IEC 61508 기반 안전 무결성 레벨 평가 및 관리방안에 관한 연구

A Study on the Management Method & Evaluation for Safety Integrity Level (SIL)

정기호*, 최용은*, 오효석*, 김재문*†

Ki-Ho Jeong*, Yong-Eun Choi*, Hyo-Seok Oh*, Jae-Moon Kim*†

초 록 본 논문에서는 전기, 전자, 프로그램 가능한 전자 안전 관련 시스템의 기능 안전을 위한 IEC 61508 국제표준에 전반적인 내용을 기반으로 IEC 61508의 Safety Integrity Level (SIL)에 대한 위험도 분석, 요건 등에 대하여 고찰하였다. 이를 바탕으로 Safety Integrity Level (SIL) 등급의 분리 방법과 할당방법에 대하여 기술하고 시스템 개발 시 할당된 SIL을 하드웨어 및 소프트웨어에 적용하는 방법 및 하드웨어와 소프트웨어의 SIL 달성 여부에 대한 위험도 평가방법 등을 통한 운영 및 예방 유지보수시 고장률 관리방안에 대하여 제시하였다.

주요어 : SIL, PFH, PFD, ISA, SIS, EUC, SSF, FMEA

1. 서 론

본 연구는 IEC 61508에 대한 적반적인 내용 중 Part.5 안전무결성레벨(SIL) 평가방법에 대한 연구로써 SIL등급의 분리 방법 과 할당방법에 대하여 설명하였다. 이를 토대로 운영 및 유지보수 단계에서의 효과적인 시스템 신뢰성, 가용성, 유지보수성 및 안전성 확보를 위한 위험도 관리(평가 분석)을 통한 안정성확보 방안을 제시하였다.

2. 본 론

2.1 안전 무결성 레벨(SIL)

SIL은 공정에 대한 위험을 허용가능 수준으로 감소시키기 위하여 시스템에서 요구하는 이용가능성을 충족시키는데 있다. SIL의 정의는 안전관련 시스템이 모든 규정된 조건하에서 정해진 시간 안에 요구되는 안전기능을 만족스럽게 수행해낼 가능성 또는 확률로 정의되며 안전에 필요한 부분으로서 위험도 저감 요소를 필요로 한다. [Table 1]은 IEC 61508과 ISA S84.01 표준에서 제시된 SIL에 따른 이용가능 상태를 분류하고 있다.

Table 1 SIL Classification

SIL			German Appl Class(AK)	Availability Required(%)	Risk Reduction Factor	Typical App
IEC 61508		4	7	>99.99	>10,000	Rail Transportation & Nuclear Power
	ISA S84	3	5-6	99.90~99.99	1,000~10,000	Utility Boiler
		2	4	99.00~99.90	100~1,000	Industrial Boiler
		1	2-3	90.00~99.00	10~100	& Chemical Process

IEC 61508에서는 SIL을 4등급, ISA에서는 3등급으로 분류하였으며, 독일에서는 SIL을 7등급으로 분류하여 사용하고 있다. 이러한 등급의 차이가 발생하는 이유는 적용 산업분야에 따른 안전성 요구사항 수준이 다르기 때문이다. SIL 4등급은 Process 산업에 적용되지 않으며 항공, 원자력 등 특수산업에만 적용된다.

[Table 1]에서 시스템의 가용도 요건에 따라 다양한 산업에서 필요한 SIL을 표시하였다. 사고가 발생하였을 경우 경제·환경에 미치는 파급효과가 큰 산업일수록 높은 SIL이 필요하다는 것을 알 수 있다. 그 중 공정산업은 보통 SIL을

† 교신저자: 한국교통대학교 교통대학원 교통정책/교통시스템공학과(goldmoon@ut.ac.kr)

* 한국교통대학교 교통대학원 교통정책/교통시스템공학과

1~3등급으로 분류하고 있다. SIL 1등급이 갖는 의미는 잠재위험이나 경제적 위험(Economic Risk) 등급이 낮으면서 90%의 이용 가능 상태를 유지하는 시스템을 의미한다. Risk Reduction Factor는 아래 제시된 식과 같이 시스템이 가지고 있는 고유위험도를 허용 가능한 위험도로 나눈 값으로 정의되며, 이것은 사고를 예방하기 위해 또는 잠재위험을 모니터링하기 위해 이용되는 요소이다.

$$Risk\,Reduction\,Factor\,(RRF) = \frac{\in herent\,Risk}{Acceptable\,Risk}$$

시스템에서 요구되는 SIL에 따라 안전 계측시스템(SIS)이 시스템에 설치되어 있다면, 이것이 요구하는 안전기능을 제대로 수행하고 있는지 평가해야 한다. 안전계측시스템(SIS)을 구성하는 장치들의 SIL 평가에 영향을 주는 요소들은 다음과 같다.

