철도차량 안전무결도(SIL) 적용 방안 연구

Train Level Application of the Safety Integrity Level

임연수*†, 오지은*, 공명상*, 강찬용*

Yeon-Su Lim*†, Ji-Eun Oh*, Myung-Sang Kong*, Chan-Yong Kang*

Abstract Railways RAMS related standard, EN50126 and EN50129 describe methodology for the Tolerable Hazardous Rate allocation and Safety Integrity Level application, based on the Risk Acceptance Principle. Almost train level safety critical functions are the integrated ones from the various sub-functions implemented by many sub-systems, while Safety Integrity Level is generally applicable for the standalone equipment providing simple function. The methodology for the train level SIL application in addition to the equipment level SIL application is proposed in this paper based on the example from the overseas railway operator for the SIL application on the Anti-Drag Function.

Keywords **:** SIL, Safety Critical Function, ISA, Passenger Door, Anti-Drag Function

초 록 철도차량 RAMS 관련 규격인 EN50126과 EN50129는 위험도 수용 원칙 (Risk Acceptance Principle)을 고려한 허용가능 위험율 (Tolerable Hazardous Rate, THR) 및 안전무결도(SIL)의 할당과 적용 방안을 기술하고 있다. 철도차량의 안전 기능은 여러 하위 시스템에 의해 구현되는 다양한 안전 기능의 통합적인 기능인 반면, 일반적으로 안전무결도는 간단한 기능을 수행하는 독립적인 장치에 적용된다. 본 논문에서는 해외 운영사의 승객 끌림 방지 기능에 대한 안전무결도 적용 사례를 통해 각 장치 레벨의 안전무결도 뿐 아니라 차량 레벨에서의 안전무결도 적용에 대한 방법론을 제시하고자 한다.

주요어 : 안전무결도, 안전 기능, 독립 안전 평가, 승객출입문, 승객 끌림 방지 기능

1. 서 론

최근 들어 국내는 물론이고 전 세계적으로 환경과 지속가능성에 대한 관심이 높아지고 있으며, 이에 따라 상대적으로 적은 에너지를 소비하면서도 대량 운송이 가능한 철도차량에 대한 수요가 꾸준히 증가하고 있다. 이러한 철도차량의 장점에도 불구하고, 대량의 승객을 운송한다는 점에서 철도차량의 사고는 치명적인 인명 사상을 야기할 수 있다. 이에 대한 대책으로, 철도차량 운영사는 각각의 안전 기능에 임의 고장 (Random Failure) 및 시스템 고장 (Systematic Failure) 관리 수준인 안전무결도 (Safety Integrity Level, SIL)를 할당하여 관리한다. 본 논문에서는 해외 철도차량 운영사의 특정 안전 기능을 사례로 들어 차량 레벨에서의 안전무결도를 보증하는 방안에 대해 기술한다.

† 교신저자: 현대로템주식회사 시스템엔지니어링팀 (yeonsu96@hyundai-rotem.co.kr)
* 현대로템주식회사 시스템엔지니어링팀

2. 본 론

2.1 안전무결도 (Safety Integrity Level, SIL)

2.1.1 안전무결도의 정의

철도차량의 RAMS (Reliability, Availability, Maintainability, Safety) 관련 규격인 EN50126-1:1999은 철도차량의 신뢰성, 가용성, 정비성, 안전성 보증을 위해 철도차량 수명주기에 따른 RAMS 관리 업무를 정의하고 있다. 특히, 요구된 안전 요구사양을 만족했음을 입증하는 문서로 종합안전대책기술서 (Safety Case)를 요구하고 있으며, 종합안전대책기술서 (Safety Case)의 작성에 대한 기준은 신호장치의 안전 관련 규격인 EN50129:2003를 참고할 수 있다.

또한, EN50129:2003의 Annex A에는 안전 요구사양과 안전무결성을 산출, 할당, 적용하는 방안을 기술하고 있으며, 철도 분야 안전 관련 시스템에서의 안전무결도 적용 방안을 기술하고 있다.

