論 文
55B-12-11

전자연동장치의 안전성 활동에 관한 연구(Ⅰ)

A Study On Hazards Identification Of Programmable Electronic Interlocking System For Safety Activity

朴 在 煐† · 李 鐘 宇*
(Park Jaeyoung · Lee Jongwoo)

Abstract - Interlocking signalling system plays key role as core system to manage railway operation. The core role of railway operation is to control routing, displaying signal and regulation for train. Interlocking system relate tightly to railway accident because collision and derailment is sometime taken place from wrong route setting and signal displaying. Safety activity for interlocking system is inevitable to avoid the accident over its life cycle. The safety activity includes hazard identification and analysis, safety requirement allocation, safety plan, safety activity and so on. The safety activity need a broad wide range work. In this paper, we concentrate on hazard identification for generic interlocking system and programmable electronic interlocking system and compare between two results. The hazards will be used for safety activity.

Key Words : 'PES Interlocking System', 'Train Control System', 'Safety', 'Hazard', 'HAZOP'

1. 서 론

연동장치는 역을 관리하는 신호시스템으로서 고유기능인 진로제어를 포함하여, CTC장치와의 인터페이스, 폐색장치와의 인터페이스를 하여, 로컬제어장치로서 기능이 확대되어 가고 있다. 연동장치가 프로그램이 가능한 전자 시스템으로 구현되면서 다양한 기능을 수행할 수 있어 철도제어시스템의 코어시스템이 되어가고 있으며, 역을 중심으로 하여 열차운용을 총괄적으로 제어를 하고 있다.

연동장치의 기능은 운전정리와 같이 운용효율을 높이는 기능과 진로제어, 열차속도제어, 건널목제어 등 안전성과 직접적인 관련이 있는 기능이 있다. 연동장치의 안전기능과 관련되어 발생되는 주요사고는 충돌, 탈선 등이 있고, 사고결과는 사망, 부상 및 시설물파손 등이 발생하고 있다[1]. 역에서는 연동장치에 의존하여, 열차의 진로, 입환, 폐색관리 등을 수행하고 있기 때문에 연동장치의 안전성 및 신뢰성이 매우 높게 요구되고 있다. 진로제어, 열차속도제어 및 건널목제어 등과 같은 Safety critical 기능은안전과 직접적인 관련이 있어, 이 기능들에 대해서 시스템 수명주기 전반에 걸쳐서 안전성확보 및 검증이 필요하다[3][4][7].

연동장치는 기계식, 전기식 및 전자식으로 구현되고 있다. 현재는 전기식 연동장치를 많이 사용하고 있으며, 점차 전자식 연동장치로 천이되어 가고 있는 도중이다[2].

기계식은 진로를 설정할 때에 정자를 이용하여 기계적으로 상호 쇄정이 되도록 하고 있다. 기계식은 일부구간에서 사용하고 있지만 거의 퇴역 단계에 있다.

전기식 연동장치는 계전기의 On-off를 이용하여 진로와 신호제어에 관련된 연동로직을 구성하고 있다[5]. 계전연동장치로 구성된 연동장치의 안전성은 계전기로 구성된 제어회로의 논리의 완벽성을 검증하는 것으로 연동검사를 통하여 이루어진다[8]. 이 연동검사는 연동장치가 설치되는 역의 진로구성을 한 연동도표를 이용하여 계전기 논리회로를 검사하는 것이다. 계전기를 이용한 연동장치는 계전기의 특성을 이용하여 안전성을 확보한다. 계전기의 고장발생은 한쪽으로 발생하도록 하여, 고장이 발생하면 안전 측으로 작동하는 방식으로 안전을 확보한다[6].

계전연동장치의 안전성은 상당히 높지만 논리적인 유연성이 상당히 떨어지고, 중후 장대하여 유지보수비가 많이 소요된다. 유연성을 높이기 위해서, Safety critical 한 부분은 계전 연동장치를 사용하고, MMI(Man-Machine Interface) 부분만을 컴퓨터를 이용하는 방법이 개발되었다[6]. 그러나 점진적으로 전기식 장치가 전자화되어가는 추세에서 연동장치의 코어 시스템을 계전연동장치로 유지하는 것을 불가능하게 된다. 이러한 단점을 극복할 수 있는 것이 전자연동장치이다. 전자연동장치는 논리적 유연성이 높아, 특이성이 높은 철도에 적용하기에 적당하다. 그러나 전자연동장치는 핵심요소인 제어기가 컴퓨터로 구성되어 고장이 랜덤하게 발생하는 특성을 가지게 되었으며, 장치의 복잡도가 증가하여 체계적인 안전성확보가 요구되었다[9].