- Hardware Fault Tolerance
- Safe Failure Fraction : SFF
- Probability of Failure On Demand : PFD
- Maintenance Intervals

2.2 SIL 분류 위험성 발생 빈도

IEC 61508과 IEC 61511에서는 안전기능의 요구사항을 보다 명확하게 나타내기 위해서 안전관련 시스템의 안전 무결성 레벨(SIL)을 시스템의 사용빈도와 연속성에 따라 두 가지 유형으로 분류하고 있다.

- 높은 동작(연속형)모드 : 시스템의 사용빈도가 높거나 연속적으로 동작하는 시스템에 적용하고, 시스템 고장률은 PFH 단위를 사용한다.
- 낮은 동작모드 : 시스템의 사용빈도가 높거나 연속적으로 동작하는 시스템에 적용하고, 시스템 고장률은 PFH 단위를 사용한다. 시스템이 필요할 때만 요구 신호에 의해 동작하는 시스템에 적용하고, 시스템의 고장률은 PFD 단위를 사용한다.(시스템의 사용빈도 년 1회 이하)

Table 2 SIL of Demand

SIL	Low Action Mode	High Action Mode
1	$\geq 10^{-5} \sim < 10^{-4}$	$\geq 10^{-9} \sim < 10^{-8}$
2	$\geq 10^{-4} \sim < 10^{-3}$	$\geq 10^{-8} \sim < 10^{-7}$
3	$\geq 10^{-3} \sim < 10^{-2}$	$\geq 10^{-7} \sim < 10^{-6}$
4	$\geq 10^{-2} \sim < 10^{-1}$	$\geq 10^{-6} \sim < 10^{-5}$

위 기준에서는 [Table 2]과 같이 동작모드별 안전 무결성 레벨(SIL)의 목표 고장률을 나타내고 있다.

2.3 SFF(Safety Failure Fraction) & HFT(Hardware Faulty Tolerance)

IEC 61508에서는 안전관련 시스템의 고장을 [Table 3]와 같이 크게 안전한 고장(Safe failure)과 위험한 고장 (Dangerous failure)으로 분류하고 있다. 안전한 고장(Safe failure)을 세부적으로 다시 나누면 검지된 안전고장(Detected safe failure)과 검지되지 않은 안전고장(Undetected safe failure)로 분류한다. 위험한 고장(Dangerous failure)도 안전한 고장처럼 검지된 위험한 고장과 검지되지 않은 위험한 고장으로 분류할 수 있다.

Table 3 System Failure Type

Failure Type	Detected	Undetected
Safe	Safe Detected λ_{SD}	Safe Undetected λ_{SU}
Dangerous	Dangerous Detected λ_{DD}	Dangerous Undetected λ_{DU}

SSF(Safe Failure Fraction) 파라미터는 시스템 전체 고장 중 안전기능의 상실을 주지 않는 고장들의 합으로 나타낼 수 있다.

$$SSF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

SFF 값은 안전한 기기(Device) 고장의 비율을 나타낸다. SFF 79%는 100가지 기기 고장의 79가지가 기기의 안전기능 상실에 영향을 주지 않는다는 의미가 된다. 즉 SFF값이 클수록 안전 관련 시스템의 신뢰성은 높다고 할 수 있다.

IEC61508에서는 하드웨어 결함 허용 (HFT)정의를 “시스템이 결함 및 에러가 발생 시에도 요구하는 기능을 계속해서 수행할 있는 능력”이라 정의하고 있다. HFT는 SFF와 함께 사용되어 Risk Area를 결정하고 두 값에 따라 [Table 4] 같은 SIL 테이블이 결정된다.

