컴퓨터기반 자동열차제어장치의 안전성 확보에 관한 연구

論 文
54B-6-1

A study on An Application for Ensuring Safety of Computer Based Automatic Train Control System

辛 德 浩† · 李 鍾 宇*
(Ducko SHIN · jongwoo LEE)

Abstract - This paper propose the safety design of automatic train control system which is used for controlling and monitoring train speed not to excess a permitted speed. Safety activities are shown for the computerized system to achieve a required safety requirement. The safety activities are composed of system dynamic modelling to identify potential hazards contained in the target system, to analyze sub system faults to provoke the hazards. Risks analysis are carried out to estimate losses caused from the hazards to allocate safety requirement. We proposed design solutions for sub system to meet safety requirement.

Key Words : Modelling, Safety, Computerized Control System, Hazard, Redundancy, ATC

1. 서 론

컴퓨터시스템을 이용한 제어는 산업분야에 폭넓게 사용되고 있으며, 이러한 분야에서 컴퓨터의 건전성 보장은 신뢰성과 안전성에 상당부분 의존하고 있다. 이러한 분야에서 발생하는 컴퓨터의 고장은 전체 시스템을 마비시키고 경우에 따라서는 대형사고로 이어질 수 있다. 예를 들어서 항공기에 있어서 제어컴퓨터의 고장은 항공기의 손실로 이어질 수 있으며, 원자로 노심 제어용 컴퓨터의 이상동작은 노심 용융 등의 커다란 사고로 이어질 수 있다. 철도에서의 열차의 속도를 제어하는 시스템의 이상 동작은 열차속도의 제어를 실패하여 탈선 혹은 충돌을 일으켜 커다란 사고로 이어질 수 있다.

컴퓨터 시스템은 컴퓨터를 구성하는 하드웨어, 컴퓨터 내부 소프트웨어, 운용시스템 및 응용프로그램 등 각각의 서브 시스템으로 구성되어져 있다. 이러한 컴퓨터 시스템의 내부 구조는 목표로 하는 응용동작을 수행하기 위해 직렬로 연결되기 때문에 하나의 내부시스템 결함은 시스템 전체에 영향을 미칠 수 있다. 따라서 각 시스템의 결함과 고장을 피하기 위해 다양한 방법을 채용하여 사용한다. 결함과 고장을 방지하기 위한 대표적인 방법으로서 결함회피(Fault Avoidance)와 결함허용(Fault Tolerant)이며, 인적요소가 시스템에 영향을 미치는 경우에 대해서는 시스템라이프사이클 전체(개념, 설계, 제작, 운용, 폐기)에 대해서 고려를 하며, 물리적인 요소에 대해서는 열화, 과부하 및 잡음·서지와 같은 환경적인 요소에 대해서 고려한다[1].

본 논문에서는 철도분야에서 열차의 간격제어를 위해 사용되는 자동열차제어장치를 대상으로 안전성요구사항 만족을 위한 시스템구조 모델링과 정량적인 위험측 고장률 산출을 목적으로 한다. 안전필수시스템인 자동열차제어장치는 안전요구사항을 만족하기 위해 과거에는 바이탈 릴레이를 이용하여 논리를 구성하였으나 현재에는 기능향상 및 다양한 인터페이스를 위해 전자화된 장치에 의해서 제어되고 있다. 본 논문의 전반부에서는 자동열차제어장치의 안전성확보를 위해 위험원 도출, 사고영향 분석 및 안전기술의 적용방법을 제시하였으며, 다중의 고장에 대한 안전성확보를 위해 설계된 시스템 내부와 안전관련기능의 고장검지를 위한 회로에서 다중고장이 발생한 경우를 모델링 하였다. 후반부에서는 자동열차제어장치에 대한 안전성요구사항을 만족하기 위한 구성방법을 제안하고 제안된 구조에 의한 시스템의 위험측 고장률을 시간에 따라 시뮬레이션 하였다. 따라서 본 논문은 자동열차제어장치에서 발생할 수 있는 위험측 고장과 안전측동작 확률에 대한 수학적 모델링을 통해 구성방법을 제안하고 시뮬레이션 결과를 토대로 안전성확보를 입증하였다.

2. 자동열차제어장치

2.1 자동열차제어장치의 기능

열차제어장치는 속도에 따라 열차의 간격을 제어하는 장치로써, 열차의 특성상 고속주행으로 인한 긴 제동거리 때문에 선행열차의 정확한 위치판단에 의한 간격제어가 매우 중요하다. 따라서 후속열차는 선행열차의 위치를 자동열차제어장치에 의존하여 선행열차에 대한 위치정보를 수신하고 열차의 간격제어를 위한 속도를 제어한다. 열차의 간격제어는 제동거리확보와, 운전간격의 최소화를 통한 효율성추구라는 반비례 요소를 고려하여 효율적이며 안전한 운전을 목적으로 한다. 자동열차제어장치의 기능을 그림 1에서 나타내었다[2].

† 교신저자, 正會員 : 광운대학교 제어계측공학과 박사과정
한국철도기술연구원 주임연구원
E-mail : ducko@krri.re.kr
* 正 會 員 : 서울산업대학교 교수
接受日字 : 2004年 8月 9日
最終完了 : 2005년 1月 20日

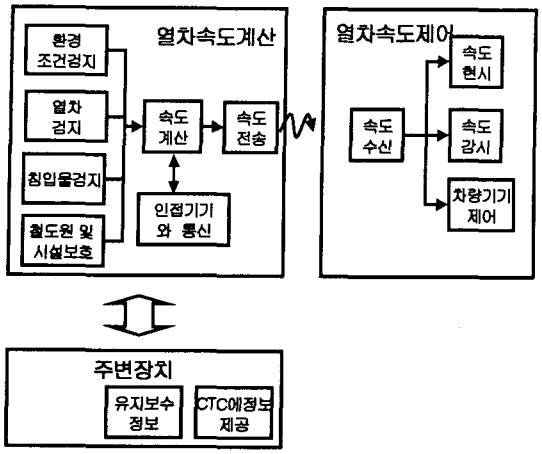

그림 1. 자동열차제어장치의 기능블록도
Fig. 1. Functional diagram of ATC system

자동열차제어장치의 기능은 열차속도계산기능, 계산된 열차속도에 따라서 열차속도를 제어하는 기능 및 주변장치로 구성되며, 그 중 열차속도계산기능과 제어기능은 안전과 직접적인 관련이 있는 바이탈기능이다.