전자연동장치는 컴퓨터화된 제어기를 이용해서 응용소프트웨어를 가동하는 것이기 때문에 고장은 제어기 자체에서 발생할 수 있고, 연동논리를 처리하는 응용 소프트웨어서도 발생할 수 있다. 전자연동장치에서 안전성확보는 기존의 방법과 다르게 활동을 하여야 한다.

† 교신저자, 正會員 : 서울産業大學 鐵道專門大學院 鐵道電氣信號工學科博士課程
E-mail : pjy7717@paran.com
* 正 會 員 : 서울産業大學 鐵道專門大學院 鐵道電氣信號工學科工學博士
接受日字 : 2006年 10月 25日
最終完了 : 2006年 11月 8日

본 논문에서는 안전성활동의 일부인 전자연동장치의 위험원(Hazard) 도출을 시도하였다. 전자연동장치의 안전성확보를 위해서 먼저 일반적인(Generic) 연동장치에 관련된 위험원을 도출하고 리스크를 분석하였으며, 전자연동장치의 위험원과 그와 관련된 사고를 도출하고 리스크를 분석하였다.

2. 연동장치

2.1 연동장치의 기능

연동장치의 기능은 Vital과 Non-vital 기능으로 분류할 수 있다. 아래 그림에서 실선으로 표시된 부분이 연동장치에 Vital에 해당된다. 연동장치의 동작주기는 현장기기의 정보획득, 제어정보생성, 제어정보의 현장기기 전송, 상태정보 획득 및 현시하는 것을 한 주기로 한다. 연동장치에 대한 요구사양에 따라 기능을 다양화 할 수 있지만, 안전성 분석에는 Vital 기능인 진로제어 및 신호기 제어 기능을 한정 지을 수 있다.

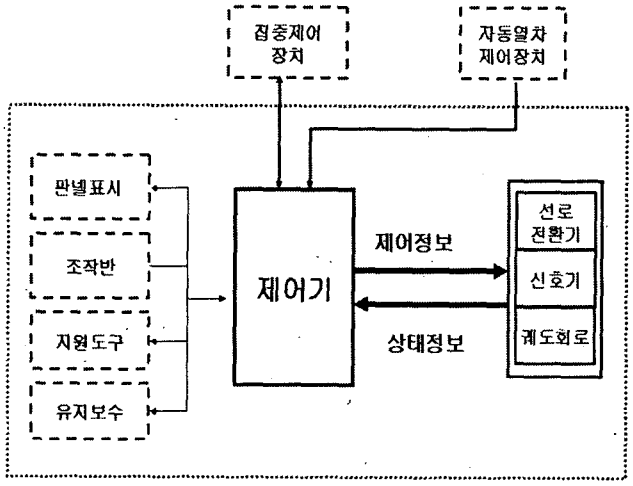


그림 1 연동장치의 구조

Fig 1 Structure of Interlocking System

2.2 연동장치의 장애 및 사고 분석

연동장치와 관련된 사고는 선로전환기의 도중전환, 연동장치 취급 시 및 신호기 등에 의한 사고가 발생을 한다. 사고는 탈선, 추돌이 발생하고, 사고의 결과는 사망, 부상, 시설물파손 등이다. 연동장치의 고장, 오작동 등은 심각한 사고를 발생시킬 수 있다[1]. 표 1로부터 철도사고 분석결과는 연동장치와 관련된 선로전환기 도중전환과 관련이 많다. 연동장치의 이상은 바로 사고로 이어질 수 있는 것을 알 수 있다.

발생된 사고를 분석하면 사고의 빈도가 운용 시마다 발생할 수 있고, 사고의 정도가 Catastrophic이므로 연동장치는 SIL 4를 만족해야하는 장치임을 알 수 있다[2][10].

연동장치의 오작동은 사고와 직접적인 관련이 있기 때문에 연동장치의 안전성을 확보하기 위해서는 안전성활동이 필요하다[2][3][10].

