

## 안전필수철도신호 선로전환기 제어모듈의 위험축고장을 예측에 관한 연구

박영수  
건설교통부

이재호 신덕호  
한국철도기술연구원

### A Study on the Dangerous Failure Rate Prediction of Point Machine for Railway Signalling Safety Critical System

Young Soo PARK  
Ministry of Construction & Transportation

**Abstract** - 본 논문은 듀얼듀플렉스구조로 설계된 한국형 고속철도 열차제어시스템의 전자연동장치 선로전환기 제어모듈에 대하여 안전성활동 체계에 따라 위험원을 도출하고 분석하여 선로전환기 제어모듈에 대한 위험축고장을 예측하였다. 시스템으로 인해 발생할 수 있는 리스크를 분석하여 리스크를 완화하기 위한 안전대책의 수준인 안전무결성레벨에서 제시하는 정량적인 기준을 만족하기 위한 위험축고장을 예측을 선로전환기 제어모듈을 대상으로 연구하였다.

#### 1. 서 론

선로전환기는 열차의 진로를 제어하는 철도신호용품으로써 선로전환기를 제어하는 모듈에 위험축고장이 발생하는 경우 열차의 탈선 및 충돌을 발생시킬 수 있는 안전필수 시스템이다. 이러한 안전필수시스템은 제어기로부터 발생될 수 있는 사고 및 위험원을 도출하고, 도출된 위험원을 발생시킬 수 있는 시스템레벨 또는 하부 시스템에 안전대책을 수립하여 관리해야한다.[1] 외국 시스템의 경우 시스템으로 발생될 수 있는 위험원을 제시하고, 제시된 위험원에 대하여 위험축고장을 제시하고 있다. 하지만 국내 철도신호분야의 경우 위험축을 설정하기 위한 안전성활동 체계가 적립중에 있으며, 철도신호관련 국제규격에서 안전무결성레벨에 따라 정량적으로 제시[2]하는 위험축고장을 만족여부를 판단하기 위한 세부적인 활동 사례가 전무한 상태이다. 따라서 본 논문에서 선로전환기 제어모듈을 대상으로 시스템레벨의 예비 위험원분석과 구성요소레벨의 위험원도출 및 분석을 통해 하부시스템으로부터 발생할 수 있는 위험원으로부터 사고로 발전되는 빈도 및 사고발생 후의 심각도를 완화하기 위한 안전대책을 제시하였으며, 제시된 안전대책을 만족하는 선로전환기 제어모듈의 위험축고장을 예측하여 안전무결성레벨 만족여부를 판단하였다.

#### 2. 본 론

##### 2.1 선로전환기 제어모듈

NS타입 선로전환기의 경우 선로전환기의 제어는 DC24V 200mA의 출력으로 선로전환기 내부의 신호계전기를 제어하며, 출력에 의해 제어된 선로전환기의 상태를 선로전환기 내부의 전환상태 신호계전기의 상태를 접점신호로 입력받는 폐회로로 구성된다.[3] 따라서 TFM 제어기 내부의 구성은 DC스위칭디바이스의 종류와 접점의 수를 제외하면 범용 내장형시스템 구조를 갖는다. 따라서 본 논문에서는 TFM 선로전환기 제어모듈에 대해서 안전필수시스템으로 설계하기 위해 기본TFM구조를 그림1과 같이 모델링하였다.

또한 안전성활동을 위한 필수요소인 기능요구사항, 인터페이스요구사항, 운영시나리오에 대하여 다음과 같이 제시하였다.

Jae Ho LEE Ducko SHIN  
Korea Railroad Research Institute

#### ■ 기능요구사항

- TFM은 전자연동장치의 명령에 의해 선로전환기를 제어해야 한다.
- 선로전환기의 전환방향인 상태정보를 실시간으로 전자연동장치에 전송한다.

#### ■ 인터페이스요구사항

- 전자연동장치 연동논리부와 RS485의 전기적 프로토콜로 Vital 통신을 수행한다.
- 선로전환기와 DC24V 250mA의 On/Off접점으로 인터페이스한다.

#### ■ 운영시나리오

- TFM내부의 고장으로 선로전환기가 전환되지 말아야 한다.
- TFM내부의 고장은 실시간으로 전자연동장치에 보고되어야 한다.

