Regular paper http://dx.doi.org/10.13067/JKIECS.2015.10.9.1001

SIL4 안전관련 시스템에 적합한 전원장치의 구조 설계에 대한 연구

유등열* · 이기서**

A Study on Architecture Design of Power Supply for SIL4 Safety Related System

Deung-Ryeol Yoo* · Key-Seo Lee**

요 약

본 논문은 안전 시스템의 구성하는 요소 중 전원 장치에 대한 안전 무결성 목표를 설정하고, 설정된 목표를 달성하기 위한 전원 장치의 구조를 설계하였다. 해당 안전 시스템은 안전 최고 등급인 SIL4(Safety Integrity Level 4)를 목표로 하였으며, 철도 응용 분야의 규격인 IEC 62425에 부합하는 구조 설계 및 변경 프로세스를 정립하여 6단계의 기본 구조 설계 방안을 적용하였다. 본 연구에서는 전원 장치의 고장으로부터 시스템의 안전 무결성을 유지할 수 있는 전원 장치의 구조를 FMEA(Failure Modes and Effect Analysis) 기법을 사용하여 도출하였으며, 해당 결과를 적용한 전원 장치는 안전 시스템에 적용할 수 있다는 것을 제시하였다. 최종적으로 전원 장치 모듈에 대한 고장빈도의 정량적 목표치를 제시하였다.

ABSTRACT

This paper introduces the architecture of the power supply in order to achieve the safety integrity target for power supply which is a part of safety related system. The integrity level for safety is set 4 and according to the IEC 62425 which is standard for railway application the architecture design is conducted and process for design is developed. The procedure for design consists with 6 steps. The architecture of power supply that is able to keep the safety integrity against of failure of power supply is derived through the analysis and it is suggested that the power supply adopted the result in this paper is suitable to apply in safety system. Also, the failure frequency that is a quantitative value for the power supply is proposed.

키워드

SIL4, Power Supply, Architecture, IEC 62425, Safety Relaed System
안전 관련 장치, 전원 장치 구조, SIL4, IEC 62425

Ⅰ. 서 론

철도, 항공, 원자력, 발전소, 공장자동화 설비 등 각 산업에서 사용되는 수많은 시스템 중에서, 해당 시스템의 고장이 사람이나 환경에 위험을 초래하게 되는 시스템을 안전 관련 시스템으로 규정하게 되며, 각 산업별로 안전 관련 지침이나 규격이 존재하게 된다. 각 지침의 요구사항에 따라서 해당 시스템은 설계되어야 하며, 설계된 시스템이 안전성 요구사항에 부합됨을 증명하고 보증해야 한다. 철도에 사용되는 신호 시스템인 경우에는 IEC 62425[1]가 적용되어 왔으며, 기계 산업에서는 IEC 61508[2]과 EN 62061[3]이, 프로세서

* 광운대학교 일반대학원 제어계측공학과(dennis.yoo@tuv-sud.kr)
** 교신저자 (corresponding author) : 광운대학교 로봇학부 교수(kslee@kw.ac.kr)
접수일자 : 2015. 08. 10 심사(수정)일자 : 2015. 09. 13 게재확정일자 : 2015. 09. 23

