논문 2022-17-20

안전무결성을 달성하기 위한 FMEDA 분석 기반 PESSRAE 설계

(Design of PESSRAE To Achieve Safety Integrity With FMEDA Analysis)

허 제 호*, 김 기 봉, 정 기 현, 안 석 찬
(Jeho Heo, Gi-bong Kim, Gi-Hyun Jung, Seokchan An)

Abstract : As the number of the installed escalators in Korea continues to increase, the accident rate is also increasing. Therefore, it would be necessary to proactively secure safety. PESSRAE is a controller that implements safety functions as electric/electronic/programmable electronic devices to respond to risks that may occur in escalators. Safety Integrity Level (SIL) is assigned to the safety functions of PESSRAE and it must be verified that the quantitative target value according to the SIL level is satisfied. In this paper, the initial PESSRAE is analyzed using the FMEDA (Failure Mode, Effects and Diagnostic Analysis), which is a quantitative safety analysis method, and design improvement specifications are derived from the analysis in order to satisfy the quantitative target values. Based on the derived design specifications, the improved PESSRAE controller was manufactured. And the appropriateness of the design was verified experimentally in a testbed environment simulating the real environment.

Keywords : PESSRAE, FMEDA, Safety Integrity, Functional Safety, SIL

Ⅰ. 서 론

1. 에스컬레이터 사고현황 및 규제

우리나라 승강기는 2019년 기준 70만대를 넘어섰으며 이 수치는 설치대 수 기준 세계 8위, 신규 설치대 수 기준 세계 3위 정도의 수준이다. '승강기'라는 단어는 대표어로, '승강기'의 범주에는 엘리베이터, 에스컬레이터 및 무빙워크 등이 포함된다 [1].

에스컬레이터 특성상 지하철, 백화점 및 쇼핑몰 등 불특정 다수가 이용하는 복합 대형 시설에 설치 운용되므로, 사소한 결함으로도 대형 인명사고로 이어질 소지가 크다. 2007년~2018년 승강기 종류별 사고 현황으로 에스컬레이터 사고가 42.14%로 가장 많이 발생하였다. 이는 승강기 종류에서 엘리베이터 91.5%이고 에스컬레이터 5%로 엘리베이터가 절대적으로 많음을 감안하면, 에스컬레이터가 설치 대수 대비 매우 높은 사고율을 보임을 알 수 있다 [2].

*Corresponding Author (jhheo@ktl.re.kr)
Received: Oct. 21, 2021, Revised: Dec. 1, 2021, Accepted: Feb 7, 2022.
J.H. Heo: KTL (Senior Researcher) / Ajou University (Ph.D. Candidate)
G.B. Kim: SERA S.E (Director)
G.H. Jung: Ajou University (Prof.)
S.C. An: KTL (Researcher)
※ 이 논문은 2022년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00122, 고안전 SW 개발을 위한 안전 분석 및 검증 도구 기술 개발).

ⓒ IEMEK J. Embed. Sys. Appl. 2022 Jun. 17(3) 157-165
ISSN : 1975-5066
http://dx.doi.org/10.14372/IEMEK.2022.17.3.157

특히 상승 운행 중 갑작스러운 역주행에 의한 인명사고가 반복적으로 발생하고 있으며, 동시 탑승자가 많은 특성상 에스컬레이터 역주행 안전사고는 건당 피해자 수가 많아 미온적 사후 대응이 아닌 안전관리 시스템 개선을 통한 예방적 안전관리가 필요하다.

이에 정부 (행정안전부)는 에스컬레이터의 위험 요소에 대해 별도의 전기안전장치의 안전기능을 통해 안전을 확보할 것을 승강기 안전부품 안전기준으로 고시하고 있다 [3].

2. PESSRAE (Programmable Electronic Systems in Safety Related Applications for Escalators and moving walks)

에스컬레이터의 안전기능을 수행하는 안전 관련 전기, 전자 및 프로그래밍 가능한 전자장치 (Safety-related E/E/PE devices)를 PESSRAE라고 지칭한다.

승강기 안전부품 안전기준에서 PESSRAE를 전원 공급장치, 센서, 기타 입력 장치, 액추에이터 및 기타 출력 장치와 같은 시스템의 모든 요소를 포함하는 전기, 전자 또는 프로그램 가능한 전자장치 (E/E/PE)를 기반으로 하는 제어, 보호 또는 감시하는 시스템으로 정의하고 있다 [3].

승강기 안전부품 안전기준에서 요구하는 안전기능의 구현이 E/E/PE로 구현되는 경우 기준에서는 안전무결성수준 (SIL)을 요구하고 있다. PESSRAE의 안전기능에 대해 최고 SIL2 수준을 요구하고 있다. SIL1은 가장 낮은 수준을 나타내고, SIL3은 가장 높은 수준을 나타내므로, PESSRAE는 중

간 정도의 SIL이 요구된다는 것을 알 수 있다 [4].

안전무결성수준을 충족하기 위해서는 안전기능을 구현하기 위해 사용된 하드웨어 및 소프트웨어의 오작동에 대응하기 위한 진단기능의 설계가 필수이다 [4].

3. 연구 동향 및 핵심연구 내용

지금까지 에스컬레이터 사고를 중심으로 사고사례 분석을 통한 승강기 이용자 안전사고예방을 위한 안전관리 방안 연구 [1, 5, 6]와 안전기능 자체의 구현과 검증과 관련된 연구 [7]가 주로 이루어졌으나, E/E/PE로 구현하여 에스컬레이터 안전기능의 안전무결성을 확보하기 위한 연구는 없었다.

안전무결성 확보를 위한 ESS (Energy Storage System) 분야 BMS (Battery Management System)와 자동차산업 EPS (Electrical Power Steering) 등 타 산업 분야의 노력은 확인할 수 있었으나 [8, 9], 승강기 분야의 안전제어기에 대한 안전무결성을 확보하기 위한 연구는 없었다.

본 연구에서는 하드웨어 안전무결성을 중심으로 회로도 수준에서 하드웨어의 잠재적인 고장위험을 찾아내고, 에스컬레이터 안전장치의 각 구성 부품에 대하여 고장모드 영향분석 (FMEDA)을 실시하여 정량적인 안전분석을 통해 초기 설계가 어떻게 개선되고, 개선된 요구사항이 목표로 하는 하드웨어 안전무결성수준을 만족하게 하는 방법을 제안한다.

