ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 63, No. 11, pp. 1526～1532, 2014
http://dx.doi.org/10.5370/KIEE.2014.63.11.1526

IEC 61508 기준 PES 기반 전자연동장치의 기능 안전도 분석에 관한 연구

A Study on the Functional Safety Analysis of PES-based Electronic Interlocking Unit according to IEC 61508

이 명 철†
(Myung-Chul Lee)

Abstract - The Electronic Interlocking unit in railway signalling system is safety-related facilities to determine route and speed for train running. In particular, the SSI(Solid State Interlocking) is Electronic Interlocking unit for high-speed railway, and it performs safety-critical function by MPM(Micro-Processor Module). Meanwhile, MPM is composed of the PES(Programmable Electronic System)-based system, and the PES-based system in railway safety-related facilities should be implemented by complying with the safety requirements defined in IEC 62425 and IEC 61508. In this paper, we performed modeling of failure rate and reliability for MPM implemented by fault tolerance methods and analyzed functional safety for MPM. Moreover, we determined SIL(Safety Integrity Level) for MPM according to the safety requirements defined in IEC 61508 based on an analyzed functional safety.

Key Words : Electronic Interlocking unit, SSI, MPM, PES, IEC 61508, SIL

1. 서 론

철도 안전설비에서 PES(Programmable Electronic System) 기반 시스템은 전기/전자/프로그램 가능한 장치에 대한 안전관련 시스템의 기능 안전성에 대해 기술하고 있는 국제 표준 규격인 IEC 61508의 안전 요구사항을 반드시 준수하면서 설계하도록 요구되고 있다[1-2]. IEC 61508에서는 단일계(1oo1) 및 이중계(1oo2, 2oo2), 삼중계(2oo3)의 등의 하드웨어 여분을 이용한 결함-허용 방식에 따른 정량적인 안전성 분석 방식을 설명하고 있고, 이러한 정량적인 안전성 분석 결과에 따라 SIL(Safety Integrity Level)을 결정하도록 권고하고 있다. SIL의 결정은 계통적 고장(Systematic failure)에 대한 정성적인 안전성 분석 방법과 임의적 고장(Random failure)에 대한 정량적인 안전성 분석 방법으로 구분된다.

표 1 THR에 따른 SIL의 할당
Table 1 SIL assignment according to THR

SIL	THR [$hour^{-1}/function$]
4	$10^{-9} \leq THR < 10^{-8}$
3	$10^{-8} \leq THR < 10^{-7}$
2	$10^{-7} \leq THR < 10^{-6}$
1	$10^{-6} \leq THR < 10^{-5}$

† Corresponding Author:Dept.of Railroad SystemEngineering, Woosong Univerity, Korea.
E-mail: yk5397@hanmail.net
Received : February 28; Accepted : October 21

Random failure에 대한 정량적인 안전성 분석 방법은 Table 1에서와 같이 4개의 등급으로 구분하여, 특정 시스템의 THR(Tolerable Hazard Rate)에 따른 안전성 등급을 할당한다[1, 3-4]. Table 1에서와 같은 SIL의 결정 방법은 철도 안전설비의 안전성 분석 방법으로서 반드시 활용하도록 요구되고 있으며, 열차 충·추돌과 같이 대형 인명사고를 유발할 수 있는 안전-필수 기능일수록 높은 SIL을 부여하도록 하고 있다. 따라서 높은 신뢰성과 안전성이 요구되는 철도안전설비의 안전-필수 기능은 SIL 4의 안전등급이 할당되어야 하고, SIL 4를 입증하기 위해서는 IEC 61508에 제시된 정량적 안전성 분석 방법에 따라 시스템의 안전 기능 별 THR을 산출해야 한다[5].

2. 전자연동장치 개요

철도신호시스템에서 전자연동장치(Electronic Interlocking unit)는 역 구내에서 열차의 운행과 차량의 입환 작업을 안전하고 신속하게 수행하기 위하여 신호기, 선로전환기, 궤도회로 등의 신호보안장치를 전기적으로 연쇄하거나 컴퓨터 소프트웨어에 의한 데이터베이스화 및 로직을 상호 연쇄하여 열차에 대한 진로 취급이나 신호설비 취급 시 오동작이나 부정 동작을 방지하도록 구성한 장치이다.

전자연동장치의 기능은 운전정리와 같이 운용효율을 높이는 기능과 진로제어, 열차속도제어, 건널목제어 등의 안전성과 직접적인 관련이 있다. 전자연동장치의 기능과 관련되어 발생되는 주요사고는 충·추돌, 탈선 등이 있고, 사고결과는 사망, 부상 및 시설물 파손 등으로 나타난다. 역에서는 전자

연동장치에 의존하여 열차의 진로, 입환, 폐색 제어 등을 수행하고 있기 때문에 전자연동장치의 안전성 및 신뢰성이 매우 높게 요구되고 있다. 진로제어, 열차속도제어 및 건널목 제어 등과 같은 안전-필수(Safety-Critical) 기능은 안전과 직접적인 관련이 있어, 이 기능들에 대해서 시스템 수명주기 전반에 걸쳐서 안전성확보 및 검증이 필요하다[6].