표 1 철도에서 연동장치관련 사고현황

Table 1 Accidents Related to Interlocking System in Railway

발생일	과도상태	사고	피해정도	비고
77.1.30	선로전환기 도중전환	탈선	부상 2명	여객열차
85.3.26	선로전환기 도중전환	탈선	열차 및 시설파손	
87.2.5	선로전환기	탈선	열차 및 시설파손	
89.5.4	선로전환기 도중전환	탈선	탈선	이선진입
89.7.4	선로전환기불량	탈선	기물파손	여객열차
90.1.28	선로전환기 도중전환	탈선	사망 2명 부상 50명	여객열차
90.6.21	착오현시, 진로설정	추돌	사망 4명 부상 21명 열차 및 시설파손	여객열차 및 화물열차
94.4.22	신호현시 오류	추돌	부상 9명	여객 및 단기차량
96.2.21	선로전환기 고장	탈선	경상 21명 열차 및 기물파손	여객열차
98.8.29	선로전환기 도중전환	탈선	부상 및 열차파손	화물
98.11.15	선로전환기 고장	탈선	열차파손	화물
98.12.28	연동장치 장애	탈선	열차파손	여객
99.3.23	수신호취급	탈선	열차파손	수신호
01.11.18	선로전환기 도중전환	탈선	열차파손	전동차

3. 연동장치 사고와 기능

3.1 연동장치의 Vital기능

연동장치의 Vital기능은 진로기능과 신호기능이다. 진로기능은 진로의설정과 선로전환기의 단독전환이다. 신호기능은 열차의 속도를 제어하는 기능이다. 진로가 설정되면 신호기가 통과신호를 현시하고, 설정이 되지 않으면 신호기는 정지신호를 현시하도록 되어있다.

3.2 신호기 현시오류 사고

신호기 현시 오류에 의한 사고는 크게 두 가지로 나눌 수 있다. 진로가 생성되지 않은 진로에 통과신호가 현시되는 경우와 제한 속도이상으로 속도를 현시하는 경우가 있다.

진로가 설정되지 않고 통과신호가 현시되는 경우에는 진로의 중복설정, 선로전환기와의 불일치 등이 있을 수 있다. 이러한 경우에 열차가 진입하면 열차와의 충·추돌 혹은 탈선 사고가 발생할 수 있다.

진로가 측선진로로 설정되어 있는 경우에는 진로에 진입하는 열차의 속도를 제한하여야 한다. 측선진로는 곡선 형태이기 때문에 속도를 제한하지 않을 경우에는 탈선 등의 사고가 발생할 수 있다.

신호기의 현시오류에 의해 충·추돌, 탈선 등의 사고가

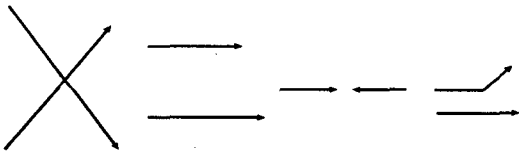
발생할 수 있다. 신호현시 오류는 진로설정이 안된 곳에 통과신호를 현시됨으로서 열차와 충·추돌이 발생할 수 있거나, 탈선을 할 수가 있다. 부본선으로 진로가 개통이 되었을 때 감속신호를 현시하지 않고 진행신호를 현시하는 경우는 분기부 곡선부분에서 허용속도이상으로 주행을 하기 때문에 탈선사고가 발생할 수 있다.

3.3 진로경합에 의한 충돌 및 탈선원인

연동장치의 진로는 진입하려는 진로의 신호기부터 다음 신호기까지로 진로가 정의 된다. 진로의 중복은 열차의 충돌을 야기한다. 따라서 연동장치는 진로의 경합을 고려하여, 진로가 중복되지 않도록 한다.

진로의 경합에는 그림 2와 같이 4개의 형태가 있다. 그림 2의 ①은 2개의 진로가 교차하는 경우이며, 교차부분에 분기기가 없다. 그림 2의 ②는 2개의 진로가 공유 선로전환기로 향하는 방향이 전부 일치한다. 예를 들면 같은 지점에 입환신호와 폐색신호가 설치되어 착점 버튼을 공유하는 경우로서, 동일구간에서 통과 형태가 다른 경우로서 각각의 진로로 되어 있다. 그림 2의 ③은 2개의 진로에서, 2개의 진로는 선로전환기를 공유하지 않지만, 착점이 일치하기 때문에, 반대방향이라 한다. 마지막으로 그림 2의 ④는 2개의 진로가 공유하는 선로전환기의 방향이 다른 것을 제외하고는 일치한다.

역구내의 진로경합은 이 4개의 형태 중 하나로 분류된다.



