SIL 인증을 위한 FMEDA 프로세스 연구 : 화염검출기 사례를 중심으로

김성규¹ · 김용수^{2*}

¹경기대학교 대학원 산업경영공학과 / ²경기대학교 산업경영공학과

A Study on FMEDA Process for SIL Certification : A Case Study of a Flame Scanner

Sung Kyu Kim¹ · Yong Soo Kim²

¹Department of Industrial and Management Engineering, Graduate School, Kyonggi University

²Department of Industrial and Management Engineering, Kyonggi University

In this article, we introduced the estimation method by ‘Safety Integrity Level’(SIL) for the criterion of safety assurance and performed a case study on a flame scanner. SIL requires probabilistic evaluation of each set of equipment used to reduce risk in a safety related system. FMEDA(Failure Modes, Effects and Diagnostic Analysis) method is widely used to evaluate the safety levels and provides information on the failure rates and failure mode distributions necessary to calculate a diagnostic coverage factor for a part or a component. Basically, two parameters resulting from FMEDA are used for SIL classification of the device : SFF(Safe Failure Fraction) and PFD(Probability of Failure on Demand). In this case study, it is concluded that the flame scanner is designed to fulfill the condition of SIL 3 in the aspect of SFF and PFD.

Keyword: SIL, functional safety, FMEA, FMEDA, SFF, PFD, flame scanner

1. 서 론

안전이란 일반적으로 위험이 생기거나 사고가 발생할 염려가 없는 상태로서, 시스템적 측면에서는 시스템의 고장을 야기할 수 있는 모든 위험원의 위험도(Risk)가 허용수준 이내로 제어된 상태라고 할 수 있다(Shin *et al.*, 2009). 이러한 안전의 개념에 포함되는 기능안전은 안전을 제공하기 위한 장치나 시스템과 같은 안전장치들의 기능 및 관련된 신뢰성 측면을 대상으로 한다. 즉, 위험 상황에서 특정 안전장치가 설계대로 작동된다면, 기능안전(functional safety)이 우수하다고 평가할 수 있는 것이다. 기능안전의 대표적인 예로 화염 및 가스 감지 시스템, 자동

차 에어백 시스템 등을 들 수 있다(Suh *et al.*, 2012).

이러한 기능안전에 대한 위험도를 감소시키기 위해 IEC(International Electrotechnical Commission)는 IEC 61508, IEC 61511 등을 제정하였다. IEC 61508 Electrical/Electronic/Programmable Electronic Safety-Related Systems(E/E/PES)에서는 기능안전성에 대하여 센서, 논리연산자, 액추에이터로 구성된 전기, 전자, 프로그램 가능한 전자장치를 이용하여 안전관련 시스템을 작동시키는 안전기능으로 정의하고 있으며, SIS(Safety Instrumented System)를 고려하여 해당 안전시스템의 기능안전에 대한 타당성을 검증하였다(IEC 61508-0, 2010; Suh *et al.*, 2012).

기능안전의 임무를 수행하는 SIS는 센서와 단일 또는 다중의

*연락처 : 김용수 교수, 443-760 경기도 수원시 영통구 광교산로 154-42 경기대학교 산업경영공학과,

Fax : 031-244-3534, E-mail : kimys@kgu.ac.kr

투고일(2012년 08월 17일), 심사일(1차 : 2012년 09월 07일, 2차 : 2012년 10월 03일), 게재확정일(2012년 10월 03일).

제어기로 구성되어 개인, 장비, 환경에 대한 보호 시스템을 의미한다. SIS의 수행목적은 안전성 향상 또는 위험의 감소를 위해 잠재위험의 모니터링과 사고가 발생하였을 경우 사전에 계획된 프로그램을 통해 피해결과를 최소화하는 데 있다. 이러한 SIS는 공정에 대한 생산량을 증대시키거나 공정효율을 높이는 효과는 없으나 사고에 대한 손실을 감소시킴으로써, 유지보수 비용과 위험 비용을 절감시킨다(Jin *et al.*, 2002). SIS의 기능안전성은 안전기능성과 안전무결성으로 구성되어 있다. 즉, 해당 SIS가 어떤 안전기능을 수행하는가, 그리고 해당 안전기능을 얼마나 안전무결하도록 수행될 수 있는가를 의미한다. 초기에 정의되는 기능과 달리 안전무결성은 실제 안전시스템의 성능을 나타내므로, 이러한 안전무결성을 정량적으로 평가하기 위하여 SIL(Safety Integrity Level)을 활용한다(Kim *et al.*, 2010).

SIL 인증은 단위공정의 작동빈도에 따라 저 요구(Low demand) 작동모드와 고 요구(High demand) 및 연속적인(Continuous) 작동모드로 구분되며, 고장발생 확률이 각각 PFD(Probability of dangerous Failure on Demand)와 PFH(Probability of dangerous Failure per Hour)로 산출되어 모든 고장의 안전고장 비율을 의미하는 SFF(Safe Failure Fraction)와 장치의 구조를 의미하는 HFT(Hardware Fault Tolerance)에 따른 최대 SIL 등급의 제약에 따라 기능안전에 대한 정량적인 평가를 수행할 수 있다.

