열차집중제어장치와 전자연동장치 인터페이스의 안전성평가에 관한 연구

論 文
54B-7-1

A Study on Safety Assessment of CTC/EI Interface

申 碩 均† · 李 其 西*
(Seok-kyun SHIN · Key-seo LEE)

Abstract - In this paper we analyzed a dangerous failure and a safety requirement based on HIA (Hazard Identification and Analysis) of an interface model between CTC (Centralized Traffic Control) system and EI (Interlocking) system, and assigned SIL (Safety Integrity Level) by way of an risk estimation of the interface, which employed PHA (Preliminary Hazard Analysis) for the interface of the track control system, being managed as separated system between the centralized traffic control system and the interlocking system, An estimation which satisfies a safety reference of the international standard has been achieved through a quantification of the system failure rate and the dangerous failure rate of the interface model.

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

1. 서 론

본 논문은 열차집중제어장치(CTC, Centralized Traffic Control System)와 전자연동장치(EI, Electronic Interlocking)로 구성된 열차진로제어시스템에서 사령실에 설치되어 열차의 운영을 총괄하는 CTC와 지역역에 설치되어 열차의 진로를 제어하는 전자연동장치의 인터페이스에 대한 안전성평가를 수행하였다.

열차진로제어시스템은 열차가 진행할 진로 상에 있는 분기기를 진행하는 방향으로 전환하여 열차나 차량이 완전히 통과할 때까지 분기기를 쇄정하는 것을 의미하며, 동일한 진로에 다른 차량이 진입하는 일이 없도록 정차장 내의 안전을 확보하고 열차 운전업무의 효율을 높이는 설비이다.[1] 이러한 진로제어 제어설비를 구성하는 열차집중제어장치와 전자연동장치는 열차진로제어라는 하나의 시스템기능을 수행하면서, 각각의 시스템 크기가 광범위하여 국내외적으로 열차집중제어장치와 전자연동장치를 독립된 시스템으로 분류하고, 예비위험원분석을 통한 리스크평가의 차이가 있을 수는 있으나, 대부분 안전무결성레벨이 열차집중제어장치는 2, 전자연동장치는 4를 기준으로 관리되고 있다. 안전무결성 레벨은 1부터 4까지의 4단계로 분류하며, 시스템으로부터 발생될 수 있는 사고의 크기와 빈도가 높을수록 4에 가깝다.[2]

위와 같은 열차집중제어장치와 전자연동장치의 분리관리는 시스템의 구축을 별도의 사업으로 추진하는 과정으로 인한 결과로도 볼 수 있으며, 따라서 각 시스템의 인터페이스 설계 시에 별도의 안전관리가 절실히 요구된다.

본 논문에서는 진로제어시스템의 인터페이스구성 및 철도분야 안전 활동에 대한 개략적인 서술을 포함하며, 열차집중제어장치와 전자연동장치 인터페이스의 모델링 및 인터페이스의 예비위험원분석(PHA, Preliminary Hazard Analysis)을 통한 리스크를 평가하고 모델의 위험원도출 및 분석(HIA, Hazard Identification and Analysis)을 수행하여 목표안전레벨의 만족여부를 평가하였다.

2. 본 론

2.1 진로제어시스템의 구성

열차진로제어설비의 고장은 위험측으로 발전하여 사고로 이어지는 경우에, 열차의 탈선, 충추돌 등의 심각한 결과를 초래할 수 있으므로 철도신호분야에 대표적인 안전필수 설비이다.

본 절에서는 열차집중제어장치와 전자연동장치에 대한 개략적인 정의 및 역할과 진로제어를 위한 명령의 데이

† 교신저자, 正會員 : 광운대학교 제어계측공학과 박사과정
E-mail : elmo@microtrack.co.kr
* 正 會 員 : 광운대학교 제어계측공학과 교수
接受日字 : 2004年 8月 9日
最終完了 : 2004年 12月 31日

터호름 그리고 이러한 명령과 데이터의 전송을 위한 인터페이스에 대하여 서술하였다.