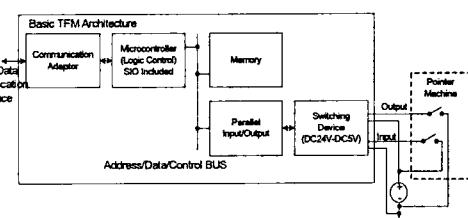


그림1 선로전환기의 기본구성

#### 2.2 선로전환기 제어모듈의 예비위험원분석

예비위험원분석은 대상시스템으로 인해 발생할 수 있는 사고의 심각도와 발생빈도인 리스크를 예측하고, 리스크를 허용할 수 있는 수준으로 완화하기 위한 안전대책을 수립하여 대상시스템의 안전요구사항 제시를 목적으로 한다.[1]

본 논문에서는 영국의 철도운영기관인 Network-Rail의 철도위험원목록을 토대로 선로전환기 관련 위험원을 표1과 같이 정의하였다.[4]

#### 표1 선로전환기제어관련 위험원

Hazard Code	Hazard Description
HW075	선로전환기 도중전환
HP066, HW076	선로전환기의 밀착실패
HP067, HW077	선로전환기 불일치

제시된 위험원에 대하여 표2와 같이 예비위험원분석을 수행하여 선로전환기제어모듈의 안전요구사항을 제시하였다.

표2 TFM의 예비위험분석

시스템 명 : TFM의 선로전환기 제어									
No	작성기 간	2일	작성날짜	2005.01.21	2005.01.27				
분석단계	최초 :	?	수정 :	□	부가 :	□			
위험 원번호	위험 원 내용	대상	심각도	빈도	크기	대책안 :	대책안 후	심각도	빈도
HW 075	선로전환기 도중전환	W P	A	3	I	D : 선로전환기 전환제어를 2개 이상의 제어기가 판단한다. E : 열차접근시 선로전환기는 제어되지 않는다. S : 단일소자의 결함으로 선로전환기는 제어되지 않는다.	A	5	III
HP0 66 HW 076	선로전환기 밀착실패	W P	A	3	I	D : 선로전환기의 밀착실패는 실시간으로 보고된다. E : 선로전환기 밀착실패시 해당 진로를 폐쇄한다. S : 단일소자의 결함으로 선로전환기 밀착감시가 오동작하지 않는다.	A	5	III
HP0 67 HW 077	선로전환기 불일치	W P	A	3	I	D : 선로전환기의 불일치는 실시간으로 보고된다. E : 선로전환기 불일치시 해당 진로를 폐쇄한다. S : 단일소자의 결함으로 선로전환기 불일치감시가 오동작하지 않는다.	A	5	III

#### ■ 선로전환기 제어모듈의 안전요구사항

- 선로전환기 전환제어를 위한 논리판단은 복수개 이상의 제어기가 수행해야 한다.
- 단일소자의 결함으로 선로전환기는 제어, 밀착감시 실패, 불일치감시실패 되지 않는다.
- TFM은 안전무결성레벨 4의 대책이 적용되어야 한다.

예비위험분석은 시스템 상위레벨의 위험원에 대한 분석으로 선택된 위험원도 사고와 매우 밀접하다. 따라서 하부구성요소에 대한 위험원도출 및 분석을 통해 구성요소의 고장으로 인해 사고가 발생되는 시나리오를 작성하여 하부구성요소별로 안전대책의 수준인 안전무결성레벨을 할당해야 한다. 본 논문의 그림1과 같은 선로전환기제어모듈의 고유기능과 듀얼듀플렉스구조를 위한 기능으로 발생할 수 있는 위험원을 표3과 같이 제시하였다.

표3 듀얼듀플렉스구조 선로전환기 제어모듈의 구성요소

구 분	구성요소(Element)	번 호	Guide Word종류
TFM 고유기능	연동논리부로부터 바이탈정보 수신	TFMH01	직렬통신
	연동논리부로부터 바이탈정보 송신	TFMH02	직렬통신
	선로전환기전환의 논리수행	TFMH03	접점정보
	선로전환기 쇄정의 논리수행	TFMH04	제어정보
여분구조 관련기능	선로전환기상태확인의 논리수행	TFMH05	접점정보
	경립발생의 검지(비교회로 기능)	TFMH08	접점정보
	타개 고장에 의한 계절체	TFMH09	접점정보

#### 2.3 선로전환기 제어모듈의 위험원도출 및 분석

표3의 구성요소 각각에 대하여 표4와 같은 위험원도출을 수행해야 한다. 위험원도출은 Hazop Study기법을 사용하여 하부구성요소의 고장인 일탈(Deviation)로 발생되

는 위험원을 예측하였다.