기존의 SIL 등급 평가 연구에서는 주로 FTA(Fault Tree Analysis) 기법을 활용하였으며, HAZOP(HAZard and OPerability), LOPA(Layer of Protection Analysis), FMEA(Failure Mode and Effect Analysis) 기법 및 플로우차트 등을 적용하여 기능 안전에 대한 분석이 진행되었다. 그러나 본 연구에서는 FMEDA(Failure Modes, Effect and Diagnostic Analysis) 기법을 활용하여 SIS에 대한 정량적인 측정치를 도출함으로써 SIL 등급을 결정하였으며, 화염검출기(Flame scanner)를 대상으로 사례연구를 실시하였다.

2. 관련 문헌 연구

관련 문헌 연구에 앞서 기능안전에 대하여 IEC 61508과 IEC 61511에 대해 살펴보면 IEC 61508은 안전관련 전자/전기/프로그램 가능한 전자 시스템의 기능안전으로서 모든 산업 전반에 활용되는 국제표준이고, IEC 61511은 IEC 61508을 근거로 한 표준으로 장치산업을 위한 기능안전에 관한 표준이다(Suh *et al.*, 2012).

이러한 국제표준은 일반적인 안전규격과 소프트웨어에 대한 국제표준으로 구분되어 제시된다. 그러나, 소프트웨어의 경우 안전기능이 할당된 소프트웨어의 안전성에 대한 시스템적 오류가 정의되지 않은 경우가 다수이므로, SIL을 부여할 수 있는 정량적 분석 대신 정성적 분석에만 의존하는 실정이다. 따라서 소프트웨어 검증은 아직까지 개발과정에 대한 문서에 주로 의존하여 분석되며 극히 일부만 테스트에 의한 정량적인

분석이 이루어지고 있다. 따라서 정성적인 SIL 등급 부여를 위해 그에 상응하는 소프트웨어 안전무결성을 확보해야 한다(Cho *et al.*, 2010; Jo *et al.*, 2010).

철도분야에서는 철도시스템의 신뢰성, 가용도, 유지보수성, 안전성의 명세 및 입증에 대한 국제규격인 IEC 62278을 통해 안전 확보 기준인 SIL에 대한 요구사항 수립, 설계 및 제작, 설치, 운영, 유지보수 등의 단계별 검증을 거쳐 안전을 입증하는 것을 권고하였으며, 철도시스템 소프트웨어의 경우 IEC 62279에 의해 표준화되었다(Shin *et al.*, 2009; Jo *et al.*, 2010).

SIS와 SIL 인증에 관한 사례를 살펴보면 화재, 폭발, 독성물질 누출과 같은 중대 산업사고의 잠재위험이 있는 화학공장의 기능안전에 대한 연구로 Kim *et al.*(2011)은 화학공장의 보다 높은 SIL 적용을 위해 시범공정에 HAZOP와 LOPA 기법을 활용하여 잠재위험을 분석함으로써, SIS 추가 설치로 인한 비용과 위험도를 동시에 고려한 허용된 범위에서 최적화된 SIL을 선택하는 연구를 수행하였으며, Ko *et al.*(2006)은 Ethyl Benzene plant의 공정에서 발생하는 화재 및 폭발을 방지하는 SIS에 대하여 FTA 등 신뢰도 분석을 수행함으로써 해당 시스템이 목표 SIL등급인 3등급에 도달하였음을 입증하는 연구를 수행하였다. 또한, Ko *et al.*(2003)은 이러한 화학공장 및 가스시설의 소방수 공급 시설에 대한 공통원인고장을 도출하고 FTA를 통하여 펌프 설치 대수에 따른 PFD를 산출하여 시스템의 SIL등급을 판정하는 연구를 수행하였다.

철도분야에서도 열차제어 시스템에 관한 SIL 인증의 연구가 수행되었다. 먼저 Joung and Kim(2004)은 개발 중인 경량전철의 위험요인을 분석함으로써, 열차제어 시스템의 기능안전에 대한 위험요인별 고장모드의 심각도와 발생빈도를 도출하여 향후 SIL 인증을 위한 토대를 마련하는 연구를 수행하였으며, Shin *et al.*(2009)도 열차제어 시스템에 대한 SIL 할당 및 입증에 관한 연구를 수행하였다. 또한, Choi *et al.*(2009)은 열차의 차상 ATP 시스템에 대하여 FTA를 수행함으로써 SIL 등급을 판정하는 연구를 수행하였으며, Chang *et al.*(2009)은 고속철도의 자동연동 장치에 대한 FMEA 및 FTA를 수행하여 SIL 등급을 판정하는 연구를 수행하였다. 반면, Jo *et al.*(2010)은 철도시스템 소프트웨어의 SIL인증을 위한 국제표준의 검증항목 중 정량적인 테스트 커버리지 결과를 도출할 수 있는 자동화 도구를 개발하는 연구를 수행하였다.