1) 열차집중제어장치(CTC)

열차집중제어장치는 광범위한 구간 내를 운행하는 다수의 열차를 한곳의 종합사령실에서 자동으로 원격 제어하여 그 구간 내의 열차를 일괄 통제하고 조정한다.[1]

열차집중제어장치의 대표적인 기본기능은 트래픽관리, 이벤트관리, 이벤트경고, 열차표시 그리고 외부인터페이스 관리이다. 이러한 기능 중 본 논문의 논점은 열차집중제어장치와 전자연동장치의 인터페이스이다. 기존의 인터페이스는 열차집중제어장치의 하부시스템인 데이터전송장치(DTS, Data Transmission System)를 통해 중앙데이터전송장치(CDTS, Central Data Transmission System)로부터 역에 설치되어 전자연동장치와 인터페이스 하는 지역데이터전송장치(LDTS, Local Data Transmission System)로 구성되어, 진로요구, 운전모드의 전환, 지역데이터전송장치의 계절체 명령 등이 전송되며, 명령수행의 결과 및 현장의 상태는 지역데이터전송장치로부터 중앙데이터전송장치로 다시 전송된다.

2) 전자연동장치(EI)

전자연동장치는 현장의 신호기와 선로전환기를 사용하여 열차의 진로를 물리적으로 제어하며, 궤도회로를 통해 역구내 열차의 위치를 추적하는 기능을 수행한다.

진로제어는 열차집중제어장치로부터 요구되거나 역의 표시제어부로부터 입력되는 진로취급요구에 의해 연동논리에 의한 취급을 수행하고 표시데이터를 열차집중제어장치 및 표시제어부로 전송한다.

3) 열차집중제어장치와 전자연동장치 인터페이스

열차집중제어장치와 전자연동장치의 인터페이스를 위해 설치되는 지역데이터전송장치의 사용은 연동장치 발전과정과 밀접한 관계를 갖는다. 초기에 열차의 위치를 궤도회로로 입력받아 선로전환기와 신호기를 통해 열차의 진로를 제어하는 기능을 기존에는 비교적 높은 신뢰성이 입증된 신호용 계전기를 사용한 시퀀스 논리회로를 통해 연동논리를 구현하였다. 이러한 기존의 구성을 갖는 전기연동장치를 열차집중제어장치 개념의 도입에 따라 중앙 사령에서 제어 및 감시하기 위해 지역데이터전송시스템을 사용하여 직렬통신으로 인터페이스 하는 그림1과 같은 구조로 발전되었다. 따라서 열차집중제어장치로부터의 제어정보와 전자연동장치로부터의 표시정보는 중앙데이터전송시스템과 지역데이터통신시스템 간에는 직렬통신을 통해 전송되고, 전자연동장치와의 인터페이스도 직렬통신데이터로 인터페이스 한다.

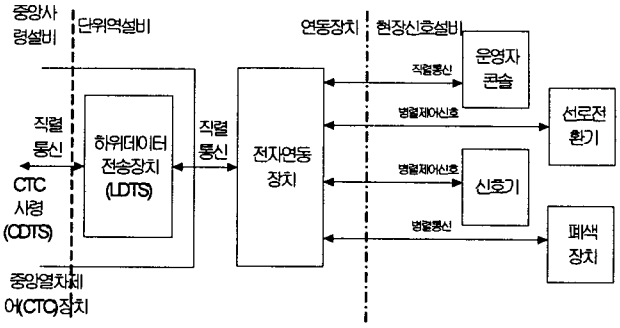

그림 1 CTC와 EI 인터페이스

Fig. 1 Interface between CTC and EI

이러한 구성은 기존의 전기연동장치가 설치된 역에 필수적으로 요구되며, 신설역 및 전자연동장치가 설치된 역에서는 전자연동장치의 직렬데이터 통신을 통해 입력받을 수 있는 CDTS정보를 LDTS를와 EI의 인터페이스에 의해 VME 버스신호로 변환하여 연동처리를 수행하도록 설계된다.

2.2 철도시스템 안전성활동

안전성활동은 대상시스템으로 인해 발생할 수 있는 사고를 예측하여, 사고의 크기와 빈도에 해당하는 리스크(Risk)를 사회적으로 받아들일 수 있는 수준으로 완화시키기 위한 활동이다. 따라서 안전성활동의 단계는 시스템 예비위험원분석(PHA, Preliminary Hazard Analysis), 위험원도출 및 분석(HIA, Hazard Identification and Analysis), 사고시나리오 예측, 위험측고장정의, 안전대책수립을 통해 체계적인 리스크의 평가 및 관리를 수행한다. 다음은 각 단계별 세부사항을 정리한 내용이다.

안전성평가는 평가된 리스크를 허용할 수 있는 범위로 완화시키기기 위해 사용된 안전대책들이 안전무결성레벨의 범위 안에 있는지를 확인하는 과정이다.