기본적으로 시스템 요구 사양은 비 안전 요구 사양 (Non-Safety Requirement)과 안전 요구 사양 (Safety Requirements)으로 분류될 수 있으며, 안전 요구 사양은 안전무결성 요구 사양 (Safety Integrity Requirements)과 안전 기능 요구 사양 (Safety Functional Requirements)으로 분류될 수 있다. 마지막으로 안전무결성 요구 사양은 시스템 고장 무결도 (Systematic Failure Integrity)와 임의 고장 무결도 (Random Failure Integrity)로 구분된다.

시스템 고장이란 정량화 할 수 없는 인적 오류나 품질 관리 또는 소프트웨어 등에서 발생하는 고장을 의미하며, 임의 고장이란 정량화 할 수 있는 부품의 유한한 신뢰성 등에 기인하는 고장을 의미한다. EN50126-1:1999와 EN50129:2003에서는 안전무결도를 시스템 고장 무결도와 임의 고장 무결도의 균형을 맞추기 위한 해당 안전 기능에 대한 안전 기대치 (요구조건)로 정의하고 있다.

2.1.2 안전무결도 (Safety Integrity Level, SIL)의 할당

EN50129:2003의 Annex A는 이러한 안전무결도의 산출을 위해 우선 철도 운영사 (Railways Authority)에 의해 허용가능 위험율 (Tolerable Hazardous Rate, THR)이 정의되어야 한다고 설명하고 있다. 허용가능 위험율 (Tolerable Hazardous Rate, THR)을 정의하기 위해 철도 운영사는 우선 위험도 수용 원칙 (Risk Acceptance Principle)을 정해야 한다.

대표적인 위험도 수용 원칙으로는 ALARP (As Low As Reasonable Practicable) 원칙, GAMAB (Globalement Au Moins Aussi Bon) 원칙, 그리고 MEM (Minimum Endogenous Mortality) 원칙이 있으며, 각 국가의 안전 당국 (Safety Authority)의 별도 지침이 없는 경우, 철도 운영사 (Railways Authority)가 운영하는 철도 환경에 따라 적절한 안전 수용 원칙을 정의해야 한다.

ALARP 원칙은 영국에서 주로 사용하면서 원칙이 정의된 것으로 말 그대로 실행 가능한 위험도를 낮추어야 한다는 의미를 내포하고 있으며, 경제성 원칙에 입각하여 위험도를 저감해야 한다는 원칙이다.

GAMAB 원칙은 프랑스에서 제시한 위험도 수용 원칙으로, 신규로 도입되는 시스템은 기존의 시스템이 가지고 있는 위험 수준 (위험측 고장율)보다 적어도 같거나 작아야 한다는 원칙이다.

마지막으로 MEM 원칙은 독일에서 제시한 위험도 수용 원칙으로, 개개인의 사망률 통계에 기반하여, 기술적인 요인(신규 철도의 도입과 같은)으로 인한 개개인의 사망률이 자연 사망률의 특정 비율 이하로 관리해야 한다는 원칙으로, 각 국가의 철도 사고 통계에 의해 특정 비율은 변경된다.

이러한 위험도 수용 원칙을 고려하여 철도 운영사는 시스템 정의 (System Definition), 위험원 식별 (Hazard Identification), 결과 분석 (Consequence Analysis), 위험도 평가 (Risk Estimation) 및 허용가능 위험율 할당 (THR Allocation)의 절차를 통해 허용가능 위험율을 정의한다.

철도 운영사에 의해 허용가능 위험율 (THR)이 정의되면, SIL은 EN50129:2003의 Annex A에 제시되어 있는 아래 표에 의해 할당될 수 있다.

Table 1 SIL Table proposed in EN50129:2003 Annex A

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	SIL 4
$10^{-8} \leq THR < 10^{-7}$	SIL 3
$10^{-7} \leq THR < 10^{-6}$	SIL 2
$10^{-6} \leq THR < 10^{-5}$	SIL 1

2.2 차량 레벨의 안전무결도 (Safety Integrity Level, SIL) 적용

EN50126-1:1999에도 언급되어 있듯이, 일반적으로 SIL은 하나 또는 그 이상의 간단한 기능을 수행하면서 동일 기능을 수행하는 또 다른 장치로 대체될 수 있는 독립적인 장치에 적용되어야 한다. 이러한 이유로 안전무결도 인증서 또한 전자연동장치, 차상신호장치, 제동제어장치와 같이 독립적인 장치에 부여된다. 본 논문에서는 해외 철도 운영사의 특정 안전기능의 사례를 통해 독립적인 장치가 아닌 차량 레벨의 안전 기능에 할당된 안전무결도를 적용하는 방안을 제시한다.