표4 하부구성요소의 위험원도출(Hazop Study)

HAZOP Study 대상: 대기이중제구조 TFM(연동논리부로부터 바이탈정보수신)								
참조도면번호:			개선번호:			소요시간:		
참여구성원: RAMS건설팀부서, 시스템 검토그룹(SRG) 회의일자:								
기능	Guide Word	이상현상	원인	결과	안전대책	기타사항	세부조치내역	조치의주체
No	연동논리부로부터 바이탈정보수신	シリ얼리더보드 고장 컨트롤러 고장	TFM 제어불능	데이터 수신률 늦滞체	선로전환기 제어권 상실	연동논리부로부터 데이터수신기능 결합 검증회로		
More	연결된 모든シリ얼리더보드의 고장 (수신단 전압상승)	케이블에 이상전압 유도	TFM 제어불능	통신체널 다중화	선로전환기 제어권 상실	직렬포트의 다중화		
Less	연동논리부로부터 바이탈정보수신	연결부의 저항값 상승	TFM 제어불능	연결부의 주기적 보수	선로전환기 제어권 상실	내구성이 강한 커넥터 사용		
As well as	입력비트초과된오정보입력	シリ얼데이터 복조클럭 오류 (컨트롤러 고장)	관계없는 선로전환기 전환	복조된 데이터 확인	선로전환기 제어권 상실	복조된 데이터의 검증회로		
(T F M H0 1)	입력비트미달된오정보입력	シリ얼데이터 복조클럭 오류 (컨트롤러 고장)	관계없는 선로전환기 전환	복조된 데이터 확인	선로전환기 제어권 상실	복조된 데이터의 검증회로		
Rever se	입력비트전역오정보입력	シリ얼리더보드 고장 컨트롤러 고장	관계없는 선로전환기 전환	복조된 데이터 확인	선로전환기 제어권 상실	복조된 데이터의 검증회로		
Early	어댑터의 고장(Vibration으로 데이터 폭주)	シリ얼리더보드 고장	오동작	복조된 데이터 확인	선로전환기 제어권 상실	복조된 데이터의 검증회로		

표4의 하부구성요소 위험원에 대한 안전대책을 모두 적용하여 듀얼듀플렉스구조의 선로전환기제어모듈을 설계하였으며, 그림2와 같은 구조를 갖는다.

표5 듀얼듀플렉스 TFM의 평균 확률고장률

하부시스템	기호	Failure Rate per Hour ( $10^{-6}$ )	수량	기타
MC68302	$\lambda_{Controller}$	0.025189	1	16Bit Microprocessor
684000	$\lambda_{Memory}$	0.063352	1	8Bit SRAM
29F040	$\lambda_{Flash}$	0.005696	1	8bit Flash Memory
TPL523	$\lambda_{SH24}$	0.220860	1	24V to 5V Switching Dev.
TPL532	$\lambda_{SH35}$	0.220860	1	5V to 24V Switching Dev.
27C020	$\lambda_{Dram}$	0.667491	1	Dual port Memory
DS1232	$\lambda_{RESET}$	0.060934	1	Reset Device
75176	$\lambda_{SerialAdap}$	0.253600	1	RS485 Serial Adaptor
8255	$\lambda_{PIO}$	0.198550	1	Peripheral IO

## 2.4 선로전환기 제어모듈의 위험축고장률예측

그림2와 같은 안전필수구조의 선로전환기제어모듈의 위험축고장률은 그림3과 같이 위험원의 연관관계를 분석한 결합트리에 의해 예측할 수 있다. 위험축고장률의 기초데이터가 되는 구성요소의 고장률은 표5와 같이 전기전자부품의 고장을 예측지침인 MIL-HDBK-217에 의해 산출하였다.