그밖에도 Suh *et al.*(2012)은 선박 내에서 발생하는 연료 누출로 인한 화재를 방지하는 시스템의 설비 대안에 위험도 감소 기법을 적용하여 안전성을 향상시키는 방안을 연구하였으며, Sammarco(2007)는 프로그래밍 가능한 PLC-based ESD(Emergency Shut Down) system과 hardwired ESD의 정량적인 안전도 분석을 수행하였다. Goble and Brombacher(1999)는 고장모드를 활용하여 프로그램 가능한 전자 시스템의 FMEDA를 적용하는 기법을 소개하였으며, Kim *et al.*(2010)은 IEC 61508 표준을 기반으로 SIL의 평가요소에 대하여 플로우차트로 명시함으로써, 요구된

는 SIL도출을 위한 가이드라인을 제공하는 연구를 수행하였다. 또한, Jin *et al.*(2002)은 SIS의 기능안전을 분석하기 위해 신뢰도 분석 기법을 적용하여 SIL 등급을 도출하는 과정을 7단계의 프로세스로 정의하여 415V BUS를 대상으로 FTA 기법을 활용하여 SIL인증을 재현하는 연구를 수행하였으며, Lundteigen and Rausand(2009)는 IEC 61508에 정의된 SIL 등급 판정을 위한 시스템의 구조적 제약에 대한 연구를 수행하였다.

3. SIL 판정기준 및 FMEDA 프로세스

3.1 SIL인증 및 등급판정기준

SIL은 IEC 61508 표준에서 제시되는 기능안전성 정의에 따라, 일반적으로 1부터 4까지의 등급을 지니며 등급의 숫자가 높을수록 요구되는 안전무결성 수준이 높음을 의미한다. SIL의 등급을 할당하기 위해서는 공정 및 설비의 안전시스템에 대한 신뢰성을 정량적으로 측정해야 하며, 이를 위해 FMEDA, HAZOP, Consequence Analysis, Risk Matrix 및 FTA와 같은 기법들이 활용된다. 이러한 기법을 바탕으로 도출된 PFD 또는 PFH, HFT(Hardware Fault Tolerance), SFF(Safe Failure Fraction)를 통하여 SIL 등급을 판정하게 되는 것이다.

PFD와 PFH는 요구고장확률과 위험고장확률로서, 시스템이 특정한 기능을 작동하도록 요구받았을 때 실패할 확률을 의미한다. 이러한 고장확률은 작동모드에 따라 구분되며, 저 요구 작동모드와 고 요구 및 연속적인 작동모드를 판단하는 기준은 IEC 61508-4(2010)에 따라 장치의 작동 빈도가 연간 1회 이하일 경우 저 요구 작동모드로 구분하고 작동 빈도가 연간 2회 이상이거나 연속적일 경우 고 요구 및 연속적인 작동모드로 구분한다. 이에 따라, 저 요구 작동모드는 PFD, 고 요구 및 연속적인 작동모드는 PFH가 산출되고 <Table 1>의 목표 고장 기준에 의하여 SIL 등급이 판정된다.

본 연구대상은 1001 구조를 갖으며, 설치환경에서 안전을 저해하는 화염발생 빈도가 연간 1회 이하인 저 요구 작동모드로서, 이에 해당하는 PFD인 식 (1)을 사용하였다.

Table 1. Safety integrity levels-target failure measures for a safety function operating(IEC 61508-1, 2010)

Safety Integrity Level (SIL)	Demand mode of operation	
	Average probability of a dangerous failure on demand of the safety function (PFD)	Average frequency of a dangerous failure of the safety function[h-1] (PFH)
SIL 4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
SIL 3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
SIL 2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
SIL 1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

$$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE} \quad (1)$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_{DU} + \lambda_{DD}} \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_{DU} + \lambda_{DD}} MTTR$$

λ_{DU} : Undetected dangerous failure rate(per hour)

λ_{DD} : Detected dangerous failure rate(per hour)

t_{CE} : Channel equivalent mean down time(hour)

T_1 : Proof test interval(hour)

MRT : Mean repair time(hour)

$MTTR$: Mean time to restoration(hour)

하드웨어 결함 허용수준인 HFT는 장치의 안전기능 질적 특성(Safety Quality)을 표현하며, 시스템의 구조에 따라 0(단일 구조), 1(이중화 구조), 2(삼중화 구조)로 구분된다. 또한, 장치의 모든 구성 요소에 대한 고장모드 및 고장 발생에 따른 시스템의 동작이 완전히 정의되어 있으며, 탐지되거나 혹은 탐지되지 않는 위험고장을 설명하기 위하여 충분히 신뢰할 수 있는 고장 데이터가 있을 경우 type A로 구분되고, type A가 아닌 모든 장치는 type B로 구분되어 SIL 판정 기준이 차별된다. 또한, 최소 하나 이상의 구성 요소가 type B에 해당한다면 장치는 type B로 간주되어야 한다(<Table 2>, <Table 4> 참조; IEC 61508-2, 2010).