산업에서는 IEC 61508[2], IEC 61511[4]등이 적용되어 왔다. 안전성 목표는 SIL1에서부터 SIL4까지 4단계의 등급으로 적용되며, 시스템에 부여되는 안전성 등급은 해당 시스템이 사용되는 목적에 따라서 해당 시스템의 고장으로 발생하는 사고가 얼마만큼의 인명 사상이나 환경 피해를 유발하는 지에 따라서 결정하게 된다. 일반적으로 시스템은 전원장치, 입력장치, 연산처리장치, 출력장치로 구성된다. 만일 안전 기능을 수행함에 있어서 위에서 언급된 4개의 장치가 모두 사용된다면, 목표로 하는 SIL의 정량적 목표가 각 하부장치에 할당되어야 한다. 본 연구에서는 각 하부시스템에 정량적 목표를 할당하여, 전원 장치의 정량적 목표를 설정하는 것부터 시작할 것이다. 안전과 관련된 정량적 목표를 할당하였다면, 기본 설계를 진행해야 한다. 기본 설계는 기능 블록 단위로 설계가 이루어지고, 설계된 기능블록에 대하여 각 고장 모드를 도출하고, 각 고장 모드의 위험성 평가를 진행해야 한다. 위험성 평가로부터 해당 고장 모드가 위험한 사고를 유발한다고 결론이 되면, 해당 고장모드를 제거하거나 발생빈도를 경감시킬 수 있는 방안이 도출되어야 한다. 이렇게 도출된 대책이 다시 기능 블록 설계에 반영되어, 구조 설계가 종료된다. 안전 레벨에 따라 허용되는 시스템의 구조는 IEC 62425의 표 E.4를 기반으로 적용할 것이며, 본 연구에서는 SIL4에 시스템에 적용할 수 있는 전원 장치의 내부 구조를 설계하여 제시하려고 한다. 설계된 전원 장치 구조의 부합성은 상세 설계 및 상세 설계로부터 획득한 신뢰성 데이터를 이용하여 증명하려고 한다. 본 연구에서는 10년에서의 전체 시스템의 THR(Tolerable Hazard Rate)이 $4x10^{-9}$/hour이하를 만족할 수 있도록 설정하고, 시스템의 구조가 composite fail-safety 인 경우에 전원 장치의 구조 설계 방법과 정량적 목표치의 수준을 제시하려고 한다. 현재까지의 연구는 안전성 측면에서의 전원 장치에 목적보다는 성능이나, 기능 향상을 위한 연구[6-9]가 주로 이루어져 왔다. 본 연구에서는 성능 목표와 함께 안전성 목표라는 요구사항을 동시에 만족시킬 수 있는 구조에 대한 연구를 진행하려고 한다.

II. 본 론

2.1 정량적인 안전 목표 설정

시스템의 일반적인 구조는 그림1과 같이 구성된다. 시스템은 기본적으로 전원 장치, 입력 장치, 연산 및 처리장치, 출력장치로 구성된다. 이러한 구조의 시스템은 그림 2와 같은 신뢰성 블록도로 표현할 수 있으며, 목표로 하는 시스템의 THR(Tolerable Hazard Rate)을 각 하부 시스템이나 장치에 할당할 수 있다. 전원장치에는 25%에 해당하는 HR(Hazard Rate)을 할당하는 것으로 정의하였으며, 이로 인해 표1과 같이 각 하부장치에 대한 HR을 할당하였다.

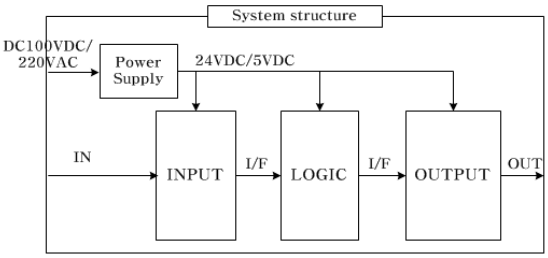

그림 1. 기본적인 시스템 구조

Fig. 1 Basic system architecture

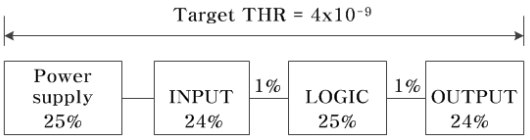

그림 2 기본 시스템의 신뢰성 블록도

Fig. 2 Reliability Block Diagram of basic system

SIL(Safety Integrity Level) 등급에 따른 정량적 목표치인 THR은 표2와 같이 정의되며, 그림 2에서 정의한 시스템 목표인 THR 값은 표2에서 보이는 바와 같이 SIL4를 만족하는 정량적 수치라 하겠다. 인터페이스 항목에 1%의 정량적 목표치의 할당은 통신을 사용했을 경우에만 해당된다. 본 연구에서는 통신은 사용하지 않은 것으로 가정한다.