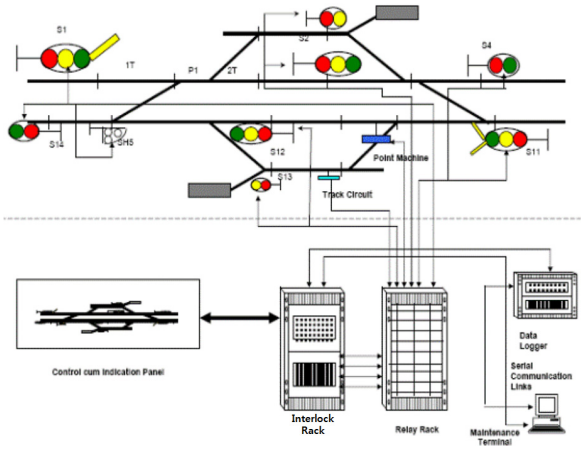

그림 1 전자연동장치 인터페이스 구성도

Fig. 1 Electronic Interlocking System Interface block diagram

특히 경부고속철도에 설치된 고속선 전자연동장치 SSI (Solid State Interlocking)는 역 구내 구간에서 열차의 충돌 및 탈선을 방지하기 위해 진로 및 신호 등을 일괄적으로 연동 처리하는 기능을 수행하는 장치로서 프랑스의 Alstom社에서 공급하여 운영되어 왔으나 수년 전부터 국산화를 위한 개발 사양이 도출되었다.

SSI는 크게 일반운영, 연동기능, 로깅 및 유지보수의 3가지 기능을 제공한다. SSI의 이러한 기능들은 기능 오동작 시 열차 사고로 이어질 수 있는 안전-필수 기능이므로 SSI의 내부 구성은 어떠한 시스템의 결함(fault)으로부터 고장(failure)을

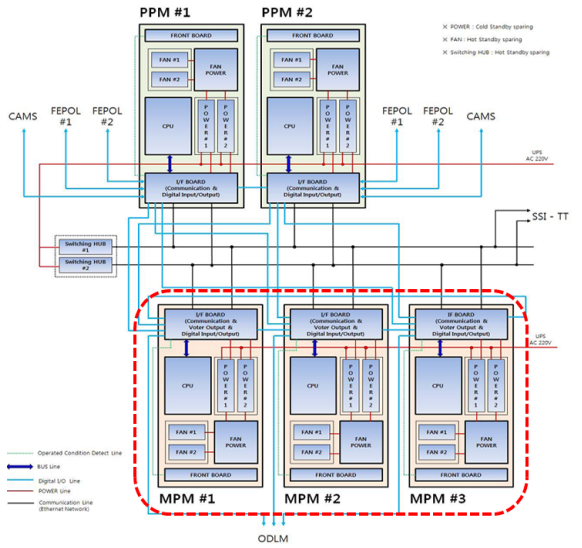

그림 2 2oo3 방식의 MPM 모듈 구성

Fig. 2 MPM module composition applying 2oo3 method

방지할 수 있는 결함-허용(fault-tolerant) 방식의 열차제어모듈로서 구성된다. SSI의 안전-필수 기능을 수행하기 위해서, 내부 구성은 Fig. 2와 같이 2 out of 3(2oo3) 방식의 MPM (Micro-Processor Module)으로 구성된다.

2oo3 방식의 결함-허용 모듈은 시스템에서 발생되는 동일한 기능을 다중으로 구성하여 신뢰성 및 안전성을 향시키는 방법으로, 3개의 출력신호 중에 2개의 출력신호가 동일하면 정상동작을 출력하는 구조로 설계된다. 이러한 2oo3 방식은 SSI에 구성된 MPM과 같이 PES(Programmable Electronic System) 기반으로 구성된다[5, 7].

3. 정량적인 안전성 분석 방법

정량적인 안전성 지표인 THR을 도출하기 위해서는 다음의 Fig. 3과 같은 프로세스를 통해 THR을 계산할 수 있다[8].