제안하는 방법으로 초기 설계된 에스컬레이터 안전장치의 하드웨어 및 펌웨어를 분석하고, 분석결과를 통해 정량적 목표 값에 영향을 미치는 높은 고장모드를 찾고, 이를 제거하거나 줄이기 위해 설계 개선 및 진단기능을 추가로 설계하여 에스컬레이터 안전장치의 하드웨어 및 펌웨어를 재설계한다. 그리고 이를 에스컬레이터 안전장치로 제작하여 잠재적인 부품결함이나 펌웨어 오작동 발생한 경우에도 에스컬레이터의 안전이 확보될 수 있음을 실험으로 검증한다.

Ⅱ. 본 론

1. 안전무결성 (Safety Integrity)

안전무결성은 하드웨어 안전무결성과 시스템적 안전무결성 (Systematic Safety Integrity)으로 구성되어 있다. 시스템적 안전무결성은 제어기 개발 과정 중에 사람으로 인한 에러의 개입을 최소화하기 위해 체계적인 방법론 적용하는 것과 관련된 무결성으로 본 논문에서는 다루지 않는다. 본 논문에서는 안전기능이 구현된 PESSRAE 제어기의 설계를 FMEDA 방법으로 분석하고 개선하는 방법을 통해 정량적인 목표 값을 기반으로한 하드웨어 안전무결성을 어떻게 달성하는지 보인다.

하드웨어 안전무결성은 그림 1 [10]과 같이 구조적 제약과 안전기능에 대한 시간당 위험 고장률 목표값을 만족하는 경우 목표 무결성 수준을 달성할 수 있고 본다.

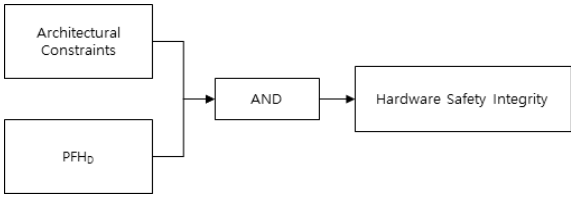

그림 1. 하드웨어 안전무결성 구성

Fig. 1. Hardware Safety Integrity

표 1. 구조적 제약 달성 방안

Table 1. Architectural Constraints

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60%	Not permitted	SIL1	SIL2
60% - < 90%	SIL1	SIL2	SIL3
90% - < 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

1.1 구조적 제약 (Architectural Constraints)

구조적 제약이란 안전기능을 수행하는 하드웨어 결함 허용수준 (HFT, Hardware Fault Tolerance)과 안전 고장 비율 (SFF, Safe Failure Fraction) 지표를 통해 안전 기능의 설계의 구조적인 특징을 제약하는 것을 말한다.

구조적 제약은 HFT와 산출된 SFF의 값이 다음의 표 1 [11]을 만족하여야 한다. 예를 들어 하드웨어 결함 허용수준이 1이고 안전 고장비율이 60%보다 크고 90% 작은 값이라면 SIL2를 만족할 수 있다는 의미이다.

1.1.1 하드웨어 결함 허용수준 (HFT)

하드웨어 결함 허용수준은 결함 또는 오류가 존재할 때 안전기능을 지속적으로 수행하기 위해 필요한 기능 단위 (장치)의 개수를 의미한다. 즉, 하드웨어 결함 허용수준이 N이라는 것은 N개의 결함까지는 안전기능의 오동작을 초래하지 않고 작동할 수 있지만, N+1개의 결함이 존재하게 되면 안전기능의 오동작을 초래하게 되는 것을 의미한다.

1.1.2 안전 고장 비율 (SFF)

안전 고장비율은 E/E/PE 안전관련 시스템에서 발생하는 고장 중 안전기능의 오동작을 직접적으로 초래하지 않는 고장의 비율 정도를 나타내는 값을 의미하고 다음과 같은 식으로 구할 수 있다.

$$SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{DD}}{\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU}}. \quad (1)$$

λ_S : 안전 고장 (safe failures)

λ_{DD} : 검출되는 위험 고장 (detected dangerous failures)

λ_{DU} : 검출되지 않는 위험 고장 (undetected dangerous failures)

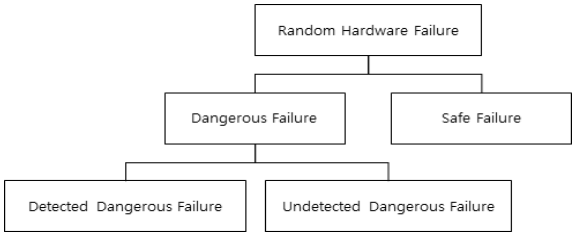

그림 2. 하드웨어 우발고장 분류 [10]
Fig. 2. Random Hardware Failure Category

표 2. 시간당 위험 고장률 (PFH_D) 목표값 [11]
Table 2. Target Failure Rate for PFH_D

SIL	Average frequency of a dangerous failure of the safety function [h-1] (PFHD)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

안전 고장비율의 값이 증가할수록 안전기능의 실패를 발생시키는 위험 고장 발생 확률이 낮다는 것을 의미한다. 안전 고장비율을 도출하기 위해서는 모든 고장모드의 영향을 판단할 수 있는 상세한 하드웨어 설계도가 필요하다. 동일한 형태의 잠재고장 또는 결함 존재하는 경우에도 대상 제품의 종류, 형태, 구조 등의 상이한 요소 때문에 다른 결과를 초래할 수 있으므로, 적용분야 또는 제품에 대한 상세한 이해가 선행되어야 한다.

위에서 설명한 안전 고장비율은 간단히 표현하면 전체 하드웨어 우발고장 중 안전기능의 손실을 초래하지 않는 고장의 비율이 어느 정도인지를 제시하는 척도이다. 하지만 안전 고장비율은 다양한 종류의 하드웨어 우발고장들로 구성되어 있다. 따라서 올바른 안전 고장비율을 도출하기 위하여 하드웨어 우발고장의 종류에 대한 명확한 정의와 이해가 요구된다. 하드웨어 우발고장의 종류에 대한 분류와 정의는 그림 2와 같다.

안전 고장 (λ_S)은 비록 해당 고장이 발생하더라도 안전기능의 목적을 달성하는데 영향을 미치지 않는 고장을 말한다. 위험 고장 (λ_D)은 고장이 발생한 경우, 안전기능의 오동작을 유발하여 위험 상황으로 전개될 수 있는 가능성이 있는 고장을 말한다.