표 1. 하부 장치로 할당된 정량적 목표치

Table 1. Target value allocated into sub equipment

Part	Ratio	THR (/hour)
Power supply	25%	$1x10^{-9}$
INPUT	24%	$0.96x10^{-9}$
LOGIC	25%	$1x10^{-9}$
OUTPUT	24%	$0.96x10^{-9}$
Communication between INPUT and LOGIC	1%	$0.04x10^{-9}$
Communication between LOGIC and OUTPUT	1%	$0.04x10^{-9}$

표 2. SIL 테이블

Table 2. SIL table

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

이러한 구조와 할당은 단일 시스템으로 시스템을 설계했을 때의 목표이며, SIL4인 안정 기능을 단일 시스템에서 수행하도록 설계하는 것은 현실적으로 어렵다. 그래서 이중화 구조의 composite fail-safety를 만족하는 시스템을 설계하여 적용하는 것으로 하였다.

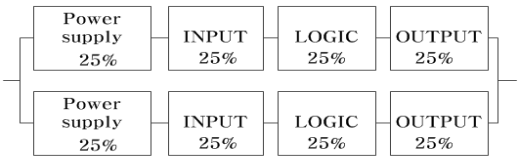

그림 3. 이중화 구조와 내부 할당 비율의 정의

Fig. 3 Dual structure and allocation ratio

그림 3은 이러한 구조의 RBD(Reliability Block Diagram)를 나타내며, 내부 구성 모듈에는 균등하게 목표치를 할당하는 것으로써 정의하였다.

2.2 시스템 구조 분석 과정 정립

시스템의 정량적 목표를 달성하기 위한 시스템의 구조를 설계하는 과정을 그림4와 같이 정의하였다. 기본 구조 설계 이후 기본 구조에 대한 분석을 수행하고, 완료된 기본 구조를 바탕으로 상세 설계를 진행한다. 상세설계는 회로 레벨로 진행하는 것을 의미하며, 상세 설계 이후에는 부품 소자 레벨에서 분석을 수행하여 정량적 분석을 수행한다. 정량적 분석에는 부품 소자에 대한 신뢰성 분석 및 고장 계통 분석을 수행한다. 전원 장치의 구조 설계는 기본 구조 설계 및 분석에 한하여 진행된다고 볼 수 있다. 이후의 상세 설계 및 과정은 본 연구에서는 상세히 제시하지 않으며, 수행 결과만 제시된다.

기능 분석 단계의 프로세스 정의
단계1: 기능 단위의 범위 설정과 식별 ID 부여
단계2: 각 기능 단위에 입출력을 정의
단계3: 각 기능 단위에 대한 고장 모드 도출
단계4: 각 고장 모드 별 시스템 영향 정의
단계5: 위험한 고장에 대한 대비책 도출
단계6: 도출된 예방책을 적용한 구성도의 재구성