Table 4 Hardware Fault Tolerance

SFF	HFT(Taype A- Simple Subsystem			HFT(Type B- Complex Subsystem		
Lev	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	Not Allowed	SIL1	SIL2
60%~90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90%~99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

2.4 SIL 결정방법

SIL 결정방법은 크게 나누어 위험요인을 도출하고 위험요인에 대한 안전대책을 확인, 수립하는 정성적 평가와 위험요인별 사고로 발전할 수 있는 확률과 사고피해 크기를 정량적으로 계산하여 위험도를 수치로 계산하고 허용범위를 벗어난 위험에 대한 안전대책을 세우는 정량적인 평가가 있다. IEC61508, IEC 61611에서는 SIL 결정방법으로 다음과 같은 방법을 제공하고 있다.

- IEC61508: 정량적, 정성적(RiskGraph) 방법 및 위험한 사건 심각도 매트릭스(정성적)
- IEC61511: 정량적(Semi), Risk Graph, Layer Of Protection Analysis(LOPA)

2.4.1 정성적 방법 (Rick Graph)

SIL을 결정하는 정성적인 방법 중 Risk Graph 방법은 정밀한 위험률, 정확한 계산, 복잡한 모델링 등이 필요하지 않고, 어느 분야에서나 적용하기가 용이하여 가장 많이 사용하는 방법이다. Risk Graph는 [Figure 1]에 나타나 있는 사고의 심각도(C), 사고의 발생빈도 및 노출시간(F), 사고 회피 가능성 확률(P), 사고 발생 확률(W) 등의 요소들을 결합하여 SIL을 결정한다.

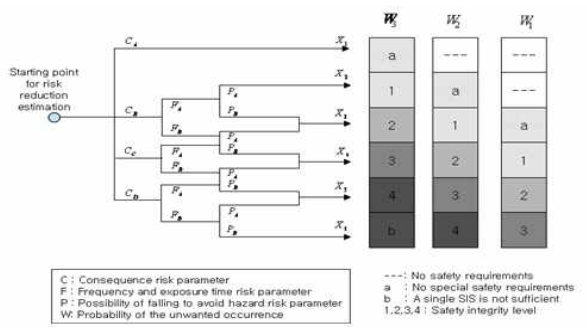

Fig. 1 Rick Graph

2.4.2 정량적 방법 (Rick Graph)

허용위험도가 수치로 제시된 경우, 안전관련 시스템의 SIL에 대한 목표치가 설정된 경우 사용된다.

- 허용위험도를 결정
- 허용위험도 충족 요구 위험도감소($\triangle R$) 결정
- 요구된 위험도 감소량을 안전계측시스템(SIS), 타 기술의 안전관련 시스템, 외장형 위험도 감소 설비로 분배
- 요구동작모드결정[높은(연속),낮은 동작모드]

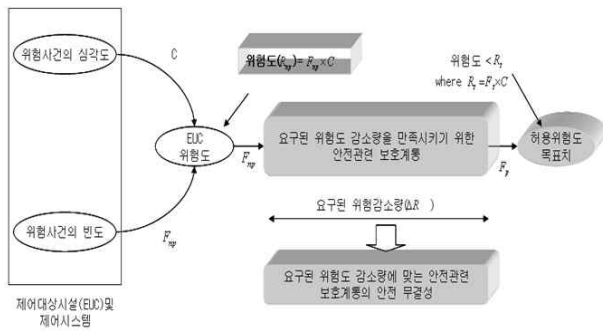

Fig. 2 SIL Determination Procedure for Safety related Protection system

우선 어떠한 보호설비도 추가하지 않았을 때 제어대상 시설(EUC)의 위험도에 대한 발생빈도(F_{np})와 심각도(C)를 결정하여 요구되는 위험도 수준이 달성되는지를 결정한다.

Table 5 Risk Level Matrix

Frequency	Severity			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasionary	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

위험도 수준 평가 후 특정한 상황에 있어서 심각도가 일정하다고 가정하고 요구된 위험도 감소량(ΔR)을 만족하는 안전관련 보호계통의 기동 요구시 평균고장확률 (PFD_{avg})을 FMEDA, FTA 분석을 통해 계산한다. 계산된 PFD_{avg}는 [Table 5]를 참조하여 SIL 등급을 결정한다. 만약 낮은 동작모드의 $PFD_{avg} = 10^{-2} \sim 10^{-3}$인 경우 SIL2 이다.

