2002년도 대한전기학회 하계학술대회 논문집 2002.7.10-12

철도신호의 Fail Safe/Fault Tolerant 시스템에 대한 검증방법에 대한 연구

이종우, 정의진, 황종규, 신덕호
한국철도기술연구원 철도신호통신연구팀 경기도 의왕시 월암동 374-1

A Study On Verification Methodology On Railway Signalling System related to Fail Safe/ Fault Tolerant

LEE Jongwoo, JOUNG Euijin, HWANG Jonggyu, SHIN Duckho
Korea Railroad Research Institute, 374-1 Weolamdong Euiwangsi Kyungkido S. Korea

Abstract - *Railway signalling system always is required high safety and reliability. The failure of the train control system can provoke a serious accident. In this paper, we show how to achieve the safety and reliability by dividing signalling system into vital and non functions, studying operational environment.*

1. 서 론

철도신호보안시스템은 속도제어 및 진로제어 기능으로 구성되어있다. 속도제어의 방법은 지상장치에서 선행열차의 위치와 열차속도에 영향을 미치는 인자들을 검지하여 열차 안전속도를 연산하여 열차의 속도를 결정하도록 한다. 열차의 진로제어는 2개 이상의 열차가 동일한 진로에 진입하지 않도록 하여, 열차의 충·추돌을 방지하도록 한다.

신호보안시스템의 안전성과 신뢰성을 확보하기 위해서는 열차운용을 어떻게 할 것인가(Mission Scenario)와 신호시스템의 운용환경(Operational Environment)은 어떠한가를 먼저 규명하여야 한다. 신호시스템의 운용방안은 열차의 운용방안과 직결된다. 그림 1은 열차와 신호시스템 간의 운용시나리오를 나타내고 있다.

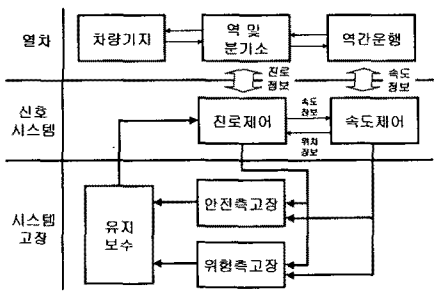

그림 1. 열차와 신호시스템과의 관계

열차속도제어는 다음과 같은 요구사항을 만족시켜야 하며

- 열차의 제어속도 : 200km/h, 열차의 최대 제동능력 : 0.7m/s
- 200km/h의 속도(간격)제어
- 충분한 제동거리와 overlap 확보
- 열차운행 영향을 주는 환경사항 검토
- 차상장치에 주행속도의 현시
- 열차의 위치검지

진로제어의 운용은 다음과 같은 요구사양을 만족하여야 한다.

- 최대 진로 제어 수 : 500 진로제어가능
- 주어진 시간 내에 동일 진로에 2개 열차의 진입 금지
- 제어되지 않은 진로의 열차 진입금지

신호시스템의 운용환경은 간략하게 표시를 하면 다음과 같은 환경요구사양을 만족하여야 한다.

- 온도 -40 ~ 70℃
- 진동 2G
- 상대습도 90%
- EMI

신호 시스템의 RAMS에 대한 분석은 첫 번째 단계는 운용시나리오 상태도를 구성하는 것이다. 상태도는 운용시나리오에서 여러 단계를 표시해 주며, 하나의 상태에서 다른 상태로 전환할 수 있도록 하는 입력 트리거(trigger)의 상태를 나타내어 준다.

예를 들어서, 연동장치의 진로요청에 진로설정의 상태로 진행하기 위해서, 연동장치는 먼저 모든 상태가 만족하는 가의 시험을 수행하며, 연동장치가 최소운용가능 상태인가를 시험한다. 단, 이러한 예에서, 최소한 기능수행 가능형태는 모든 하부 시스템이 완벽하다라는 것을 요구하지는 않는다.

신호장치의 최소운용 가능상태의 정의는 고장이 존재하더라도 활용을 할 수 있도록 한다. 고 활용성은 즉, 가용성, 고 신뢰도, 절대적 안전성으로서, 신호장치의 시스템 요구사항이기 때문에, 제어 컴퓨터 구조는 결함이 존재한다해도 운용을 할 수 있도록 충분한 다중화가 구성되어야 한다.