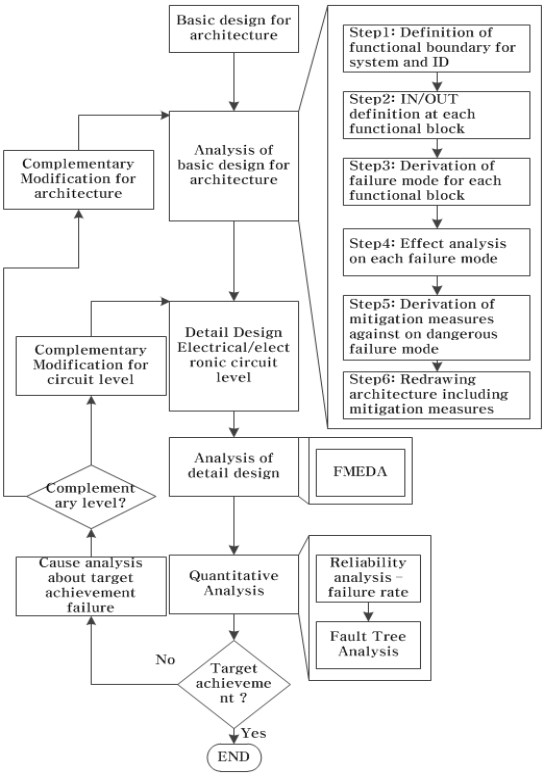

그림 4. 시스템 구조 분석 과정

Fig. 4 Analysis process for system architecture

III. Power Supply 구조 설계

일반적인 전원 모듈은 그림 5같은 구성을 갖는다. 외부로부터 입력되는 전원을 수신한 후, 전원 변환 과정을 거쳐 원하는 전원을 생성하는 원리다. 출력된 전원을 이용하여 더 높은 전위를 갖는 전원을 생성하기도 한다. 전원 변환 과정에서는 DC/DC converter나 voltage regulator 등의 디바이스를 사용한다. 변환된 전원은 평활회로를 거쳐 더욱 안정된 전압을 출력하도록 구성된다. 그림 5에서 제시된 전원 모듈이 SIL4에 적용하는 것이 적합한 것인지 아닌지는 분석 과정을 통하여 적합성을 평가해야 하며, 부족한 사항에 대해서는 기능을 보완하여 적용해야 한다. 분석 과정에 이용하는 방법은 FMEA(Failure Mode and Effect Analysis)를 수행하여 단일 고장에 대한 영향 분석을 수행하였다.

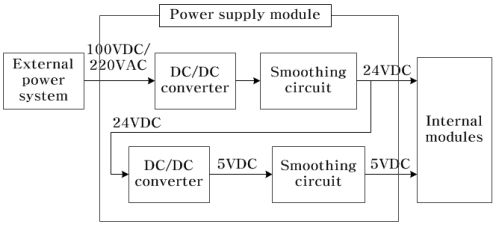

그림 5. 기본적인 전원장치의 내부 구조

Fig. 5 Basic internal structure of power supply

3.1 1단계 설계

그림 6과 같이 그림 5에 제시된 기능 구성도에 식별 ID를 부여한다. 그림 5에서 정의된 하나의 기능이 다른 기능과 합쳐질 수도 있으며, 상세하게 더 세분화될 수도 있다. 여기서는 그림 5에 제시된 구성과 동일한 기능 레벨로 분석하도록 하였다.

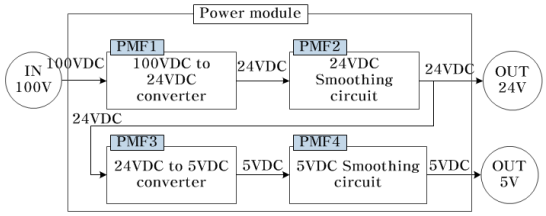

그림 6. 전원 구성도에 식별 ID 부여

Fig. 6 Identification at basic structure of power supply

3.2 2단계 설계

그림 6에서 정의한 사항과, 전원장치의 기능 상태를 분석하여 입출력을 정의한다. 표3은 전원 장치에 대한 입출력을 정의한 것이다.

표3. 전원 장치의 내부 기능 블록의 입출력 정의

Table 3. Input/output definition of functional block

ID	FUNCTION	INPUT	OUTPUT
PMF1	100VDC to 24VDC converter	100VDC	24VDC
PMF2	24VDC smoothing	24VDC	24VDC
PMF3	24VDC to 5VDC converter	24VDC	5VDC
PMF4	5VDC smoothing	5VDC	5VDC

3.3 3단계 설계

전원 모듈의 내부 기능 블록에 대한 고장 모드를 도출한다. 이에 대한 결과는 표4와 같다.

표4. 전원 모듈의 기능 블록에 대한 고장 모드

Table 4. Failure mode power supply

ID	Failure mode
PMF1	Interruption
	Over-voltage(above 24VDC)
	Low-voltage(below 24VDC)
	Oscillation (waveform voltage)
	Stuck to ground
	100VDC supply bacause short between input and output
PMF2	Interruption
	Low-voltage(below 24VDC)
	Oscillation (waveform voltage)
	Stuck to ground
PMF3	Interruption
	Over-voltage(above 5VDC)
	Low-voltage(below 5VDC)
	Oscillation (waveform voltage)
	Stuck to ground
	24VDC supply bacause short between input and output
PMF4	Interruption
	Low-voltage(below 5VDC)
	Oscillation (waveform voltage)
	Stuck to ground
PMF5	Interruption
	Over-voltage(above 3.3VDC)
	Low-voltage(below 3.3VDC)
	Oscillation (waveform voltage)
	Stuck to ground
	24VDC supply bacause short between input and output

ID	Failure mode
PMF6	Interruption
	Low-voltage(below 3.3VDC)
	Oscillation (waveform voltage)
	Stuck to ground

3.4 4단계 설계

4단계에서는 3단계에서 도출한 각 고장 모드에 대하여 시스템 영향을 분석한다. 영향 분석은 최종 시스템의 상태에 대하여 바로 도출하는 것이 아니라, 분석 레벨을 포함하는 다른 시스템으로의 영향과, 해당 기능을 포함하는 상위 블록의 영향, 상위 블록을 포함하는 하부 시스템의 영향, 하부 시스템을 포함하는 시스템의 영향 순으로, 영향의 범위를 확장하여 분석하는 것이 분석의 오류를 최소화 하는 방법이며, 이러한 분석 과정을 통하여 얻어진 결과는 추후 정량적 목표를 달성하기 위해 수행하는 FTA[5]에서 활용될 수 있다.

