2022 년도 한국철도학회 춘계학술대회 논문집 KSR2022S039

고신뢰성 디지털 제어기기의 IEC-61508 SIL 인증 사례 연구

IEC-61508 SIL Certification Case Study of High Reliability Digital Control Devices

황청환*, 박재현*†, 전성준**, 박성재**

Cheonghwan Hwang*, Jaehyun Park*†, Seong-joon Jeon*, Seong-jae Park**

초 록 현대의 철도차량은 다수의 전자·전기 시스템과 통신을 기반으로 운용되는 종합시스템으로 이를 구성하는 제어기의 신뢰성과 안정성은 안정적인 철도시스템을 운영하는데 필수적인 요소이다. 철도분야를 비롯하여, 발전소, 화학 플랜트 등 고도의 안정성이 요구되는 분야에서는 국제적으로 IEC-61498 SIL 인증 체계하에서 신뢰성을 검증하고 있다. 본 논문은 철도차량에 사용되는 디지털 제어기의 SIL 인증 사례를 통하여 국내에서 SIL 인증 획득에 애로점과 개선사항을 공유하고자 한다. 본 논문에서 제시하는 애로점과 개선사항은 일차적으로는 철도차량 및 신호체계를 고도화하는데 활용할 수 있으나, 발전소를 비롯한 다양한 산업분야에서도 공통적으로 적용될 수 있을 것이다.

주요어 : IEC-61508, SIL(Safety Integrity Level), 안전무결성수준, 신뢰성, 열차제어시스템

1. 서 론

현대의 철도차량은 다수의 전자/전기 시스템과 통신을 기반으로 운용되는 종합시스템이다. 그러나 철도차량의 제어시스템이 디지털화됨에 따라 제어기기의 시스템 오류는 인명에 큰 영향을 주는 대형사고로 직결될 수 있으므로 제어기기의 안전 기능에 임의 고장(Random Failure) 및 시스템 고장(Systematic Failure)을 체계적으로 관리하는 RAMS (Reliability, Availability, Maintainability, and Safety) 활동과 기능 안전에 대한 인증이 필수 사항으로 자리를 잡아가고 있다[1,2]. 이와 같은 안전기능에 대한 국제 인증으로 널리 사용되는 규격은 IEC-61508 SIL(Safely Integration Level)로, 최근 들어서 해외 및 국내에서 발주되는 대부분의 신규 철도차량사업에서는 신호시스템뿐만 아니라 승강문이나, 열차제어시스템 등에도 SIL 인증을 요구하고 있다[3].

본 논문은 열차의 승강문 제어기(Door Control Unit; DCU)의 IEC-SIL 인증 사례를 통하여 철도차량의 고신뢰성 디지털 제어기기의 SIL 인증 경험을 소개하고자 한다.

† 교신저자: 인하대학교 공과대학 정보통신공학과(jhyun@inha.ac.kr)
* 인하대학교 대학원 전자컴퓨터공학과
** 인터콘시스템스 기술연구소

2. 본 론

2.1 IEC-61508 SIL 인증체계

SIL 인증은 개발 대상 시스템의 개념 설계 단계부터 폐기 단계에 이르는 전체 수명주기 단계 동안에 시스템 개발 단계와 맞물려서 수행되며, 해당 시스템 또는 시스템을 구성하는 하위시스템 및 컴포넌트들이 명시된 기능을 정상적으로 수행하고 있고, 안전하게 정상 운용되고 있는 정도를 정성적이거나 정량적인 척도로 입증하는 절차로, 철도 시스템의 목표인 정해진 수준의 철도 수송을 안전하게 달성할 수 있는지를 평가하고 인증하는 절차이다. SIL 인증을 통하여 철도 제품에 사용되는 소프트웨어, 하드웨어 및 모든 부품이 안전하고 견고한 방식으로 상호 작용하도록 개발되고 모든 관련 CENELEC 표준(EN

50126, EN 50128 및 EN 50129)에 대한 규정 준수를 입증하여 인적 피해가 발생할 위험을 최소화할 수 있다.