Table 2. Determination of HFT Level based on Channel Structures of SIS

HFT	세부검증항목
0	단일 채널 사용, 한 건의 오류가 안전 상실을 초래할 수 있음
1	이중화, 안전 상실이 두 하드웨어 오류가 동시에 발생하는 경우 일어남
2	삼중화, 안전 상실이 세 하드웨어 오류가 동시에 발생하는 경우 일어남

SFF는 시스템의 모든 고장을 대비 안전고장의 비율을 의미하며, 고장의 안전여부와 탐지여부에 따라 <Table 3>와 같이 네 가지 고장유형으로 구분된다. 구분된 각각의 고장률을 바탕으로 식 (2)와 같이 SFF를 산출할 수 있으며, 산출된 SFF는 HFT와 함께 <Table 4>에 따라 최대 SIL 등급의 제약(architectural constraints)을 판정한다. 이러한 제약은 장치의 서브시스템 수준에서 적용되어 이를 통하여 장치의 최대 SIL 등급의 제약을 판정할 수 있다(Sammarco, 2007).

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \quad (2)$$

λ_S : Total safe failure rate(per hour)

λ_{DU} : Undetected dangerous failure rate(per hour)

λ_{DD} : Detected dangerous failure rate(per hour)

Table 3. Failure Rates based on Safety and Detectability(SINTEF, 2010)

	safe failures	dangerous failure
undetected	λ_{SU}	λ_{DU}
detected	λ_{SD}	λ_{DD}
sum	λ_S	λ_D

Table 4. Hardware safety integrity : architectural constraints on type A and type B safety-related subsystems(IEC 61508-2, 2010)

Safety Integrity Level	Hardware Fault Tolerance					
	type A			type B		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	-	SIL 1	SIL 2
60%~90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90%~99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

3.2 SIL 인증을 위한 FMEDA 프로세스 수립

FMEDA는 시스템의 설계단계에서부터 제품의 신뢰성을 분석하는 FMEA의 확장된 기법으로써, 시스템의 구성 항목이 고장이 나는 경우 제품에 어떠한 영향을 미칠 것인가를 체계적으로 분석하는 작업으로 시스템의 구성, 기능, 고장모드, 고장모드의 영향, 고장을 탐지하는 능력을 모두 고려하며 진단유효범위(Diagnostic coverage)를 제공한다(Keum *et al.*, 2008). 따라서, 이러한 FMEDA는 기능안전에 대한 정량적인 평가가 요구되는 SIL인증에 필요한 기준들을 산출하는데 매우 적합하다고 할 수 있으며, 본 연구에서는 SIL 인증을 위한 FMEDA 프로세스를 6단계로 정리하였다(<Figure 1> 참조).

Figure 1. FMEDA Process for SIL Certification

먼저 1단계는 FMEDA의 기본이 되는 FMEA를 수행하는 단계로 실무자를 비롯한 FMEA 관련 작업자들의 인터뷰를 통하여 시스템의 신뢰성블록다이어그램을 작성하고 고장모드의 열거 및 대상 고장모드를 선정한다. 또한, 선정된 고장모드를 바탕으로 추정원인을 검토하며, 고장이 미치는 심각도, 발생도, 검지도를 검토하여 위험우선도(RPN : Risk Priority Number) 및 고장등급을 판정하는 단계이다.

2단계에서는 FMEA를 통하여 선정된 고장모드에 대한 고장률을 할당하는 단계이다. 그러나 고장모드에 대한 고장률의 경우 많은 제조사들이 자사 제품의 고장데이터를 관리하고 있지 못한 실정이다. 따라서 각 부품의 고장모드에 따른 고장률은 보편적으로 사용하는 미 국방성의 표준인 MIL-HDBK-217F와 민간기업에서 작성된 SN29500, Telcordia SR-332, Exida Electrical and Mechanical Component Reliability Handbook 등과 같은 고장률 기준 값을 사용한다. 또한, 위 기준 값에 동일한 구성품이 존재하지 않을 경우 그와 가장 유사한 항목의 고장률을 따르도록 한다.

3단계에서는 이전 단계에서의 고장모드와 고장률을 바탕으로 고장의 안전 및 위험고장 여부와 탐지가능 및 탐지불가능 여부를 판정한다. 안전고장과 위험고장에 대한 기준은 IEC 61508에서 명시된 바와 같이, 특정 부품의 고장이 시스템을 고장 상태로 가져갈 잠재력이 있다면 위험고장으로 정의하며, 시스템에 영향을 미치지 않는다면 안전고장으로 정의한다. 또한, 온라인 진단에 의한 탐지가능 여부에 따라 탐지가능 고장과 탐지불가능 고장으로 각각 구분할 수 있다(<Table 3> 참조).

4단계는 이전 단계의 결과 값을 바탕으로 PFD 및 PFH, SFF, HFT 값을 산출하며, 5단계에서는 4단계에서 산출된 값을 바탕으로 SIL 등급을 판정한다. 판정된 SIL 등급이 목표하는 SIL 등급 이상이면 6단계를 통하여 본 프로세스는 종료되나 그 반대의 경우 FMEA로 돌아가 시스템의 설계 수정 및 구성품 교환을 통하여 위험도를 절감시킴으로써, 목표하는 등급에 도달할 수 있도록 하여야 한다.