2.4.3 고장영향 분석

운영 및 유지보수시 각 장치별 고장모드에 대한 고장영향 평가를 위한 FMEA 수행 (a.계층구조 및 신뢰성 블록도 b.안전고장 및 위험고장 분류, 진단율 계산)

- 위험 고장진단율(DC_D)= $\frac{\sum\lambda_{DD}}{\sum\lambda_D}$
- 안전고장 비율(SFF) = $\frac{\sum\lambda_S+\sum\lambda_{DD}}{\sum\lambda_S+\sum\lambda_D}$

Table 6 FMEA

Code LRU	LRU Description	Failure Mode	Failure Mode Ratio	Safety Assessment			Failure Rate ($F/10^9hr$)	Failure Rate of Mode	Failure Rate of Module			Failure Rate of Subsystem		
				Safe	Dangerous	Detected			λ_S	λ_D	λ_{DD}	λ_S	λ_D	λ_{DD}
1.1	Central Computer Unit (CCU)													
1.1.1	CPUS Board	No Operation	63.6%		√	Yes	25.1867	16.0187	9.1680	16.0187	16.0187	32.2018	56.2648	55.6270
		Shorted	13.6%	√		Yes		3.4254						
		Wire Bond Failure	12.6%	√		Yes		3.1735						
		Opened	9.9%	√		Yes		2.4935						
		Loose	0.3%	√		Yes		0.0756						
1.1.2	GW Board	No Operation	63.6%		√	Yes	17.4614	11.1055	6.3559	11.1055	11.1055			
		Shorted	13.6%	√		Yes		2.3748						
		Wire Bond Failure	12.6%	√		Yes		2.2001						
		Opened	9.9%	√		Yes		1.7287						
		Loose	0.3%	√		Yes		0.0524						
1.1.3	Memory Board	No Operation	63.6%		√	Yes	18.1218	11.5255	6.5963	11.5255	11.5255			
		Shorted	13.6%	√		Yes		2.4646						
		Wire Bond Failure	12.6%	√		Yes		2.2833						
		Opened	9.9%	√		Yes		1.7941						
		Loose	0.3%	√		Yes		0.0544						
1.1.4	DI Board	No Operation	63.6%		√	Yes	12.8280	8.1586	4.6694	8.1586	8.1586			
		Shorted	13.6%	√		Yes		1.7446						
		Wire Bond Failure	12.6%	√		Yes		1.6163						
		Opened	9.9%	√		Yes		1.2700						
		Loose	0.3%	√		Yes		0.0385						
1.1.5	DO Board	No Operation	63.6%		√	Yes	13.8659	8.8187	5.0472	8.8187	8.8187			
		Shorted	13.6%	√		Yes		1.8858						
		Wire Bond Failure	12.6%	√		Yes		1.7471						
		Opened	9.9%	√		Yes		1.3727						
		Loose	0.3%	√		Yes		0.0416						
1.1.6	PS Board	No Operation	63.6%		√	No	1.0028	0.6378	0.3650	0.6378	0.0000			
		Shorted	13.6%	√		Yes		0.1364						
		Wire Bond Failure	12.6%	√		Yes		0.1264						
		Opened	9.9%	√		Yes		0.0993						
		Loose	0.3%	√		Yes		0.0030						
1.2	Bus Input/Output (BIO)	Opened	33.3%		√	Yes	15.7158	5.2334				0.0000	15.7158	10.4668
		Shorted	33.3%		√	Yes		5.2334						
		Timing Error	33.3%		√	No		5.2334						

3. 결 론

본 SIL 평가방법에 대한 연구를 통해 운영 및 유지보수 단계에서의 각 장치별 위험도 및 고장영향에 대한 위험도 분석방안을 제시하였으며, 해당 위험, 고장률 분석을 통해 더 나아가 선제적이고 안정적인 유지보수를 위한 관리기준의 방향을 제시하였다.

참고문헌

[1] IEC 61508. International Standard for the functional Safety of electrical, electronic and Programmable electronic equipment

[2] MIL-STD-1629A, Procedure for Performing a Failure mode, Effect and Criticality Analysis

[3] MIL-HDBK-217F, Reliability Prediction of Electronic Equipment

[4] Fault Tree with Aerospace Application', Version 1.1, NASA Publication, August 2002