2.2.1 사례 연구

일반적으로 철도 차량의 승객 출입문에는 장애물 검지 기능이 있어, 승객이나 장애물 등이 승객 출입문에 끼일 경우 출입문을 다시 열거나 추진을 차단하는 안전 기능이 포함되어 있다. 일부 특정 운영사에서는 이러한 장애물 검지 기능과는 별개로, 장애물 검지 기능으로는 검지할 수 없는 얇은 옷깃이나 가방의 끈 등이 승객 출입문에 낀 상태로 차량이 출발하는 사고를 방지하기 위해 승객 끌림 방지 기능 (Anti-Drag Function)을 요구하는 경우가 있다. 본 논문에서는 이러한 승객 끌림 방지 기능 (Anti-Drag Function)에 SIL 4가 할당된 경우를 사례 연구의 대상으로 삼아 차량 레벨에서 어떻게 안전무결도를 적용하였는지를 기술하고자 한다.

2.2.2 안전 기능 정의

안전 기능으로써 승객 끌림 방지 기능을 정의하기 위해서는 해당 기능을 수행하기 위한 하위 기능을 정의해야 한다. 승객 출입문으로 인한 승객 끌림을 방지하기 위해서는 우선 승객 출입문에 승객의 옷깃이나 소지품 등이 출입문 사이에 끼었음을 감지할 수 있어야 한다. 또한, 승객의 옷깃이나 소지품 등이 끼었음이 감지되면 차량의 제어 회로는 비상 제동을 체결하도록 명령을 보내야 하며, 제동 장치는 차량 제어회로의 명령에 따라 비상 제동을 체결해야 한다. 마지막으로 차량이 정지된 상태를 유지할 수 있도록 차량의 추진력을 차단해야 한다. 이를 표로 정리하면 다음과 같다.

Table 2 Definition of Safety Function

SIL Allocated Safety Function	Required Sub-Function
Anti-Drag Function	Passenger Door System : Detection of Thin Obstacles
	Vehicle Control Circuit : Emergency Brake Trigger
	Brake System : Emergency Brake Application
	Traction System : Traction Cut-off

2.2.3 차량 레벨 시스템 구성

상기와 같이 안전 기능이 정의되었으므로, 각각의 하위 안전 기능을 수행할 수 있도록 차량 레벨에서 시스템을 구성해야 한다.

승객 출입문

승객의 옷깃이나 핸드백의 끈과 같이 얇은 장애물을 검지하지 위해서는 출입문 구동 모터의 전류를 측정하거나 스위치를 이용하여 출입문이 완전히 닫혔음을 확인하는 등의 일반적인 장애물 검지 방식과는 다른 설계가 구현되어야 한다. 이를 위해 각 출입문 패널의 모서리 고무 쿠션 (Rubber Leading Edge Seal)을 아래와 같이 특별한 형상으로 설계하였다. 또한 각 모서리의 고무 쿠션 안에는 전기 테이프 스위치 형태의 센서가 각각 2개씩 설치하여, 아래 그림과 같이 얇은 장애물이 낀 상태로 차량이 출발하는 경우에는 붉은 화살표 방향으로 힘이 작용하게 되어 얇은 장애물의 출입문 끼임을 검지할 수 있도록 설계 하였다.