각기 다른 적용분야에 대해서 치명적인 상태에 이르는 위험 측 고장에 이르는 상태에 대한 확률적 평가는 각기 다른 차이점이 존재를 한다. 예를 들어서, 점보기와 같은 상용 교통 수단의 자동조정장의 신뢰도 요구사양은, 즉 시스템 고장의 받아들일 수 있는 것을 확률적으로 기술하면은 $10^{-10}/flight\ hour$ 이다. 군용 비행기에 대해서는 비행기가 손실을 발생할 수 있는 확률은 $10^{-7}/hour$이다. 고장 확률적 측면에서, 신호시스템의 하드웨어와 소프트웨어에서 요구되는 신뢰도 요구사양은 대체적으로 10^{-9} ~ 10^{-10}이다.

고 운용성(Dependability)은 특정 시스템이 제공하는 서비스의 질을 나타낸다. 신뢰도, 가용도, 안전도 및 유지보수성은 어떤 시스템의 운용성을 정량화 하는데 사용되는 측정수단이다. 정확한 정의는 그것을 측정할 수 있는 단위로서 나타낼 수 있다. 가끔 미묘한 의미는 결함허용 시스템의 여러 가지 측면을 나타내는 곳에서 정확한 의미 표시와 연결되는 정의가 포함된다. 각종 단위는 이론적으로 정량화 할 수 있고, 경우에 따라서는 정확한 값으로 표시하는 것은 매우 어렵다. 그렇다 하더라도, 그러한 항목은 시스템의 운용성의 정량적 표시 방법으로 널리 사용되고 있다. 신호시스템의 확인 방법에 대해서는, 정확한 숫자 값이 각각의 운용도 단위에 설정되어야 한다. 결함허용설계는 주어진 시스템에 대해서 그러한 운용성 측정값을 개량시키기 위해서 사용된다.

서론에서는 신호보안시스템이 요구사항에 대해서 논하였다. 다음에 본문에서는 신호보안 시스템의 기능정의,

기능분석, 안전성 할당, H/W와 S/W 구현방법 및 평가 기술에 대해서 논하고자 한다.

2. 신호보안시스템의 안전성 및 신뢰성 분석

2.1 기능요구사양

열차운행을 안전하고 효율적으로 운행하기 위해서 그림 2에서 나타낸 기능이 포함된다. 운행에 필요한 기능은 지상, 차상 및 중앙제어기능으로 나누어져 있다. 지상은 열차들의 제어, 진로제어, 보호기능 및 환경감시 기능이 있고, 차상기능은 자기열차 위치검지기능, 감시기능 및 차량감시 기능으로 구성되어있고, 중앙제어기능으로서는 진로계획, 전체시스템의 상태감시 및 통신기능으로 구성되어 있다.

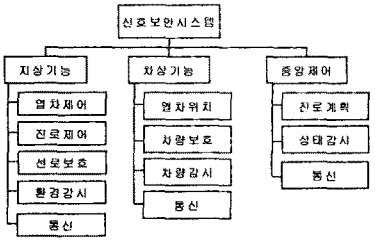

그림 2. 속도 및 진로제어의 주요기능

그림 2의 각 기능은 상관관계를 가지고 있으며, 각 기능은 자기기능을 수행하여, 다른 기능으로 천이 되며, 각 기능에 따라서 조건에 해당되면 다른 기능으로 천이 된다. 각 기능은 명령을 주는 기능과 명령을 받아서 실제로 작동이 되는 기능으로 분류된다.

지상기능은 전체열차의 운행에 관련되는 기능들을 수행을 하며, 차량기능은 한 열차에 대해서만 수행되며, 중앙제어기능은 감시, 진로계획 등 비 실시간에 적용되는 기능이라 할 수 있다.

2.1.1 지상기능

지상기능은 열차간의 제어, 진로제어, 선로에의 제한속도 부가 혹은 일기 환경검지 등 지상에서 수행하기에 적합한 기능들로 구성되어 있다. 지상기능은 속도에 영향을 미치는 변수의 규명과 그 변수를 근거로 하여 열차의 속도를 제어하는 것이다. 열차속도에 영향을 미치는 변수로는 선행열차의 위치, 열차가 운행하는 주변환경의 일기상태, 선로변에서의 작업 및 선로로의 지장물 등이 열차운행에 영향을 미친다. 열차의 위치검지, 주변환경정보 및 보호장치는 열차의 속도에 영향을 미치는 인자로서 입력데이터 제공기능을 수행하고 있다. 입력데이터를 이용하여 연산을 통하여 차상에 속도 혹은 위치정보를 전달하고, 차상제어기능은 열차속도를 감시(제어)를 한다.

· 열차제어기능

열차제어기능은 열차의 속도와 열차에 비상제동을 명령하는 기능이다. 열차의 속도를 제어하기 위해서, 선행열차의 위치를 검지하여, 후속열차와의 거리를 결정하며, 이 거리와 후속열차 열차의 제동력에 따라 속도를 결정하여 열차를 제어한다.

