety requirements to such hazards. This paper describes this procedure to realize system safety.

## 1. 서 론

철도시스템은 다른 교통 수단과는 달리 대규모 인원을 고속으로 이동시키기 때문에 자칫 사고라도 발생할 경우 대형사고로 번질 위험이 있기 때문에 안전성이 매우 중요하게 요구된다. 이러한 시스템의 안전성 확보를 위해서는 개발 시작단계부터 안전성에 의한 검토를 하여 현장시험에 의해 안전성 평가, 확인을 하여야만 한다. 이를 위해 보안제어 시스템의 개념설계, 안전성 해석, 설계, 제조, 운용, 보수, 수정 등의 일련의 과정을 통한 안전성 라이프사이클과, 요구되는 안전성 레벨 기준을 설정하고 이에 따라 기술 요건을 정하는 안전성 인테그리티 레벨 개념을 도입하는 방식이 중요하다 할 수 있다. 안전성 라이프사이클에서 안전성 해석은 본래 시스템 설계, 제조 전 단계에서 적용하지만 안전성 해석을 통하여 안전 논리 구성을 명확히 하고, 시스템의 안전성을 재확인할 수 있다. 본 논문에서는 안전성 해석 절차에 대하여 논의하고자 하였으며, 대상 시스템으로 무선을 이용한 열차제어시스템을 고려하였다. 무선을 이용한 열차제어시스템에서의 간격제어는 궤도회로를 열차가 단락하여 위치검지를 하는 고정폐색과는 크게 다르다. 따라서 개발 초기부터 안전성에 대하여 검토하고, 현장시험으로 안전성을 평가, 확인하여야 한다.

## 2. 사전 안전성 해석

높은 안전성이 요구되는 시스템에서는 일반적인 시스템과는 달리 그림 1에 표시한 안전성 라이프사이클과 안전성 인테그리티 레벨의 2가지 개념을 도입하여 안전성 관리를 행할 필요가 있다.

안전성 리이프사이클은 보안제어 시스템의 개념 설계, 사전 안전성 해석, 설계, 제조, 운용, 보수, 수정 등의 일련의 과정을 라이프사이클로 하여 그 각 단계에서의 적절한 활동을 정한 것이다. 또 수정시에는 그 영향도에 대응하여 적절한 단계로 귀환하게 된다. 안전성 인테그리티 레벨은 요구된 안전성의 레벨에 응답하는 기준을 설정하고 그 기술 요건을 정하는 것이다.

안전성 라이프사이클 중 사전 안전성 해석의 결과를 토대로 상세 설계, 제조에 반영하고, 요구되는 안전성을 달성한다. 사전 안전성 해석을 단계별로 살펴보면 맨 처음으로 대상 시스템의 기본 사양을 명확히 하고, 사고가 발생하여 인간 또는 재산상에 피해를 가할 위험이 있는 해저드 및 그 구성요소를 특별히 정하는 해저드 해석을 한다. 또 시스템의 안전성 레벨을 산출하여 평가하는 리스크 해석을 한다.

다음에 이러한 해석 결과를 기본으로 안전성 요구사양을 정리한다. 안전성 요구사양에서는 달성하기 적절한 목표인 안전성 인테그리티 레벨과, 안전성을 유지하기 위해 실현하기 적절한 기능을 명확히 한다.

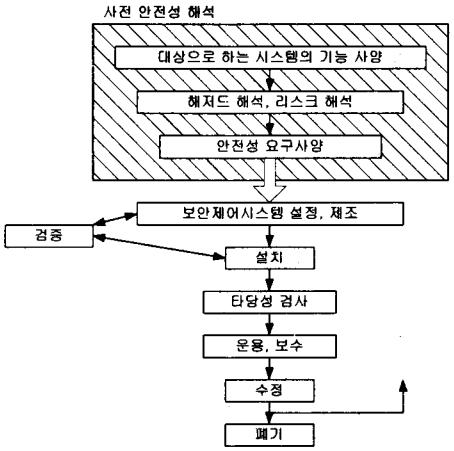


그림 1. 안전성 라이프사이클

## 3. CARAT의 사전 안전성 해석

무선이용 열차제어시스템에서 간격제어 기능의 구현을 위해서는 안전논리 구성을 명확히 하기 위해 2장에서 기술한 사전 안전성 해석을 참고로 하여 체계적인 순서를 정하여 해석을 하여야 한다.