①크로싱진로 ②병행진로 ③대향진로 ④병행진로

그림 2 진로경합의 종류
Fig. 2 Route Concurrence Type

그림 2는 진로의 경합에 대한 것으로 동시의 진로가 생성되는 경우를 나타낸 것이다.

크로싱 진로의 경우에는 열차간 측면 충돌, 병행진로는 추돌, 대향진로는 충돌, 분기병행진로는 탈선이 발생할 수 있다. 이러한 경합진로가 발생하지 않도록 쇄정을 한다

3.4 경합진로의 쇄정(Locking)

연동의 기본은, 진로를 설정할 때에, 그 진로와 경합하는 진로를 설정되지 못하도록 쇄정하는 것이다. 쇄정 방법에는 직접법과 간접법이 있다. 직접법에는 진로를 허용하는 신호기를 쇄정하는 것이고, 간접법에는 진로상의 선로전환기를 쇄정함으로서 간접적으로 조작레버를 해정하는 방법이 있다. 신호기를 쇄정을 하면 진로설정 버튼의 취급이 불가능해진다.

어떤 진로를 설정하기 위해서는 선로전환기를 반위에 전환하여 쇄정해야 하는 경우도 있다. 이러한 경우 선로전환기가 이 정위에 쇄정되어 있으면, 조작레버를 동작시켜도 진로는 쇄정되지 않는다. 이 경우 직접법에 의한 쇄정에는 신호기를 해정하지 않는 한, 경합 진로 설정으로 이행되지 않지만, 간접법에는 대응되는 선로전환기 만이 쇄정되어 있기 때문에 작업능률이 높다. 따라서 진로의 쇄정은 가능한 간접법에 의한 것이 추천되고 있다. 그림 2의 경합진로에 있어서 ①,②,③은 직접법에 의하고, ④는 간접법에 의하는 것을 원칙으로 한다. 그러나 다음에 기술하는 ①의 형태에도 간접법을 적용할 수 있는 경우가 있다.

경합진로는 어떤 진로와 경합하는 진로가 진로 상 궤도 또는 착점을 공유하는 진로를 탐색하는 것에 의해 얻어진다. 이는 3.3에서 기술한 대향진로를 공유하는 것으로서 직접법에 의해서 쇄정한다. 궤도회로를 공유하는 진로의 쇄정에는 진로경합을 2개의 부류로 나누어, 직접법과 간접법을 사용하는 것을 분리할 필요가 있다. 원래 직접법으로 쇄정하도록 고려된 진로 중에도 진로 외에 선로전환기를 사용한다면 간접법으로 쇄정을 하는 경우도 있다[11].

(1) 공유선로전환기가 없는 진로의 쇄정

이것은 3.3절에 기술된 평면교차로에 있어, 직접법으로 쇄정 하는 것을 원칙으로 하지만, 그림 4와 같은 배선형태에는 직접법 보다 간접법으로 쇄정 하는 것이 가능하다. 즉 진로 r_1을 설정할 때마다, 진로 r_2의 진로 상 선로전환기 w_1을 정위에 전환하여 쇄정하여 둔다면 r_2는 w_1에 의해서 간접적으로 쇄정된다. 이러한 예와 같이 공유 선로전환기가 없는 진로의 경우는, 공유궤도회로 내에 쌍동 선로전환기(1번에 선로전환기가 동시에 동작한다.)가 2조가 있는 쇄정부에 절연이 있다면 간접방법으로 이외에는 직접법으로 쇄정한다[12][13].

(2) 공유 선로전환기가 있는 진로

공유하는 선로전환기 중에 있는 진로에 의해 방향이 다른 것이 있다면 간접법으로 하고, 그 외에는 직접법으로 한다.

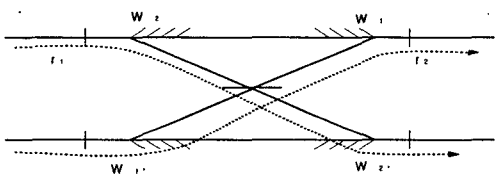


그림 3 직접쇄정과 간접쇄정 방법의 예
Fig. 3 An Example of Direct and Indirect Locking Methods

4. 연동장치의 HAZOP

4.1 연동장치 모델링

연동장치의 Vital 기능은 연동처리장치와 현장기기에 포함되어 있다. 연동처리장치는 선로전환기와 신호기의 제어명령을 결정하는 곳이고, 현장제어장치와 현장기기는 제어명령을 실행한다. 사고의 분석의 결과로는 제어기에서 발생할 수 있는 연동장치장애, 현장기기에서 발생하는 선로전환기의 도중전환, 신호현시잘못 등이 있다.