열차속도계산기능은 열차허용속도를 계산한다. 검지기능을 이용하여 선행열차의 위치를 검지하여 후속열차의 속도를 계산하며, 환경검지기능은 일기상태를 검지하여 열차의 허용최대주행속도를 결정하고, 침입물 검지기능은 선로에 차량 혹은 암석 등이 선로에 침입하였을 때의 속도제한 및 선로변 작업원을 보호하기 위하여 열차주행허용속도를 제한한다. 자동열차제어장치는 각 조건에서 계산된 속도 중 가장 낮은 속도값을 선택하여 열차에 전송 하며, 열차는 이것을 허용속도로 인지하여 주행한다.

열차속도제어기능은 수신된 열차속도를 현시하고, 현시된 속도를 초과하면 제동을 체결하여 열차를 안전한 속도로 낮추는 기능도 수행한다.

마지막으로 주변기기를 통하여 자동열차제어장치의 제어정보, 상태정보, 그리고 유지보수정보 등과 같은 각종 정보를 송·수신한다.

2.2 자동열차제어장치의 동적모델

자동열차제어장치의 열차속도 제어에 사용되는 정보는 각 하부기능에 의해서 계산되며, 그림2는 자동열차제어장치의 열차속도계산과 열차제어정보생성 그리고 외부 인터페이스를, 제한된 시간내에 반복적으로 수행하는 내부 흐름을 모델링한 것이다. 따라서 열차검지, 속도계산, 속도코드 송수신 그리고 속도감시에 따른 열차의 제어에서 결함발생으로 인한 오류로 인해 정보의 변형이 발생하면, 차량은 주행속도를 허용속도 이상으로 해석하는 위험측고장이 발생하며, 이러한 경우 열차주행의 안전성이 저해된다.

2.3 자동열차제어장치의 시스템구성

자동열차제어장치 하부시스템을 정보입력, 데이터 처리, 그리고 차량제어의 3개 그룹으로 크게 나누었다. 자동열차제어장치 하부시스템에 대한 분류는 다양한 접근이 가능하지만 본 논문에서는 한국형고속철도에서 적용된 분류기준을 사용하였다.

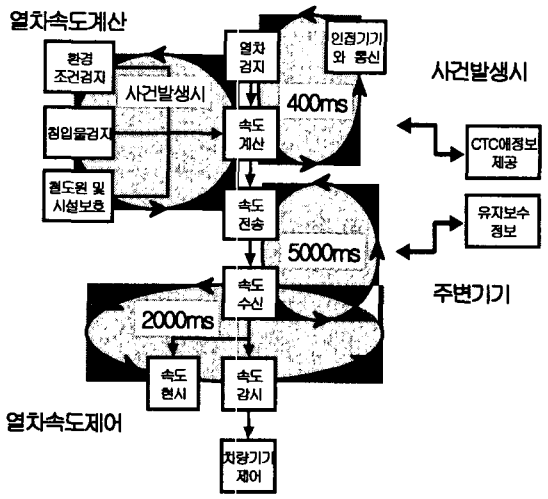

그림 2. 자동열차제어장치의 동적 기능도
Fig. 2. Dynamic functional diagram of ATC system

첫 번째 그룹은 열차의 속도를 설정하는 입력 데이터 부분으로, 그림2에서 환경검지, 침입물검지, 철도원·시설보호 및 열차검지로 표현된 부분이다. 환경검지장치는 강우계, 강설계 및 강풍계로 구성되며, 강풍, 강설 및 강수량의 입력이 열차의 정상운행에 지장을 발생할 수준으로 입력되면 신호를 전송한다. 장애물 검지장치는 교량 혹은 선로 변 사면으로부터 침입한 차량 혹은 낙석을 검지하는 것으로 외부 물체가 선로로 침입하면 케이블이 절단되도록 구성하여 개회로에 의한 검출방식이 사용된다. 선로 보수원의 보호장치는 유지보수 지역의 스위치를 작동함으로써, 유지보수여부를 결정하며, 유지보수가 수행될 경우에는 열차가 그 지역을 제한 속도이상으로 주행하지 못하도록 한다. 열차검지장치는 변조된 신호를 궤도회로를 통해 레일에 인가하며 이 신호에 의해 발생되는 자장에 의해서 차상에 정보를 전달한다. 또한 차륜에 의해서 레일이 폐회로를 구성하면 수신 단에서는 신호가 검지되지 않아 열차의 존재여부를 판단한다.

두 번째 그룹은 열차속도계산과 열차속도의 전송을 수행한다. 열차속도계산 장치는 환경검지장치, 장애물 검지장치, 철도원 보호장치 및 열차검지에서 입력된 신호를 조합하여 열차 속도를 계산하고, 부호화하여 전송장치를 통해 전송한다. 전송장치는 수신된 코드 정보를 반송파에 실기 위해 변조한 후, 전류를 증폭하여 레일에 전송한다.

세 번째 그룹은 차량을 제어하는 차상장치이다. 수신장치는 레일에 흐르는 신호로부터 발생되는 자장과 전자기유동(magnetic coupling)을 통하여 정보를 획득하며, 이 신호를 복조 및 디코딩을 통하여 코드정보를 복원한다. 차량의 속도현시장치는 수신장치에서 얻어진 허용속도와 열차의 타코메터에서 얻어진 속도를 현시한다. 속도감시장치는 허용속도와 열차주행속도를 비교하여 열차가 어느 속도이상으로 주행하면 기관사에게 경고한 후 제동신호를 인가하여 안전속도이하로 열차의 속도를 감소시킨다.

2.4 자동열차제어장치의 안전성 요구사양

사고의 발생을 자발행위와 사고를 당하는 경우를 구분해서, 어느 정도 위험에 노출되고 있는지, 혹은 수용할 수 있는지를 표1에 나타내었으며, 안전성 요구수준으로서 제안되는 수치를 예로 든 것이다[3].