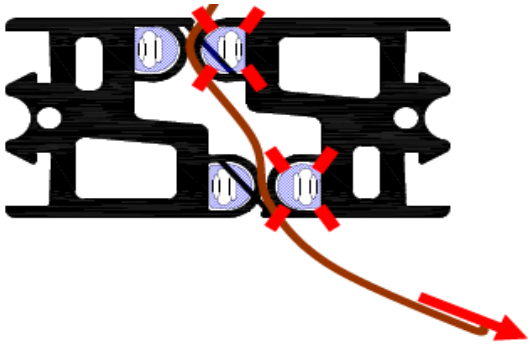

Fig. 1 Design of Leading Edge Seal of Passenger Door Panel

차량 제어 회로

각각의 승객 출입문이 얇은 장애물을 감지한다 하더라도 차량 제어 회로가 이 신호를 적절히 사용하지 못한다면 승객이 출입문에 끼어 끌려 가는 사고를 방지할 수 없다. 이러한 사고를 방지하기 위해, 각 출입문 패널 모서리에 설치되어 있는 센서를 출입문 제어장치 (Door Control Unit, DCU)를 통해 차량 제어 회로에 루프 형태 (Door Loop)로 연결하였다. 출입문 루프의 끝에는 승객 끌림 방지 루프 계전기 (All Door Anti-Drag Loop Relay) 를 설치하였으며, 승객 끌림 방지 루프 계전기 (All Door Anti-Drag Loop Relay)의 NO (Normal Open) 접점을 차량의 비상제동 루프 (Safety Loop)에 직접 연결하였다. 이에 따라 전체 열차의 어느 출입문에서든 하나의 센서라도 얇은 장애물이 끼었음을 감지하면, 차량 제어 회로의 승객 끌림 방지 루프 계전기 (All Door Anti-Drag Loop Relay) 가 여자 되며, 이에 따라 차량의 비상제동 루프 (Safety Loop) 또한 개방 (Open) 되도록 설계하였다.

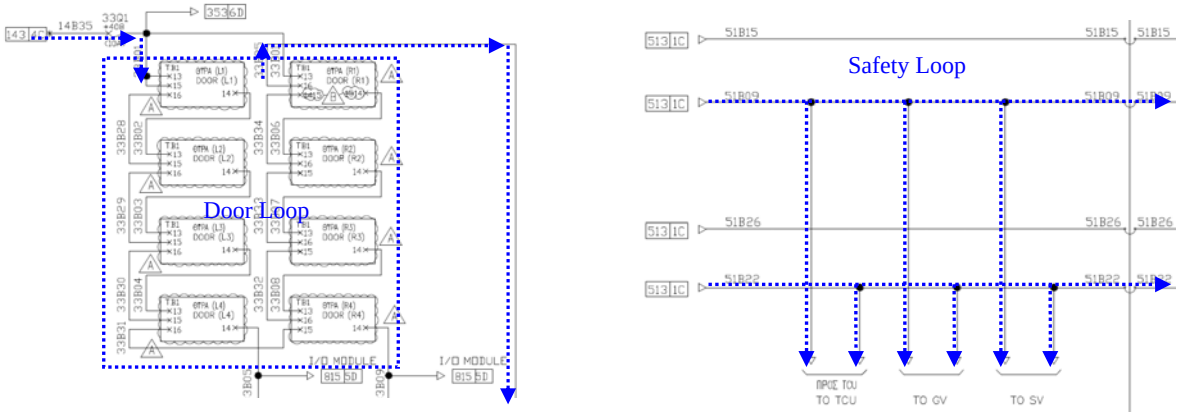

Fig. 2 Door Loop and Safety Loop Design

제동 시스템

차량 제어 회로에서 비상 제동 명령이 주어졌을 때 (비상 제동 루프가 개장 되었을 때) 요구되는 비상제동력을 보증하기 위해 EP2002 분산 제동 제어 시스템을 적용하였다. EP2002 분산 제동 제어 시스템은 전자 제어 부품들과 기계적인 공압 부품들이 하나의 소형화된 밸브로 통합된 제동 시스템으로, 수행하는 기능에 따라 Smart Valve, Gateway Valve, 그리고 Rio Valve로 구분된다. 각각의 EP2002 밸브는 차량에서 요구되는 기능에 따라 차량 레벨로 구성되며, 본 사례에서는 6량으로 구성된 한 편성에 Gateway Valve 4개와 Smart Valve 8개로 구성되어 각각의 EP2002 밸브가 하나의 대차를 제어하도록 구성 하였다. 각각의 EP2002 밸브는 차량 제어 회로의 비상 제동 루프 (Safety Loop)에 직접 연결되어 있어 비상 제동 루프 (Safety Loop)가 개방 (Open)되면 편성 전체에서 비상 제동을 체결한다. 또한, 중복 설계 (Redundancy)를 적용하여 하나의 EP2002 밸브가 고장 나더라도 (하나의 대차가 비상 제동력을 공급하지 못하더라도) 차량에서 요구하는 비상 제동력을 공급할 수 있도록 설계하였으며, 이를 통해 비상 제동이 SIL4에 상응하는 허용가능 위험율(THR)을 만족하였다.