2.2.1 예비위험원분석(PHA)

예비위험원분석은 대상시스템의 기능적인 측면을 대상으로 대표적 사고 및 위험원을 정의하여, 정의된 위험으로 인한 사고의 리스크를 평가하고, 안전대책적용 후의 리스크를 평가하여 안전대책으로 인해 리스크를 얼마나 완화시킬 수 있는지를 검토하는 단계이다. 예비위험원분석단계에서는 위에서 기술한 바와 같이 시스템의 개략적인 기능요구사항만을 토대로 하며, 하부시스템의 상세설계단계의 정보를 요구하지 않는다. 따라서 제시되는 안전대책들도 설비보완, 안전대책수립, 교육체계수립 등의 개념적인 대책들만을 제시한다. 따라서 예비위험원분석은 프로젝트의 생성초기에 수행되어야 하며, 기본적인 사용자 요구사항(UR, User Requirement)을 토대로 수행하여 하부시스템 기능요구사항 및 안전요구

사항 작성 시에 참조로 사용해야 한다. 그림 2는 일반적인 예비위험원분석지의 양식이다.

시스템 영 : CTC/EI 인터페이스										
시스템 번호		작업기간	2일	작성날짜	2004.12.30 2005.01					
분석단계		최초 : ?		수정 : ?	부가 : ?					
위험원 번호	위험원 내용	위험원 대상	사고 심각도	발생 빈도	위험도 크기	대책안 : D : 설계변경, E : 안전대책, S : 안전소자, W: 경고체제, P : 절차/교육	대책안 실시 후			
							사고 심각도	발생 빈도	위험도 크기	
HN001		N	B	3	3B (II)		C	4	4C (III)	
HN005		N	B	4	4B (III)		D	4	4D (IV)	

그림 2 예비위험원분석 문서화 양식
Fig. 2 PHA Documentation Form

2.2.2 위험원도출 및 분석(HIA)

위험원도출 및 분석은 대상시스템으로 인한 사고의 원인이 되는 위험원을 도출하고 분석하여 안전대책을 수립하는데 목적이 있다. 따라서 본 단계는 시스템의 세부설계 및 하부시스템 기능할당 그리고 설계과정과 병행된다. 그러므로 본 단계를 통한 안전대책은 매우 기술적이며, 안전대책으로 인한 안전성의 향상도 정량적으로 제시된다.

위험원의 도출과 분석에는 각각 여러 가지 기법들이 사용된다. 위험원도출을 위한 기법은 "그렇다면 무엇이 나타나는가(What if)", 시스템 부품간의 상호작용을 관찰하는 "부분분석", 무엇과 어떻게 연관하여 "검사항목"을 제정하는 방법, 시스템의 기능고장과 고장의 영향을 분석하는 "FMEA" 방법 및 부품과 부품간의 상호작용을 조사하고, 설계영역에서 벗어나는 요소를 조사하여, 원인과 결과의 연관관계를 조사하는 HAZOP(Hazard and Operability)이 있다.[4][5] 또한 도출된 위험원의 분석을 위해서는 FTA(Fault Tree Analysis)와 ETA(Event Tree Analysis)가 마찬가지로 상호보완적으로 사용된다.

본 논문에서는 모델링된 인터페이스의 위험원도출을 위해 HAZOP을 사용하였으며, 도출된 위험원의 분석을 위해서는 FTA를 사용하였다.

2.2.3 사고시나리오에 의한 위험측고장정의

본 단계는 위험원도출 및 분석단계와 별도의 단계로 분류하지만 매우 밀접한 연관관계를 가지고 있다. 위험원도출 및 분석에 의해 위험원이 정의된 사고로 전이되는 과정을 파악할 수 있으며, FTA를 통한 분석데이터를 바탕으로 구성요소 또는 기능의 위험원발생으로 인한 사고발생까지의 데이터를 통해 위험측고장을 정의하고, 정의된 위험측고장의 발생확률을 정량적으로 예측한다. 또한 사고의 크기와 빈도에 해당하는 리스크를 평가하여 안전무결성레벨을 할당하고, 필요에 따라서는 하부시스템단위별로 안전무결성레벨을 할당한다.