표 1. 자발행위와 사고를 당하는 경우의 비교

Table 1 A comparison of accidents from intentional and unintentional activites

자발행위($\times 10^{-5}/h$)		재난($\times 10^{-7}/h$)	
흡연	500	교통사고	500
자동자운전	17	홍수	7
모토사이클	2000	지진	7
축구	4	토네이도	22
		비행기추락	1
		원자력발전	1
		낙뢰	7
		자연사	125,000

표1에서 재난으로 사망하는 경우는 $x\times 10^{-7}/h$정도가 된다. 영국에서는 작업장에서 발생하는 사망사고를 FAFR(Fatality Accident Frequency Ratio)로 정하여 요구수준을 $x\times 10^{-7}/h$으로 제시하고 있다. 이러한 안전요구사항은 사망사고에 대하여 사회가 합리적으로 받아들일 수 있는 수준을 의미하며, 철도분야 안전필수 시스템에 의한 사망사고 발생율은 10^{-9} $10^{-10}/h$(1시스템당 10~100만년에 1회)를 사회적인 기준에서 타당한 값이라고 영국에서 제시되고 있다. 따라서 본 논문에서는 열차의 간격을 제어하는 안전필수 시스템인 자동열차제어장치의 안전성요구사양을 $10^{-9}, 10^{-10}/h$라고 할당하였다.

3. n개의 하부시스템으로 구성된 시스템의 안전성 분석

본 절에서는 복수개 이상의 하부시스템으로 구성된 안전필수분야 제어장치의 안전성 분석을 위해 고장검지 장치를 내장하지 않거나, 내장하는 경우의 시스템고장률 그리고 이러한 하부시스템 들로 구성된 제어장치의 상태에 대한 해석방식을 제안하였다.

3.1 고장검지장치를 내장하지 않은 시스템의 상태도

자동열차제어장치의 내부구성은 앞에서 설명한 바와 같이 몇 가지 하부시스템으로 구성되어 있다. 따라서 본 절에서는 여러 개의 하부시스템으로 이루어진 자동열차제어장치 작동상태에 대한 모델링을 수행하였다. 고장검지장치를 내장하지 않는 하부시스템 상태는 정상동작 상태, 안전측 고장상태 및 위험측 고장상태로 나눌 수 있다. 그림3은 위와 같은 구조의 하부시스템으로 구성된 자동열차제어장치 상태천이도를 나타낸 것이다.

임의 하부시스템 고장률을 λ로 하고 고장이 발견될 확률을 C로 한다면, 정상상태는 $1-\lambda\Delta t$, 안전측 고장 $\lambda\Delta tC$, 위험측 고장율은 $\lambda\Delta t(1-C)$가 된다[4]. 안전측 고장은 자동열차제어장치에 대하여 사고를 발생시킬 수 있는 원인으로써, 이러한 기능과 관련된 모듈에서 고장발생이 검출되어 의도된 안전한 상태도 수렴되는 것을 안전측 고장이라 정의하고, 고장발생을 검출지하지 못하여 예측할 수 없는 상태로 되는 것을 위험측 고장이라 정의한다.

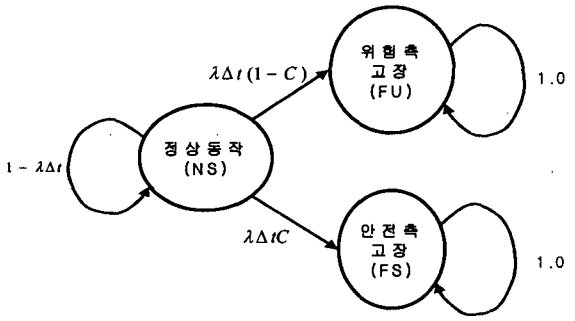

그림 3. 자동열차제어장치의 정상, 안전측고장 및 위험측고장상태 천이도

Fig. 3. Three state Markov modeling for normal, safe failure and unsafe failure of ATC

그림 3의 상태천이도에 따라서 각 상태의 확률은 다음과 같다.

$$p_{NS}(t+\Delta t)=(1-\lambda\Delta t)p_{NS}(t) \quad (1)$$

$$p_{FS}(t+\Delta t)=\lambda\Delta tC\,p_{NS}(t)+p_{FS}(t) \quad (2)$$

$$p_{FU}(t+\Delta t)=\lambda\Delta t(1-C)p_{NS}(t)+p_{FU}(t) \quad (3)$$

이 시스템의 모든 상태들의 합은 다음과 같다.

$$p_{NS}(t)+p_{FS}(t)+p_{FU}(t)=1 \quad (4)$$

제안 1:안전측 고장과 위험측 고장은 상호 배타성을 갖는다.
증명: 그림 3과 같이 단일 고장이 발생하는 경우에 바이탈 기능에서 고장이 검출되면 안전측 설계에 의해 시스템은 안전측으로 작동을 하고, 논바이탈 기능에서 고장이 발생하면 위험측 고장으로 발전할 가능성이 없으므로 안전측 고장이 된다. 또한 바이탈 기능 고장이 발생하였을 경우 고장을 검지하지 못하는 경우에만 위험측 고장으로 천이되므로 안전측 고장과 위험 측 고장과는 서로 배타적 관계이다.

제안 1과 같이 시스템이 안전하게 동작할 확률 $p_{FSO}(t)$는 정상적인 상태와 안전측 고장상태를 합한 확률과 같으며, 다음과 같이 나타낼 수 있다.

$$p_{FSO}(t)=p_{NS}(t)+p_{FS}(t) \quad (5)$$

따라서 임의의 시간 t에서 $p_{FSO}(t)$의 확률을 구하면, 식(2)에 식(5)를 대입하여 다음과 같이 표현할 수 있다.

$$p_{FSO}(t+\Delta t)=p_{FSO}(t)-(1-C\lambda\Delta t)p_{NS}(t) \quad (6)$$

제안 2 : 결함검지장치가 내장된 시스템의 고장검지율 $C(t)$는 $C(t)=1-\lambda_d(t)$로 정의할 수 있다.

증명 : 고장의 발생 여부를 검지하는 장치가 정상적으로 작동하면 시스템의 고장여부를 검지할 수 있다. 하지만 검지장치에서 고장이 발생하면 시스템의 고장여부를 감지할 수 없다. 따라서 검지장치의 고장율을 $\lambda_d(t)$라 할 때, 시스템에서 고장이 정확하게 검지될 확률은 $C(t)=1-\lambda_d(t)$이 된다.