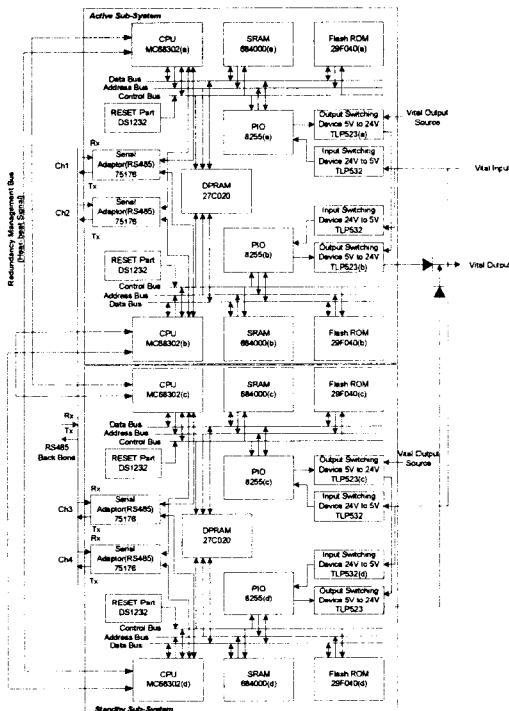


그림2 안전필수 듀얼플렉스 선로전환기 제어모듈

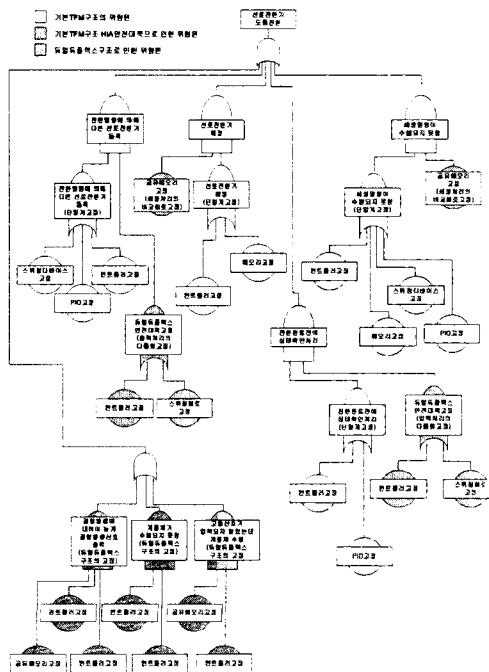


그림3 선로전환기 도중전환의 사고시나리오

그림3의 구성요소고장률에 의한 선로전환기 제어관련 위험원의 위험축고장률을 다음과 같이 계산하였다.

$$\begin{aligned}
 \lambda_{HP075} = & \lambda_{Dmem} \lambda_{Controller} + \lambda_{Controller} \lambda_{Controller} + \lambda_{Dmem} \lambda_{Controller} \\
 & + (\lambda_{SwitchingDev} + \lambda_{PIO} + \lambda_{Controller}) (\lambda_{Controller} + \lambda_{SwitchingDev}) \\
 & + \lambda_{Dmem} (\lambda_{Controller} + \lambda_{Memory}) \\
 & + (\lambda_{Controller} + \lambda_{PIO}) (\lambda_{Controller} + \lambda_{SwitchingDev}) \\
 & + (\lambda_{Controller} + \lambda_{Memory} + \lambda_{SwitchingDev} + \lambda_{PIO}) \lambda_{Dmem} \\
 = & 4\lambda_{Dmem} \lambda_{Controller} + 3(\lambda_{Controller})^2 + 3\lambda_{SwitchingDev} \lambda_{Controller} \\
 & + 2\lambda_{PIO} \lambda_{Controller} + (\lambda_{SwitchingDev})^2 + 2\lambda_{PIO} \lambda_{SwitchingDev} \\
 & + 2\lambda_{Dmem} \lambda_{Memory} + \lambda_{Dmem} \lambda_{SwitchingDev} + \lambda_{PIO} \lambda_{Dmem} \\
 = & 5.9686 \times 10^{-13}
 \end{aligned}$$

동일한 방법으로 선로전환기 제어관련 위험원에 대한 위험축고장률을 예측하여 표6과 같은 결과를 얻었다. 이러한 위험축고장을 예측은 안전필수분야 제어기에 대하여 반드시 제시되어야 하며, 본 논문에서 예측한 위험축고장률은 표2의 예비위험원분석에 의한 위험원들의 리스트크레벨1에 대한 안전대책의 수준인 안전무결성레벨(SIL)4의 위험축고장을 기준인  $10^{-8}$ 미만을 모두 만족하는 결과이다.

표6 듀얼플렉스구조 선로전환기의 위험축고장률

위험원 번호	위험원명	위험축고장률( $10^{-12}$ )
HW075	선로전환기 도중전환	0.5968
HP066, HW076	선로전환기의 일작실패	1.1694
HP067, HW077	선로전환기 불일치	2.1342

## 3. 결 론

본 논문에서 수행한 안전성활동을 통한 안전필수시스템의 정량적 위험축고장률예측은 시스템 안전목표 달성을 여부를 판단하는 기준이이며, 위험축고장률예측의 방법으로 사용된 예비위험원분석데이터와 위험원도출 및 분석데이터는 안전활동의 전진성과 적합성을 판단하는 자료로써 시스템의 안전인증기관 또는 최종사용자의 시스템 안전기준 적합성의 판단데이터로 활용되어야 한다.

## [참 고 문 헌]

- [1] IEC62278, "Railway applications-Specification and demonstration of reliability, availability, maintainability and safety(RAMS)", 2002
- [2] IEC61508-2, "Functional safety of electronic/programmable electronic safety-related systems Part2:Requirements for electrical/electronic/programmable electronic safety-related systems", 2000
- [3] 김영태, "신호제어시스템", p65-85, 테크미디어, 2003
- [4] RAILTRACK "Engineering Safety Management Issue 2.0", Volume3, Section 10, Safety Planning, p3-p13, 1997