2.2.4 안전대책 수립

표 1과 표 2와 같이 시스템 또는 하부시스템단위로 할당된 안전무결성레벨(SIL, Safety Integrity Level)에 따라서 성능측면 및 안전측면의 고장률관리를 수행한다.[2]

표 1 안전무결성레벨에 따른 성능측면의 고장률
Table. 1 Based Failure-rate with SIL in Performance

SIL	성능측면의 고장률(/Hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

표 2 안전무결성레벨에 따른 위험측면의 고장률
Table. 2 Based Dangerous Failure-rate with SIL in Performance

SIL	안전측면의 위험측고장률(/Hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

수립된 안전대책은 안전무결성레벨에서 정의하는 시스템 또는 하부시스템 위험측고장률이 허용등급 안에 있도록 관리하는 것으로, 설계단계에서는 권고데이터의 형식으로, 시스템 도입 후에는 시간에 따라 고장률이 변화하는 하드웨어 시스템 등의 요인에 따라 안전성유지를 위한 활동주기 등의 데이터를 제공한다.

2.3 열차집중제어장치와 전자연동장치 인터페이스 안전성평가

본 논문에서 제시하는 안전성평가를 위해서는 열차집중제어장치와 전자연동장치의 인터페이스를 모델링해야 한다. 인터페이스모델은 현재 한국철도공사에 구축되어 있는 시스템의 설계를 최대한 반영하였으며, 안전성평가를 위하여 국내에는 수행된 적인 없는 열차집중제어장치와 전자연동장치 인터페이스에 대한 안전성활동도 수행하였다.

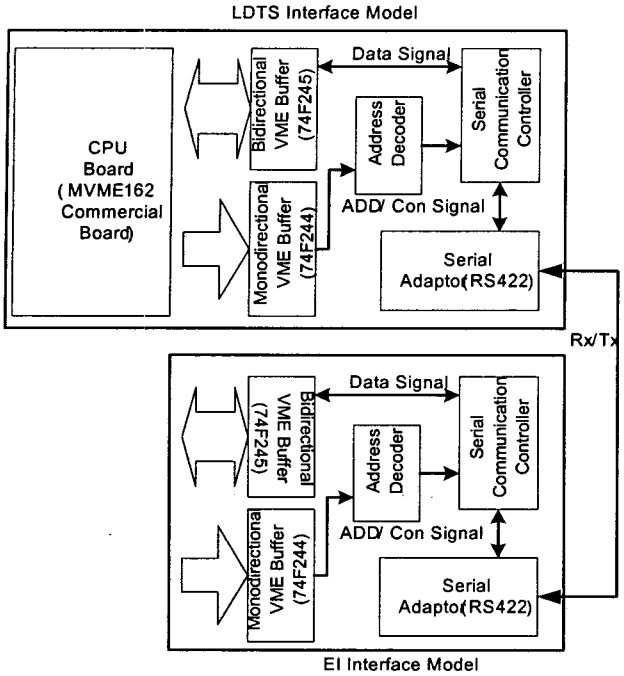

그림 3 인터페이스모델의 구성도
Fig. 3 Specific Diagram of Interface Model

2.3.1 인터페이스 모델링

열차집중제어장치와 전자연동장치 인터페이스의 구성은 그림 1을 바탕으로 하였으며, 안전성평가를 위한 인터페이스 부분의 상세구조는 그림 3과 같이 모델링하였다.

2.3.1.1 열차집중제어장치측 인터페이스모델

중앙데이터전송시스템과 직렬 통신하여 전자연동장치와 인터페이스 하는 지역데이터전송시스템의 구성은 다음과 같다.

- 중앙데이터전송시스템으로부터 RS422통신으로 데이터를 송수신한다.(CPU보드와는 VME인터페이스)
- 지역정보전송시스템은 자체의 CPU보드를 갖는다.(모토롤라사의 MVME162)
- 전자연동장치와 RS422통신으로 데이터를 송수신한다.(CPU보드와는 VME인터페이스)

위 지역정보전송시스템 모델을 구성하는 부품들은 표3과 같으며, MIL-HDBK-217을 통한 고장률의 예측치를 함께 표시하였다. 단위 부품의 고장률 예측치는 위험측고장률의 정량화에 사용된다.

2.3.1.2 전자연동장치측 인터페이스모델

한국철도공사에서 사용하는 전자연동장치는 규격화가 되어있다. 따라서 본 논문에서는 한국철도공사에서 사용하는 전자연동장치 사양을 근거로 열차집중제어장치와의 인터페이스에 해당하는 부분을 다음과 같이 모델링하였다.

- 열차집중제어장치와 RS422통신으로 데이터를 송수신한다.(CPU보드와는 VME인터페이스)

또한 인터페이스의 모델링에는 다음과 같은 전제조건을 사용한다.