3.2 고장검지장치를 내장한 하부시스템의 위험측 고장률

자동열차제어장치를 구성하는 각각의 하부시스템에서 고장검지장치는 설계에 따라 다양한 형태로 적용될 수 있다. 고장검지장치의 기본적인 형태는 그림4와 같이 구성을 한다.

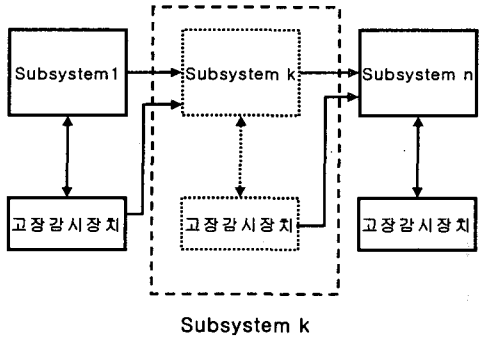

그림 4. 서브시스템에 고장검지장치가 설치된 예

Fig. 4. An Example of failure detector installed to a subsystem

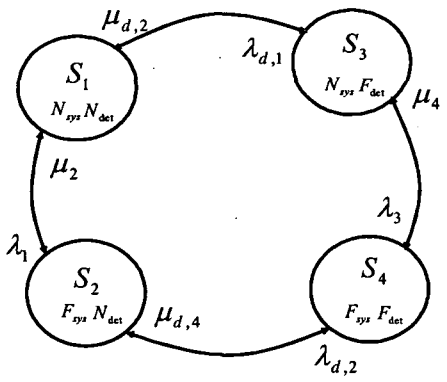

그림 5. 고장검지 장치가 부착된 하부시스템k의 상태도

Fig. 5. State Diagram of Subsystem k equipped failure detector

그림 4는 고장감시장치를 내장한 자동열차제어장치의 블록다이어그램이며, 그림5는 그림4와 같은 구조의 상태도를 나타낸 것이다. 상태도에서 N은 정상상태, F는 고장상태를 나타내며, 첨자는 시스템상태와 고장검지장치를 나타낸다. S_1은 서브시스템과 고장검지기가 정상인 상태, S_2는 시스템고장, 고장검지기 정상, S_3는 시스템 정상, 검지기고장 이며, S_4는 시스템과 고장검지기가 고장인 상태이다. 하부시스템이 정상인 경우(S_1과 S_3)는 고장감시장치의 고장여부와 상관없이 정상적으로 동작이 되지만, S_2 인 경우에는 안전측 고장상태가 되며, S_4인 경우에는 시스템이 위험측 고장상태가 된다. 따라서 하부시스템의 고장과 고장감시장치에서 고장이 발생하였을 경우(S_4)에만 위험 측으로 고장이 발생할 수 있다. 이러한 논리에 의해 하부시스템 k의 정상측($\lambda_{NS,k}$), 안전측($\lambda_{FS,k}$) 및 위험측($\lambda_{FU,k}$) 고장율을 다음과 같이 표현하였다.[3].

$$\lambda_{FU,k}\cong\lambda_k(\lambda_{d,k}r_k)+\lambda_{d,k}(\lambda_k r_{d,k}) \tag{7}$$

단 $r_{d,k}=1/\mu_{d,k}$ 와 같이 r은 수리율의 역수이다.

$$\lambda_{NS,k}=1-\lambda_k \tag{8}$$

$$\lambda_{FS,k}=\lambda_k-\lambda_{FU,k} \tag{9}$$

따라서 식(9)와 같이 고장감시장치를 내장한 단일구조 시스템의 정상상태 고장률, 위험측고장률 그리고 안전측 고장률을 제시하였다.

위와 같은 시스템 상태분석에 의해 자동열차제어장치의 안전성확보를 위한 설계는 고장 검지율 C_k를 높이는 것이며, 위험측 고장발생빈도를 낮추기 위해서는 하부시스템의 고장률 λ_k와 고장검지장치의 고장률 $\lambda_{d,k}$을 낮추어야만 하부시스템과 그 하부시스템의 고장검지 회로에서 고장이 발생하는 경우 고장을 검지하는 능력인 C_k가 높아지고 시스템의 안전성이 향상된다는 결과를 얻었다.

3.3 n개의 하부시스템으로 구성된 자동열차제어장치에서 정상, 안전 및 위험측 고장확률

여러 개의 하부시스템이 직렬 혹은 병렬로 연결되어 있을 때에도 복수개 이상의 고장에 의해 각 하부시스템의 고장이 전체시스템 고장으로 확산될 수 있다. 따라서 여러 개의 하부시스템이 직렬로 연결되어 있을 때에 시스템의 정상활동 확률, 안전측 고장 및 위험 측 고장률을 규명할 필요가 있다.

정리 1 : 하부시스템의 기능이 직렬로 구성되어있는 시스템에서 하부시스템 k의 위험측 고장확률 $p^k_{FU}(t)$는 하부시스템 $k-1$의 출력과 관계없이 하부시스템 k의 위험측 고장률과, 하부시스템 k는 정상이고 하부시스템 $k-1$에서 위험측 고장이 발생하여 하부시스템 k에 위험 값이 입력될 확률의 합이다. 즉

$$p^k_{FU}(t)=\left(1-(p^k_{NS}(t)+p^k_{FS}(t))\right)\cdot\left(p^{k-1}_{FU}(t)+p^{k-1}_{NS}(t)\right)+p^{k-1}_{FU}(t)\cdot p^k_{NS}(t)$$

이다.