또한, 검출된 위험 고장 (λ_{DD})은 위의 위험 고장 중 진단기능으로 검출되는 고장을 말하며, 검출되지 않는 위험 고장 (λ_{DU})은 위의 위험 고장 중 진단기능으로 검출되지 않는 고장을 말한다.

1.2 시간당 위험 고장률 (PFHD)

시간당 위험 고장률은 안전기능의 오동작 수준을 정량적으로 나타내는 지표이다. 시간당 위험 고장률은 하드웨어 우발고장률을 바탕으로 다양한 신뢰성 모델링을 통한 예측기법을 사용하여 추정한다. 신뢰성 모델링을 통해 추정된 고장률은 E/E/PES 안전무결성 요구사항 명세를 바탕으로 도출된 목표 고장 기준에 SIL 등급에 따라 그 범위 안에 들어야 한다. 시간당 위험 고장률 목표값은 표 2 [11]와 같다.

2. FMEDA 기법 [12]

하드웨어 안전무결성 달성을 확인하기 위한 지표인 SFF 및 잔존하는 고장률 산출을 위해서 FMEDA 방법을 통한 분석이 필요하다.

FMEDA는 하드웨어 회로도 상의 파트, 컴포넌트 수준에서 각각의 부품의 고장 모드가 타 부품과 시스템 및 사용자에게 미치는 영향과 고장의 원인을 상향식 (bottom-up)으로 분석하는 정량적인 안전분석 방법이다.

FMEDA를 수행하는 단계는 다음과 같다.

1단계) 회로도 상의 부품 및 기능식별
2단계) 고장률 도출
3단계) 고장 모드 / 고장 모드 분포 도출
4단계) 영향 분석 및 고장형태 분석
5단계) 진단기능 및 커버리지 식별
6단계) 잔존하는 고장률 및 SFF 값 산출

1단계는 분석 대상이 되는 하드웨어 회로도 수준의 부품 리스트를 산출하는 것이다. 여기에는 제어기를 구성하고 있는 모든 소자와 컴포넌트가 포함된다.

2단계는 정량적인 분석의 기본데이터가 되는 하드웨어 소자 및 컴포넌트의 고장률 값을 도출하는 것이다. 하드웨어 소자 및 컴포넌트의 고장률은 임의 값이 아니라 널리 알려진 산업 소스 (예, IEC TR 62380, IEC 61709 등), 필드 통계치 및 전문가 판단을 통해 산출할 수 있다. FMEDA 분석이 이 값을 기준으로 분석되기 때문에 신뢰할 수 있는 소스로부터 해당 값을 도출하는 것이 중요하다. 본 논문에서는 SIEMENS의 SN29500 [13]을 기반으로 고장률이 도출되었다.

3단계는 하드웨어 소자 및 컴포넌트의 고장 모드 및 고장 모드 분포를가 산출하는 것이다. 이 역시 정량적인 값이기 때문에 믿을 만한 소스에서 산출될 수 있어야 한다. 본 논문에서는 FMD2016 [14]을 기준으로 기계적인 고장모드를 전기/전자적인 관점에서 동일하게 간주 될 수 있는 고장모드로 정제하여 사용하였다.

4단계에서는 회로 내 소자 및 컴포넌트의 기능 관점에서 영향을 분석하여 최종 안전기능의 정상 동작에 영향을 미치는 여부에 따라 안전고장, 검출된 위험 고장, 검출되지 않은 위험 고장으로 분류하게 된다.

5단계에서는 회로 내 소자 및 컴포넌트의 고장 모드가 위험 고장으로 분류된 경우, 해당 위험 고장에 대응하기 위한 진단기능의 존재 여부와 진단기능이 해당 고장 모드를 얼마나 잘 대응할 수 있는지의 커버리지 값을 기반으로 검출되는 위험 고장의 비율 및 값을 산출한다.

6단계에서는 회로 내 모든 소자와 컴포넌트에 대해 1~5단계 과정을 반복하고 각각의 고장 값을 기반으로 잔존하는

고장률 값과 SFF 값을 산출하여 SIL 기준의 설계 적절성을 판단하게 된다.

3. PESSRAE 초기 설계 및 분석

개발한 PESSRAE은 총 9개의 안전기능을 수행한다. 본 논문에서 제시한 방법을 통해 모든 안전기능의 무결성 확보가 분석되고 검증되었다. 다만, 본 논문에서 제시한 방법을 효과적으로 설명하기 위해 과속감지 기능에 초점을 맞춰 설명하고자 한다. FMEDA 분석을 통해 초기 설계의 하드웨어 안전무결성의 취약점이 어떻게 식별되고 취약점을 개선하기 위한 설계 사양 개선 과정을 설명하고자 한다.

3.1 PESSRAE 초기 설계

PESSRAE의 과속방지 기능은 엔코더를 통해 입력된 펄스 신호를 기반으로 에스컬레이터의 평균속도를 산출하고 이 평균속도가 정격속도를 120% 초과하는 경우, 안전라인 릴레이를 오픈시켜 에스컬레이터 구동 모터에 인가되는 전원을 끊는 안전기능이다.

과속방지 기능을 수행하기 위한 PESSRAE 제어기 구조는 입력 인터페이스, 로직 모듈, 출력 액추에이터로 구성되어 있다. 입력 인터페이스는 엔코더 센서의 전원단과 제어기 내부 전원을 분리하기 위해 포토커플러를 사용하여 설계되었다. 속도 산출과 과속여부 판단을 위한 로직 모듈을 구현에는 ATMEL사의 SAM 시리즈 MCU가 사용되었다. 출력 액추에이터는 안전릴레이로 구성되었다. 이 안전릴레이의 오픈은 전체 에스컬레이터 시스템에서 에스컬레이터의 구동 모터로 입력되는 전원을 차단하는 역할을 한다. 에스컬레이터의 안전상태는 정지 상태로 과속이 발생한 경우, PESSRAE 제어기가 과속을 판단하여 안전릴레이를 오픈시킴으로써 전체 에스컬레이터 시스템의 안전을 확보할 수 있게 된다. 초기 설계의 개념적인 회로도는 그림 3과 같다.