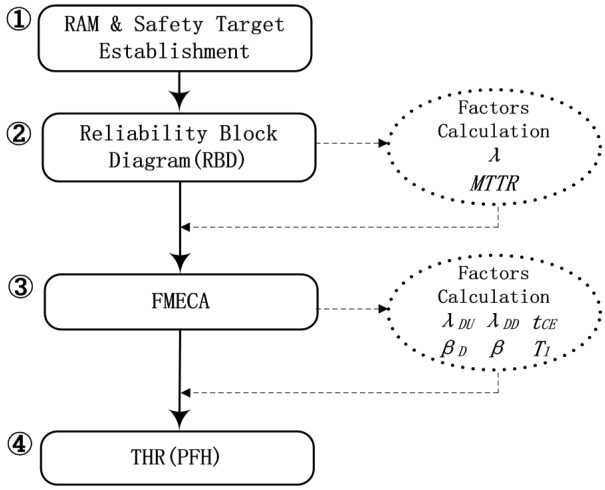

그림 3 THR 분석 과정

Fig. 3 THR analysis process

첫 번째, 특정 장치 또는 시스템의 RAM(Reliability, Availability and Maintainability) 및 안전성(Safety)에 대한 목표 값을 수립한다. 두 번째, 수립된 RAM 목표 값을 입증하기 위해 신뢰성 블록다이어그램인 RBD(Reliability Block Diagram)를 작성하여 고장률 λ를 도출하고, 고장률 λ를 근거로 평균 수리시간인 MTTR(Mean Time To Repair)을 계산한다. 세 번째, 특정 장치 및 시스템에서 발생 가능한 고장 유형 및 고장 원인을 식별하고, 고장 영향을 및 결과를 기록하는 FMECA(Failure Modes Effects and Criticality Analysis) 활동을 수행한다. FMECA 활동을 통해 분석된 고장 영향 및 결과 중 안전에 영향을 미치는 고장모드를 별도로 식별하여, IEC 61508에 정의된 검출되지 않은 위험측 고장률 λ_{DU}, 검출된 위험측고장률 λ_{DD}, 검출되지 않은 공통 원인고장(Common Cause Failure : CCF) 비율 β, 검출된 공통 원인고장 비율 β_D, 등가평균 정지시간 t_{CE}, 증명 시험 간격 T_1 등의 인자들을 계산한다. 네 번째, 계산된 인자들을 활용하여 IEC 61508에 정의된 정량적인 안전성 계산 공식에

따라 최종 THR을 산출한다.

IEC 61508에서는 정량적인 안전성 지표로서 저요구 작동 모드에서의 평균 고장 확률인 PFD(Probability of Failure on Demand)와 고요구 작동 모드에서의 시간 당 고장 확률인 PFH(Probability of Failure per Hour)를 제시하고 있는데, 철도 안전 국제 표준 규격인 IEC 62425에서는 THR 값은 PFH 값을 활용하도록 권고하고 있다. 따라서 본 논문에서 계산되는 THR 값은 IEC 61508에서 언급된 PFH를 나타낸다[4, 8-10].

4. 결함허용모듈의 안전성 모델링

고속선 SSI에 구성되어있는 핵심 모듈은 2oo3 방식의 결함-허용 모듈로 구성되어 시스템의 신뢰성 및 안전성을 높이고 있다. 세 개의 결함허용모듈은 각각 하드웨어적으로 동일하며, 동일한 소프트웨어를 사용한다. 결함허용모듈의 안전성을 모델링하기 위해서 서론에서 제시된 정량적인 안전성 분석 방법을 사용한다.

먼저 RAM 분석 수준을 정의하기 위해 RBD (Reliability Block Diagram) 분석 기법을 사용한다. RBD는 논리적인 기호를 사용하여 시스템 내의 고장관계를 나타내며 일반적으로 RBD에서 사용되는 신뢰도는 고장율[λ]과 시간[t]로 계산된다. MPM의 높은 신뢰도를 확보하기 위해 하나의 Funcion Operation으로 구성된 n개의 병렬시스템을 사용한다. 이 경우, 전체 시스템 신뢰도 $R(t)$과 시스템의 고장율 λ는 식(1)과 식(2)와 같다[3, 11].

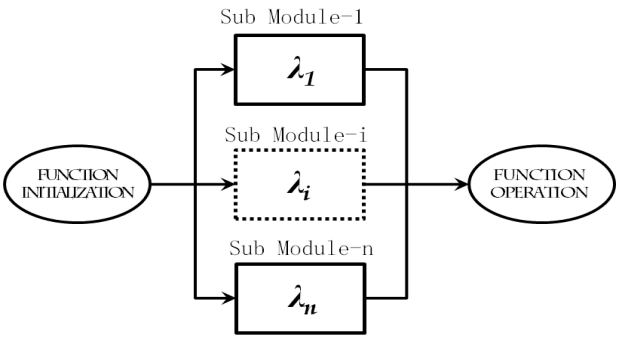

그림 4 2oo3 결함허용모듈의 병렬 구성 RBD
Fig. 4 Parallel-composition RBD for 2oo3 Fault-tolerant Module

$$R(t)=1-\prod_{i=1}^{n}(1-e^{-\lambda t}) \tag{1}$$

$$\lambda(t)=-\frac{d}{dt}ln\left[1-\prod_{i=1}^{n}(1-e^{-\lambda t})\right] \tag{2}$$

유지보수도의 평가지표는 예측치 기반의 MTTR을 사용한다. MTTR은 현장에서 유지보수 인력에 의해 교체가 가능한 최하위현장 수리구성요소(Line Replaceable Units : LRU) 단위로, 시스템에서 발생된 고장을 발견에서부터 조치 및 시험 후, 기능 복귀까지의 시간을 정의한 것이다. MTTR의 계산은 식(3)과 같다[3, 11].

$$MTTR=\frac{\sum_{i=1}^{n}(\lambda_i\times MTTR_{LRU})}{\sum_{i=1}^{n}\lambda_i} \tag{3}$$

정량적인 안전성 분석 수준을 정의하기 위해 IEC 61508에 정의된 분석 기법을 사용한다. IEC61508-6에서는 1oo1, 1oo2, 2oo2, 1oo2D, 2oo3의 결함-허용(Fault Tolerant) 모듈에 따른 THR 분석 기법을 정의하고 있다[1].