3.5 5단계 설계

4단계에서 도출한 각 고장 모드에 대한 시스템 영향이 위험을 초래하는 항목에 대해서는 해당 위험이 발생하지 않도록 대비책을 도출하였다. 즉 해당 고장 모드가 위험을 초래하지 않도록 해야 하는 것이 요구된다. 이를 위해서는 해당 고장모드가 발행한 원인을 파악하여, 원인이 발생하지 않도록 하거나, 해당 고장모드가 발생한 상태에서 고장 모드의 영향이 상위로 확대되는 것을 방지할 수 있는 방안이 도출되어야 한다.

표6. 도출된 예방책

Table 6. Derived mitigation measures

ID	Mitigation measures(: MM)
MM01	Over-voltage detection and output voltage cut-off
MM02	Under-voltage detection and output voltage cut-off
MM03	Oscillation detection and output voltage cut-off
MM04	100VDC detection at output and cut-off

3.6 6단계 설계

위의 1단계부터 5단계까지의 분석 과정을 거치면서, 위험한 고장모드에 대한 대비책의 도출이 완료되었다.

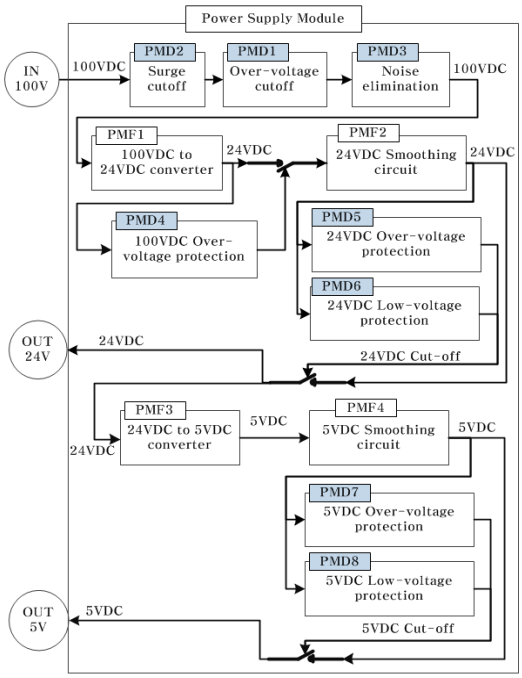

그림 7. SIL4를 위한 전원 장치 구조

Fig. 7 Power supply architecture for SIL4

그림 7은 도출된 예방책들을 적용한 최종 구조도를 정의한 것이다.

Ⅳ. 설계 검증

설계에 대한 검증은 고장 계통 분석을 통하여 수행하였다. 그리고 신뢰성 데이터는 IEC TR 62380을 적용하여 도출하였다. 고장 계통 분석에 대한 결과는 그림 8과 같이 도출되었다

각 고장 모드에 대한 고장율은 표7과 같이 도출되었다. 이는 회로에 사용된 소자에 대한 고장 분석을 수행한 결과이다.

표 7. 위험 고장 모드의 고장율

Table 7. Failure rate for dangerous failure mode

Circuit	λ_safe (/h)	λ_dangerous (/h)
Power converting	1.489E-08	1.5285E-08
smoothing circuit	4.87348E-09	1.2532E-09
Over/under voltage detection and cutoff	2.87014E-08	2.3454E-08

