열차종합제어장치(TCMS) 안전기능레벨(SIL#2) 적용

Application of TCMS SIL#2

서정규*, 신명준*, 서상준*†, 신광균*, 한정수**

Jeong-gyu Seo*, Myong-Jun Shin*, Sang-Jun Seo*†, Kwang-Kyun Shin*, Jeong-Soo Han**

초 록

철도차량의 품질과 기술이 발전하고 있지만 고장과 사고는 빈번하게 발생하고 있으며, 이에 따라 열차의 안전성을 확보하고 인증 받는 기술은 더욱 대두되고 있다. 국내외 시행청은 안전성 확보를 위해 안전인증(SIL: Safety Integrity Level)을 요구하고 있고, 국제규격에 등재된 EN50126, EN50128, EN50129 에 따라 평가기관인 ISA (Independent Safety Assessment) 에게 인증을 받을 수 있다. 현대로템 통신시스템팀은 국내 최초로 열차종합제어장치(TCMS) 에 SIL#2 인증을 받았으며 말레이시아 KVMRT2, 코레일 과천안산선, 경원선, 1호선의 안전인증레벨 SA(Specific Application) SIL#2 적용에 성공하였다. 본 논문에서는 실질적으로 양산 차량에 적용할 수 있는 SIL#2 인증 적용과정을 소개한다.

주요어 : 열차종합제어장치, TCMS, CCU, 안전기능레벨2, 안전인증, SA, 현대로템

1. 서 론

이 문서는 현대로템 열차종합제어장치(TCMS) SIL#2 적용 프로세스를 소개하며 인증에 필요한 설계 방법과 산출물에 대하여 설명한다.

2. 본 론

2.1 SIL#2 인증 프로세스 (하드웨어)

2.1.1 하드웨어 설계

열차종합제어장치(TCMS: Train Control and Monitoring System) 는 많은 제어기능이 있고 시행청의 요구사항에 따라 제어로직이 자주 변경되므로 효과적인 인증방법을 위해 중앙제어장치인 CCU (Central Control Unit)의 기능 중 안전에 관련된 기능을 선별하여 SCU (Safety Control Unit) 장치 설계 및 SIL#2 인증 프로세스를 수행한다.

Table 1 SCU Digital Input, Output

Data	Description
DI	Safety Proving Loop Normal Status
	Safety Interlock Lamp Activated
	Brake Not Released
	Safety Interlock Lamp (Maintain)
	Safety Interlock Lamp (Flashing)
DO	Traction Cut by Stuck Brake
	TMS SIL2 Major Failure

2.1.2 하드웨어 위험분석 검증

SIL#2 인증을 위한 위험분석은 FTA (Fault Tree Analysis)를 활용한다. FMECA (Failure Mode Effects & Criticality Analysis) 에서 위험항목으로 식별 된 항목을 기반으로 제어장치의 하위 결함 트리(소자의 고장률) 부터 제어 보드, 렉 단위까지 고장률을 계산한다. 말레이시아 KVMRT2 SCU 의 경우 Winchill 프로그램을 사용하여 실패 비율 $3.69213e^{-7}$ 으로 고장률 조건을 안정적으로 만족했다.

(SIL#2 : $1*10^{-7} \leq$ 고장률 $\leq 1*10^{-6}$)

† 교신저자: 현대로템 시스템연구실 통신시스템팀(sjseo@hyundai-rotem.co.kr)
* 현대로템 시스템연구실 통신시스템팀
** 현대로템 시스템연구실