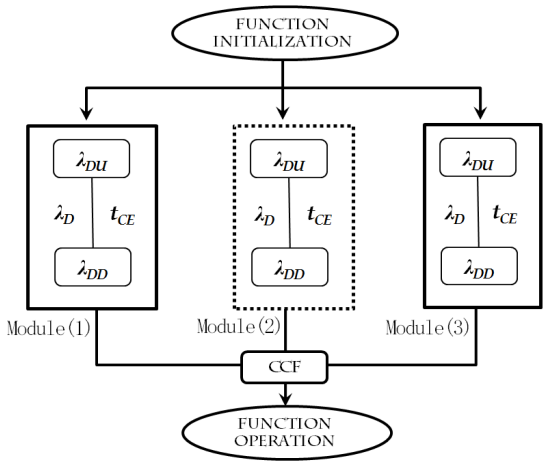

그림 5 2oo3 결함허용모듈의 병렬 구성
Fig. 5 Parallel-composition for 2oo3 Fault-tolerant Module

위험측 고장율 λ_D는 검출되지 않은 위험측 고장율 λ_{DU}와 검출된 위험측 고장율 λ_{DD}의 합으로 식 (4)와 같이 나타낼 수 있고, λ_{DU}와 λ_{DD}는 식(5)와 식(6)과 같다[1].

$$\lambda_D=\lambda_{DU}+\lambda_{DD}=\frac{\lambda}{2}[Failure/hour] \tag{4}$$

$$\lambda_{DU}=\frac{\lambda}{2}(1-DC)[Failure/hour] \tag{5}$$

$$\lambda_{DD}=\frac{\lambda}{2}DC[Failure/hour] \tag{6}$$

식(5) 및 식(6)에서 언급된 진단범위 DC(Diagnostic Cover age)는 검출된 위험측 고장률 λ_{DD}와 위험측 고장률 λ_D의 비율로 나타내며, 식(7)과 같다[1, 12].

$$DC=\frac{\Sigma\lambda_{DD}}{\Sigma\lambda_D}=\frac{\Sigma\lambda_{DD}}{\Sigma\lambda_{DD}+\Sigma\lambda_{DU}}[\%] \tag{7}$$

2oo3 모듈에 따른 등가 평균 정지 시간 t_{CE}는 증명시험간격 T_1과 평균복구시간 MTTR(Mean Time To Repair)을 근거로 계산되며, 식(8)과 같다[1, 12].

$$t_{CE}=\frac{\lambda_{DU}}{\lambda_D}(\frac{T_1}{2}+MTTR)+\frac{\lambda_{DD}}{\lambda_D}MTTR[Hour] \tag{8}$$

식(1)~(8)에 주어진 파라메터를 근거로 2oo3 결함-허용

모듈의 THR은 식(9)와 같다[1, 12].

$$THR_{2oo3} = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 \cdot t_{CE} + \beta_D \lambda_{DD} + \beta\lambda_{DD}[Hour^{-1}] \quad (9)$$

5. 시뮬레이션

THR_{2oo3}를 계산하기 위해 고속선 SSI MPM 모듈에 대한 각각의 파라메터에 대한 정의가 필요하다. 각각의 파라메터에 대한 정의는 Table 2와 같으며, 시뮬레이션 도구로는 Matlab 프로그램을 사용하였다[13-16].

표 2 파라메터의 정의
Table 2 Definition of parameter

Parameter	Define
Failure Rate	λ= 5.25×10^{-6} [/hour]
Proof Test Interval	T_1 = 0 ~ 6 month
Diagnostic Coverage Factor	DC = 20%, 40%, 60%, 80%, 90%, 99%
Detected Common Cause Factor	β = 2%, 10%, 20%
Undetected Common Cause Factor	β_D = 1%, 5%, 10%

Table 2로부터 고장률 1×10^{-8}[/hour]를 가진 하나의 Function Operation으로 구성된 2oo3의 SSI 신뢰도를 분석

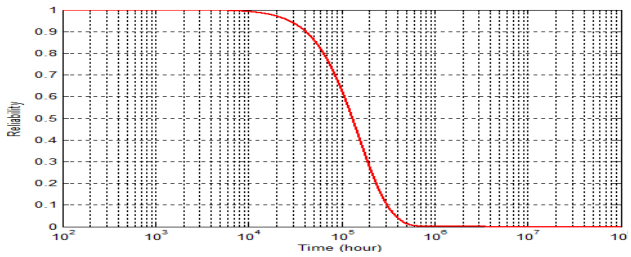

그림 6 2oo3에서 SSI 신뢰도[MATLAB]
Fig. 6 Reliability of SSI in 2oo3[MATLAB]