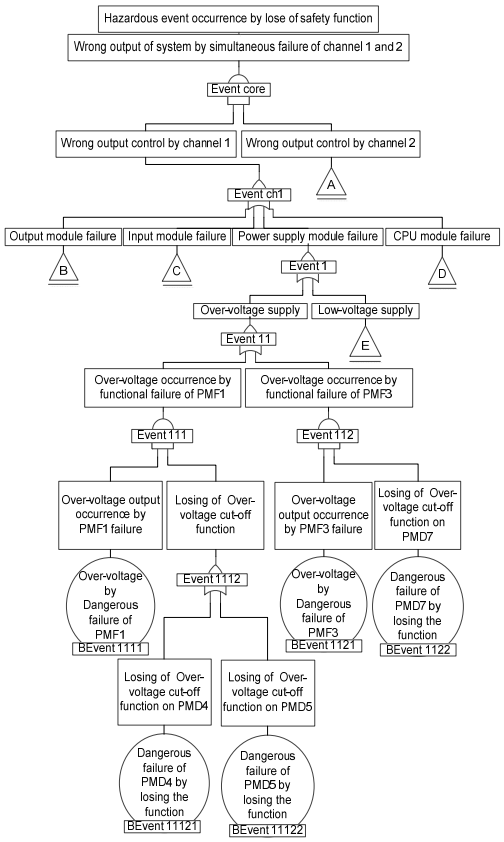

그림 8. 고장계통분석 결과

Fig. 8 Fault Tree Analysis result

기본 고장율로부터 FTA(Fault Tree Analysis)[5]를 구성하는 상위 이벤트는 다음의 식 (1)에서 식 (4)와 같이 계산된다.

Failure frequency W:

$$W(t) = \lambda e^{-\lambda t} \tag{1}$$

Component unavailability Q:

$$Q(t) = 1 - e^{-\lambda t} \tag{2}$$

OR gate:

$$Q_{OR} = Q_1 + Q_2$$
$$W_{OR} = W_1 + W_2 \tag{3}$$

AND gate:

$$Q_{AND} = Q_1 \cdot Q_2$$
$$W_{AND} = Q_1 \cdot W_2 + Q_2 \cdot W_1 \tag{4}$$

표 8은 그림 8과 표 7을 이용하여 각 이벤트에 대한 고장빈도와 비가용도를 산출한 것이다. 이때 전원장치의 수명주기를 10년으로 적용하였다.

표 8. 각 이벤트에 대한 고장빈도와 비가용도의 산출

Table 8. Failure frequency and unavailability

Event ID	Dangerous Failure Rate (FIT)	W (Failure Frequency) (/h)	Q (Unavailability)
Event Core	-	1.41395E-09	3.12266E-05
Event ch1	-	1.26515E-07	0.005588075
Event 1	-	3.16287E-08	0.001397019
Event 11	-	1.83692E-08	0.000811436
Event 111	-	1.22462E-08	0.000540957
BEvent 1111	15.285	1.50817E-07	0.013300417
Event 1112	-	4.59541E-07	0.040672201
BEvent 11121	23.454025	2.29771E-07	0.020336101
BEvent 11122	23.454025	2.29771E-07	0.020336101
Event 112	-	6.12308E-09	0.000270479
BEvent 1121	15.285	1.50817E-07	0.013300417
BEvent 1122	23.454025	2.29771E-07	0.020336101
Event 12	-	1.32595E-08	0.000585583
Event 121	-	6.62975E-09	0.000292791
BEvent 1212	23.454025	2.29771E-07	0.020336101
Event 122	-	6.62975E-09	0.000292791
BEvent 1222	23.454025	2.29771E-07	0.020336101
Event 1211	-	1.63335E-07	0.014397618
BEvent 12111	15.285	1.50817E-07	0.013300417
BEvent 12112	1.2532	1.25182E-08	0.001097201
Event 1221	-	1.63335E-07	0.014397618
Bevent 12211	15.285	1.50817E-07	0.013300417
Bevent 12212	1.2532	1.25182E-08	0.001097201

각 년도 별 전원 장치와 시스템에 대한 고장빈도의 추이가 표 9와 같이 도출되었다. 14년의 시스템의 고장빈도는 3.8155×10^{-9}/h로서 목표한 수치와 부합하지만, 15년에서는 부적합 한 것으로 도출되었다.