연동장치의 동작은 일반적으로 다음과 같은 절차에 의해서 수행된다.

① 연동제어기는 관리 범위에 있는 선로의 열차점유정보를 주기적으로 획득을 한다.
② 열차점유점보와 진로요청정보를 근거로 하여 진로를 설정한다.
③ 해당 선로전환기들을 진로의 방향으로 전환을 한다.
④ 제어기는 선로전환기들의 전환을 확인하고, 확인이 되지 않으면 정해진 횟수만큼 ③과 ④의 절차를 반복 시도한다. 전환이 완료되면 다음단계로 진행을 하고, 전환을 성공하지 못하면 고장신호를 보내고, 다음 조치를 수행한다.
⑤ 해당진로의 신호기를 진행신호로 현시시킨다.
⑥ 열차가 진로에 진입하면, 신호기가 정지로 바뀌고 진로가 닫힌다.

위의 시나리오에 따라 각 연동장치의 설계안이 달라질 수는 있지만 대부분은 거의 동일한 형태로 주어진다. 위의 절차 중에서 하나의 단계에서 일탈이 발생하면 사고로 이어질 수 있다. 따라서 각 단계마다 기능이 정확하게 작동이 되도록 하여야 한다.

4.2 연동장치의 HAZOP

연동장치의 모델링을 근거해서, 연동장치의 위험원 도출을 시도하였다. 연동장치의 기능 확대에 따라 발생될 수 있는 위험원도 확대될 수 있으며, 그림 4의 모델을 이용하여 위험원을 도출하였다.

①의 경우에는 설정하려는 진로에 있어서 열차의 존재여부를 판단하는 것으로, 열차위치 정보가 잘못되었을 경우에는 진로설정에 문제가 발생할 수 있으며, 궤도회로의 오류 또는 연동제어기의 점유정보 인식에 고장이 있을 수 있다. 열차가 없는 경우에 열차가 존재하는 것으로 인식한다면 이는 안전에 영향을 미치지 않고, 단지 진로를 설정할 수가 없게 된다. 반면에 열차가 있지만 열차가 없는 것으로 인식을 하면 사고가 발생된 개연성이 매우 높아진다.

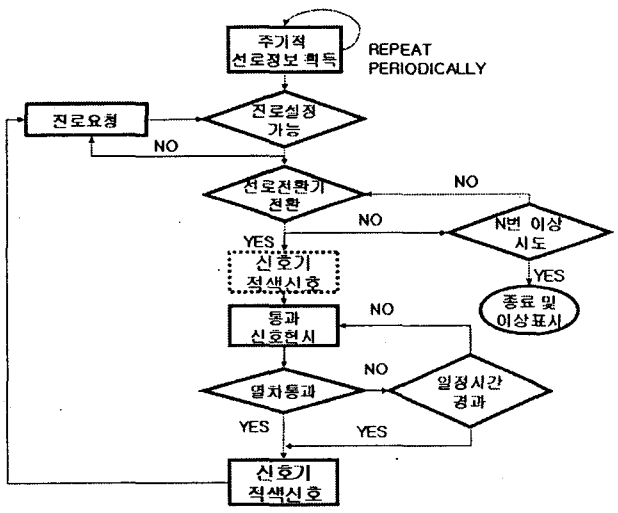


그림 4 연동장치의 진로설정프로세스
Fig. 4 Route Setting Process of Interlocking System

②의 단계서 발생할 수 있는 사고의 경우는 현장정보의 변질에서 기인될 수 있다. 중복된 진로가 설정이 되지 않도록 경합되는 진로에 대한 쇄정을 한다. 쇄정된 정보가 변질되는 경우가 있으며, 이러한 변질된 정보를 근거로 진로를 설정가능성이 있다. 정보오류의 경우에는 현장정보 획득을 정확하게 하였더라도, 내부 프로세스과정에서 현장정보의 변형이 발생할 수 있다. 현장정보의 변질의 경우는 시스템 자체의 고장에서 기인될 수 있거나, 프로세스에 오류가 있을 때 발생을 한다. 이러한 정보의 변형은 열차가 존재하지만 열차가 없다는 것으로 주어지는 정보를 갖고 있거나, 또는 하나의 진로를 다른 진로로 인식을 하는 등 아주 다양한 현상으로 나타날 수 있다. Fail safe한 정보변질은 안전에 영향이 없지만, Fail unsafe의 경우에는 사고로 직결될 수가 있다.