· 진로제어기능

진로제어기능은 열차의 진로를 요청 받아, 열차진로설정 연산에 필요한 조건을 획득하여, 진로조건이 만족할 때에 신호기 제어를 하여 필요한 진로를 얻는다. 진로를 제어할 때의 입력조건으로는 진로요청과 그에 관계된 다른 진로의 설정여부, 신호기기의 상태, 열차의 위치를 입력데이터로 활용하여 연산을 수행한다.

· 선로보호장치기능

보호장치기능은 지장물검지, 차축열검지 및 선로작업원 보호의 3가지로 나눌 수 있다. 선로 상에 침입물을 검지하기 위해서 선로 위의 교량과 사면에 지장물 침입 검지장치를 설치하여, 지장물이 검지되었을 때 열차의 속도를 제한하는 것이다. 차축열 검지장치는 열차 차축에 과도한 열이 발생하였을 때 이것을 검지하여 열차의 속도를 제한한다. 선로 작업원 보호장치는 선로에 작업이 있는 개소에 열차의 속도를 제한하여 작업을 보호하는 장치이다. 이 기능에 장애가 발생되면 사고로 이어질 수 있으므로 바이탈 기능이어야 한다.

· 환경감시기능

차상제어장치는 지상에서 허용된 속도 혹은 지상에서 검지한 선행열차위치를 전송받아 열차속도를 제어하는 기능이다. 열차속도의 제어는 지상에서 수신된 허용된 속도 혹은 선행열차의 위치를 검지하여 차상에서 연산하여, 허용된 속도이상으로 주행을 할 때에는 상용 혹은 비상제동을 인가하여 열차를 정지시키는 기능이다. 이 기능이 장애를 발생하면 사고를 유발한다. 이 기능 또한 바이탈한 기능이다.

· 통신기능

통신기능은 인접열차검지장치 혹은 보호장치 등 외부와 통신을 담당하는 기능이다. 모든 기능은 내부, 근거리 혹은 원거리 통신을 이용하여 외부와 정보교환을 한다. 기능이 오동작을 하면은 사고로 이어질 수 있으므로, 이 기능은 바이탈한 기능이다.

2.1.2 차상기능

차상기능은 차량이 주행을 하면서 안전과 운행효율을 확보하도록 하는 기능이다. 차상기능은 열차의 주어진 정보를 이용하기 위한 위치정보, 열차보호를 위한 제동기능, 열차의 상태를 알아보기 위한 감시 및 통신으로 구성되어 있다.

· 열차위치(바이탈기능)

이 값은 차상에 열차위치를 제공하여 열차가 열차진행방향, 속도 및 가속도를 결정하도록 한다. 열차위치정보는 열차가 가속을 하거나 감속을 할 때에 필요한 정보이다.

· 차량보호(바이탈기능)

차량보호기능은 차량이 사전에 설정된 진로와 일치하는 가를 확인하고, 차상장치의 상태를 검지한다. 열차가 허용된 속도이상으로 주행을 할 경우에는 비상제동을 인가하며, 비 정상상태에서는 비상속도제어를 수행을 하며, 여러 가지의 경우에 대비해서 지상과의 통신기능 등이 포함된다.

· 차량감시

열차상태를 지속적으로 감시하여, 안전에 영향을 주는 요인에 이상이 발생하였을 경우 열차를 정지시키거나, 역에 도착을 하였을 때 열차를 수리할 수 있도록 하는 기능이다.

2.1.3 중앙제어기능

중앙제어 기능은 열차의 운용을 위한 기능이다.

· 진로제어(운용기능)

진로제어기능은 열차운용의 효율을 높이기 위하여 사전에 열차의 진로를 계획을 하는 기능이다. 열차의 진로를 최적으로 제어를 하여, 주어진 자원을 최대한으로 활용을 할 수 있도록 한다.

· **상태감시기능**

지상장치와 차상장치의 기능을 원격으로 관리하는 기능이다. 이 기능은 바이탈 장치는 아니나, 현재의 고장이 미래에 커다란 사고로 발생하지 않도록 사전예방과 고장이 발생하였을 때 즉시 대처할 수 있도록 하는 기능이다.

· **통신기능**

통신기능은 지상장치와 차상장치간의 통신을 할 수 있도록 하는 기능이다. 이 통신기능은 지상장치와 차상장치에 제어정보를 제공하도록 하며, 그 장치들의 상태정보를 획득하도록 한다.

2.2 기능분석

앞에서 요구사양에서 나타난 기능을 근거로 하여 실제적으로 시스템을 구현할 수 있도록 기능분석을 수행한다. 앞에서 도출한 기능을 제어기능, 보호기능 및 감시기능의 3가지로 분류할 수 있다. 표 1은 열차제어 기능을 3가지로 분류하여 나타내었다.