4. 화염검출기의 FMEDA를 통한 사례연구

본 연구의 대상인 화염검출기(Flame Scanner)는 서브시스템인 Amplifier와 Sensor로 구성되며, <Figure 2>와 같은 형태로 화력발전소, 열병합발전소, 산업용 보일러 등에서 사용되는 버너의 on/off 상태와 화염의 비정상적인 작동을 감시하여 보다 안전한 버너운영이 이루어질 수 있도록 제어신호를 출력하는 화염감지시스템으로서 <Figure 3>과 같이 버너 내부에 총 4개의 화염검출기가 설치된다. 또한, 2개 이상의 화염검출기가 정상 작동할 경우 안전기능을 수행할 수 있다. 특히, 버너의 화염을 강도(intensity) 및 진동수(frequency)로 구분하여 화염을 검출하는 듀얼 타입 시스템의 개념을 채택하여 화염의 종류를 구별하거나 화염의 상태를 분석할 수 있다(<Figure 3>, <Figure 4> 참조).

Figure 2. Flame Scanner

본 연구에서는 이러한 화염검출기의 FMEDA를 수행하기 위하여 먼저 제조기업의 실무자와의 인터뷰를 진행하였으며, 그 결과 총 2종의 서비스시스템의 224개의 부품구성을 파악하고 해당 부품에 존재하는 고장모드, 고장모드에 따른 영향에 대하여 정의하였다.

제조사에서 자사 제품의 부품 고장률을 별도로 관리하고 있지 않으므로, 본 연구에서는 유럽에서 보편적으로 사용하고 있는 독일 SIEMENS사에서 작성된 SN29500을 활용하였으며, LED 부품에 관한 고장률의 경우 Telcordia사의 Telcordia SR-332를 참고하여 고장률을 산정하였다. 본 연구에 사용된 두 기준에서도 제시되지 않은 부품의 고장률은 비교적 유사한 부품의 고장률로 할당하였다.

Figure 3. Example: Application of Flame Scanner

또한, 컴포넌트 단위의 고장률은 MIL-HDBK-217F에 따라 모든 부품은 직렬로 연결되어 있으며, 고장분포는 지수분포를 따른다는 가정을 활용하였으며, IEC 61508-4에 따라 고장모드의 안전 및 탐지여부를 판정하였다. 이와 같은 가정 및 기준에 따라 화염검출기에 대한 FMEDA를 실시하였으며, 두 종의 서

Figure 4. Inner Circuit Diagram of Flame Scanner

브시스템 중 Sensor의 FMEDA 결과는 <Table 5>와 같다. 위험 우선도는 기준에 따라 각각 5등급으로 구분되는 Severity(심각

도), Detection Rate(검지도), Occurrence rate(발생도)의 곱으로 계산되며, 값이 클수록 개선이 시급히 요구되는 부품 또는 모듈

Table 5. FMEDA for Sensor of Flame Scanner(FIT : failure per billion hours)

SubSystem	Component	Qty	Possible Failure	Final Effect	Severity	Failure Rate (FIT)	Occurrence rate	Detection Rate	Criticality (RPN)	Safemode	Detectability	λ_{SD} (FIT)	λ_{SU} (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)	C^S	C^D
SENSOR												0.00	0.00	138.60	0	-	1.00
Barrel Lens	LENS	1	contamination	Amp. outputs burner trip signal even though burner flame is normal	4	0.00	1	3	12	0	1	0.00	0.00	0.00	0.00		
Auto Self Check Circuit	ADG1436YRUZ	1	all kind of failures	no auto self checking	4	10.00	3	3	36	0	1	0.00	0.00	10.00	0.00		
	RESISTOR	2	all kind of failures	no auto self checking	4	0.60	1	3	12	0	1	0.00	0.00	0.60	0.00		
	CAPACITOR	2	open	minor problems possible	4	4.00	2	3	24	0	1	0.00	0.00	4.00	0.00		
			short	no auto self checking													
			other	minor problems possible													
Surge Protector Circuit	VARIATOR	1	all kind of failures	power supply disrupted	4	1.00	2	3	24	0	1	0.00	0.00	1.00	0.00		
	INDUCTOR	1	all kind of failures	power supply disrupted	4	1.50	2	3	24	0	1	0.00	0.00	1.50	0.00		
	CAPACITOR	1	open	power supply disrupted	4	2.00	2	2	16	0	1	0.00	0.00	2.00	0.00		
			short	power supply disrupted													
			other	power supply disrupted													
I/V Convertor (LOG AMP.)	LOG101	1	all kind of failures	no signal converting	4	10.00	3	3	36	0	1	0.00	0.00	10.00	0.00		
	TL062CD	1	all kind of failures	no signal converting	4	10.00	3	3	36	0	1	0.00	0.00	10.00	0.00		
	AD780/2.5V	1	all kind of failures	no signal converting	4	10.00	3	3	36	0	1	0.00	0.00	10.00	0.00		
	RESISTOR	10	all kind of failures	no signal converting	4	3.00	2	3	24	0	1	0.00	0.00	3.00	0.00		
	CAPACITOR	9	open	minor problems possible	4	18.00	3	3	36	0	1	0.00	0.00	18.00	0.00		
			short	no signal converting													
			other	minor problems possible													
	INDUCTOR	2	open	no signal converting	4	3.00	2	3	24	0	1	0.00	0.00	3.00	0.00		
			short	no signal converting													
			other	no signal converting													
	ZENER DIODE	1	all kind of failures	no signal converting	4	1.00	2	3	24	0	1	0.00	0.00	1.00	0.00		
	PIN HEADER 1x4	1	open	no signal converting	4	0.00	1	3	12	0	1	0.00	0.00	0.00	0.00		