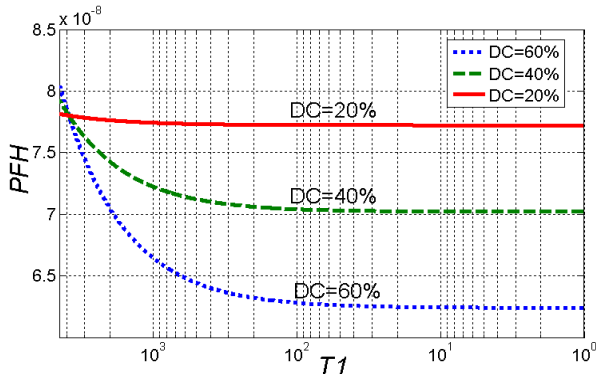

그림 7 β(2%) 및 β_D(1%) 일때의 THR_{2oo3}(1)[MATLAB]
Fig. 7 THR_{2oo3}(1) applying β(2%) and β_D(1%)[MATLAB]

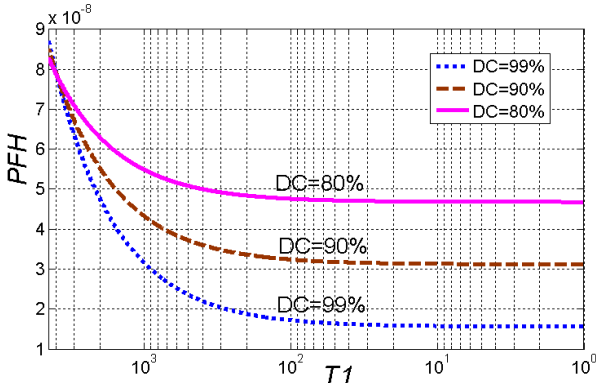

그림 8 β(2%) 및 β_D(1%) 일때의 THR_{2oo3}(1)[MATLAB]
Fig. 8 THR_{2oo3}(1) applying β(2%) and β_D(1%)[MATLAB]

표 3 DC 및 T_1에 따른 THR_{2oo3}(1)
Table 3 THR_{2oo3}(1) *in the aspect of DC and* T_1

DC \ T_1	1 month	3 month	6 month
20%	7.70×10^{-8} [hour^{-1}/function]	7.70×10^{-8} [hour^{-1}/function]	7.80×10^{-8} [hour^{-1}/function]
40%	7.10×10^{-8} [hour^{-1}/function]	7.40×10^{-8} [hour^{-1}/function]	7.80×10^{-8} [hour^{-1}/function]
60%	6.50×10^{-8} [hour^{-1}/function]	7.10×10^{-8} [hour^{-1}/function]	7.90×10^{-8} [hour^{-1}/function]
80%	5.20×10^{-8} [hour^{-1}/function]	6.40×10^{-8} [hour^{-1}/function]	8.10×10^{-8} [hour^{-1}/function]
90%	3.90×10^{-8} [hour^{-1}/function]	5.70×10^{-8} [hour^{-1}/function]	8.30×10^{-8} [hour^{-1}/function]
99%	2.70×10^{-8} [hour^{-1}/function]	5.00×10^{-8} [hour^{-1}/function]	8.40×10^{-8} [hour^{-1}/function]

하면, Fig. 6과 같다.

Fig. 6에서 보듯이, 시간이 흐를수록 신뢰도는 감소하며, 약 50,000시간(약 5.7년)이후에는 신뢰도가 급격이 감소한다.

Common Cause Factor(CCF)와 관련된 β와 β_D를 각각 2%, 1%라고 가정하면, 증명 시험 간격 T_1에 따른 THR_{2oo3}(1)은 Fig. 7 및 Fig. 8과 같다.

진단범위 DC 및 증명 시험 간격 T_1에 따른 PFH2oo3(1)은 Table 3과 같다. 증명 시험 간격을 1개월, 3개월, 6개월

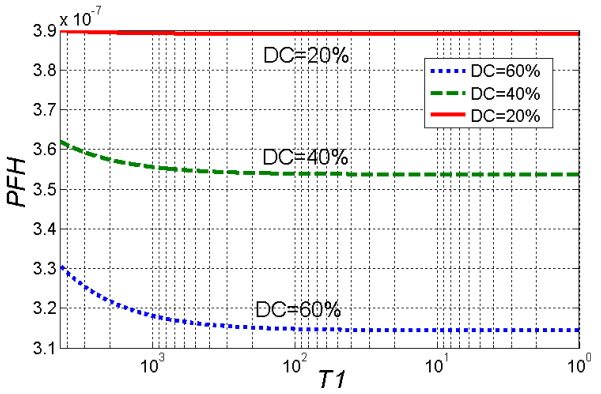

그림 9 β(10%) 및 β_D(5%) 일때의 THR_{2oo3}(2)[MATLAB]
Fig. 9 THR_{2oo3}(2) applying β(10%) and β_D(5%)[MATLAB]