증명 : 그림4에서 시간 t에 시스템 $k-1$이 정상적인 출력상태 $p^{k-1}_{NS}(t)$, 안전측 고장출력상태 $p^{k-1}_{FS}(t)$ 및 위험측 출력상태 $p^{k-1}_{FU}(t)$이고, 하부시스템 k는 정상적인 상태 $p^k_{NS}(t)$, 안전측 고장상태 $p^k_{FS}(t)$ 및 위험측 고장상태 $p^k_{FU}(t)$이다. 하부시스템 $k-1$에서 고장이 발생되어 고장을 검지하지 못하였을 경우에

위험측 출력이 발생하고, 이러한 위험측 입력은 하부시스템 k의 상태와 상관없이 위험 출력을 발생시킨다. 따라서 그림6의 실선과 같이 위험입력이 시스템 k의 정상상태에 입력되면 하부시스템 k의 위험측 동작확률 $p^k_{FU}(t)$은 $p^k_{FU}(t)=p^k_{NS}(t)p^{k-1}_{FU}(t)$가 된다. 또한 하부시스템 k가 위험측 상태인 경우에는 서브시스템 $k-1$의 상태와 상관없이 위험출력이 되므로, 이 경우는 $p^k_{FU}(t)$는 $p^k_{FU}(t)=(1-(p^k_{NS}(t)+p^k_{FS}(t)))(p^{k-1}_{FU}(t)+p^{k-1}_{NS}(t))$ 가 된다. 따라서 서브시스템 k의 위험 출력확률은 k자체의 위험 출력과 이전 단계로 부터의 위험출력 입력에 대한 합이 된다.

제안 3 : 서브시스템 k에서 안전측 고장이 발생한 경우는 전체 시스템은 안전측으로 작동된다.
증명 : 제안1의 고장상태의 상호배타적인 특성에 의해 안전측 고장은 안전측 고장상태로 만 천이되므로 안전측 고장상태로 시스템전체가 동작하며, 안전측에서 위험측으로 천이되는 경우는 위험측 고장으로 취급한다.

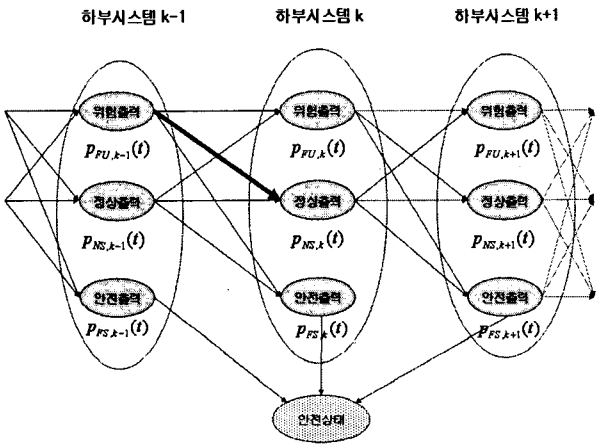

그림 6. 하부시스템 k-1의 위험측 출력이 서브시스템k가 정상상태일 때 입력되어도 위험출력이 생성된다.
Fig. 6. Normal state subsystem k yields unsafe output when subsystem k-1 is under unsafe failure.

정리 2 : 그림 6와 같이 n $(n\geq 1)$개의 하부시스템이 직렬구조로 안전관련 기능을 수행하는 시스템의 출력은 안전측으로 동작된 하부시스템 k의 안전측 출력 이거나, n번째 하부시스템의 출력이다.(시스템의 최종출력 종류)
증명 : 그림6에서 k번 째 하부시스템에서 안전측 고장이 발생 하면 제안3에서와 같이 시스템이 안전모드로 작동되기 때문에 출력은 안전측 상태로 되며, 모든 서브시스템이 안전측 출력 상태가 발생하지 않으면 최종단인 n번째 하부시스템에서 정상출력, 안전출력 및 위험출력이 발생된다.

정리 3 : 그림 6과 같이 직렬구조로 안전관련 기능을 수행하는 구조에서 하부시스템 k의 출력 발생은 이전 시스템 $(1, 2, \cdots, k-1)$들의 상태가 모두 정상출력 또는 위험측 출력이거나 k가 위험측 출력을 발생하는 2가지 상태만 존재한다.(하부시스템의 출력발생 조건)
증명 : 정리2와 같이 하부시스템 k에서 출력이 발생하면 이전 서브시스템 $(1, 2, \cdots, k-1)$은 모두 안전상태 또는 위험측상태이다. 따라서 이전시스템 $(1, 2, \cdots, k-1)$은 정상출력이거나, k가 직접 k-1에 의해 위험측출력 또는 k내부의 고장에 의해 위험측출력을 발생시키는 상태만 존재한다.

자동열차제어장치 구성에 있어서 시스템은 그림6과 같이 하나의 입력에 의해서 시스템 출력이 발생되는 경우와 그림7과 같이 복수개 이상의 입력으로 최종시스템 출력이 발생되는 경우가 있다. 또한 동일한 기능을 다중계로 구현한 다중계 시스템의 경우에는 여러 개의 입력 값에서 시스템이 가장 안전한 상태로 작동되는 값을 내부적으로 선택하여 고장을 억제한다.

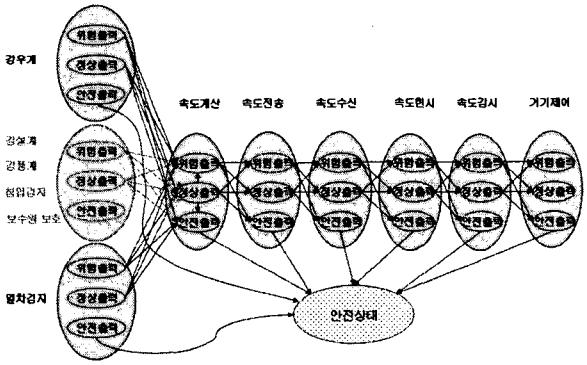

그림 7. 자동열차제어 장치의 각 기능별 직렬 및 병렬연결도
Fig. 7. Sequentail and parallell connection diagram of subfunctions for ATC subfunction states

정리 4 : 그림 7과 같이 직렬계 k개와 병렬계 p개로 이루어진 안전필수 시스템 $(k+p=n)$에서 전체시스템이 정상적으로 작동할 확률은 n개의 직렬구조 시스템과 동일하다.
증명 : 각 입력시스템은 안전한 동작을 수행하기 위한 입력값을 생성하는 것으로서 모든 입력시스템이 정상적으로 동작을 하여야 하며, 하나의 하부시스템에서 고장이 발생할 경우에도 전체시스템의 바이탈한 동작에 영향을 미친다. 따라서 자동열차제어장치와 같은 바이탈 시스템에서 모든 입력 서브시스템이 정상적으로 작동하기 위해서, 각각의 하부시스템 직렬구조로 간주할 수 있다.