이라 판단할 수 있다. Severity는 부품의 고장이 수명에 영향을 미치지 않으면 1등급, 일시적 고장은 2등급, 원격으로 고장 수리가 가능하면 3등급, 부품 또는 모듈의 교체가 요구되면 4등급, 회복이 불가능하면 5등급으로 정의하였으며, Detection Rate는 시스템이 부품의 고장이 일어나기 전에 탐지하면 1등급, 부품 고장발생 시점에 탐지하면 3등급, 부품의 고장 탐지가 불가능하면 5등급으로 정의하였다. 또한, Occurrence rate은 Failure rate(고장률)에 따라 등급이 결정되며, Failure rate이 1×10^{-9} 미만이면 1등급, 1×10^{-9} 이상이고 1×10^{-8} 미만이면 2등급, 1×10^{-8} 이상이고 1×10^{-7} 미만이면 3등급, 1×10^{-7} 이상이고 1×10^{-6} 미만이면 4등급, 1×10^{-6} 이상이면 5등급으로 정의하였다.

Failure rate열의 단위는 10^9 시간동안의 고장횟수인 FIT(failure in time)로 정의하였다. Safe Mode(안전모드)열은 안전고장이면 1, 위험고장이면 0의 값을 나타내고, Detectability(탐지가능도)열은 탐지가 가능하면 1, 불가능하면 0의 값을 의미한다. 또한 λ_{SD} (탐지 가능한 안전고장)열은 Failure rate, Safe Mode, Detectability열의 곱으로 계산되며, λ_{SU} (탐지 불가능한 안전고장)열은 Failure rate, Safe Mode, (1-Detectability)의 곱으로 계산된다. λ_{DD} (탐지 가능한 위험고장)열은 Failure rate, (1-Safe Mode), Detectability의 곱으로, λ_{DU} (탐지 불가능한 위험고장)열은 Failure rate, (1-Safe Mode), (1-Detectability)의 곱으로 계산된다.

또한, 진단유효범위는 C^S (안전진단유효범위)열과 C^D (위험진단유효범위)열에 서브시스템 단위로 각각 식 (3)과 식 (4)에 따라 계산하였다(Goble and Brombacher, 1999).

$$C^S = \frac{\sum_{all\ components} \lambda_{component\ i}^{SD}}{\sum_{all\ components} \lambda_{component\ i}^{SD} + \sum_{all\ components} \lambda_{component\ i}^{SU}} \quad (3)$$

$\lambda_{component\ i}^{SD}$: detected safe failure rate of component i

$\lambda_{component\ i}^{SU}$: Undetected safe failure rate of component i

$$C^D = \frac{\sum_{all\ components} \lambda_{component\ i}^{DD}}{\sum_{all\ components} \lambda_{component\ i}^{DD} + \sum_{all\ components} \lambda_{component\ i}^{DU}} \quad (4)$$

$\lambda_{component\ i}^{DD}$: detected dangerous failure rate of component i

$\lambda_{component\ i}^{DU}$: Undetected dangerous failure rate of component i

FMEDA를 통하여 안전 및 탐지여부에 따라 4가지로 구분된

고장률을 바탕으로 먼저 SFF를 산출하였으며, HFT는 단일구조, type은 실제 필드데이터가 아닌 SN29500 및 Telcordia SR-332에 따른 값을 사용하였으므로 type B로 채택하여 <Table 4> 기준에 따라 최대 SIL 등급 제약을 산출하였다. 화염검출기의 서브시스템인 AMP. ASSEMBLY와 SENSOR의 SIL 등급 제약을 판정하여 IEC 61508-2(2010)의 Merging Rule에 따라 장치의 최대 SIL 등급 제약을 판정하였다(<Table 6> 참조). Merging Rule은 단일 채널(직렬) 장치의 SIL 등급 제약을 판정할 경우 각 서브시스템의 가장 낮은 SIL 등급 제약을 따르도록 명시하고 있다. 따라서 화염검출기의 최대 SIL 등급 제약은 'SIL 3'으로 판정하였다.