일반적으로 안전성 인테그리티 레벨은 위험한 사건이 발생하는 빈도와 그 영향도로부터 결정하는 리스크를 이용하여 정한다. 무선을 이용한 열차제어시스템은 높은 안전성 레벨이 요구됨과 동시에 사건의 발생빈도에 관하여 정량적인 데이터가 필요하나 그 데이터가 충분하지 않으므로 정량적인 리스크 해석은 어렵다. 이에 따라 해저드를 추출하여 특별히 선정된 해저드에 대하여 안전성 대책을 완전히 구축하기 위한 해석을 하게 된다.

다음은 이에 따른 해석 순서를 표시한 것이다.

(1) 해저드 추출
시스템 구성을 명확히 하여 사고가 진전할 가능성이 있는 해저드를 완전히 추출한다.

(2) 해저드를 선정

정성적인 해석에 의해서 사고로 진전할 가능성이 있는 해저드를 선정한다.

(3) 안전성 논리 구성의 명확화

선정된 해저드에 대하여 고려할 대책을 기록한다. 또, 해저드가 발생한 경우에 있어서 안전 측 동작을 명확히 정의하는 안전성 대책을 생각할 수 있다. 세부 사항으로 평상시 운전 중의 기기의 고장, 제어계 불량, 시스템의 동작상태, 고장 발생시의 복구방법 등이 있다.

### 3.1 시스템의 구성

무선을 이용한 열차제어시스템은 그림 2와 같이 간격제어부와 포인트 제어부로 나눌 수 있다.

#### 3.1.1 간격 제어

차상에서의 위치검지는 속도발전기 등을 이용하여 열차의 위치정보를 산출하고 지상에 무선으로 전송한다. 지상국에서 열차의 추적은 관할 내 전체 열차위치를 관리함과 동시에 각 열차에 대하여 주행이 허용되는 위치(주행허가위치)를 산출하고, 차상에 전송한다. 조종제어계에서는 주행허가 위치를 초과하지 않도록 연속적으로 보안속도 패턴을 설정하고, 열차속도가 패턴을 초과하면 비상 브레이크를 걸게 된다.

#### 3.1.2 포인트 제어

포인트 제어계는 기존의 연동장치에 해당하는 부분으로 가상 블록 개념을 도입하여 선로전환기를 포함한 블록과 일반 블록으로 나누어 이동폐색을 실현할 수 있다. 진로요구는 진로제어계 또는 표시제어반에서 열차번호를 부가하고, 주행로 요구를 하고, 포인트 제어계는 주행로 탐색을 한다. 탐색은 지장 주행로와 경합하는 블록 체크, 요구된 주행로 내의 선로전환기를 포함한 블록 및 일반 블록의 쇄정처리를 실행하고, 추적제어계에 대하여 열차번호를 부가하여 블록 진입허가를 출력한다. 주행로의 해정은 추적제어계로부터 블록해방에 의해 수행된다.

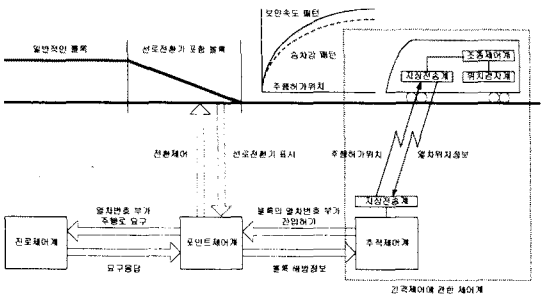


그림 2. 무선이용 열차제어 시스템의 구성

### 3.2 해저드의 해석

시스템에서 해저드를 추출하고 사고로 진전할 해저드에 대하여 그 구성요소를 선정한다. 해저드 해석에 있어서 각 장치의 기능 레벨로부터 bottom-up으로 해저드를 추출하고, FT(Fault Tree)해석에 의해 시스템 전체를 관점으로 한 top-down 방식의 해저드를 선정한다.