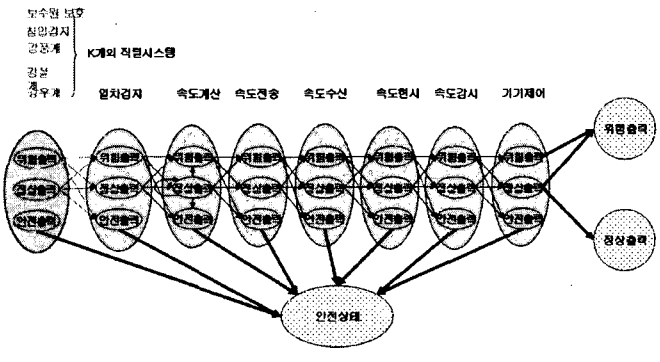

그림 8. 자동열차제어 장치의 각 기능별 직렬연결도
Fig. 8. Sub functions sequental connection diagram for ATC subfunction states

그림8은 안전필수 기능수행을 위한 k개의 병렬하부시스템을 k개의 직렬 하부시스템으로 변경시킬 수 있다. 시스템의 출력상태는 그림9에서 나타낸 것과 같이 정상출력, 안전출력 및 위험출력이 있다.

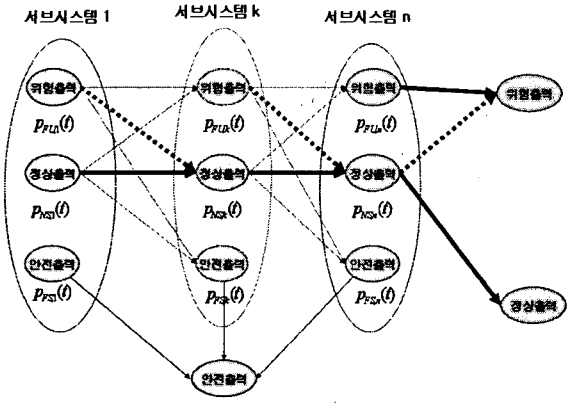

그림 9. 하부시스템 k-1이 위험측 출력상태이면 하부시스템 k가 정상상태일 때에도 전체시스템 최종출력은 위험출력이 생성된다.

Fig. 9. Normal state subsystem k yields unsafe output when subsystem k-1 is under unsafe failure

n개의 직렬구조 하부시스템으로 구성된 시스템에서 주어진 순간 t에서 시스템 상태확률 $p^n_{NS}(t)$, $p^n_{FU}(t)$ 및 $p^n_{FS}(t)$은 제안3, 정리2 및 정리 4를 사용하면은 다음과 같이 된다.

정상동작상태 $p^n_{NS}(t)$는 각 서브시스템이 정상적으로 작동되는 상태이다.

$$p^n_{NS}(t)=\prod_{i=1}^{n} p^{i}{}_{NS}(t) \tag{10}$$

위험측 출력 확률은 정리3에 따라서 다음과 같이 정의된다.

$$p^k_{FU}(t)=\left(1-(p^k_{NS}(t)+p^k_{FS}(t))\right)\cdot\left(p^{k-1}_{FU}(t)+p^{k-1}_{NS}(t)\right) +p^{k-1}_{FU}(t)\cdot p^k_{NS}(t) \tag{11}$$

고장에 의한 안전측 출력확률은 정리2와 4에 따라서 다음과 같이 정의된다.

$$p^n_{FS}(t)=\sum_{i=1}^{n} p^i_{FS}(t) \tag{12}$$

하부시스템 n가 안전상태로 될 확률 $p^n_{FS}(t)$의 확률은 다음과 같이 정의된다.

$$p^n_{FS}(t)=\left(1-(p^k_{FU}(t)+p^k_{NS}(t))\right)\left(p^{n-1}_{FU}(t)+p^{n-1}_{NS}(t)\right) \tag{13}$$

따라서, 시스템이 안전하게 동작할 확률은 다음과 같이 된다.

$$p_{FSO}(t)=p_{NS}(t)+p_{FS}(t) \tag{14}$$

4. 한국형 고속철도 자동열차제어장치 위험측 고장률평가

4.1 자동열차제어장치의 위험원 도출, 규명 및 위험도분석

자동열차제어장치에서 대표적으로 나타나는 위험원은 "허용속도보다 높은 속도 값의 설정"이며, 각 하부시스템에서 발생되는 위험측 고장은 "허용속도보다 높은 속도 값의 설정"으로 정의할 수 있다. 열차속도계산, 속도정보의 전송, 차상정보처리 등에 의해서 입력조건이 실제허용 속도보다 덜 제한적인 값으로 입력되면 열차침수, 운행지장, 전복, 지장물과의 충돌, 인사사고 및 열차의 충·추돌이 발생할 수 있다.

다음의 그림10, 11, 12, 13에서 회색으로 표시된 부분은 기능이 정상적으로 작동되지 않아서 앞에서 제시한 위험원이 발생할 수 있는 경우를 나타낸 것이며, 이러한 하부시스템 고장발생으로 인한 안전측 고장상태와 위험측 고장상태를 그림으로 표현하였다.

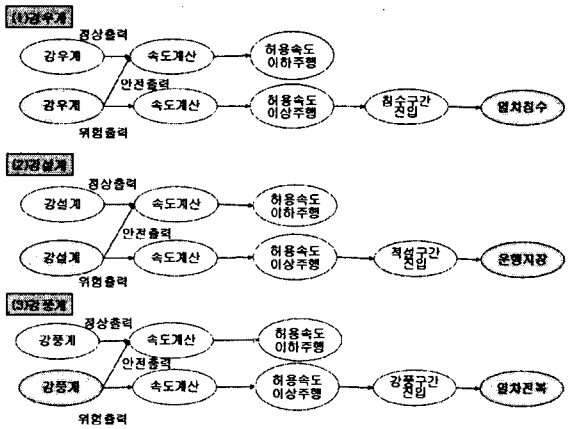

그림 10. 속도제한변수에 m이한 열차속도제어 시나리오(환경검지기능)

Fig. 10. A scenario for train speed control with speed constraint condition(climatic condition)