3.2 초기 설계 FMEDA 분석

그림 3의 초기 회로도 상에서 RL6 릴레이의 고장모드를 분석하여 하드웨어 우발고장 형태를 분류하면 표 3과 같다. 사용한 고장률 단위는 FIT (Failure In Time)으로 $10^{-9}h^{-1}$을 의미한다. 1 FIT는 10^{9}h 시간에 한번 고장나는 것을 의미한다. 각 파트의 초기 고장률은 SN29500 [13]의 고장률 모델식을 기반으로 산출하였다. 예를 들어, RL6의 릴레이 고장률은 수식 (2)에 따라 릴레이 사양을 기반으로 도출되었다.

$$\lambda = \lambda_{ref} \times \pi_L \times \pi_E \times \pi_T \times \pi_K. \quad (2)$$

λ_{ref} : 기본 고장률 (failure under reference condition)
λ_L : 부하 인자 (factor for load dependence)
λ_E : 환경 인자 (factor for environment dependence)
λ_T : 온도 인자 (temperature dependence factor)
λ_K : 고장 기준 인자 (factor for failure criterion)

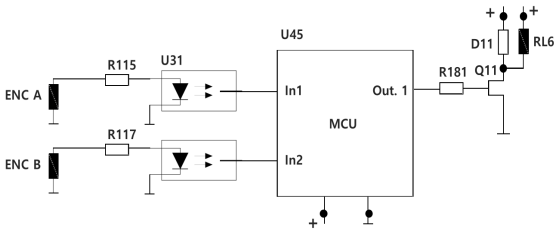

그림 3. 초기 개념 회로도
Fig. 3. Initial Conceptual Electronic Circuit

표 3. RL6 안전릴레이 고장 분류
Table 3. Failure Mode of RL6

Part	Failure Rate	Failure Mode	FIT
RL6 (500FIT)	Open (60%)	Safe Failure (λS)	300
	Short (40%)	Undetected dangerous Failure (λDU)	200

릴레이가 Open 되는 고장모드는 에스컬레이터의 안전라인을 오픈시켜 에스컬레이터 구동 모터의 전원을 차단하기 때문에 고장이기는 하지만 안전한 형태로 나타나는 안전고장으로 분석할 수 있다. 그러나 릴레이가 Short, 즉 웰딩 되는 고장모드는 릴레이의 오픈 제어가 불가능하므로 위험 고장으로 분류될 수 있다. 그리고 RL6가 Short 된 상태를 진단하거나 확인할 수 있는 설계가 없으므로 최종적으로 검출되지 않는 위함 고장으로 분류되었다.

정량적인 고장률 값은 RL6의 초기 고장률 500 FIT 값을 기준을 Open (60%), Short (40%)의 고장모드의 고장비율에 따라 각각 안전 고장 (λ_S) 300 FIT, 검출되지 않는 위험 고장 (λ_{DU}) 200 FIT로 산출되었다.

그림 4는 초기 설계에 대해 FMEDA를 수행한 전체 결과이다. 과속방지 기능과 관련된 하드웨어 회로도 수준의 파트와 컴포넌트에 대해 2장에서 설명한 FMEDA 방식을 적용한 것이다. 과속방지 기능관점에서 PFHD 값은 약 467 FIT가 SFF 값은 57.26%가 각각 산출되었다. 이 SFF 값은 잔존고장률 관점에서는 SIL 2를 달성하기 위한 범위에 들지만, 구조적 제약 관점에서는 SIL 2를 달성할 수 없음을 확인하였고, 이를 통해 PESSRAE의 최초 설계안은 하드웨어 안전무결성수준을 달성할 수 없음을 확인하였다.

4. 설계 개선

구조적 제약 관점에서 SIL 2를 달성하기 위한 방법은 다음의 3가지가 존재한다.

방안 1) HFT = 0, 90% < SFF < 99%,
방안 2) HFT = 1, 60% < SFF < 90%,
방안 3) HFT = 2, 0% < SFF < 60%

설계 수정을 위해 선택할 수 있는 방법을 표 4와 같이 하드웨어, 소프트웨어, 안전무결성 관점에서 비교하여 두 번째 방법을 선정하였다.

Failure Rate / Failure Mode						Failure Effect (Safety Aspect)								
Category	Ref.	Part function	failure rate (FIT)	failure mode	failure mode dist. (%)	안전 관련 고장 영향	SF01 영향성	Diagnostic	DC (%)	λDd	λDu	λS (λSd+λSu)	λS+λDd	Safety related λS+λDd
ENC A/B	R114	1k noise protection	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.08	0.01	0.00	0.08	0.08
				open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
	R115	3.3k / diode(A-C) load	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.08	0.01	0.00	0.08	0.08
				open	60.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.11	0.01	0.00	0.11	0.11
	R116	3.3k / diode(A-C) load	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.08	0.01	0.00	0.08	0.08
				open	60.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.11	0.01	0.00	0.11	0.11
	R117	1k noise protection	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.08	0.01	0.00	0.08	0.08
				open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
	U31	High Speed Transistor Optocouplers	10.0000	open	50.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	4.50	0.50	0.00	4.50	4.50
				short	10.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.90	0.10	0.00	0.90	0.90
				drift	40.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	3.60	0.40	0.00	3.60	3.60
	R112	10k / Pull-up	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.08	0.01	0.00	0.08	0.08
				open	60.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.11	0.01	0.00	0.11	0.11
	R113	10k / Pull-up	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.08	0.01	0.00	0.08	0.08
				open	60.00%	신호입력 불가 -> 속도측정 불가능	O	ENC A/B상 비교	90.0%	0.11	0.01	0.00	0.11	0.11
MCU	U45	Core	12.1505	연산오류 및 데이터 읽기/저장 오류	100.00%	안전기능 수행 불가능	O	없음	0.0%	0.00	12.15	0.00	0.00	0.00
	C15	전원안정화 - VDDCORE	0.7851	short	31.27%	전원 공급 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.25	0.00	0.00	0.00
				open	6.77%	영향 없음	X			0.00	0.00	0.05	0.05	0.05
				drifts	61.87%	전원 공급 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.49	0.00	0.00	0.00
	C16	전원안정화 - VDDCORE	0.7851	short	31.27%	전원 공급 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.25	0.00	0.00	0.00
				open	6.77%	영향 없음	X			0.00	0.00	0.05	0.05	0.05
				drifts	61.87%	전원 공급 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.49	0.00	0.00	0.00
	Y1	crystal	30.0000	short	49.50%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	14.85	0.00	0.00	0.00
				open	50.50%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	15.15	0.00	0.00	0.00
	C19	clock generation	0.7851	short	31.27%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.25	0.00	0.00	0.00
				open	6.77%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.05	0.00	0.00	0.00
				drifts	61.87%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.49	0.00	0.00	0.00
	C20	clock generation	0.7851	short	31.27%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.25	0.00	0.00	0.00
				open	6.77%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.05	0.00	0.00	0.00
				drifts	61.87%	클락생성 불가 -> 안전기능 수행 불가능	O	없음	0.0%	0.00	0.49	0.00	0.00	0.00
안전라인 릴레이	R181	TR bias current 생성	0.2123	short	40.00%	영향 없음	X			0.00	0.00	0.08	0.08	0.08
				open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
	Q11	TR switch	1.6443	short	37.50%	C-E short : 안전상태 달성 불가능	O	없음	0.0%	0.00	0.62	0.00	0.00	0.00
				open	62.50%	영향 없음	X			0.00	0.00	1.03	1.03	1.03
	D11	역전압 방지	16.3613	short	60.00%	안전상태 달성 불가능	O	없음	0.0%	0.00	9.82	0.00	0.00	0.00
				open	40.00%	영향 없음	X			0.00	0.00	6.54	6.54	6.54
	RL6	Relay	500.0000	short	40.00%	안전상태 달성 불가능	O	없음	0.0%	0.00	200.00	0.00	0.00	0.00
				open	60.00%	영향 없음	X			0.00	0.00	300.00	300.00	300.00
보조브레이크 릴레이	R189	TR bias current 생성	0.2123	short	40.00%	영향 없음	X			0.00	0.00	0.08	0.08	0.08
				open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
	Q15	TR switch	1.6443	short	37.50%	C-E short : 안전상태 달성 불가능	O	없음	0.0%	0.00	0.62	0.00	0.00	0.00
				open	62.50%	영향 없음	X			0.00	0.00	1.03	1.03	1.03
	D13	역전압 방지	16.3613	short	60.00%	안전상태 달성 불가능	O	없음	0.0%	0.00	9.82	0.00	0.00	0.00
				open	40.00%	영향 없음	X			0.00	0.00	6.54	6.54	6.54
	RL8	Relay	500.0000	short	40.00%	안전상태 달성 불가능	O	없음	0.0%	0.00	200.00	0.00	0.00	0.00
				open	60.00%	영향 없음	X			0.00	0.00	300.00	300.00	300.00
		Total	1093.0008							9.9173	467.1505			625.8475
		safety-related part/component	**1093.0008**							PFH	467.1505			57.26%