③의 경우에는 선로전환기의 불일치에 의한 사고가 발생할 수 있다. 선로전환기의 불일치에 따른 신호현시는 열차가 진행을 하여 열차가 탈선을 할 우려가 있다. 불일치가 발생하지 않도록 쇄정을 사용한다. 열차가 통과할 때 선로전환기가 도중에 전환을 하면 사고가 발생하기 때문에 선로전환기의 도중전환이 절대로 발생하지 않도록 하여야 한다.

선로전환기가 전환이 되지 않을 때에는 보통 3번 정도 시도를 하여, 노이즈에 의한 동작실패 여부를 확인한다. 여러 번의 시도하는 것은 한번 시도에 의해서 선로전환기가 작동이 안 되어 고장처리를 할 경우에는 진로설정이 불가능하게 되어 운용상 많은 손실을 입게 될 수 있기 때문이다.

④의 경우에는 신호기 현시의 잘못에 의한 사고가 발생할 수 있다. 진로가 설정되지 않은 상태에서 통과신호를 현시할 수 있다. 이러한 경우에는 열차간의 충돌 혹은 탈선이 발생할 수 있다.

표 2 일반연동장치 PHA 를 위한 HAZOP활동
Table 2 HAZOP Activity for Generic Interlocking System PHA

기능	세부기능	Applied Guide words	위험원	결과	사고결과	발생빈도
현장정보획득	열차위치검지	other han	열차위치검지실패	충돌, 추돌	Catastrophic (사망, 부상, 기물파손)	frequent
	신호현시상태	Less of	신호현시상태실패	충돌, 추돌, 탈선		
	선로전환기상태	other than	선로전환기상태검지실패	탈선		
진로설정	진로설정	more than other than	진로설정실수	충돌, 추돌, 탈선		
선로전환기전환	도중전환	more of	도중전환	탈선		
신호기능	잘못현시	less of	잘못현시	충돌, 추돌, 탈선		

앞에서 언급한 사고를 방지하기 위해서 신호기와 선로전환기 상호간에 연동을 시키고, 진로가 설정되었을 때에는 다른 곳에서 경합진로에 진로를 설정하지 못하도록 한다. 연동장치와 관련하여 HAZOP결과는 표 2와 같다.

표 1에서 나타난 사고결과에 의하면 연동장치와 관련된 사고의 발생빈도는 종종 발생을 하며, 사고의 크기는 치명적이며, 사고결과와 발생빈도에 근거하여 리스크를 결정하면은 SIL4에 해당한다.

4.3 전자연동장치의 HAZOP

연동장치의 Vital 기능의 구성은 그림 5와 같다. 연동장치는 선로전환기, 신호기의 상태정보와 궤도회로와 자동열차제어장치로부터 열차위치 정보를 획득한다. 계전연동장치에서는 관련된 정보를 실내 기계실의 계전기로부터 획득을 하였다. 각 신호기기는 기기실까지 제어선이 연결되어 있으며, 모든 정보는 계전기의 접점으로부터 획득을 한다.

전자연동장치의 경우에는 모든 정보를 광케이블과 같은 통신을 이용하여 제어를 한다. 연동처리장치부터 현장기기까지의 제어정보와 현장기기에서 제어기까지의 상태정보는 Vital 정보이다. 이러한 정보가 왜곡이 발생하는 경우에는 사고가 발생할 수 있다.

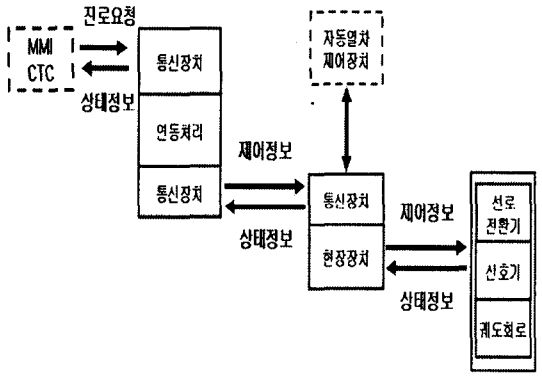


그림 5 전자연동장치의 Vital 기능
Fig. 5 Vital Function of PES Interlocking System

각 서브시스템이 사고에 대해서 어떠한 기인을 하는 가를 밝혀내기 위해서 HAZOP활동을 하였다. 그림 5는 전자연동장치의 Vital 기능을 모델링한 것이다. 앞 절에 밝혀내 위험원에 대해서 전자 연동장치에 적용을 하였다. 전자연동장치의 작동 프로세스는 다음과 같다.