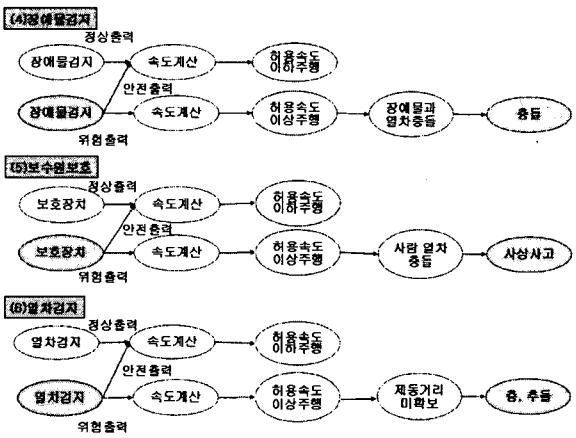

그림 11. 속도제한변수에 의한 열차속도제어 시나리오(보수원 보호, 침입물검지, 열차검지)

Fig. 11. A scenario for train speed control with speed constraint conditions(railway man protection, intrusion detection, train detection)

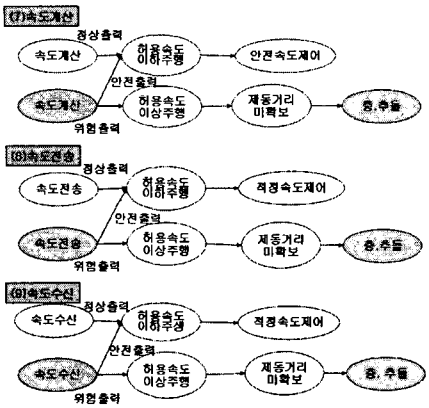

그림 12. 열차속도 정보송수신에서 열차제어 시나리오

Fig. 12. A scenario for speed code transmission

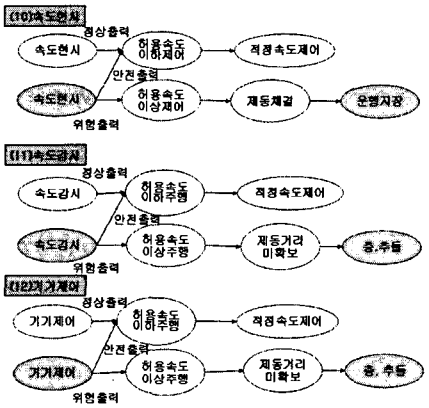

그림 13. 차량속도 감시 및 제어 시나리오

Fig. 13. A scenario for train speed monitoring and control

따라서 자동열차제어장치의 안전성확보는 그림10, 11, 12, 13에서 도출된 위험측 상태고장의 발생을 억제하여 사고확률을 저감시키는 것을 목적으로 한다.

4.2 자동열차제어장치의 안전필수 기능과 관련된 하부시스템

자동열차제어장치 하부시스템들에 대한 하부시스템별 특성을 표2에 나타내었다. 하부시스템의 고장률은 한국형 고속철도시스템 자동열차제어장치의 고장률을 대입하였으며, 평균수리시간(MTTR)은 1시간으로 하였다. 표2에서는 자동열차제어장치의 각 하부시스템의 고장빈도와 고장검지장치의 고장발생률은 식(7)을 이용하여 예측하였다.

표 2. 자동열차제어장치 각 시스템의 구성(안) 및 1시간동안(Δt) 고장확률

Table 2. Sub systems design proposals for ATC and probability of subsystems' failure for 1 hour

주요 기능	구성장치	입력 값	출력 값	하부시스템고장확률	고장검지장치 고장확률	위험 측 고장확률
환경검지장치	강우계	강수량	ON/OFF	1×10^{-4}	1×10^{-4}	1×10^{-8}
	강설계	강설량	ON/OFF	1×10^{-4}	1×10^{-4}	1×10^{-8}
	강풍계	풍속	ON/OFF	1×10^{-5}	1×10^{-5}	1×10^{-10}
장애물검지	도통전선절단	외부 힘	ON/OFF	1×10^{-1}	1	1×10^{-10}
철도원보호장치	ON/OFF Switch	외부 힘	ON/OFF	1×10^{-1}	1	1×10^{-10}
열차검지장치	ON/OFF Switch	레일단락	ON/OFF	1×10^{-1}	1	1×10^{-10}
속도계산	H/W & S/W	복수의 ON/OFF	정수 값	5×10^{-5}	5×10^{-5}	2.5×10^{-9}
속도전송	전자회로	정수 값	자기장	1×10^{-5}	1×10^{-5}	1×10^{-10}
속도수신	전자회로	자기장	정수 값	1×10^{-5}	1×10^{-5}	1×10^{-10}
속도현시	H/W 및 S/W	정수 값	정수 값 현시	5×10^{-5}	5×10^{-5}	2.5×10^{-9}
속도감시	전자회로 H/W 및 S/W	정수 값	ON/OFF	5×10^{-5}	5×10^{-5}	2.5×10^{-9}
기기제어	전자회로	정수 값	ON/OFF	1×10^{-5}	1×10^{-5}	1×10^{-10}

4.3 자동열차제어장치의 안전측 출력확률

n개의 하부시스템으로 구성된 시스템에서 서브시스템 i의 시스템 자체 고장률과 검지장치의 고장률을 앞에서와 같이 각각 $\lambda_i(t)$, $\lambda_{d,i}(t)$라고 정의하면 하부시스템의 상태는 다음과 같이 표시된다[3].

$$p_{NS,i}(t)=p_{NS,i}(T>t)=R_i(t)=\exp\left[-\int_0^t \lambda_i(\xi)d\xi\right] \tag{15}$$

$$p_{FU,i}(t)=p_{FU,i}(T>t)=Q_{FU,i}(t)=1-\exp\left[-\int_0^t \lambda_{FU,i}(\xi)d\xi\right] \tag{16}$$

$$\begin{aligned} p_{FS,i}(t) &= p_{FS,i}(T>t)=Q_{FS,i}(t) \\ &=\left(1-\exp\left[-\int_0^t \lambda_i(\xi)d\xi\right]\right)-p_{FU,i} \end{aligned} \tag{17}$$

위 식을 이용하여 한국형 고속철도시스템의 정상동작상태, 위험측 고장상태, 안전측 고장상태의 시간에 대한 시뮬레이션을 그림14에 나타내었다. 또한 그림15는 표2의 자동열차제어장치 안전관련 기능들에 대한 고장률을 대입하여 자동열차제어장치 전체의 위험측고장 발생을 시간에 따라 시뮬레이션한 결과를 제시하였다.