그림 4. 초기 설계 FMEDA 분석 결과
Fig. 4. Random Hardware Failure Category

표 4. 설계 수정 방안 비교
Table 4. Comparison among design solution

No.	Hardware Cost	Software Cost	Integrity
1	No additional cost	Increase in design/change manpower (High)	Relay Failure Rate High
2	Production cost doubled	Increase in design/change manpower (Medium)	Relay Failure Rate Reduced
3	Production costt tripled	Increase in design/change manpower (Medium)	Overspec

하드웨어 추가비용 상승이 없는 방안 1도 가능한 방법이긴 하나 FMEDA 분석에서 볼 수 있는 것처럼 초기 고장률이 상당하고 잔존 위험 고장률에 많은 비율을 차지하고 있어 적절하지 않고 방안 3은 하드웨어를 3중화하는 방법으로 하드웨어 제작 비용 상승 상당하여 방안 2를 적절한 방법으로 결정하여 설계를 개선을 수행하였다.

방안 2를 위한 설계 개선 내용은 다음과 같다.

1) 그림 5와 같이 MCU를 두 개 두어 과속에 관한 판단을 그림 5와 같이 이중화하였다. 그리고 그림 5의 Mon 포트를 통해 통신을 통한 상호 모니터링 진단기능을 추가하였다.

2) 로직 설계 이중화에 따라 입력부 역시 그림5의 U37를 추가하여 이중화 설계를 진행하였다. 또한, ENC A와 ENC B 상을 비교하는 로직과 이중화된 로직에서 산출하고 있는

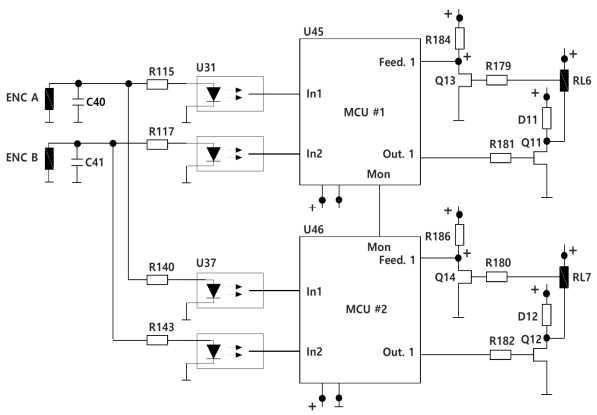

그림 5. 설계 개선 후 회로도 개념
Fig. 5. Conceptual Electronic Circuit After Improvement

평균속도 값을 오차 범위 내에서 서로 확인하도록 진단기능을 추가하였다.

3) 안전라인에 직렬로 그림 5의 RL7 릴레이를 추가하여 이중화 하였고 MCU#2 따로 제어하도록 하였다. 또한, 릴레이가 웰딩된 것을 확인하기 위해 릴레이 피드백 신호 확인 회로를 추가하여 릴레이 상태를 모니터링 할 수 있는 진단기능을 추가하였다.