표 1. 열차제어시스템기능분류

제어	보호	감시
열차위치	간격제어	진로계획
속도제어	선로보호	상태현시
진로제어	비상정지	
환경감시	비상제동	
열차상태감시	진단	

이 기능을 이용하여 그림 3과 같이 세부기능을 도출하였다. 세부기능 분석에서는 속도제어와 진로제어기능을 결합하여서 상호작용관계를 나타내었다.

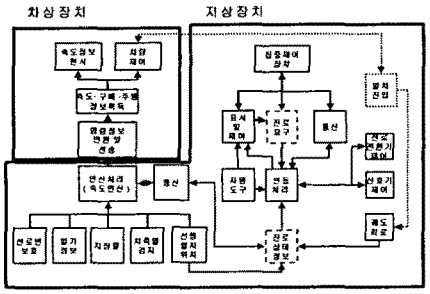

그림 3. 열차제어시스템의 세부기능

2.2.1 속도제어기능 분석

속도제어 상세기능은 그림 3에서와 같은 기능으로 분류될 수 있다. 선로변 보호기능, 일기 검지기능, 지장물 검지기능, 차축열 검지기능 및 선행열차검지 기능이 입력 값으로 얻어지며, 연산기능은 이 입력 값을 이용하여 안전속도를 연산한다. 연산된 기능은 고정데이터를 포함된 속도정보를 코드화한다. 코드화된 정보는 전송에 알맞게 변조되어 차상으로 전송된다. 차상장치는 변조된 정보를 복조하여 속도를 비롯한 주행정보로 변환을 한다. 이 정보를 차상에 현시하며, 속도제어를 수행한다.

선로변 보호기능

선로변 보호기능은 작업원이 선로에서 작업을 할 때에 양방향 열차를 안전속도 이하로 제한하는 기능이다. 고속열차의 경우 자기보호기능이 없기 때문에 열차운행 시 선로에서 작업을 할 때에는 작업구간의 속도를 제한한다. 이 기능은 사람에 의해서 기능을 작동시키며, 해제시킨다. 이 기능의 고장은 인명사고를 발생시킬 수 있으므로 바이탈 기능이다.

일기검지기능

일기 검지기능은 강우량, 강설량 및 풍속을 검지하는 기능이다. 일기는 급작스럽게 발생될 수도 있지만 대부분 서서히 진행이 되기 때문에 예측이 가능하다. 이 값은 일정주기마다 검지하고, 일정 값을 초과할 경우에만 속도제한을 행한다. 이 기능의 고장은 커다란 사고의 원인보다는 열차운행에 지장을 초래한다.

지장물 검지기능

지장물 검지기능은 선로변의 사면 붕괴나 선로 위의 교량에서 지장물이 추락하여 선로에 지장물이 침입하는 것을 검지한다. 지장물이 침입을 하면 검지선이 절단이 되어 열차가 서행으로 주행하도록 한다. 이 기능작동은 지장물 침입에 의해서만 작동된다. 이 기능의 고장은 사고로 이어질 수 있다.

차축열 검지기능

차축열 검지기능은 차축의 베어링이 파손되었을 때 차축에서 마찰에 의해서 과도한 열이 발생하여, 차축을 소착시킬 수 있다. 차축열이 정해진 온도 이상으로 되면 속도제한을 가하게 된다. 이 장치의 고장은 사고를 유발할 수 있다.

열차검지기능 (바이탈기능)

선행열차의 검지는 후속열차의 속도결정에 중요한 기능이다. 이 기능이 오동작을 할 경우에는 사고로 직접적으로 연결될 수 있다. 이 기능의 동작은 상태의 변화가 발생하였을 때 이를 검지하여 작동하는 것으로 바이탈 기능이다.

연산기능 (바이탈기능)

이 기능은 각종 입력데이터를 이용하여 열차의 주행속도를 결정한다. 연산기능은 선행열차의 위치, 지장물의 검지여부, 차축열의 상태, 일기상태 및 속도제한 정보를 이용하여 최적의 열차속도를 결정한다. 이 기능의 작동은 일정주기마다 지속적으로 수행한다. 이 기능이 오동작하면 안전 제어속도를 제공할 수 없으므로 사고로 연결될 수 있다. 이 기능은 바이탈 기능이다.

명령변환 및 전송 (바이탈기능)

연산결과에서 생성된 열차속도와 고정정보를 혼합하여, 이 정보를 열차에 송신이 용이하도록 변조와 송신을 행한다. 이 기능 동작은 연산동작 이후에 주기적으로 이루어진다. 이 기능이 잘못 동작하면 사고로 이어질 수 있다. 이 기능은 바이탈이다.