- 모델링된 인터페이스에 공급되는 전원공급장치는 모델에서 제외한다.
- 열차집중제어장치 지역정보전송시스템의 소프트웨어는 요구되는 안전무결성레벨에 부합하도록 설계되어, 안전성활동에서 제외한다.

위 전자연동장치 인터페이스모델을 구성하는 부품들은 표 3의 'EI 인터페이스'와 같으며, MIL-HDBK-217을 통한 고장률의 예측치를 함께 표시하였다. 단위 부품의 고장률예측치는 위험측고장률의 정량화에 사용된다.

표 3 LDTS/EI 인터페이스모델의 구성품과 고장률
Table. 3 Components and Failure-rate of LDTS/EI Interface Model

구성품	수량	Unit고장률(10e-6)	고장률(10e-6)
인터페이스 모델	1		1.287305
1. EI 인터페이스	1		1.143652
- SCC	1	0.004089	0.004089
- ADD Decoder	1	0.004254	0.004254
- VME Adaptor	4	0.032842	0.131370
- Serial Bridge	1	0.003939	0.003939
2. LDTS 인터페이스	1		1.143652
- CPU Board	1	1.000000	1.000000
- VME Adaptor	4	0.032842	0.131370
- SCC	1	0.004089	0.004089
- ADD Decoder	1	0.004254	0.004254
- Serial Bridge	1	0.003939	0.003939

Note. ADD : Address
SCC : Serial Communication Controller

2.3.2 인터페이스모델의 예비위험원분석

모델링된 열차집중제어장치와 전자연동장치의 인터페이스에서 발생되는 위험원으로 인한 대표적 사고는 표 4와 같다.

자동열차제어장치와 전자연동장치에서 표 4에서와 같이 인터페이스에서 발생되는 열차위치정보관련 위험측고장에 의해 열차지연사고까지 발생시킬 수 있다. 따라서 4가지 위험원에 대하여 예비위험원분석을 실시하면 표 5와 같다.

표 4 인터페이스모델의 대표적사고와 위험원
Table. 4 Accidents and Hazard log of the Interface Model

사고	위험원	번호
열차지연	CTC모드와 지역모드 변경기능의 오류	PHA01
	EI에 의한 열차위치정보가 안전측으로 오동작	PHA02
	EI에 의한 선로전환기 위치정보 오류	PHA03
	EI에 의한 열차위치정보가 위험측으로 오동작	PHA04

예비위험원분석에서 안전대책실시전과 실시 후에 위험원에 대한 사고의 심각도 및 발생빈도는 리스크매트릭스방식을 사용한 것으로써, 위험도의 크기가 I-II는 반드시 리스크를 완화하여야 하며, III-IV는 적용이 가능한 시스템의 리스크이다.

표 5 인터페이스 모델의 예비위험원분석
Table. 5 PHA of the Interface Model

시스템 명 : CTC/EI 인터페이스									
시스템번호		작업기간	1일	작성날짜	2005.02.26 2005.02				
분석단계		최초 : ?		수정 : □	부가 : □				
위험원번호	위험원내용	위험원대상	사고심각도	발생빈도	위험도크기	대책안: D : 설계변경, E : 안전대책, S : 안전소자, W: 경고체제, P : 절차/교육	대책안 실시 후		
							사고심각도	발생빈도	위험도크기
PHA01	모드전환오류	N	B	3	3B (II)	D : 모드변경정보의 복조화 P : 운영인력의 지역모드 변경절차 수립	C	4	4C (III)
PHA02	궤도점유안전측오류	N	B	4	4B (III)	D : 궤도점유정보 전송의 오류검지 P : 비정상점유시 확인절차 수립	D	4	4D (IV)
PHA03	선로전환기정보오류	N	B	4	4B (III)	D : 선로전환기 전환정보 전송의 오류검지 P : 불일치정보 입력시 확인절차 수립	D	4	4D (IV)
PHA04	궤도점유위험측오류	N	B	4	4B (III)	D : 궤도점유정보 전송의 오류검지 P : 불일치정보 입력시 확인절차 수립	D	4	4D (IV)

이러한 리스크의 평가는 별도의 한 분야이며, 본 논문에서는 리스크의 완화가 가능함을 보이기 위해 사고의 발생빈도를 감소시키는 대책안을 통해 리스크의 완화를 보이고 있다.