SFF Analysis Worksheet

Failure Rate /		Failure Rate / Failure Mode					Failure Effect (Safety Aspect)								
HW Block Name	Category	Ref.	Part function	failure rate (FIT)	failure mode	failure mode dist. (%)	안전 관련 고장 영향	SF01 영향성	Diagnostic	DC (%)	λDd	λDu	λS (λSd+λSu)	λS+λDd	Safety related λS+λDd
Encoder 신호	ENC A/B	R114	1k noise protection	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	99.0%	0.08	0.00	0.00	0.08	0.08
					open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
		R115	3.3k / diode(A-C) load	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	99.0%	0.08	0.00	0.00	0.08	0.08
					open	60.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	99.0%	0.13	0.00	0.00	0.13	0.13
		R116	3.3k / diode(A-C) load	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	99.0%	0.08	0.00	0.00	0.08	0.08
					open	60.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	99.0%	0.13	0.00	0.00	0.13	0.13
		R117	1k noise protection	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	99.0%	0.08	0.00	0.00	0.08	0.08
					open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
		U31	High Speed Transistor Optocouplers	10.0000	open	50.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	90.0%	4.50	0.50	0.00	4.50	4.50
					short	10.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	90.0%	0.90	0.10	0.00	0.90	0.90
					drift	40.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	90.0%	3.60	0.40	0.00	3.60	3.60
		R112	10k / Pull-up	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	90.0%	0.08	0.01	0.00	0.08	0.08
					open	60.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	90.0%	0.11	0.01	0.00	0.11	0.11
		R113	10k / Pull-up	0.2123	short	40.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	90.0%	0.08	0.01	0.00	0.08	0.08
					open	60.00%	신호입력 불가 -> 속도측정 불가능	O	1) ENC A/B상 비교 2) 상호모니터링 이중화	90.0%	0.11	0.01	0.00	0.11	0.11
MCU	MCU	U45	Core	12.1505	연산오류 및 데이터 읽기/저장 오류	100.00%	안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	12.03	0.12	0.00	12.03	12.03
		C15	전원안정화 - VDDCORE	0.7851	short	31.27%	전원 공급 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.24	0.00	0.00	0.24	0.24
					open	6.77%	영향 없음	X			0.00	0.00	0.05	0.05	0.05
					drifts	61.87%	전원 공급 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.48	0.00	0.00	0.48	0.48
		C16	전원안정화 - VDDCORE	0.7851	short	31.27%	전원 공급 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.24	0.00	0.00	0.24	0.24
					open	6.77%	영향 없음	X			0.00	0.00	0.05	0.05	0.05
					drifts	61.87%	전원 공급 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.48	0.00	0.00	0.48	0.48
		Y1	crystal	30.0000	short	49.50%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	14.70	0.15	0.00	14.70	14.70
					open	50.50%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	15.00	0.15	0.00	15.00	15.00
		C19	clock generation	0.7851	short	31.27%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.24	0.00	0.00	0.24	0.24
					open	6.77%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.05	0.00	0.00	0.05	0.05
					drifts	61.87%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.48	0.00	0.00	0.48	0.48
		C20	clock generation	0.7851	short	31.27%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.24	0.00	0.00	0.24	0.24
					open	6.77%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.05	0.00	0.00	0.05	0.05
					drifts	61.87%	클락생성 불가 -> 안전기능 수행 불가능	O	상호모니터링 이중화	99.0%	0.48	0.00	0.00	0.48	0.48
Relay 제어	안전라인 릴레이	R181	TR bias current 생성	0.2123	short	40.00%	영향 없음	X			0.00	0.00	0.08	0.08	0.08
					open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
		Q11	TR switch	1.6443	short	37.50%	C-E short : 안전상태 달성 불가능	O	1) 릴레이 제어 피드백 확인 2) 상호모니터링 이중화	99.0%	0.61	0.01	0.00	0.61	0.61
					open	62.50%	영향 없음	X			0.00	0.00	1.03	1.03	1.03
		D11	역전압 방지	16.3613	short	60.00%	안전상태 달성 불가능	O	1) 릴레이 제어 피드백 확인 2) 상호모니터링 이중화	99.0%	9.72	0.10	0.00	9.72	9.72
					open	40.00%	영향 없음	X			0.00	0.00	6.54	6.54	6.54
		RL6	Relay	500.0000	short	40.00%	안전상태 달성 불가능	O	1) 릴레이 제어 피드백 확인 2) 상호모니터링 이중화	99.0%	198.00	2.00	0.00	198.00	198.00
					open	60.00%	영향 없음	X			0.00	0.00	300.00	300.00	300.00
	보조브레이크 릴레이	R189	TR bias current 생성	0.2123	short	40.00%	영향 없음	X			0.00	0.00	0.08	0.08	0.08
					open	60.00%	영향 없음	X			0.00	0.00	0.13	0.13	0.13
		Q15	TR switch	1.6443	short	37.50%	C-E short : 안전상태 달성 불가능	O	1) 릴레이 제어 피드백 확인 2) 상호모니터링 이중화	99.0%	0.61	0.01	0.00	0.61	0.61
					open	62.50%	영향 없음	X			0.00	0.00	1.03	1.03	1.03
		D13	역전압 방지	16.3613	short	60.00%	안전상태 달성 불가능	O	1) 릴레이 제어 피드백 확인 2) 상호모니터링 이중화	99.0%	9.72	0.10	0.00	9.72	9.72
					open	40.00%	영향 없음	X			0.00	0.00	6.54	6.54	6.54
		RL8	Relay	500.0000	short	40.00%	안전상태 달성 불가능	O	1) 릴레이 제어 피드백 확인 2) 상호모니터링 이중화	99.0%	198.00	2.00	0.00	198.00	198.00
					open	60.00%	영향 없음	X			0.00	0.00	300.00	300.00	300.00
			Total	1093.0008							471.3589	5.7089			1087.2891
			safety-related part/component	**1093.0008**							PFH	11.4178	MCU#1, MCU#2 동일 회로 x2	SFF	**99.48%**

그림 6. 개선된 설계 FMEDA 결과
Fig. 6. Refined FMEDA for Redesigned PESSRAE

표 5. 개선결과
Table 5. Refined FMEDA Results

Category	Before	After
PFH_D(FIT)	467.15	11.42
HFT	0	1
SFF(%)	57.26%	99.48%

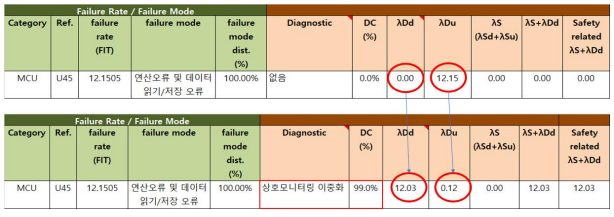

그림 7. 개선후 FMEDA 비교
Fig. 7. Comparing the result of FMEDA after improvement

Ⅲ. 개선결과

1. 수정된 FMEDA 분석 결과

그림 6의 개선된 설계사양에 대한 FMEDA의 결과와 표 5를 보면 과속방지 기능 관점에서 PFH_D 값은 467.15 FIT가 보수적으로 11.42 FIT로 개선되고 SFF 값은 57.26%에서 99.48%로 개선 된 것을 확인 할 수 있었다. 따라서 하드웨어 안전무결성 관점에서 SIL2 수준을 달성되었음을 확인할 수 있었다.

이런 결과는 설계개선 전에 검출되지 않는 위험 고장 (λ_{DU})으로 분류되었던 고장이 진단기능으로 인해 검출되는 위험 고장 (λ_{DD})으로 식별되면서 검출되지 않는 위험 고장 (λ_{DU})이 감소하여 PFH_D 값이 개선되고 (1)의 분모 인자인 λ_{DD}이 증가하면 SFF 값이 개선된 것이다.