PFD는 proof test interval인 T_1 (1개월, 3개월, 6개월, 1년, 2년, 10년)에 따라 변하나 본 연구에서 λ_{DU} 가 '0' 값을 가지므로 T_1 이 PFD에 영향을 미치지 못하였다. 또한, IEC 61508-6(2010)에서는 위험고장에 대한 자동감지가 가능한 장치의 경우 MRT(Mean repair time)과 MTTR(Mean time to restoration)을 8(시간)으로 가정하고 있으므로 이를 적용하여 계산하였다. 그 결과, 산출된 PFD는 '4.68E-06'으로 <Table 1> 기준을 참조하여 'SIL 4' 등급에 부합하나 최대 SIL 등급 제약이 'SIL 3'이므로 최종 'SIL 3'으로 판정하였다.

사례연구 결과, PFD 관점에서는 최상위 등급인 'SIL 4'에 부합하는 수준이나 서브시스템의 구조가 모두 단일 구조로 HFT가 '0'에 해당하므로 아무리 높은 SFF에도 최대 'SIL 3'으로 제약되어 있는 것이다. 그러나 본 장치는 버너 내부에 중복 설치되어 안전기능을 수행하므로 단일 구조로 설계된 서브시스템으로도 목표하는 안전 수준에 도달할 수 있다.

5. 결 론

최근 부품 신뢰도의 향상으로 인하여 시스템 신뢰도 역시 지속적인 향상이 이루어지고 있으나, 시스템의 고장은 대형 안전사고로 이어질 수 있다. 따라서 특정 부품의 고장이 전체 시스템의 안전에 위해를 가할 수 있으므로, 전체 시스템의 위험을 감지하고 안전을 확보할 수 있는 안전장치가 요구된다. 이와 같이 시스템의 기능안전을 담당하는 안전장치는 위험 발생 시 올바르게 작동해야 하며, 위험에 대한 지속적 모니터링이 이루어져야 한다. 즉, 안전장치의 기능안전에 대한 위험을 최소화하는 것은 매우 중요하므로, 기능안전의 안전무결성에 대한 정량적 평가치인 SIL 인증은 발전소 및 대형 설비 등에 보편적

Table 6. Architectural constraints on Subsystem of Flame Scanner

SubSystem 6	SFF (%)	HFT type	C^S (%)	C^D (%)	$\sum \lambda_S$ (FIT)	$\sum \lambda_D$ (FIT)	$\sum \lambda_{DD}$ (FIT)	$\sum \lambda_{DU}$ (FIT)	Determination of SIL (architectural constraints)
AMP. ASSEMBLY	100.00	B	100.00	100.00	89.42	446.10	446.10	0.00	SIL 3
SENSOR	100.00	B	-	100.00	0.00	138.60	138.60	0.00	SIL 3

으로 요구되고 있다.

이러한 SIL 인증 시 다양한 기법들이 사용되고 있으나, 본 연구에서는 FMEDA 기법을 활용하여 SIL 인증을 위한 기준 값을 산출하였다. 또한, 화염검출기를 대상으로 사례연구를 실시함으로써 화염검출기의 SIL 등급을 판정하고 SIL 기준 값을 도출하는 FMEDA의 적용 과정을 1~6단계의 프로세스로 제시하였다. 그 결과 안전장치의 기능안전에 대해 정량적 평가 및 정성적 평가를 수행하였다.

FMEDA 기법을 통해 각 고장모드 별 안전 및 위험여부와 탐지 가능여부를 판단함으로써, 단순 고장률에 따라서가 아니라 탐지 불가능한 위험고장을 기준으로 시스템의 우선 개선점을 찾아낼 수 있다. 이는 낮은 고장률을 갖는 고장모드라 하더라도 탐지되지 않는 위험한 고장일 수 있으며, 반대로 높은 고장률을 갖는 고장모드가 안전고장일 수 있다는 것을 의미한다. 즉, 신뢰성 측면에서는 높은 고장률을 갖는 고장모드가 중요 개선점이 될 수 있으나, 안전성 측면에서는 고장률과 더불어 위험고장 여부 및 탐지 가능 여부에 따라 주요 개선 영역을 결정하는 것이다. 따라서 FMEDA는 SIL 인증과 더불어 안전에 대한 분석에 유용한 기법으로 활용될 수 있을 것이다.

본 연구에서는 아직 국내에서 보편화되지 않은 기능안전에 대한 국제 인증인 SIL 인증에 대한 개요와 판정기준 및 기준 값을 소개하였다. 또한, SIL 인증을 위한 FMEDA 프로세스를 제시함으로써, 대형 설비 및 발전 장비를 납품하는 국내의 많은 중소기업에 가이드라인이 되리라 판단한다.