#### 3.2.1 해저드 추출

시스템에서 허용할 수 없는 해저드를 전부 추출한다. 이 추출에서는 기존 열차제어시스템에 대한 해저드에 더하여 무선을 이용한 열차제어시스템 특유의 해저드를 고려할 필요가 있다. 해저드 간에는 계층관계가 있기 때문에 이상사건과 원인사건으로 분류하여 정리할 수 있다.

(1) 간격제어에서의 해저드

이동폐색에 의한 간격제어에서는 주행허가 위치를 초과하지 않도록 제어하고 있다. 주행허가 위치는 선행열차의 위치검지계에서 산출된 열차위치에 따라, 추적제어계에서 갱신한다. 조종제어계에서는 주행허가 위치를 시점으로 연속적인 속도제한인 보안속도 패턴을 설정하고 속도 조사를 자신의 열차의 위치검지계에서 산출한 위치를 기본으로 하여 행한다. 따라서 열차속도가 보안속도 패턴을 초과하는 경우에는 충돌하게 된다. 표 1에 보안속도 패턴에 관한 해저드 추출 예를 나타내었다. 이상사건으로는 주행허가 위치 불량, 보안속도 패턴 설정 오류, 보안속도 패턴 초과 인식 불량 등을 생각할 수 있고 각각에 대하여 다음의 원인사건을 생각할 수 있다.

표 1. 해저드 추출 예

| 보안속도 패턴에 관한 해저드 | |
|---|---|
| 이상 사건 | 원인 사건 |
| 주행허가위치 불량 | .선행열차 추적불량<br>- 선행열차의 위치송신 불량<br>- 선행열차의 추적제어계 불량<br>- 전송불량 |
| 보안속도 패턴 설정 오류 | . 차상데이터의 잘못된 등록<br>. 임계속도 설정 불량 |
| 보안속도 패턴 초과 인식 불량 | . 자기 열차 위치 검지 오류<br>- 활주에 의한 차상 계산 오류<br>- 속도발전기의 단선<br>- 설비개선시의 버전 업 불량 |

(2) 연동기능에서의 해저드

간격제어계에서 주행허가 위치를 초과하지 않도록 제어가 행해지기 때문에 포인트제어계에서는 열차과주 개념은 생각하지 않아도 된다. 또한 종래의 연동장치에서의 과주 여유거리에 관한 신호기간 또는 신호기와 선로전환기간의 연쇄 등도 고려하지 않아도 된다. 기존의 접근쇄정과는 달리 열차의 정지 가능위치에 따라 블록 쇄정 또는 무시소해정을 하게 된다. 따라서 이동폐색에서의 간격제어를 염두에 둔 기능 및 새로운 기능에 불량이 발생한 경우에는 열차통과 중에 선로전환기 전환 등의 사고가 발생할 수 있다. 이상 사건으로는 블록 해정 불량과 쇄정불량 등을 생각할 수 있고, 원인사건으로는 열차추적 불량 등을 생각할 수 있다.

#### 3.2.2 해저드의 선정

사고로 진전할 해저드를 기능 레벨별로 선정하기 위해서 충돌·탈선 사고에 대하여 FT 해석을 할 수 있다. 예를 들어 열차가 주행허가 위치를 과주하여 충돌하는 사건을 살펴보면, 열차 주행 중에 활주·공전에 기인하는 위치검지 불량으로 추적제어계에서 열차추적 불량이 발생한다면 이러한 잘못된 열차 위치를 근거로 후속열차의 주행허가 위치가 설정되고, 후속열차가 속도조사 및 패턴을 초과하여 운행할 경우, 브레이크 제어가 정상적으로 기능을 하여도 선행열차에 충돌하게 된다.