예를 들어, 그림 7과 같이 MCU의 오동작에 대해 2중화에 따른 상호모니터링하는 진단기능 추가로 인해 기존의 λ_{DU}의 값이 0 FIT 에서 12.03 FIT로 줄고, λ_{DD}의 값이 12.15 FIT에서 0.12 FIT로 늘었음을 확인할 수 있다.

상호 모니터링하는 기능은 MCU #1과 MCU #2 내부에서

그림 8. 설계 변경된 PESSRAE
Fig. 8. Re-designed PESSRAE

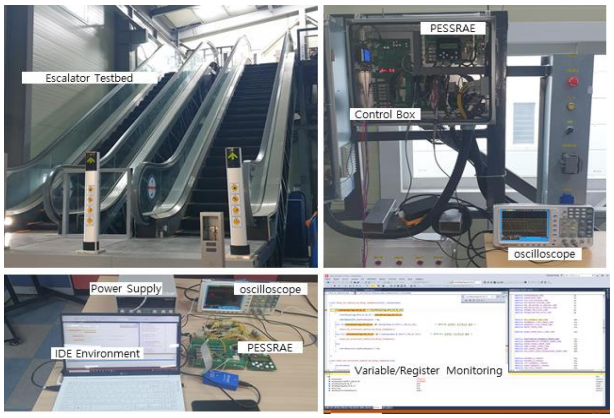

그림 9. 시험환경
Fig. 9. Test Environments

발생할 수 있는 결함인 연산 오류, 메모리 오류, 주변 장치 오류 등에 대응하기 위한 진단기능이다. 이런 오류들은 안전기능의 정상적인 동작을 저해하는 요인으로 하드웨어 안전무결성 달성을 위해서는 반드시 해결되어야 하는 결함이다.

이처럼 하드웨어 안전무결성 달성을 위해 설계를 개선하는 과정은 진단기능이 개선되면 될수록 안전기능이 오동작하게 되는 고장률 즉, 검출되지 않는 위험 고장 (λ_{DU})이 줄어들게 된다. 이 과정은 요구되는 정량적 목표값을 달성할 때까지 반복적으로 수행된다.

2. 구현된 PESSRAE 보드

그림 8은 상시 수정된 설계 사양을 반영하여 이중화 형태로 구현한 PESSRAE 보드이다. 하드웨어 설계 이중화와 추가된 진단기능 소프트웨어를 추가로 구현하여 제작하였다. 해당 사진은 에스컬레이터 테스트베드의 제어반 내에 시험을 위한 장착된 사진이다.

3. 실험환경

그림 9는 구현된 PESSRAE의 안전기능과 진단기능을 테스트하기 위한 실험환경으로 시스템 수준의 시험환경과 제어기 소프트웨어 디버거 수준의 시험환경으로 2가지 형태로 진행하였다.

먼저 시스템 수준의 시험환경은 에스컬레이터 실제 환경을 모사한 에스컬레이터 테스트베드, 에스컬레이터를 구동하

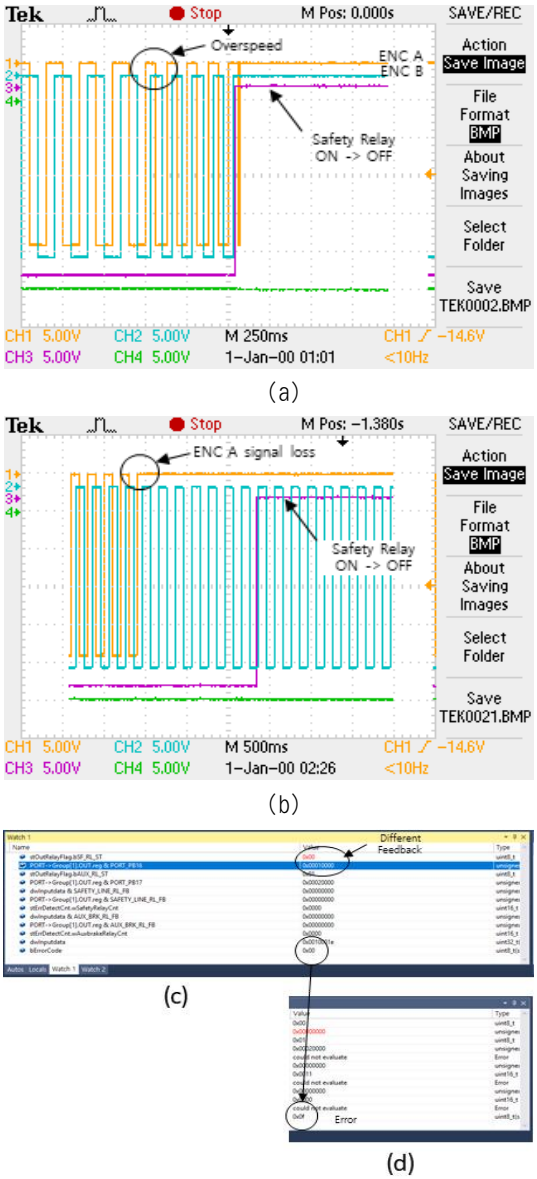

그림 10. PESSRAE 테스트 결과
(a) 과속검출 안전기능시험 결과
(b) ENC 신호 비교 진단기능 시험 결과
(c) 안전릴레이 피드백 모니터링 진단기능 오류주입
(d) 오류주입 시험 후, 에러 발생 확인 결과
Fig. 10. Test results for PESSRAE
(a) Safety Function Test Result
(b) ENC signal comparison diagnostic Test Result
(c) Relay Feedback Monitoring diagnostic Test
(d) Test result of (c)

기 위한 제어반, 안전라인 제어 릴레이와 보조 브레이크 제어 릴레이를 모니터링을 위한 오실로스코프로 구성된다.

테스트베드는 높이 4.5m이고 각각 52장의 스텝을 연결하여 상행, 하행으로 양방향으로 구성되어 있다. 속도는 모두 0.5m/sec 로 상행 구동기는 11KW, 6POLES, 60Hz, 정격 전압 380 V, 정격 전류 23.5A의 사양으로 제작되었고 하행용 구동기는 5.5KW, 4POLES, 60Hz, 정격 전압 380V, 정격 전류 11A 사양으로 제작되었다.

소프트웨어 디버거 수준의 시험환경은 시스템 수준에서 테스트 케이스 생성이 어려운 경우, 소프트웨어 변수 및 MCU 레지스터값을 변조하여 오류를 주입하기 위한 환경으로 PESSRAE에 디버거를 연결하여 IDE 환경 변수 모니터링을 통해 수행되었다.