참고문헌

- IEC 61508-0 (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems-part 0 : Functional safety and IEC 61508.
- IEC 61508-1 (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems-part 1 : General requirements.
- IEC 61508-2 (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 2 : Requirements for electrical/electronic/programmable electronic safety-related systems.
- IEC 61508-4 (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 4 : Definitions and abbreviations.
- IEC 61508-6 (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 6 : Guidelines on the application of IEC 61508-2 and IEC 61508-3.
- SIEMENS SN 29500-1 (1996), Failure rates of components-Expected values, General.
- SIEMENS SN 29500-2 (1999), Failure rates of components-Expected values for integrated circuits.
- SIEMENS SN 29500-3 (1997), Failure rates of components-Expected values for discrete semiconductors.
- SIEMENS SN 29500-4 (1999), Failure rates of components-Expected values for passive components.
- SIEMENS SN 29500-6 (1996), Failure rates of components-Expected values for electrical and optical connectors and sockets.
- SIEMENS SN 29500-7 (1997), Failure rates of components-Expected values for relays.
- Telcordia SR-332 (2006), Reliability prediction procedure for Electronic equipment : Issue 2.
- SINTEF (2010), Reliability Prediction Method and Data for Safety Instrumented Systems, Trondheim, Norway.
- Chang, S.-H., An, G.-Y., Lee, D.-G., and Lee, J. (2009), A study on the SIL application for electronic interlocking equipment of high speed line, 2009 Fall Conference Publication of the Korean Society for Railway, 3442-3447.
- Cho, C.-H., Kang, C.-Y., and Hwang, J.-H. (2010), Study on ISA's assessment to software process for EN50128 SIL4, 2010 Spring Conference Publication of the Korean Society for Railway, 838-849.
- Choi, J.-R., Kim, Y.-S. and Shin, S.-K. (2009), SIL Assessment and Validation of ATP On-Board System using Fault Tree Analysis, 2009 Fall Conference Publication of the Korean Society for Railway, 1439-1447.
- Goble, W. M. and Brombacher, A. C. (1999), Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems, *Reliability Engineering and System Safety*, 66(2), 145-148.
- Jin, S.-H., Song, K. H., Yeo, Y.-K. and Kim, I.-W. (2002), Development of the SIS Evaluation Method Based on Reliability Analysis, *Journal of the Korean Institute of Gas*, 6(1), 66-73.
- Jo, H.-J., Hwang, J.-G., Shin, S.-K. and Oh, S.-M. (2010), Analysis of S/W Test Coverage Automated Tool and Standard in Railway System, *Journal of academia-industrial technology*, 11(11), 4460-4467.
- Joung, E.-J. and Kim, Y.-M. (2004), A Hazard Identification and Analysis for the Train Control System of Light Rail Transit, *The Transactions of KIEE*, 53B(2), 99-106.
- Keum, J.-Y., Suh, Y.-S., Lee, J.-K., and Park, J.-Y. (2008), Measurement of a Diagnostic Coverage for a Digital Signal Processor Board Using an FMEDA, *Journal of Applied Reliability*, 8(2), 101-111.
- Kim, G.-Y., Ko, B.-G., Jang J. S., and Chan, S.-I. (2010), Assessment Procedure of Safety Integrity Level(SIL) Based on Flowchart, *Journal of Applied Reliability*, 10(2), 107-122.
- Kim, J. H., Kim, B. S., Yang, J. M., Jang, C. B., Kim, M. S., Jung, S. Y., and Ko, J. W. (2011), A Study of Risk Reduction by SIL(Safety Integrity Level) Determination, *Journal of the Korean Institute of Gas*, 15(5), 57-62.
- Ko, J.-S. and Kim, H. (2003), Reliability Analysis on Firewater Supply Facilities based on the Probability Theory with Considering Common Cause Failures, *Journal of Korean Institute of Fire Science and Engineering*, 17(4), 76-85.
- Ko, J.-S., Kim, H., and Lee, S.-K. (2006), Reliability Analysis on Safety Instrumented System by Using Safety Integrity Level for Fire-Explosion Prevention in the Ethyl Benzene Processes, *Journal of Korean Institute of Fire Science & Engineering*, 20(3), 1-8.
- Lundeigen, M. A. and Rausand, M. (2009), Architectural constraints in IEC 61508 : Do they have the intended effect?, *Reliability Engineering and System Safety*, 94(2), 520-525.
- Sammarco, J. J. (2007), Programmable Electronic and Hardwired Emergency Shutdown Systems : A Quantified Safety Analysis, *IEEE Transactions on Industry Applications*, 43(4), 1061-1068.
- Shin, D., Baek, J.-H., Lee, K.-M., and Lee, J.-H. (2009), A Study on the SIL Allocation and Demonstration for Train Control System, 2009 Spring Conference Publication of the Korean Society for Railway, 855-859.
- Suh, S., Yang, Y., Chung, S., and Ryu, W. (2012), Fire Safety Assessment Based on FSA and Risk Reduction of Machinery System Considering Functional Safety, *Journal of the Society of Naval Architects of Korea*, 49(3), 239-246.

김 성 규

경기대학교 산업경영공학과 학사
현재 : 경기대학교 산업경영공학과 석사과정
관심분야 : 신뢰성공학, 데이터마이닝

김 용 수

한국과학기술원 산업공학과 학사
한국과학기술원 산업공학과 석사
한국과학기술원 산업공학과 박사
현재 : 경기대학교 산업경영공학과 조교수
관심분야 : 통계 및 데이터마이닝, 품질경영,
신뢰성공학