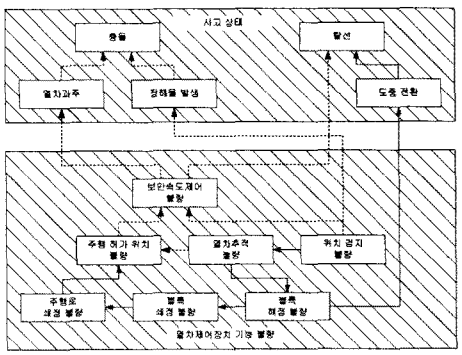


그림 3. 기능불량의 영향과 사고형태

이러한 FT해석 결과를 기본으로 각 기능에 불량이 발생한 경우에 시스템 전체로의 파급하는 영향 및 사고 형태를 그림 3에 표시하였다. 그림 3은 위치검지 기능에 불량이 발생한 경우에 있어서 기능불량이 전파하는 과정을 표시한 것이다. 실선으로 표시한 것처럼 포인트 제어계에서는 열차추적 불량이 전달되어 블록의 해정 및 쇄정이 불량하게 된다. 그 결과 추적제어계에서 주행로로의 진입허가 요청을 전송하게 되고 주행허가 위치의 설정불량이 발생한다. 열차추적 불량은 블록 해정 불량으로 파급되어, 열차통과 중에 선로전환기를 전환하는 사고가 발생할 수 있다.

### 3.3 안전논리 구성의 명확화

해저드 해석으로 선정한 해저드에 대하여 안전측 동작을 정의하며, 이 정의에 따라 각 제어계에 리스크 저감에 필요한 안전성 대책을 안전유지 요건으로 작성한다.

#### 3.3.1 안전측 동작의 정의

시스템에서 안전측 동작의 정의를 표 2에 표시하였다.

표 2. 해저드에 대한 안전측 동작의 정의

| 해저드 | 간격제어에 관한 제어계 | | 포인트 제어계 | |
|---|---|---|---|---|
| | 발생 사건 | 안전측 동작 | 발생 사건 | 안전측 동작 |
| 위치검지 불량 | 좌동 | . 비상 브레이크<br>. 정지여유거리를 설정 | | |
| 차상지상간의 전송 단절 | 좌동 | 주행허가 위치, 열차추적 불량과 같음 | | |
| 추적제어계간 교신 차단 | 좌동 | . 이상추적제어계 관할 내에 주행허가 위치를 설정하지 않는다.<br>. 주행허가 위치를 되돌리고, 보안속도 패턴 초과에 비상 브레이크를 건다. | | |
| 보안속도 패턴 초과 | 좌동 | 위치검지 불량과 같음 | 미허가 블록 잘못된 선로 진입 | . 간격제어의 안전성<br>. 미허가 블록 선로정유에서 블록 및 선로전환기 쇄정 |
| 정지가능 위치 초과 | 좌동 | | | |
| 주행허가 위치 불량 | 좌동 | | | |
| 열차추적 불량 | 좌동 | 후속열차를 방호 | | |
| 블록 해방 불량 | 좌동 | | 블록 해정 불량 | 이상 블록 쇄정 |
| 주행로 쇄정 불량 | | | 주행로 쇄정 불량 | 이상 주행로 쇄정 |
| 선로전환기 제어 불량 | | | 선로전환기 제어 불량 | . 고장선로전환기를 고장모드 등록<br>. 이상 선로전환기 블록 진입 불허가 |
| 진로 요구 불량 | | | 실제로 존재하지 않는 주행로 요구 | 블록 쇄정 해정 처리를 하지 않는다. |

본 시스템에서의 안전측은 간격제어에 대하여는 열차의 정지, 또 포인트 제어계에서는 블록 및 선로전환기의 쇄정을 생각할 수 있다. 안전측 동작은 해저드에 기인하는 리스크를 충분히 저감할 수 있는 경우와 양 제어계의 안전측 동작을 필요로 하는 경우로 나누어 생각할 수 있다. 양 제어계의 안전측 동작을 필요로 하는 해저드로서는 역 구내에서 열차가 보안속도 패턴을 초과하는 경우, 해당 열차를 정지하면서 다른 열차와의 접촉 및 충돌을 막기 위하여 모진한 블록 및 블록 내 선로전환기의 쇄정이 필요하다.

또 각 제어계에서 간격 제어에 관한 제어계와 포인트 제어계로 분류하여 정의하여 두고, 간격제어에 관한 제어계가 정지한 경우에는 포인트 제어계에서 선로전환기를 쇄정하고, 포인트 제어계가 정지한 경우에는 간격제어에서 안전성을 확보한다.