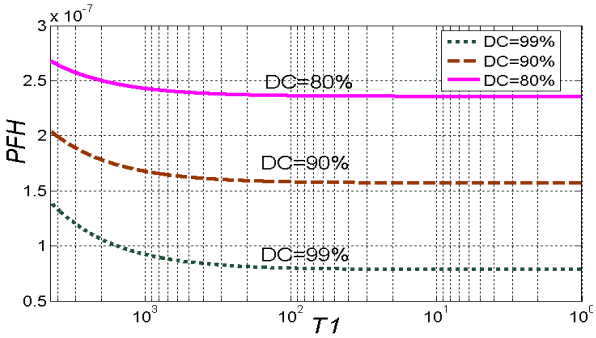

그림 10 β(10%) 및 β_D(5%) 일때의 THR_{2oo3}(2)[MATLAB]
Fig. 10 THR_{2oo3}(2) applying β(10%) and β_D(5%)[MATLAB]

표 4 DC 및 T_1에 따른 THR_{2oo3}(2)ㅅ
Table 4 THR_{2oo3}(2) *in the aspect of DC and* T_1

DC \ T_1	1 month	3 month	6 month
20%	3.89×10^{-7} [hour^{-1}/function]	3.89×10^{-7} [hour^{-1}/function]	3.89×10^{-7} [hour^{-1}/function]
40%	3.55×10^{-7} [hour^{-1}/function]	3.57×10^{-7} [hour^{-1}/function]	3.61×10^{-7} [hour^{-1}/function]
60%	3.17×10^{-7} [hour^{-1}/function]	3.22×10^{-7} [hour^{-1}/function]	3.30×10^{-7} [hour^{-1}/function]
80%	2.40×10^{-7} [hour^{-1}/function]	2.51×10^{-7} [hour^{-1}/function]	2.66×10^{-7} [hour^{-1}/function]
90%	1.64×10^{-7} [hour^{-1}/function]	1.79×10^{-7} [hour^{-1}/function]	2.02×10^{-7} [hour^{-1}/function]
99%	1.01×10^{-7} [hour^{-1}/function]	1.08×10^{-7} [hour^{-1}/function]	1.37×10^{-7} [hour^{-1}/function]

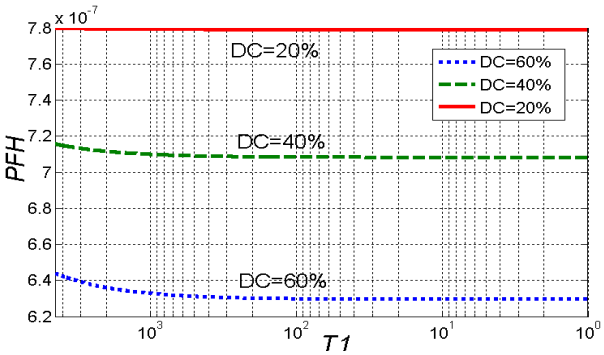

그림 11 β(20%) 및 β_D(10%) 일때의 THR_{2oo3}(3)[MATLAB]
Fig. 11 THR_{2oo3}(3) applying β(20%) and β_D(10%)[MATLAB]

단위로 수행하였으며, 증명 시험 간격이 증가할수록 THR_{2oo3} (1)은 약간씩 증가되었다. 또한 진단범위를 높게 책정할수록 THR_{2oo3}(1)도 감소되었고, 20% 진단 범위 책정 시에는 증명 시험 간격에 관계없이 비슷한 THR_{2oo3} 결과 값을 도출하였다.

CCF와 관련된 β와 β_D를 각각 10%, 5%로 가정하여 시뮬레이션을 수행한 결과 THR_{2oo3}(2)는 Fig. 9 및 Fig. 10과 같이 분석되었고, β와 β_D를 각각 20%, 10%로 가정하여 시뮬레이션을 수행한 결과, THR_{2oo3}(3)은 Fig. 11, Fig. 12와 같이 분석되었다. 한편 THR_{2oo3}(2), THR_{2oo3}(3)의 결과 패턴은 THR_{2oo3}(1)과 유사하게 분석되었다. 단, 6개월 증명 시험 간격에서 진단 범위가 높을수록 THR_{2oo3}(2), THR_{2oo3}(3)이 감

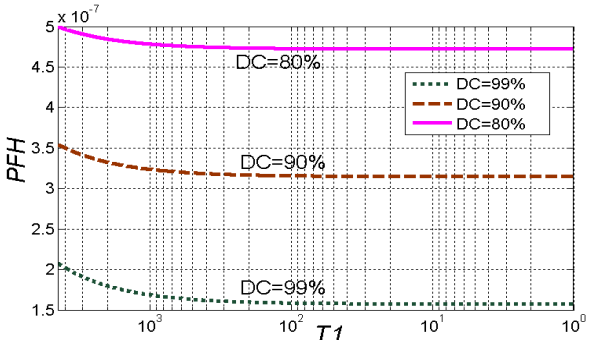

그림 12 β(20%) 및 β_D(10%) 일때의 THR_{2oo3}(3)[MATLAB]
Fig. 12 THR_{2oo3}(3) applying β(20%) and β_D(10%)[MATLAB]