① 제어기는 현장기기의 상태정보를 수집, 처리하여 진로설정 및 신호기를 제어한다. 신호기기의 상태정보 및 진로설정 정보에 대한 변질이 발생하면, 제어가 발산을 하므로 연동장치와 관련된 사고가 발생할 수 있다. 제어기의 정보변질은 정보의 송·수신, 내부프로세스 및 제어기 자체고장 등에 의해서 발생될 수 있다.

② 현장장치는 신호기, 선로전환기로 부터 상태정보를 획득하고, 궤도회로로부터 열차위치정보를 획득하여 상태정보 및 열차위치정보를 제어기로 송신하고, 제어기로부터 제어정보를 수신하여 신호기 및 선로전환기를 작동시킨다. 현장장치의 제어정보나 상태정보가 변질되면 연동장치와 관련되어 사고가 발생할 수 있다. 현장장치의 정보변질은 정보의 송·수신, 내부프로세스 오류 및 현장장치의 고장에서 발생될 수 있다.

③ 신호기는 열차의 통과여부를 결정하고, 선로전환기는 열차의 진로를 결정하고, 궤도회로는 열차위치 정보를 제공한다. 신호현시 오류는 열차의 충·추돌을 유발하며, 및 선로전환기 상태정보가 제어가 되지 않을 경우에는 현장장치는 상태정보를 제어기에 전송하여 고장처리를 하고 진로를 폐쇄한다. 궤도회로의 고장, 신호기 및 선로전환기의 불일치는 사고를 발생시킬 수 있다. 궤도회로의 열차검지 실패, 선로전환기의 도중전환, 신호기 현시 오류는 사고를 발생시킬 수 있다.

표 3 전자연동장치의 HAZOP 활동
Table 3 HAZOP Activity for PES Interlocking System

기능		세부기능	Applied Guide word	위험원	결과	사고결과	발생빈도
제어기		정보 송수신	None of More of Less of Part of More than Other than	정보 송수신 에러	충돌, 추돌	Catas-trophic (사망, 부상, 기물 파손)	fre-quent
		프로세싱		프로세싱 고장			
		제어기		제어기 고장			
현장장치		정보 송수신	None of More of Less of Part of More than Other than	정보 송수신 에러	충돌, 추돌, 탈선		
		프로세싱		프로세싱 고장			
		제어기		제어기 고장			
현장기기	신호기	현시	Less of	현시오류	충돌, 추돌, 탈선		
	선로전환기	상태	None	상태오류	탈선		
		전환	Other than	도중전환	탈선		
	궤도회로	열차위치	Other than	열차위치 오류	충돌, 추돌		

4.4 전자연동장치의 안전성 요구조건

전자연동장치는 그림 5에서 명시한 것처럼 3개 부분으로 분리할 수 있다. 각 부분에서 발생되는 사고는 표 3에서 나타내었다. 전자연동장치의 위험측 및 안전측의 상태도를 나타내면 그림 6과 같이 된다.

그림 6에서와 같이 하나의 서브시스템에 위험측 고장이 발생하였을 경우에는 시스템이 위험 측 동작을 하게 된다. 따라서 전자연동장치 각 서브시스템의 위험 측 고장은 SIL4(고장률 $< 10^{-10}/h$)의 요구사양을 만족해야 한다[표 4].

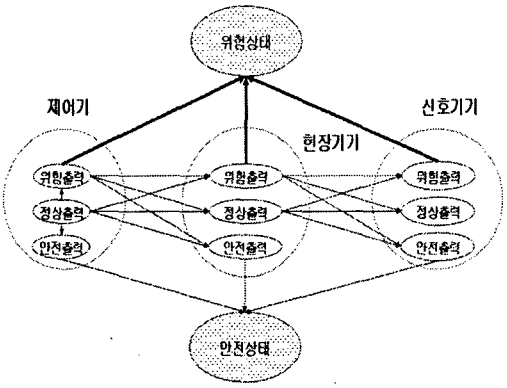


그림 6 전자연동장치의 출력상태도
Fig. 6 State Diagram of Outputs of Solid State Interlocking

표 4 전자연동장치 안전요구사양
Table 4 Safety Requirement for PES Interlocking System

기능	안전요구 사양	위험측 출력 고장률	결과
제어기	SIL4	$< 10^{-10}/h$	충돌, 추돌
현장장치	SIL4	$< 10^{-10}/h$	충돌, 추돌, 탈선
신호기	SIL4	$< 10^{-10}/h$	충돌, 추돌, 탈선
선로 전환기	SIL4	$< 10^{-10}/h$	탈선
			탈선
궤도회로	SIL4	$< 10^{-10}/h$	충돌, 추돌