열차제어정보의 수신 (바이탈)

명령변환 및 전송기능에 송신된 정보를 수신하여, 복조를 하여 열차제어 및 속도현시 기능에 필요한 정보를 제공한다. 이 기능의 동작은 미리 설정된 주기 내에 작동이 되도록 되어있다. 이 기능의 오동작은 사고를 유발할 수 있다. 이 기능은 바이탈 기능이다.

차량제어

지상에서 송신 정보를 이용하여, 허용속도와 주행속도를 비교하여 열차의 속도를 제어한다. 열차가 허용속도 이상으로 주행할 경우에 제동명령을 인가하여 열차를 허용속도 이하로 낮춘다. 이 기능의 동작은 미리 설정된 주기로 일정하게 동작한다. 이 기능의 오동작은 사고를 유발할 수 있다. 이 기능은 바이탈이다.

속도현시

지상에서 수신된 정보를 기관사가 열차를 안전하게 제어하기 위해서 필요한 정보를 차상 현시장치에 현시를

한다. 이 기능은 주어진 주기와 사건이 발생하였을 때 필요한 정보를 현시한다. 이 기능은 운용에 영향을 미치는 기능이다.

2.2.2 진로제어기능 분석

진로제어를 수행한 세부기능은 진로요청 정보를 획득하기 위한 제어반과 통신기능이 필요하다. 입력정보로서 신호기, 선로전환기 및 궤도회로 정보의 입력기능을 갖는다. 위에서 입력된 값을 이용하여 연동처리 기능에서는 진로허가 여부를 결정한다. 진로가 허가되면 신호기 제어와 선로전환기를 제어하는 제어기능과, 신호기기가 정상적으로 작동을 하였는지 감시를 하는 기능이 필요하다.

진로제어 및 표시기능

열차진로 명령과 현재의 진로상태를 표시하는 기능이다. 열차진로 명령을 키보드나 제어 판넬을 이용하여 명령할 수 있고, 또는 외부에서 요청된 진로를 판독하여 열차진로명령을 내릴 수 있다. 상태표시기능은 조작자가 진로처리와 기타 명령을 수행하기 위한 정보를 제공한다. 이 기능은 조작자나 외부에서의 입력이 발생하였을 경우와 진로상태 혹은 신호기기의 정보가 변경되었을 때 작동된다. 이 기능의 고장이 발생하였을 때는 운용에 지장을 초래한다.

연동처리기능 (바이탈기능)

연동처리기능은 외부에서 진로요청을 수신하여 진로를 설정하는 기능이다. 이 기능에서 진로를 설정하기 위해서는 진로설정에 필요한 정보를 외부로부터 받아들여 진로설정을 한다. 진로를 설정하기 위해서는 진로설정에 필요한 조건을 검색하여 진로설정조건에 만족하는지를 검사한다. 진로설정조건을 만족하면 진로설정허가를 내리고, 신호기기를 동작하도록 명령을 내리며, 진로상태를 확인한 후에 진로설정을 마친다. 진로가 사용되기 전까지는 다른 진로설정에 의해서 진로가 방해받지 않도록 쇄정을 한다. 진로설정조건을 획득하기 위해서는 상태정보를 미리 설정된 주기에 따라 얻는다. 설정진로를 사용한 후에는 진로해정을 수행한다. 이 기능은 주기적으로 상태정보를 수집하며, 진로해정은 진로를 사용한 후에 해정조건을 만족할 때에 진로설정을 푼다. 이 기능의 오동작은 사고로 바로 직결되므로 바이탈 기능이다.

열차위치검지기능

열차위치검지기능은 자동열차제어 장치의 기능으로서 경우에 따라서는 자동열차제어장치로부터 제공받는다. 열차위치검지기능은 열차진로설정에서 가장 중요한 기능중의 하나이다. 열차가 진로 내에 있을 때 선로전환기를 전환하면 도중전환이 되어 바로 탈선사고가 발생하며, 열차가 접근구간에 있을 때 선로전환기를 전환하면 전환도중에 열차가 선로전환기에 도달하여 바로 사고로 연결된다. 열차위치검지기능은 미리 설정된 일정주기 혹은 열차가 진입하자마자 동작을 한다. 이 기능의 오동작은 사고로 직결되므로 바이탈기능이다.

신호기 및 선로전환기 상태검지

신호기 및 선로전환기의 상태는 진로설정에 필수조건이다. 진로설정기능은 신호기의 상태정보(단심 및 제어궤환)와 선로전환기의 정위, 반위 및 동작 중의 표시정보를 얻는다. 정확한 상태정보를 얻지 못하면, 연동기능에서는 잘못된 입력정보를 가지고 진로설정여부를 결정하기 때문에 잘못된 제어정보를 출력할 수 있다. 이 기능은 바이탈 기능이다.