표 5 DC 및 T_1에 따른 THR_{2oo3}(3)
Table 5 THR_{2oo3}(3) *in the aspect of DC and* T_1

DC \ T_1	1 month	3 month	6 month
20%	7.79×10^{-7} [hour^{-1}/function]	7.79×10^{-7} [hour^{-1}/function]	7.79×10^{-7} [hour^{-1}/function]
40%	7.09×10^{-7} [hour^{-1}/function]	7.11×10^{-7} [hour^{-1}/function]	7.15×10^{-7} [hour^{-1}/function]
60%	6.31×10^{-7} [hour^{-1}/function]	6.36×10^{-7} [hour^{-1}/function]	6.34×10^{-7} [hour^{-1}/function]
80%	4.76×10^{-7} [hour^{-1}/function]	4.85×10^{-7} [hour^{-1}/function]	4.98×10^{-7} [hour^{-1}/function]
90%	3.21×10^{-7} [hour^{-1}/function]	3.33×10^{-7} [hour^{-1}/function]	3.52×10^{-7} [hour^{-1}/function]
99%	1.65×10^{-7} [hour^{-1}/function]	1.81×10^{-7} [hour^{-1}/function]	2.05×10^{-7} [hour^{-1}/function]

소되는 점은 THR_{2oo3}(1)과는 상이하게 분석되었다.

시뮬레이션 결과 도출된 THR_{2oo3}(1), THR_{2oo3}(2), THR_{2oo3}(3) 결과값으로 Table 1을 참고하여 SIL을 할당하면 Table 6과 같다.

표 6 THR_{2oo3} 분석 결과에 따른 SIL의 할당
Table 6 SIL assignment according to THR_{2oo3} analysis results

THR[hour^{-1}/function]	SIL
$10^{-8} \le THR_{2oo3}(1) < 10^{-7}$	3
$10^{-7} \le THR_{2oo3}(2) < 10^{-6}$	2
$10^{-7} \le THR_{2oo3}(3) < 10^{-6}$	2

THR_{2oo3}(2)와 THR_{2oo3}(3)는 SIL 2로 결정되었고, THR_{2oo3}(1)은 SIL 3으로 결정되었다. 만약 특정 시스템 또는 장치에서 요구되는 안전 요구사항이 SIL 3이라고 가정하면, 진단범위 DC 및 증명 시험 간격 T_1, 공통 원인 고장 β 및 β_D 등과 같은 설계 및 시험 인자를 적절하게 제어하여 Table 6에서 언급된 THR_{2oo3}(1)을 도출할 수 있다.

6. 결 론

본 논문에서는 철도안전 국제 규격인 EN 50126, EN

50129에서 언급되는 THR과 관련된 SIL 요구사항을 만족하기 위해 IEC 61508에서 제시된 고 요구 작동모드에서의 THR을 분석하였다. 2oo3 모듈로 구성된 고속선 SSI의 MPM 모듈에 대한 고장률을 근거로 SSI의 신뢰도 및 IEC61508에서 제시된 THR_{2oo3}의 계산 공식을 적용하여 증명 시험 간격 T_1과 진단범위 DC에 따른 THR_{2oo3}값을 계산하였고, 결과 값을 근거로 SIL을 결정하였다. 본 논문의 결론은 다음과 같다.

1) PES 기반 안전-필수 열차제어시스템은 IEC 61508에서 권고하는 THR 분석 방법을 활용하여 단일계(1oo1) 및 이중계(1oo2, 2oo2), 삼중계(2oo3)의 하드웨어 여분을 이용한 결함-허용 방식에 따른 정량적인 안전성 분석을 수행하고 정량적인 안전성 분석 결과에 따라 SIL(Safety Integrity Level)을 결정해야 한다.
2) 2oo3 결함허용모듈의 THR 계산 시에는 고장률 λ, 유지보수도 MTTR, 검출되지 않은 위험측고장율 λ_{DU}, 검출된 위험측고장율 λ_{DD}, 등가평균정지시간 t_{CE}, 진단범위 DC, 증명시험간격 T_1, 공통 원인 고장 β 및 β_D의 필요 인자를 먼저 예측 및 분석하여야 한다.
3) 특히 진단범위 DC는 진단시험을 통해 검출되는 고장모드로써 결정된다. 단순한 부품(레지스터, 캐패시터, 트랜지스터 등)에 대한 단선 또는 단락은 100%로 결정되어야 하며, 보다 복잡한 유형의 부품은 60%, 80%, 99%로 제한을 두어 결정하는 것이 좋다[1, 17-18].
4) 또한 CCF와 관련된 공통 원인 고장 β 및 β_D의 결정은 시스템에 대한 다양성, 중복성, 복잡성, 데이터의 피드백, 인터페이스, 환경적 통제 등을 고려한 추정치로써 결정된다. 일반적으로 β는 $2\times\beta_D$로써 가정되며 β_D의 결정은 논리시스템의 경우 0.5%에서 5% 사이로, 센서 또는 최종단의 출력시스템의 경우 1%에서 10% 사이로 제한을 두는 것이 좋다[1, 19-20].
5 본 논문에서는 최종 THR_{2oo3}(1)을 도출하여 SIL 3으로 결정하였지만, 최근 안전-필수 열차제어시스템에서 요구하고 있는 SIL 4를 결정할 수 있는 안전성 분석이 수행되어야 한다.
6) 결함허용모듈에서 SIL 4를 도출하기 위해서는 설계 단계에서 장치의 고장률 λ, 유지보수도 MTTR, 검출되지 않은 위험측고장율 λ_{DU}, 검출된 위험측고장율 λ_{DD}, 등가평균정지시간 t_{CE}, 공통 원인 고장 β 및 β_D 등의 요소를 고려하여 설계하여야 한다.
7) 결함허용모듈에서 SIL 4를 도출하기 위해서는 시험 단계에서 증명시험간격 T_1 요소를 고려하여 검증하여야 한다.