2.2 IEC-61508 SIL 인증 사례

철도차량에 사용되는 승강문 제어기(Door Control Unit; DCU)는 열차의 안정적인 운행과 승객의 안전에 직접적인 영향을 미치는 품목으로 국내외 철도 운영사에서는 SIL2급 인증을 요구하고 있다. 이에 따라 국내철도차량에 납품하는 DCU의 경우 TUV Rheinland 사로부터 SIL 인증을 획득하였다.

2.3 애로점과 개선방안

국내 철도차량에 납품하는 DCU에 대한 SIL 인증 과정에서 다양한 애로사항들이 있으며 개선방안은 다음과 같다.

SIL 인증 국제규격의 기본 요구조건이 시스템 수명주기에 따른 안전관리와 품질관리임에도 불구하고 국내에서는 제품 개발 단계에서 RAMS 활동 등에 대한 문서의 생산에 국한되어 일회성으로 진행되는 경향이 있다. 이를 개선하기 위하여 SIL 인증에 대한 올바른 인식 확대 및 국가 등의 지원 프로그램 확장 등의 효과적이고 경제적인 품질 및 안전 확보 지원방안이 수립될 필요가 있다.

또한 국내 발주자 간의 상이한 발주사양을 대체할 수 있는 표준 발주사양의 기능을 갖도록 시스템 별 기술기준을 제정하여 활용하는 것이 바람직하다. 표준에 정의된 발주자와 공급자의 역할을 고려하여 발주자 대신 예비위험분석을 수행하고 표준적인 안전기능과 목표 THR(Tolerable Hazard Rate)을 제시하고, 공급자는 주어진 THR을 하부 부품의 안전기능 SIL로 할당하고 이를 입증하도록 SIL 요구조건을 규정하는 방식이 바람직하다. 더불어, 안전핵심장치 위주로 설계 안전성 요구조건, 내구성 시험, 기능시험 등 최소 공통 요건만을 제시하는 것이 발주자와 공급자 모두에게 가장 경제적이고 효과적인 방안일 것으로 판단된다.

시스템의 안전 상태는 위험원 및 위험성 분석의 결과이며 운영 모드에 따라 달라질 수 있으며 이러한 맥락에서, 안전 무결성 수준(SIL)은 안전 기능이 시스템을 안전 상태에 가도록 요구되었을 때 의도한 대로 수행되는지를 가늠하는 신뢰성 정도에 불과하다. 고장 발생 시에 시스템이 작동을 멈추는 것과 같은 fail safe(안전측 고장) 시나리오와, 최대한 작동하게 하는 것과 같은 fail operation 시나리오에 대한 개념 및 전략에 대한 올바른 설정과 대책수립을 통해 시스템의 안전성을 확보하고 입증하는 것이 SIL 인증의 진정한 목적이자 필요성임을 이해당사자 모두가 이해하여야 한다.

3. 결 론

본 논문은 철도차량에 탑재된 승강문 제어기(DCU)의 IEC 61508 SIL 인증 사례를 통하여 SIL 인증 경험과 개선 사항 등을 제시하였다. SIL 인증은 디지털 제어기기의 신뢰성을 보장할 수 있는 국제적인 표준으로 철도분야뿐 아니라, 원자력, 석유화학 분야 등에서 널리 활용되고 있으므로 본 논문에서 제시한 SIL 인증 경험을 통한 애로점과 개선방안은 타 분야에서도 활용될 수 있을 것으로 보인다.

후 기

본 연구는 원자력안전위원회의 재원으로 한국원자력 안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다(과제번호 2104028).

참고문헌

[1] Y-S Lim, J-E. Oh, M-S Kong, C-Y Kang (2016) Train Level Application of the Safety Integrity Level, *Proc. of Railway Systems Autumn Conference*, pp. 953-960.

[2] Y-H Kim, S-H Lee, K-H Park, T-k Ko (2014) Railway system functional safety and certification, *Trans. Of Korean Institute of Electrical Engineers* 63(4), pp. 226-235.

[3] International Electrotechnical Commission (IEC) (2010) IEC-61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.