그림15와 같이 한국형 고속철도 자동열차제어장의 위험측 고장률은 약5000시간(약 6개월)을 정점으로 급속하게 감소하여 약25000시간(약 2년6개월)후에는 자동열차제어장치 안전성요구사항인 위험측고장률 $10^{-9}/h$를 만족함을 나타내고 있다.

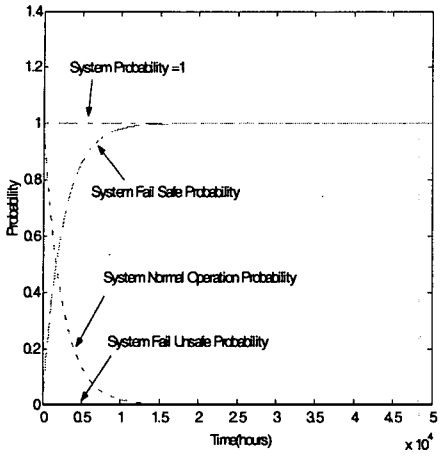

그림 14. 자동열차제어장치의 정상상태, 안전 측고장 및 위험측 고장확률(5년기준)

Fig. 14. Normal sate, Fail-safe sate, Fail-unsafe state rate for ATC

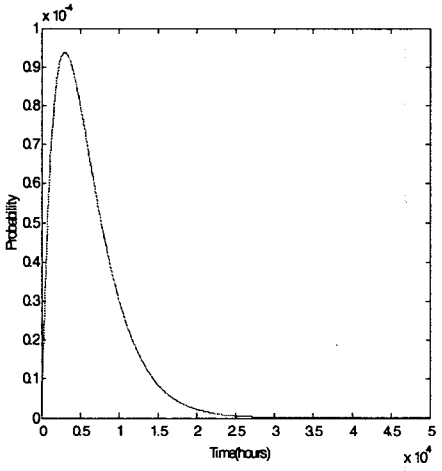

그림 15. 자동열차제어장치의 위험측 고장확률

Fig. 15. Dangerous Failure rate for ATC

5. 결 론

본 논문은 안전필수시스템인 자동열차제어장치의 안전관련 기능들에 대하여 안전성 요구사항인 위험측고장률 $10^{-9}/h$를 만족시키기 위해서 자동열차제어장치에 대한 안전측고장 및 위험측고장을 정의하고, 결함검출을 위한 검지회로를 내장한 하부시스템들에 하부시스템 자체와 검지회로내의 고장발생시 시스템 위험측 고장률을 제시하였다.

이러한 자동열차제어장치 위험측 고장률산출의 정량적인 접근은 각각의 하부시스템에 대하여 전체시스템 안전측 고장률목표 만족을 위한 하부시스템별 목표치 할당에 용이하며, 컴퓨터로 안전필수 기능을 다른 분야 제어장치의 하부시스템 위험측 고장률 할당에도 활용이 가능하다.

향후 연구과제는 안전성목표달성을 위한 시간과 설계복잡도를 효율적으로 선택하여 하부시스템의 고장률과 검지회로에 대한 고장률할당에 대한 연구가 필요하다.

부 록

$\lambda_i(t)$: 서브 시스템 i의 고장율

$\lambda_d(t)$: 고장억제 및 고장검출 장치의 고장율

$\lambda_{d,i}(t)$: 서브시스템 i에서 고장검출장치의 고장율

$\lambda_{FU,i}(t)$: 서브시스템 i에서 위험측 고장율

$\lambda_{FS,i}(t)$: 서브시스템 i에서 안전측 고장율

C : 결함검출능력(Fault Coverage Rate)

$p_{FSO}(t)$: 주어진 시간 t에서 시스템이 안전하게 동작할 확률

$p_{FS}(t)$: 주어진 시간 t에서 시스템이 안전 측으로 작동할 확률

$p_{NS}(t)$, $R(t)$: 주어진 시간 t에서 시스템이 정상적으로 작동할 확률

$p^k_{FU}(t)$: 하부시스템 k가 위험측 출력확률

$p^k_{FS}(t)$: 하부시스템 k가 안전측 출력확률

$p^k_{NS}(t)$: 하부시스템 k가 정상 출력확률

$p_i(\Delta t)$: 서브시스템 i에서 Δt 시간 동안에 고장이 발생할 확률

참 고 문 헌

[1] Defence Standard 00-58, 'HAZOP Studies on System Containing Programmable Electronics', 2000

[2] KTGV Contracts, KHRC, part TCS, 1993

[3] 鐵道總研, 'コンピュ -タ 制御信號 システムの安全性・信賴性技術', 教育資料

[4] Barry W. Johnson, 'Design and Analysis of Fault-Tolerant Digital Systems', Addison-Wesley, 1989

[5] Dhiraj K. Pradhan, 'Fault-Tolerant Computer System Design', Prentice-Hill, pp135~235, 1996

[6] Richard E. Harper et al., 'Fault-Tolerant Parallel Processor', J. Guidance, Vol 14, NO. 3, 1990

[7] 이재호 et al., '신호설비유지보수 효율화를 위한 정보전송방식 기술연구', 철도청, 용역연구보고서

[8] R. Ramkumar, Engineering Reliability : Fundamentals and Applications, prentice Hill

저 자 소 개

신 덕 호(辛 德 浩)

1975년 4월 1일생. 1998년 광운대학교 제어계측공학과 졸업, 2000년 광운대학교 제어계측공학과 대학원 석사, 2002년 광운대학교 제어계측공학과 박사수료, 2002년-현재 한국철도기술연구원 전기신호연구본부 주임연구원

이 종 우(李 鍾 宇)

1959년 3월 20일생. 1983년 한양대학교 공과대학 기계설계과 졸업, 1986년 Ecole Centrale de Nantes 석사, 1993년 Universite de Paries VI 공학박사, 서울산업대학교 교수