2.3.3 인터페이스모델의 위험원도출 및 분석

위험원의 도출은 설계사양을 바탕으로 발생할 수 있는 위험원을 확인하는 과정이다. 전체 시스템에 대한 위험원도출은 기능사양, 인터페이스사양, 운영시나리오의 3가지 측면으로 실시하지만, 본 논문의 범위인 인터페이스사양을 토대로 HAZOP Study를 통해 위험원을 도출하였다.[4][5]

HAZOP Study는 기능 또는 구성품단위로 나눠진 요소(Element)에 대하여 표 6과 같은 Guide Word에 따른 구성요소(또는 기능)의 일탈행위에 따라 결과를 예측해 보고, 각각의 결과에 대한 안전대책을 수립하는 작업이다.

표 6 일반적인 Guide Word
Table. 6 General Guide Word

Deviation Type	Guide word	의미	접점 I/F의 예
부정	No	명령이 실행되지 않는 상태	접점이 동작 안됨
정량적 변형	More	수량의 비정상증가	궤환된 접점전압상승
	Less	수량의 비정상감소	궤환된 접점전압하강
정성적 변형	As well as	기대하지 않은 동작수행	다른 접점 동작
	Part of	완전한 수행을 하지 못함	조건의 접점을 모두 살리지 못함
대체	Reverse	목적과 반대되는 결과도출	반대 접점 동작
	Other than	목적과 다른 결과도출	다른 접점 동작
시간	Early	예상시간보다 일찍 발생	접점동작시간이 빠름
	Late	예상시간보다 늦게 발생	접점동작시간이 늦음
명령 또는 흐름	Before	예상순서보다 일찍 발생	순차적 접점에서 빨리 동작
	After	예상순서보다 늦게 발생	순차적 접점에서 늦게 동작

HAZOP Study를 위한 요소는 다음과 같이 분류할 수 있다.[6]

- 구성품에 의한 분류
  - 송수신 어댑터(RS422 Bridge)
  - 직렬통신디바이스(SCC, Serial Communication Controller)
  - VME 버스 어댑터(buffer 74F244, 74F245)
  - 어드레스 디코더(74F139)
  - CPU보드(MVME162)

- 기능사양 및 운영시나리오에 의한 분류

- 열차집중제어장치로부터 진로요청
- 전자연동장치로부터 진로설정완료
- 전자연동장치로부터 궤도점유정보
- 전자연동장치로부터 지역모드신청
- 열차집중제어장치로부터 지역모드허가

기능사양 및 운영시나리오에 대하여 HAZOP Study를 수행하여 표 7과 같은 결과를 도출하였다.

도출된 위험원에 대한 분석은 그림 4와 같이 FTA기법을 사용하여, 인터페이스모델에서 위험원이 발생할 확률을 표 8과 같이 계산하였다. 시스템 부품단위 고장률예측 및 FTA를 통한 위험측고장률의 산출은 상용소프트웨어인 Relex (v7.6)를 사용하였다.

표 7 HAZOP Study

Table. 7 HAZOP Study

HAZOP Study 대상: CTC/EI 인터페이스						
참조도면번호.:			**갱신번호.:**		**소요시간:**	
참여구성원:					**회의일시:**	
기능	Guide Word	이상현상	원인	결과	안전대책	세부조치내역
CTC 진로요청	No	진로요청이 전달되지 않음	표8에 정리	열차지연	LDTS정보오류 자기진단	HIA 01
	As well AS	입력진로와 다른 진로 요청		열차지연	LDTS정보오류 자기진단	HIA 02
	Part of	완전한 진로요청의 실패		열차지연	진로요청 궤환 입력 후 확인	HIA 03
	Reverse	진로요청대신 해정을 전달		열차지연	LDTS자기진단	HIA 04
	Late	목표시간보다 늦게 요청		열차지연	쇄정소요시간 감시 및 처리	HIA 05
EI진로요청 완료	No	진로설정완료 전달실패		열차지연	인터페이스의 정보오류 자기진단	HIA 06
	As well AS	다른 진로설정완료 전달		재전송	완료정보 재전송	HIA 07
	Part of	완전한 진로설정 전송실패		열차지연	일정시간 대기 후 재전송요구	HIA 08
	Late	목표시간보다 늦게 전송		열차지연	일정시간 대기 후 재전송요구	HIA 09
궤도점유정보	No	궤도점유정보 전송실패		열차지연	열차위치 전송후 확인절차	HIA 10
	As well AS	다른 궤도점유정보 전송		열차지연	열차위치 전송후 확인절차	HIA 11
	Part of	완전한 궤도점유정보 전송실패		열차지연	열차위치 전송후 확인절차	HIA 12
	Late	목표시간보다 늦게 전송		열차지연	열차위치 전송후 확인절차	HIA 13
EI 모드변경	No	모드변경 요구전송실패		열차지연	전송실패시 지역제어절차	HIA 14
	Part of	완전한 모드변경 전송실패		열차지연	전송실패시 지역제어절차	HIA 15
	Late	목표시간보다 늦은 모드변경		열차지연	전송실패시 지역제어절차	HIA 16