전자연동장치 Safety critical 서브시스템의 위험 측 고장률(λ_i)이면, 시스템의 위험측 고장률(λ_{fu})은 그림 6을 참조하여 다음과 같이 정의할 수 있다.

$$\lambda_{fu} = \sum_i \lambda_i$$

위험 측 고장률은 SIL 4보다 작아야 한다.

$$\lambda_{fu} = \sum_i \lambda_i \leq 10^{-10}/h$$

5. 결 론

연동장치는 철도운용에 있어서 핵심적인 시스템이며, 장치의 고장이 열차충돌 및 탈선의 원인이 되는 위험원을 발생시킬 수 있으므로 안전성과 직접적 관련이 있다. 시스템의 안전성을 보장하기 위해서는 안전성활동 통해 도출된 위험원의 위험도가 허용할 수 있는 수준으로 제어되었음을 입증해야 한다. 본 논문에서는 연동장치를 구성하는 시스템과 상관없이 연동장치에 관련된 위험원을 도출하였으며, 그 위험원을 전자연동장치에 적용하여 보았다. 전자연동장치의 경우에는 각 서브시스템 별로 위험원이 존재하고 안전에 직접적인 영향을 미치는 것을 확인하였다. 따라서 전자연동장치의 경우에는 서브시스템 별로 안전성 활동을 해야 한다. 향후과제로서는 각 서브시스템별로 안전성활동을 하여, 서브시스템에 포함되는 위험원을 완화시키기 위한 대책에 대한 연구를 필요로 한다. 또한 안전성과 운용효율 간에 정비례관계가 성립되지 않으므로, 최적의 안전성 및 운용효율을 위한 안전성 목표 수립 및 설계의 Trade-off가 중요하다.

참 고 문 헌

[1] 철도청 "신호업무자료", 행정간행물 등록번호 11-1510000-000006-10, 182~185 쪽, 2002
[2] 철도청 "신호업무자료", 행정간행물 등록번호 11-1510000-00058-10, 363 쪽, 2005
[3] IEC, International Standard, IEC 62278, 2002
[4] CENELEC, European Norm, EN50126, 128, 129, 1999
[5] Railtrack, Engineering Safety Management, Issue 3, 2002
[6] 吉村 寬 et al, 信號, 交友社, 1991
[7] 財團法人 鐵道總合硏究所, 列車保安制御ソステムの安全性技術指針, 1996
[8] 한국철도공사, 연동검사기준요령
[9] Richard E. Harper et al, "Fault-Tolerant Parallel Processor", Journal of Guidance, Vol 14, N0.3, pp. 554-563
[10] 이종우 et al, "컴퓨터기반 철도신호제어시스템의 안전성 확보에 관한연구", 대한전기학회 논문지, 53B-11-1, pp. 641-646, 2004
[11] 八賀 明, "連動表を檢證するためのがアルゴリズ", RTRI Report Vol. 10, No11,pp 11-16, '96.11
[12] Akida et al. 연동도표작성용 지적CAD(1), (2) RTRI, REPORT vol4, no. 2,pp31-36 90'2
[13] 吉武 勇 et al. "運轉保安設備の解說", 日本鐵道圖書株式會社, 1984

저 자 소 개

박 재 영 (朴 在 煐)
1951년 4월 8일생. 1989년 서울산업대학교 전기공학과 졸업, 1996년 고려대학교 산업대학원 석사, 2005년~현재 한국철도공사 오송전기사무소장
Tel : 02-3149-2120
E-mail : pjy7717@paran.com

이 종 우 (李 鐘 宇)
1959년 3월 20일생. 1983년 한양대학교 공과대학 기계설계과 졸업, 1986년 Ecole Centrale de Nantes 석사, 1993년 University de Paris VI 공학박사, 2005년~현재 서울산업대학교 철도전문대학원 철도전기 신호공학과 교수
Tel : 02-970-6874
Fax : 02-978-6874
E-mail : saganlee@snut.ac.kr