신호기 및 선로전환기의 동작기능

신호기는 진입 및 출발 허가, 입환신호 및 표지의 통과 및 정지 상태를 제어하며, 선로전환기는 정위 혹은 반위로 전환을 한다. 신호기와 선로전환기는 고장시 안전측으로 동작을 하여야한다. 신호기는 고장이 발생하였을 경우 정지신호를 현시하여야 하며, 선로전환기는 현재 상태를 유지시킬 수 있어야 한다. 이 기능은 바이탈 기능이다.

신호기기기와 연산기기 간의 통신기능

연동처리기능이 신호기기를 제어하기 위해서는 두 기능간을 연결하는 통신기능을 필요로 한다. 이 기능의 동작은 연동장치 혹은 신호기기에서 제어 혹은 표시정보가 변경되었을 때 동작된다. 이 기능에서 오동작이 발생하여, 제어 및 표시정보가 오염되었을 때에는 신호기와 선로전환기가 정확한 제어를 할 수 없으므로 사고로 직결될 수 있다. 이 기능은 바이탈 기능이다.

외부장치와의 통신

열차제어의 효율을 높이기 위해서는 열차운행을 종합적으로 관리하기 위해서 인접역 혹은 중앙제어장치에서 열차제어장치를 제어하는 것이 필요하다. 외부장치와 통신기능은 시스템이 외부 시스템과 연결하여 열차제어에 관한 종합적인 정보를 교환한다. 이 기능의 동작은 미리 설정된 주기에 의해서 작동이 된다. 이 기능의 고장은 운용효율을 저하시킨다.

지원도구

진로제어장치에 운용효율성을 높이기 위해서 MMI기능을 첨가함으로서 진로제어장치의 활용성을 높일 수 있다. 이 기능은 운용효율을 향상시킨다.

2.3 안전성할당

2.2항에서 도출된 기능을 근거로 하여, 각 기능에 대해서 FMEA를 수행하였다. 수행한 결과로서 시스템에 대한 안전성을 할당하였다.

해저드 분석의 결과를 이용하여 안전성 요구사항을 나타낼 수 있다. 본문에서는 안전성 요구사항을 바이탈과 논바이탈로 나누었다. 바이탈은 사람의 생명을 위협할 수 있는 상태이며, 논바이탈은 운행지연을 초래하는 상황을 나타낸다.

2.3.1 속도제어기능의 Hazard 분석

속도제어 기능에 대하여 간략화한 해저드 분석을 수행하였다. 해저드 분석에는 고장모드와 결과, 영향 및 치명도에 대해서 분류하였다.

표 2. 속도제어기능의 Hazard 분석

기능	고장모드	결과	영향	등급
선로변보호	오동작	속도제한실패	인명사고	바이탈
일기검지	오동작	속도제한실패	운행지연	논바이탈
지장물검지	동작불량	속도제한실패	운행지연	바이탈
열차검지	동작불량	속도제한실패	추돌	바이탈
연산기능	오류	속도제한실패	추돌	바이탈
제어정보 송신	오류	이상속도현시	추돌	바이탈
차량제어	동작불량	속도제한실패	추돌	바이탈
속도현시	고장	속도제한실패	열차정지	논바이탈

2.3.2 진로제어기능의 Hazard 분석

진로제어기능의 대해서도 속도제어기능과 동일하게 Hazard 분석을 수행하였다.

표 3. 진로제어기능의 Hazard 분석

기능	고장모드	결과	영향	등급
진로제어 및 표시	오동작	진로설정불능	운행지연	논바이탈
연동처리 기능	오동작	오진로설정	탈선·충추돌	바이탈
열차위치 검지	오동작	오진로설정	탈선·충추돌	바이탈
신호기기 상태검지	동작불량	오진로설정	탈선·충추돌	바이탈
신호기기 동작기능	동작불량	오진로설정	탈선·충추돌	바이탈
신호기기와 연동처리 기능과의 통신	동작불량	오진로설정	탈선·충추돌	바이탈
외부장치와 통신기능	동작불량	진로설정불능	운행지연	논바이탈
지원도구	동작불량	운용불능	운행지연	논바이탈

2.4 H/W 및 S/W의 구현

속도제어기능과 진로제어기능을 마이크로일렉트로닉과 프로그램을 이용하여 구현하는 방법을 고려하여 보았다. 종래의 신호시스템은 부품의 고유한 기능을 이용하여 페일세이프를 확보하였다.