표 8 위험원별 사고크기와 위험측고장률

Table. 8 Risk and Dangerous Failure Rate of Hazard

위험원번호	위험측고장	SIL 할당	위험측고장 발생확률
HIA01		2	
HIA02		2	
HIA03		2	
HIA04	*단일고장조건	2	
HIA05	-LDTS Serial Bridge고장	2	
HIA06	-EI Serial Bridge고장	2	
HIA07	-LDTS CPU고장	2	
HIA08		2	
HIA09	*복합고장조건	2	1.00738e-8
HIA10	-LDTS VME Adaptor고장 AND LDTS SCC고장	2	
HIA11	-EI SCC고장 AND EI VME Adaptor고장	2	
HIA12		2	
HIA13		2	
HIA14		2	
HIA15		2	
HIA16		2	

2.3.4 인터페이스모델의 안전성평가

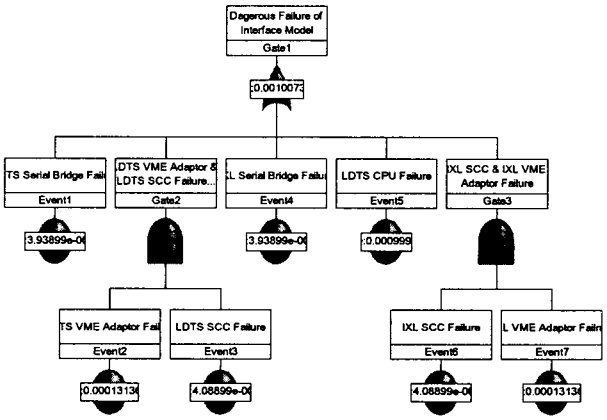

그림 4 인터페이스모델 위험측고장의 FTA

Fig. 4 FTA of the Dangerous Failure in the Interface Model

위험원도출 및 분석을 수행하여 수집된 정보를 정량적으로 계산하면 열차집중제어시스템과 전자연동장치 인터페이스 모델의 위험측고장률 1.00783e-8은 예비위험원분석을 통해 제시된 안전무결성레벨(SIL) 2의 위험측고장률 요구사항(표 2 참조)을 만족하며, 그림 5의 인터페이스모델 평균고장률 약13e-7도 성능측면의 시스템고장률 요구사항(표 1 참조)을 만족하였다.

2.3.5 인터페이스모델의 위험측고장률 시뮬레이션

위험측고장은 FTA에 의해 계산되었으며, 계산된 값을 시간에 의해 시뮬레이션 하면 표 10과 같다.

MIL-HDBK-217에 의한 고장률은 상수로 정의되지만 신뢰도는 시간의 흐름에 따라 감소한다. 그림 6은 표 10에서

나타낸 인터페이스모델 위험측고장의 FTA에 대한 시간에 따른 신뢰도의 변화이다.[3]

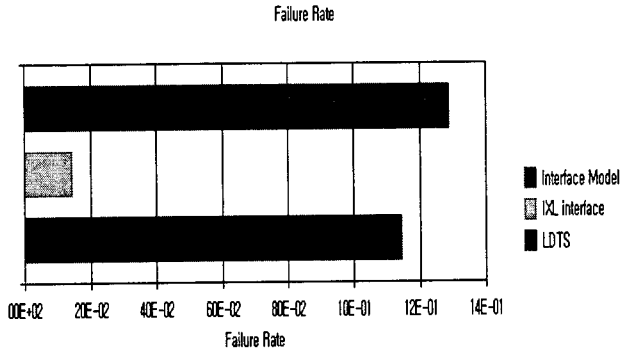

그림 5 인터페이스 모델의 고장률

Fig. 5 Failure Rate of the Interface Model

따라서 설계에 대한 안전성평가가 기준을 만족해도, 위험측고장률의 시간에 따른 예측치를 유지보수에 적용하여 시스템안전성을 유지시키는 것도 매우 중요하다.