표 9. 시간에 따른 전원 장치와 시스템의 고장빈도의 산출

Table 9. Failure frequency for power supply and system based on time

Years	Hours	Failure frequency of power upply (/h)	Failure frequency of system (/h)
6	52560	1.9169E-08	3.10571E-10
7	61320	2.23077E-08	4.91114E-10
8	70080	2.54305E-08	7.30028E-10
9	78840	2.85375E-08	1.03509E-09
10	87600	3.16287E-08	1.41395E-09
11	96360	3.47043E-08	1.87411E-09
12	105120	3.77642E-08	2.42294E-09
13	113880	4.08086E-08	3.0677E-09
14	122640	4.38375E-08	3.8155E-09
15	131400	4.68647E-08	4.67749E-09
16	140160	4.9849E-08	5.64801E-09
17	148920	5.28318E-08	6.74632E-09
18	157680	5.57993E-08	7.97486E-09
19	166440	5.87516E-08	9.34011E-09
20	175200	6.16887E-08	1.08484E-08

V. 결 론

본 연구에서는 SIL4의 정량적 목표치를 만족하도록 시스템을 구성하기 위한 설계 절차를 제시하고, 해당 설계 절차에 맞추어서 시스템을 설계한 전원 장치의 내부 구성도를 제시하며, 각 내부 구성도의 정량적 목표치의 수준을 정의하고자 하였다. 고안된 전원 장치의 구성 블록에 대한 회로 설계를 실시하여 FTA를 수행한 결과 10년에서의 시스템에 대한 고장빈도(failure frequency)가 $1.41395x10^{-9}$/h으로 처음 목표로 한 $4x10^{-9}$/h보다 작음으로 만족한 결과를 얻을 수 있었다. 또한 전원 모듈에 대한 정량적 목표치는 $3.16287x10^{-8}$/h이하로 설계되어야 함을 제시하였다. 여기서 제시된 수치는 SIL4를 만족하기 위한 시스템 구성 중에서 Dual electronic structure based on composite fail-safety with fail-safe comparison 으로 구성된 시스템에 적용하기 위한 것으로써, 전원 공급 장치에 대한 정량적인 고장 빈도에 대한 요구사항을 제시할 수 있었다. 본 연구에서는 전체 시스템을 구성하는 장치 중에서 전원 장치에 대한 설계 구성도만을 제시하였다. 다음 연구에서는 다른 모듈에 대한 구조 설계를 진행할 것이다.

References

[1] IEC 62425, “Railway applications-Communication, signaling and processing systems – safety related electronic systems for signaling,” *IEC,* Geneva, Switzerland, September 2007.

[2] IEC 61508, “Functional safety of electrical/ electronic/ programmable electronic safety-related systems,” *IEC,* Geneva, Switzerland, April 2010.

[3] IEC 62061, “Safety of machinery-Functional safety of safety-related electrical, electronic and programmable electronic control systems,” *IEC,* Geneva, Switzerland, Jan. 2005.

[4] IEC 61511-1, “Functional safety-safety instrumented systems for the process industry sector,” *IEC,* Geneva, Switzerland, Jan. 2003.

[5] IEC 61025, “Fault tree analysis(FTA),” *IEC,* Geneva, Switzerland, Dec. 2006.

[6] K. Chung, “Diagnosis of power supply by analysis of chaotic nonlinear dynamics,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 7, 2014, pp. 753-759.

[7] H. Shin, “Development of constant current SMPS for LED Lighting,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 1, 2015, pp. 111-116.

[8] Y. Jeong, “A study on control of generators based on SMPS,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no. 1, 2012, pp. 107-115.

[9] H. Shin, “Design of LED Driving SMPS for Large Traffic Signal Lamp,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 4, no. 2, 2009, pp. 123-129.

저자 소개

유등열(Deung-Ryeol Yoo)

2002년 2월 광운대학교 제어계측학과 졸업(공학사)

※ 관심분야 : 철도제어안전시스템, 제어계측, 자동화 설비, 반도체 설계, 임베디드 OS

이기서(Key-Seo Lee)

1977년 2월 연세대학교 전기공학과 졸업(공학사)
1979년 2월 연세대학교 대학원 전기공학과 졸업(공학석사)
1986년 2월 연세대학교 대학원 전기공학과 졸업(공학박사)
1981년 ~현재 : 광운대학교 정보제어공학과 교수
※ 관심분야 : 철도신호, RAMS