향후, SIL 결정 방식은 국내 철도시스템(열차제어, 통신 등)에서 보다 합리적인 안전성 평가 기법으로 활용될 수 있다.

References

[1] International Electrotechnical Commission, IEC 61508, pp.40-100, 2000
[2] Jaeyoung Park, Jongwoo Lee, A Study on the Advanced Reliability Assessment Method about Hot-Standby Sparing System for Railway Signaling, Journal of the Korean Institute of Electrical Engineers, Vol.56 No.9, pp.1589-1595, 2007
[3] Committee European de Normalisation Electrotechnique, EN 50126-2, pp.46-47, 2007
[4] Committee European de Normalisation Electrotechnique, EN 50129, pp.39-41, 2003
[5] Shinju Kang, Jongwoo Lee, IEC 61508 into PES for Train Control Systems, Journal of the Korean Institute of Electrical Engineers, Vol.62 No.8, pp.1169-1176, 2013
[6] Jonggue Hwang, Hyungjung Joe, Seungkuen Shin, Rockgoe Jung, Applying Method for Safety Activity Process of Railway Signaling Systems, KIEE, pp.1-5, 2009
[7] Seungho Jang, Gwangyeol An, Donggun Lee, Jue Lee, A Study on the SIL Application For Electronic Interlocking Equipment of High Speed Line, The Korean society for railway, pp.1-6, 2009
[8] Junggun Ji, Changhoon Kim, Nokyung Ki, Byungwook Kang, Seoungcheol Lee, Myungcheol Lee, The Quantitative Safety Analysis of Multiplex Railway Signaling Controller, pp.1-7, 2012
[9] ISA-The Instrumentation Systems and Automation Society, Safety Instrumented Functions(SIF) - Safety Integrity Level(SIL) Evaluation Techniques 1-7, pp.1-687, 2002
[10] J. Borcsok, P. Holub, Considering and Comparing Safety Parameters - using Different Calculation Approaches of PFD/PFH/HR,NY, IEEE, pp.2-6, 2011
[11] Goncalo Medeiros Pais Simoes, RAMS analysis of railway track infrastructure, pp.5-26, 2008
[12] Chi-Chung Tao, A Two-Stage Safety Analysis Model for Railway Level Crossing Surveilance Systems, IEEE, pp.1-6, 2009
[13] IKE C. Tingos, Frank L. Raposa, A Safety Considerations with railroad Electrification: A Preliminary Review and Assessment, IEEE, pp.7-72, 2004
[14] Vincent Ho, Ph.D., P/E., C.S.P., A Risk-Based Approach to Verify the Guaranteed Emergency Brake Rate, pp.1-18, 2006
[15] Yookyung Control Co., Ltd., RAM Prediction Report of SSI type Interlocking Equipment, pp.5-27, 2010
[16] Dr. Hendik Schabe, a Different Principles Used for Determination of Tolerable Hazard Rates, pp.1-8, 2011
[17] Reliability Analysis Center(RAC), Failure Mode/ Mechanism Distributions, 1991, Department of Defense, United States of America, , NU 13440-8200, Organization report
[18] Qualiat und Zuverlassigkeit techischer Systeme, Theorie, Praxis, Management, Dritte Auflage, 1991, Allessandro Birolini, Springer-Verlag, Berlin Heidelberg New York, ISBN 3-540-54067-9, 3 Aufl., ISBN 0-387-54067-9 3 ed.

[19] MIL-HDBK-217F, Military Handbook Reliability prediction of electronic equipment, 2 December 1991, Department of Defense, United States of America, Washington DC 20301.
[20] Programmable electronic systems in safety-related applications, Part 2 : General technical guidelines, Health and Safety Executive, HMSO, ISBN 0 11 883906 3, 1887.

저 자 소 개

이 명 철(Myung-Chul Lee)
1961년 11월 18일생.
2012년 서울과학기술대학교 철도전문대학원 철도전기신호공학과 졸업. 2012년~현재 우송대학교 철도시스템학과 박사과정.
Tel : 02-830-7900
Fax : 02-830-7906
E-mail : yk5397@hanmail.net