2.4.1 컴퓨터를 이용한 바이탈기능 구현원칙

컴퓨터를 이용하여 바이탈기능을 구현하기 위해서는 다음과 같은 원칙을 준수한다.

(1)일반사항
- 기능규정을 명확히 할 것
- 사용조건, 운전모드, 환경조건을 명확히 할 것
- 위험 측과 안전 측의 상태를 명확히 할당할 것
- 검출대상의 고장모드와 그 대책을 밝힐 것
- 신뢰성을 계산하고, 목표의 신뢰성이 얻어지는 것을 확인할 것
- 각종 문서화를 하고, 검토결과를 추적할 수 있을 것

(2)시스템의 기본구성
- 하드웨어 혹은 소프트웨어를 용장구성하고, 오류검출과 검출시의 안전 측 제어기구를 갖출 것.

(3)시스템이 구비해야 할 조건
- 개개의 부품(하드웨어와 소프트웨어)의 신뢰성이 충분히 높은 것. 실적이 없는 부품은 충분히 사전시험을 실시할 것.
- 각 이중계는 독립성을 가질 것
- 오류는 즉시 검출할 것
- 항시 사용하지 않는 부위에 대해서도 적극적으로 고장진단을 실시할 것
- 오류검출회로는 페일세이프일 것
- 고장 계는 분리되든가, 안전 측에 고정될 것
- 입력회로와 출력회로의 고장은 자체로, 혹은 처리장치로 검출할 수 있을 것

(4)정보전송
- 부호는 필요한 해밍거리를 확보할 것.
- 누락된 오류는 무시할 수 있을 정도로 작을 것
- 정보가 경신되는 것을 체크할 수 있을 것
- 전송정보의 체크는 페일세이프인 컴퓨터 사이에서 실시할 것

(5)맨머신
- 오조작에 대해서 방호를 취할 것
- 표시의 오류를 검출할 것
- 이상시의 처리와 그 안전성에 관해서 배려할 것

(6)소프트웨어
- 안전성이 요구되는 부분과 그렇지 않는 부분을 분리하고, 안전성이 요구되는 부분은 가능한 한 단순화할 것
- 진단 프로그램을 부가할 것
- 인루프 체커가 이루어 질 것
- 인터럽트신호를 이용하는 경우에는 고장에 의해 안전성이 훼손되지 않도록 할 것
- 타이머를 이용할 경우에는 고장에 의해 안전성이 훼손되지 않도록 할 것
- 실적이 있는 프로그램언어, 컴파일러 등을 사용할 것

2.4.2 H/W 및 S/W의 구현

신호시스템에 마이크로 컴퓨터를 도입할 때에 시스템을 페일 세이프로 하기 위한 몇 개의 구성방법이 취해진다. 기본적으로는 하드웨어 이중화와 소프트웨어 이중화로 구성된다. 하드웨어 이중화는 동일한 소프트웨어를 실장한 복수의 마이크로컴퓨터가, 데이터를 비교하고, 이상이 있어 검출할 때에는 출력을 안전 측에 고정하는 것이다. 소프트웨어 이중화에서는 1대의 하드웨어에 복수의 소프트웨어를 실장하기도 하고, 처리하는 데이터 등에 체크 부호를 부가하고, 처리결과와 출력의 정당성을 보증하는 것이다. 신호장치에 사용되고 있는 대표적인 방식을 이하에 나타낸다. 또 그것들의 기본구성을 그림 4에 나타낸다.

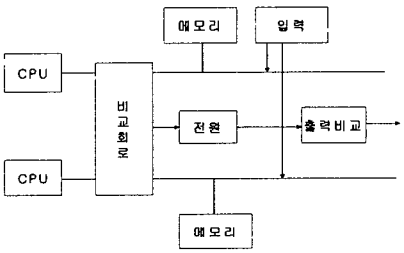

그림 4. 하드웨어의 밀접 결합 버스동기식

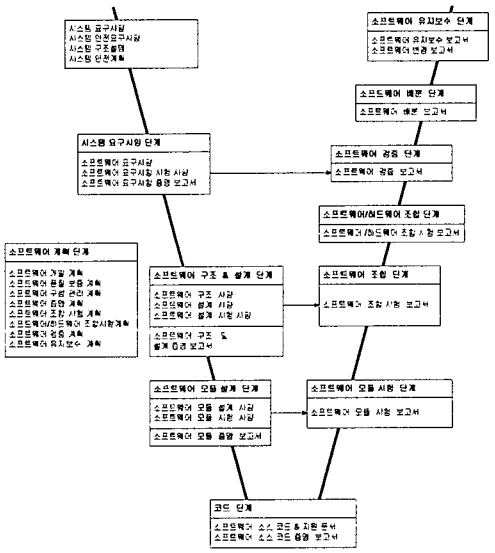

그림 5. S/W 안전성확보를 위한 절차

2.4.3 H/W 및 S/W의 구현

속도제어 및 진로제어 시스템을 구현하기 위해서 H/W와 S/W에 대해서 기능을 할당하였다.