#### 3.3.2 안전성 유지 요건

안전측 동작 정의를 기반으로 각 제어계의 안전성 유지요건을 작성한다. 안전성 유지 요건은 해저드 검지 수단과 그 대책으로 되어 있는데 대책 후의 리스크는 가능한 한 안전성 대책을 전부 고려하여 허용 레벨까지 충분하게 저감할 수 있도록 한다. 해저드는 자기 제어계 내에서 발생하는 사건과 자기 제어계와 인터페이스를 가지는 장치로부터 전파하는 사건으로 분류 가능하고 각 제어계 내에서 발생하는 해저드와 다른 제어계로부터 전파하는 해저드를 고려한 안전성 대책이 필요하다.

조종제어계의 안전성 유지요건을 표 3에 표시하였다. 조종 제어계와 인터페이스를 가지는 장치로는 위치 검지계, 추적제어계, 전송 등이 있고 각각으로부터 해저드가 전파한다.

표 3. 조종제어계 안전성 유지 요건

| 해저드 | | 검지 | 대책 |
|---|---|---|---|
| 조종제어계 | 처리부의 고장 | fail-safe CPU 구성에 의한 교신변호 신호에서 이상을 검출 | 출력 차단 |
| | 차상데이터 불량 | . 출하전 검사<br>. 지상데이터 변경시의 검사 | . 버전관리 시스템<br>. 자동열차검이 검지설비 |
| | | 동일계 내의 ROM 고장에 의한 버스 비교로 검출 | 출력차단 |
| | 전원고장 | 전압 저하의 체크 | 출력차단 |
| 조종제어계와의 I/F 장치 | 위치검지계의 불량 | . 오류체크코드, 송신통화번호체크, 합리성 체크<br>. 이상전문 | 데이터 이상을 검지하면 해당 데이터를 자름 |
| | | . 위치검지계로부터 데이터가 전송되지 않음(송신통화번호가 일정시간 무변화)<br>. 위치불확정 상태 | 비상 브레이크 |
| | 추적제어계의 불량 | . 송신통화번호 체크<br>. 교신단절 | . 주행허가 위치를 갱신하지 않음<br>. 비상 브레이크 |
| | 전송불량 | 교신단절, 합리성 검사 | 상동 |

예를 들어 위치검지계로부터 전달되는 해저드에 대하여는 활주·공전시의 안전측 위치보정과 지상자에 의한 위치보정 등은 위치검지계에 있어서 행하여지는 것으로 장치 고장 및 초기 위치 미설정 등의 해저드에 대하여는 위치검지계 단독으로 대처할 수 없는 것처럼 되어 있다. 그래서 이러한 위치검지계로부터 전파하는 해저드의 대책으로 수신한 데이터의 체크를 하고, 이상을 검지하면 해당 데이터를 파기하여 일정시간 데이터가 갱신하지 않으면 비상 브레이크가 걸린다. 또 전송 이상에 의한 주행허가 위치의 불량에 대하여는 이상을 검지하면 주행허가 위치를 갱신하지 않는 것으로 선행열차와의 충돌을 방지한다.

## 4. 결론

무선을 이용한 열차제어시스템에서 사전 안전성 해석을 적용하여, 충돌 및 탈선 사고에 있어서 고려해야하는 해저드를 선정하고, 시스템 내에서의 해저드 전파를 명확히 함과 함께 필요한 안전 논리구성을 표시하였다. 안전논리구성은 시스템 전체의 안전측 동작을 정의하여, 이 정의를 만족하는 각 제어계의 안전성 대책으로 표현되어 있다. 이러한 안전성 대책으로 열차제어시스템의 기능에 대하여 안전성 확인이 가능할 것으로 사료된다. 앞으로 발생 가능한 사건에 대한 전반적인 안전성 해석을 거쳐 전체 시스템의 안전성을 높이는 연구가 필요할 것이다.

### 〔참 고 문 헌〕


〔1〕 西堀典幸 他, "CARATの實制御試驗", 鐵道におけるサイバネティクス利用國內シンポジウム論文集, 1996.11

〔2〕 中村英夫 他, "CARAT用次世代連動裝置の開發", 鐵道におけるサイバネティクス利用國內シンポジウム論文集, 1993.11

〔3〕 山本春生 他, "CARATによるインテリジェントな速度制御の現車試驗", 鐵道總研報告, 1996.11

〔4〕 財團法人, 鐵道總合技術研究所, "列車保安制御システムの安全性技術指針, 1996.3

〔5〕 平尾裕司 他, "列車保安制御システムの安全性技術指針", 鐵道總研報告, 1996.11