표 9 안전필수시스템의 신뢰도 요구사항

Table. 9 Reliability Requirement of the Safety Critical System

SIL	MTBF(/Hour)
4	100,000 to 10,000
3	10,000 to 1,000
2	1,000 to 100
1	100 to 10

Note. Repair Rate을 무시하여 MTTR=0Hour로 가정한 수치

표 10 시간에 따른 신뢰도

Table. 10 Reliability with Time

시간(Hour)	인터페이스모델의 신뢰도	위험측고장의 신뢰도
0	1.0000	1.0000
10000	0.8792	0.9990
20000	0.7730	0.9980
30000	0.6796	0.9970
40000	0.5975	0.9960
50000	0.5254	0.9950
60000	0.4619	0.9940
70000	0.4061	0.9930
80000	0.3571	0.9920
90000	0.3139	0.9910
100000	0.2760	0.9900

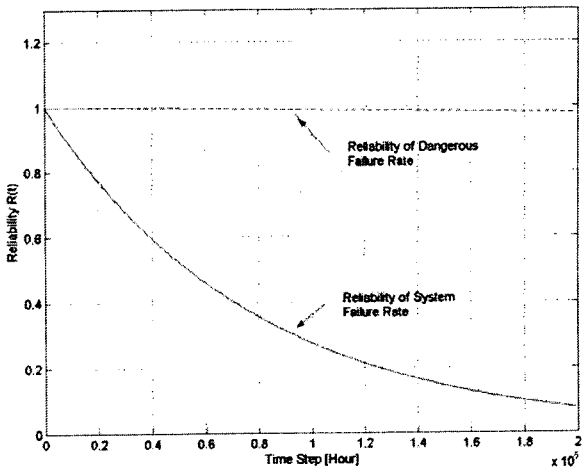

그림 6 위험측고장과 일반고장률에 의한 신뢰도

Fig. 6 Reliability of the System Failure-rate and the Dangerous Failure-rate

3. 결 론

본 연구는 열차집중제어장치와 전자연동장치의 별도시스템으로 관리되는 진로제어시스템의 인터페이스에 대한 예비위험원분석(PHA)을 수행하여, 인터페이스에 대한 리스크 평가를 통해 안전무결성레벨(SIL)을 할당하였으며, 인터페이스를 모델링하여 모델의 위험원도출 및 분석(HIA)을 통해 안전대책제시 및 위험측고장을 분석하였다.

또한 모델의 시스템고장률과 위험측고장률을 정량화시켜 관련국제규격에서 제공하는 안전기준치를 만족함을 평가하였으며, 시간의 흐름에 따른 시스템안전성관리를 위하여 위험측고장률의 시간에 따른 변화를 시뮬레이션 하였다.

이러한 연구는 시스템단위의 안전성활동 뿐만 아니라 시스템 간의 인터페이스에서 발생할 수 있는 사고의 원인에 대한 안전성활동의 중요성을 제시한 연구이며, 추후 대규모 시스템의 상호인터페이스에도 이러한 활동이 적용되어야 한다.

참 고 문 헌

[1] 김영태 저, 2003 "신호제어시스템", P86-99, 2003

[2] International Standard IEC61508 "Functional Safety of Electrical/Electronic/Programmable electronic Safety-related systems", Part 1 "General Requirements", P65, 1998

[3] Jan Pukite, "Modeling for Reliability Analysis", IEEE Press, P38-39, 1998

[4] Felix Redmill et al. "System Safety : HAZOP and Software HAZOP", John Wiley & Sons, P72-104, 1999

[5] Defence Standard 00-58, "HAZOP Studies on System Containing Programmable Electronics", P5-P25, 2000

[6] International Standard IEC61882 "HAZOP Studies - Application guide", P10-P21, 1999

저 자 소 개

신 석 균(申 碩 均)

1972년 10월 29일생. 1996년 광운대학교 제어계측공학과 졸업, 1999년 광운대학교 제어계측공학과 석사, 2002년 6월 : 광운대학교 제어계측공학과 박사수료 (주)마이크로트랙 RAMS 사업부 책임연구원

이 기 서(李 其 西)

1951년 1월 18일생. 1977년 연세대학교 전기공학과 졸업, 1979년 연세대학교 전기공학과 석사, 1986년 2월 연세대학교 전기공학과 박사 광운대학교 정보제어공학과 정교수