표 4. 속도제어기능의 기능할당

기능	H/W	S/W
선로변보호	· 단순스위치	N/A
일기검지	· 일기 검지기 · 통신장치	· 코드화
지장물검지	· 경동선	N/A
열차검지	· TR사용	N/A
연산기능	· 다중화 · 자기검사	· V사이클에 의한 개발 · 문서화 · 자기진단
제어정보 송신	· 다중화 · 폐쇄망	· 코드화
차량제어	· 다중화 · 자기검사	· 코드화
속도현시	· 다중화	· 코드화

표 5. 진로제어기능의 H/W 및 S/W 기능할당

기능	H/W	S/W
진로제어 및 표시	· 이중화	N/A
연동처리 기능	· 다중화 · 자기검사	· 부호화 · 문서화
열차위치 검지	· 궤도회로	N/A
신호기기 상태검지	· 입력소자 다중화	· 레지스터 다중화
신호기기 동작기능	· 출력소자 다중화	· 레지스터 다중화
신호기기와 연동처리 기능과의 통신	· 다중화 · 전용망 구축	· 부호화 · 전용망 구축
외부장치와 통신기능	· 다중화 · 다경로통신망사용	· Verified COTS S/W 사용
지원도구	· 이중화	· CASE Tool · Verified COTS S/W 사용

2.5 평가기술

열차제어 시스템의 안전성 및 Fault tolerant의 평가는 구성된 시스템이 안전성과 신뢰성을 요구사양을 만족하는 가늘 확인하는 것이다. 안전성의 요구사양은 바이탈기능과 논바이탈 기능으로 분리하였으며, 바이탈기능은 $10^{-9}/hour$의 위험측 고장율로 하였으며, 논 바이탈 기능의 신뢰성은 $10^{-7}/hour$로 이다.

안전성 및 신뢰성을 평가하기 위해서 그림 6과 같은 절차로 수행을 하였다. 안전성활동은 preliminary hazard 분석, hazard 분석 및 도출, 위험도 평가, 안전요구사양, 안전계획, 안전성 확보활동, 활동결과의 기록 등의 순서에 의해서 수행한다. 시스템의 안전성 평가는 각 단계에서 적정하게 안전성 활동과 기술 및 시험평가를 수행하였는가를 검토하여 안전성 확보여부를 결정한다.

신뢰성확보는 시스템의 고장부분에 대한 분석을 통하여, 고장도 평가 등을 거쳐서 신뢰도 확보활동, 기술 및 시험을 통하여 신뢰성을 확보한다. 신뢰성의 평가는 신뢰성 활동에 대한 각 단계를 평가함으로써 신뢰성이 확보되었는지의 여부를 평가할 수 있다. 신뢰성 평가체계는 그림 7에서 나타내었다.

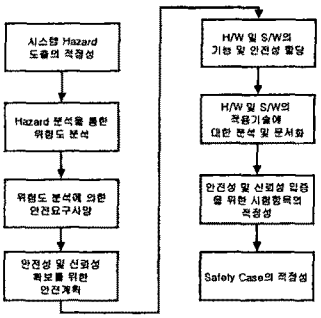

그림 6. 안정성 평가체계

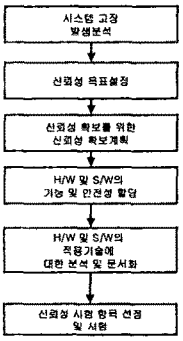

그림 7. 신뢰성 평가체계

3. 결 론

신호제어시스템에 대해서 안전성 활동에 관련된 내용과 그 평가방법에 대해서 제시를 하였다. 안전성 평가는 다단계에 걸쳐서 수행이 되므로, 항상 체계적인 절차와 안전성 문서형식이 필요하다. 안전성의 평가를 위해서는 충분한 위험요소(hazard)분석과 안전도할당이 중요하다. 또한 안전성평가를 위해서는 제 3의 기관에서 안전성활동이 적절한지를 평가할 필요가 있다.

[참 고 문 헌]

[1] 이종우 외 4인, 철도신호제품에 대한 신뢰성과 안전성 검증기준 제정연구, 연구보고서, 철도청 2001.10

[2] IEC 61508 1-6, IEC Standard, IEC 2000

[3] Hirao,Yuji abd Fukuda, Mitsuyoshi, "Software Safety Technologies for Railway Signalling", Japanese Railway Engineering No. 141, pp.12-14,1998