추진 시스템

6량으로 구성된 한 편성 중 4량에 ETRIS T100 인버터를 설치하였으며, 이를 통해 차량에 요구되는 추진력을 얻는다. 비상 제동이 체결되었을 때 추진력을 차단하기 위해 차량 제어 회로의 비상 제동 루프 (Safety Loop)를 ETRIS T100 인버터 내에 있는 ELTAS ECON 추진 제어기 (Traction Control Unit, TCU)에 직접 연결하였다. 이를 통해 비상 제동 루프 (Safety Loop)가 개방(Open) 되면 제동 시스템에서 비상 제동을 체결하는 동시에 추진력 또한 차단된다. ELTAS ECON 추진 제어기 내에서는 소프트웨어에 의한 오류로 인해 추진 차단이 실패하는 고장을 방지하기 위해 소프트웨어와는 독립적인 hard-wired를 통해 추진 차단 명령 (Safety Loop Open) 을 전달하도록 설계하였으며 이를 통해 SIL4에 상응하는 허용가능 위험율 (THR)을 만족하였다.

2.2.4 차량 레벨에서의 안전무결도 (Safety Integrity Level, SIL) 입증

승객 끌림 방지 기능 (Anti-Drag Function)에 할당된 SIL4 요구사양을 입증하기 위해서는 승객 끌림 방지 기능 (Anti-Drag Function)을 구현하기 위한 모든 하위 기능이 SIL4 요구사양을 만족함을 입증해야 한다.

승객 끌림 방지 기능 (Anti-Drag Function)을 구현하기 위한 하위 안전 기능 중, 승객 출입문에 의해 구현되는 얇은 장애물 검지 기능, 제동 시스템에 의해 구현되는 비상 제동 체결, 추진 시스템에 의해 구현되는 비상 제동 체결 시 추진 차단 기능의 경우, 앞서 설명한 바와 같이 하나 또는 그 이상의 간단한 기능으로 구성되어 있으며, 동일 기능을 수행하는 다른 장치 대체될 수 있는 독립적인 장치에 의해 구현된다.

즉, 얇은 장애물 검지 기능은 출입문 패널의 모서리 고무 쿠션 (Rubber Leading Edge Seal)에 의해 구현되고, 비상 제동 체결은 EP2002 밸브에 의해 구현되며, 비상 제동 체결 시 추진 차단은 추진 제어 장치 (TCU)에 의해 구현된다. 따라서, 각 시스템 공급사는 EN50126-

1:1990 및 EN50129:2003의 요구사양에 따라 해당 기능에 대한 종합안전대책기술서 (Safety Case)를 작성하고, 이에 대한 독립 안전 평가 (Independent Safety Assessment, ISA)를 통해 해당 기능이 요구되는 SIL4 요구사양을 만족함을 입증한다.

하지만 승객 출입문, 제동 시스템, 그리고 추진 시스템의 안전 기능이 모든 SIL4 요구사양을 만족한다 하더라도 차량 레벨에서 각각의 기능을 통합하는 차량 제어 회로의 안전이 보증되지 않는다면, 승객 끌림 방지 기능 (Anti-Drag Function)이 SIL4 요구사양을 만족했다고 말하기 어렵다. 따라서, 이미 각 장치 별 종합안전대책기술서 (Safety Case) 및 장치 별 독립 안전 평가 (ISA)를 통해 입증된 얇은 장애물 검지 기능, 비상 제동 체결, 추진 차단 기능의 안전무결도가 차량 제어 회로에 의해 통합되면서 저하되지 않음이 차량 레벨에서 입증되어야 하며, 이를 위해 추가적인 차량 레벨에서의 독립 안전 평가 (ISA)가 추가적으로 필요하다.