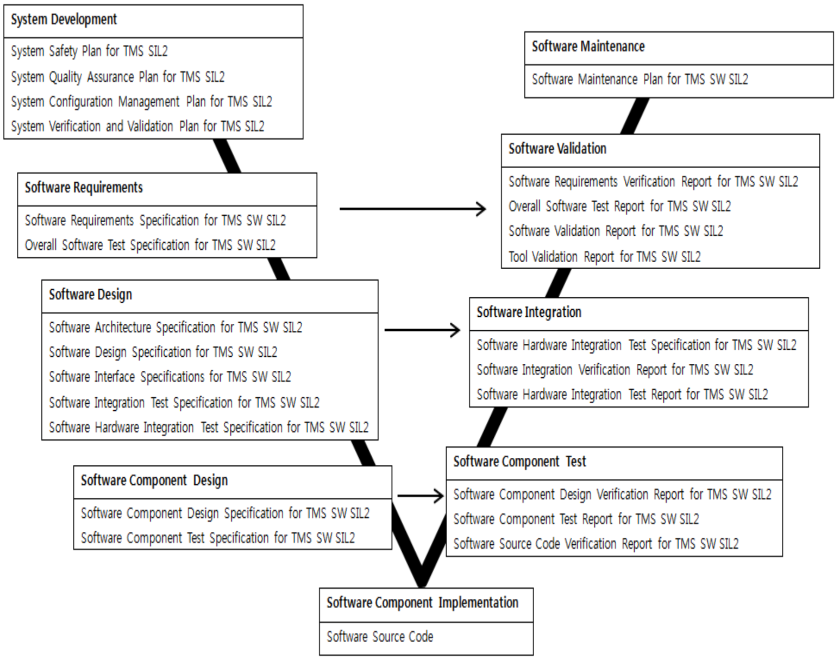

Fig. 1 SW 설계 및 검증 산출물

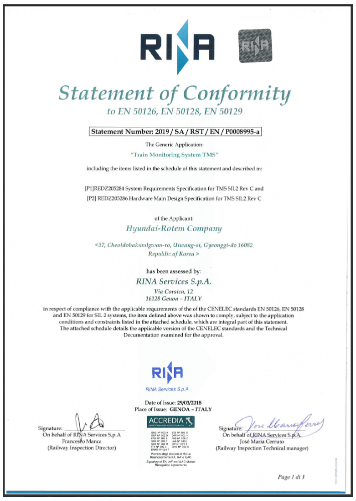

Fig. 2 SIL#2 인증서

2.2 SIL#2 인증 프로세스 (소프트웨어)

2.2.1 소프트웨어 설계

ISO 90003 및 EN50128 기반 품질보증 계획을 기반으로 시행청의 기능요구사항에 대한 SW를 설계한다. 단계별로 필요한 SW 설계 프로세스와 산출물은 **Fig. 1** 의 V모델을 기반으로 작성한다.

2.2.2 소프트웨어 검증

열차종합제어장치(TCMS) 는 SW, HW 통합 시스템에 대한 안전인증을 받아야 하므로 SW 소스코드는 IEEE-STD-829에 기반 하여 정적, 동적 테스트를 완료 후 SW, HW 통합 테스트를 수행해야 한다. Software Hardware Integration Test Report 문서에 발생 가능한 모든 Test Cases 테스트 검증 결과를 첨부해야 한다.

마지막으로 HW, SW 단계별 모든 산출물과 품질, 형상관리 계획서를 종합하여 판단한 Safety Case 보고서를 작성한다.

3. 결 론

설계와 검증이 끝나면 단계별 모든 문서를 평가기관 ISA에 제출하여 인증절차를 진행한다. 양산 적용을 위해 GA(Generic Application), SA(Specific Application) SIL#2 안전기능레벨을 받으며, 현대로템 열차종합제어장치의 안전성과 기술력을 인증 받았다.

Fig. 2 에서 ISA 인 RINA 의 평가를 받은 말레이시아 KVMRT2 열차종합제어장치 SIL#2 인증서를 확인할 수 있다.

참고문헌

[1] EN 50126(2017): Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

[2] EN 50128(2011): Railway applications – Communications, signaling and processing systems, Software for railway control and protection systems.

[3] EN 50129(2003): Railway applications – Communications, signaling and processing systems, Safety related electronic systems for signaling.

[4] Shin Han (2014): 한국철도학회 춘계학술대회 논문집 – Introduction of certify process for TMS SIL#2 system.