4. 실험결과

그림 10은 구현된 PESSRAE에 대한 안전기능과 진단기능을 테스트한 결과이다. 그림 10의 (a)는 과속검출에 대한 안전기능의 결과로 ENC A와 ENC B로 입력되는 신호가 과속기준 속도를 넘는 시간이 일정 시간 동안 지속되는 경우, 안전라인의 안전릴레이를 OFF 시켜 에스컬레이터의 전원을 차단한다. 그림 10의 (b)는 ENC A와 ENC B 신호를 비교하는 진단기능을 테스트한 결과로 ENC A 상을 소실시키는 테스트 케이스를 인가하여 안전릴레이를 OFF 시켜 에스컬레이터의 전원을 차단한다. 그림 10의 (c)와 (d)는 안전릴레이 피트백을 모니터링하는 진단기능을 시험한 결과로 소프트웨어 디버거 수준 시험환경에서 수행한 결과로 피드백을 확인하는 레지스터 필드를 임으로 조작하여 오류주입시험을 수행한 뒤, 에러 발생 여부를 확인하였다.

Ⅳ. 결 론

본 연구에서는 하드웨어의 잠재적인 고장위험을 찾아내고 분석하는데 일반적으로 많이 사용되는 FMEDA 기법을 이용하여 하드웨어 안전무결성 달성을 위해 설계가 어떻게 개선되고 요구되는 하드웨어 안전무결성수준을 만족하는 방안을 제시하였다. 또한 개선된 설계를 반영하여 PESSRAE 제작하였고 실험적으로 테스트하여 제안한 방법의 유용성을 확인하였다.

본 연구에서 제시한 방법을 통해 에스컬레이터의 능동적인 안전기능의 무결한 동작을 위협하는 요소를 식별하고 더욱 안전한 안전제어기를 설계함으로써 에스컬레이터의 사고를 예방할 수 있을 것이다.

또한, 안전과 관련된 제어기에서 안전을 위협하는 요소를 어떻게 찾아내고 설계를 개선해나가는지에 대한 본 연구에서 보인 FMEDA의 분석 방법을 타 산업 분야의 안전제어기에 적용할 수 있을 것이다.

References

[1] B. S. Kim, P. Park, "A Study on the Safety Management Plan to Prevent Safety Accident Escalator User," J. Korea Saf. Manag. Sci., Vol. 22, No. 1, March, 2020 (in Korean).

[2] https://home.koelsa.or.kr/wpge/m_135/info/info020101.do

[3] https://www.law.go.kr/행정규칙/승강기안전부품안전기준및승강기안전기준/(2019-32,20190404)

[4] IEC 62061, Safety of Machinery - Functional Safety of Safety-related Control Systems, IEC, 2021.

[5] S. G. Kwon, J. S. Kim, C. E. Kim, "A Study on A Plan to Analyze Risk Factors and Secure Safety through Analysis of Escalator Safety Accident," J. Korea Saf. Manag. Sci., Vol. 14, No. 1, pp. 55-63, 2012 (in Korean).

[6] S. G. Kwon, J. S. Kim, C. E. Kim, "A Research for Improvement Methods in the Aspect of Safety Engineering Through risk Analysis of Facilities for Multiple us," J. Korea Saf. Manag. Sci., Vol. 15, No. 1, 2013 (in Korean).

[7] B. J. Hong, C. G. Kim, K. J. Yeon, "An Empirical Study on Overspeed and Reverse Control Technology of Escalator Auxiliary Brake," Journal of Management Information Systems, Vol. 11, No 1, pp. 1119-1125 (in Korean).

[8] W. D. Kim, S. G. Lee, D. K. Kang, "Analysis of Risk Priority Number and Functionally Safe Design of Battery Management System," IEMEK J. Embed. Sys. Appl., Vol 16, No. 2, pp. 79-88, 2021 (in Korean).

[9] S. Salih, R. Olawoyin, "Computation of Safety Architecture for Electric Power Steering System and Compliance with ISO 26262," SAE Technical Paper 2020-01-0649, 2020.

[10] IEC 61508-2, Functional safety of electrical/electronic /programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safetyrelated systems, IEC, 2010.

[11] IEC 61508-1, Functional safety of electrical/electronic /programmable electronic safety-related systems - Part 1: General requirements, IEC, 2010.

[12] J. Y. Keum, Y. S. Suh, J. K. Lee, J. Y. Park, "Measurement of a Diagnostic Coverage for a Digital Signal Processor Board Using an FMEDA," Journal of Applied Reliability, Vol. 8, No. 2. pp. 101-111, 2008 (in Korean).

[13] SN29500, Siemens Norm SN 29500, SIEMENS, 2004

[14] FMD2016, Failure Mode / Mechanism Distributions - , Quanterion Solutions Incorporated, 2016.

Jeho Heo (허 제 호)

2007 Eletronic Engineering from Ajou University, (B.S.)
2012 Eletronic Engineering from Ajou University (M.S.)
2015 Eletronic Engineering from Ajou University (Ph.D Candidate)

Career:
2007~2010 brightsightAsia. Researcher
2011~2022 Korea Testing Laboratory, Team Leader
Field of Interests: Functional Safety, Artificial intelligence, Model Based Development
Email: jhheo@ktl.re.kr

KiBong Kim (김 기 봉)

1999 Information and Communication Engineering from Hoseo University

Career:
1999~SERA system Engineering Co., Ltd.
2015~Director of Tech-Research Institute
Field of Interests: Networked Control Systems, Power electronics
Email: kibongkim@serasystem.com

Ki hyun Chung (정 기 현)

1984 Eletronic Engineering from Sogang University (B.S.)
1989 Electronics and Electronic Engineering from Illinois State University (M.S.)
1990 Electronics Engineering from Purdue University (Ph.D)

Career:
1991~1992 Hyundai Semiconductor. Researcher
1993~2022 the department of Electronics Engineering at Ajou University, Professor
Field of Interests: VLSI Design, Real-Time System, Testing, Computer structure
Email: khchung@ajou.ac.kr

Seok chan An (안 석 찬)

2015 Electronics and Electronic Engineering from Yonsei University (B.S.)
2017 Electronics and Electronic Engineering from Yonsei University (M.S.)

Career:
2020~2022 Korea Testing Laboratory, Researcher
Field of Interests: Functional Safety, Artificial intelligence, Failure Modes Effects and Diagnostic Analysis
Email: anseokchan@ktl.re.kr