차량 레벨 독립 안전 평가 (ISA)를 수행하기 전에 철도차량 제작사는 안전 기능에 관련된 차량 제어 회로에 대한 고장 나무 분석 (Fault Tree Analysis, FTA) 등과 같은 정량적 위험도 평가를 통해 차량 제어 회로가 요구된 SIL에 상응하는 허용가능 위험율 (THR)을 만족함을 입증해야 한다.

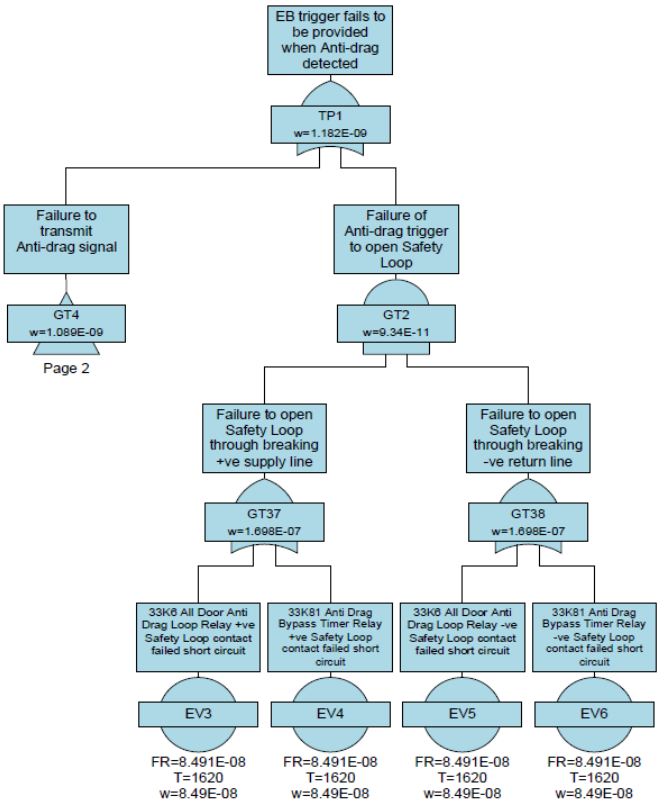

Fig. 3 Example of Fault Tree Analysis for Vehicle Control Circuit

본 논문에서 살펴본 승객 끌림 방지 기능 (Anti-Drag Function) 사례의 경우 철도차량에 안전무결도(SIL)을 적용하는 방안은 다음 표와 같이 요약될 수 있다.

Table 3 Assessment of SIL4 Compliance

SIL Allocated Safety Function	Required Sub-Function	Implemented by	Assessed by	
Anti-Drag Function	Detection of Thin Obstacles	Door	Door ISA	Train Level ISA
	Emergency Brake Trigger	Vehicle Control Circuit	FTA on VCC	
	Emergency Brake Application	Brake	Brake ISA	
	Traction Cut-off	Traction	Traction ISA	

3. 결 론

철도 차량은 수많은 부품, 장치, 시스템이 모여 통합된 기능을 수행하는 복잡한 시스템이다. 따라서 차량 레벨에서 안전 기능이 정의되어 안전무결도가 할당될 경우, 안전무결도 요구 사양이 만족되었음을 입증하기 위해 각각의 하위 안전 기능에 대한 안전무결도 만족이 담보되어야 한다. 뿐만 아니라, 차량 레벨로 통합되면서 차량 제어 회로 등에 의해 각 하위 안전 기능의 안전무결도가 저하되지 않음을 입증해야 한다.

참고문헌

[1] EN50126(1999) Railway applications- The specification and demonstration of Reliability, Availability, Maintainability and Safety(RAMS)

[2] EN50129(2003) Railway application – Communication, signaling and processing systems – Safety related electronic systems for signaling

[3] PD CLC/TR50126-2(2007) : Railway application – The specification and demonstration of Reliability, Availability, maintainability and Safety (RAMS) Part 2 : Guide to the application of EN50126-1 for safety