KIGAS Vol.6, No.1, March, 2002
(Journal of the Korean Institute of Gas)

신뢰도 분석에 근거한 SIS 평가 방법론 개발

진 상 화 · 송 광 호* · 여 영 구** · †김 인 원
건국대학교 화학공학과
* (주) LG 화학 기술연구소
** 한양대학교 화학공학과
(2002년 3월 4일 접수, 2002년 3월 18일 채택)

Development of the SIS Evaluation Method Based on Reliability Analysis

Sang-Hwa Jin · Kwang Ho Song*, Yeong-Koo Yeo and In-Won Kim**
Department of Chemical Engineering, Konkuk University, Korea
** LG Chemical Ltd., Research Park, Daejeon, Korea*
*** Department of Chemical Engineering, Hanyang University, Korea*
(Received 4 March 2002 ; Accepted 18 March 2002)

요 약

본 연구에서는 결함수목 분석법을 이용하여 Safety Integrity Level(SIL)을 평가하고 시스템의 목표한 SIL에 도달하지 못할 경우에 신뢰도 분석과 시스템 retrofit을 통해서 목표한 SIL을 만족시키게 하는 방법을 개발하였다.

신뢰도 분석에 근거한 SIL 평가 방법을 검증하기 위해서 415V Diesel BUS에 대해서 위험성 분석을 수행하였다. 기존의 415V Diesel BUS에 대한 이용가능 상태는 99.40%로 SIL 2등급에 해당된다. 개발된 평가방법을 이용하여 diesel generator와 isolator switch의 교체 후 시스템의 이용가능 상태는 99.94% SIL 3등급으로 상승되었다.

본 연구에서 제시한 신뢰도에 근거한 SIL 평가 방법을 적용하면 사고 예방과 손실감소로 일어나는 유지보수 비용의 절감 등을 가져오면 물론 시스템의 신뢰도를 극대화 할 수 있다.

Abstract - In this study a new SIS evaluation method based on the reliability analysis has been developed. It evaluates the Safety Integrity Level (SIL) using the Fault Tree Analysis (FTA), and when the SIL falls short of the systems target level, through the reliability analysis and system retrofit, this method will satisfy the aimed SIL.

A hazard evaluation was carried out on the 415V Diesel BUS to verify the SIL evaluation method based on the reliability analysis. The availability of the original 415V Diesel BUS was 99.40%, which comes under the category of SIL 2. After exchanging the diesel generator and the isolator switch using the developed evaluation method, the availability rose to 99.94%, SIL 3.

By applying the method presented in this study, not only will it reduce the maintenance cost due to the prevention of accidents and reduction of loss, but also maximize the reliability of the system.

Key words : Safety Integrity Level, Safety Instrumented System, Reliability Analysis

† 주저자 : inwon@kkucc.konkuk.ac.kr

Ⅰ. 서 론

공정산업에 대해서 위험성 최소화 또는 안전성 향상을 위하여 Instrument Society of America (ISA)와 International Electrotechnical Commission (IEC)에서는 Safety Instrumented System 표준을 개발하였다[1]. 1996년에 ANSI/ISA S84.01 표준 "Application of Safety Instrumented Systems for the Process Industries"을 공정산업에 적용하도록 하였다.

Safety Instrumented System(SIS)은 센서와 한 가지 또는 여러 가지 제어기로 구성된 제어 시스템을 말한다. 즉, SIS는 개인, 장비, 환경 또는 세 가지 모두에 대한 보호 시스템을 말한다. 이러한 SIS의 수행 목적은 안전성 향상 또는 위험의 감소를 위해 잠재위험의 모니터링과 사고가 발생하였을 경우 사전에 계획된 프로그램으로 인한 예방, 또는 사고가 발생하였을 경우에 대한 피해결과를 최소화하는데 그 목적이 있다. 공정에서 이용되는 SIS는 공정장치, 공정제어 그리고 다른 방호장비에 대한 기계적 무결성을 결정하기 위해 이용되어진다. 또한 이러한 SIS는 공정에 대한 생산량 또는 공정의 효율을 증가시키는 것은 아니며 손실감소로 인해 발생할 수 있는 유지보수 비용의 절감과 risk cost를 감소시키는 특성을 가지고 있다[2].

SIS을 수행하기 위해서는 어떤 장치나 시스템에 대한 Safety Integrity Level(SIL)의 설정이 필요하다. SIL 또는 이용가능 상태(Availability)는 공정에서 사고가 발생하였을 경우 SIS의 무결성을 간단한 통계학적인 설명을 의미한다.

Table 1. Qualitative View of SIL.

SIL	Generalized View
4	Catastrophic Community Impact
3	Employee and Community Impact
2	Major property and production Protection. Possible Injury to employee
1	Minor Property and Production Protection

Fig. 1은 IEC 61508과 ISA S84.01에서 제시된 SIL 등급에 따른 이용가능 상태를 나타낸 그림이며, 독일에서 설정한 SIL과 비교하여 표현하였다. SIL 1등급의 의미는 잠재위험(hazard)이나 경제적 위험(economic risk) 등급이 낮으면서 90%의 이용가능 상태를 의미한다. 또는 10%의 고장이 발생할 가능성으로도 표현할 수 있다. 예를 들어 SIL 1등급이라고 가정한 시스템에 대한 90%의 이용가능상태의 의미는 10번 시스템이 운전되어 질 때 시스템이 한번은 고장이 발생한다는 것을 의미한다. Fig. 1에서 Risk Reduction Factor는 식 (1)로 정의되어지며 SIS에서 사용되어진다[3].

$$Risk\ \ Reduction\ Factor(RRF) = \frac{Inherent\ Risk}{Acceptable\ Risk} \quad (1)$$

Safety Integrity Levle			Corresponding German Appl. Class(AK)	Availability Required	Risk Reduction Factor	Typical Application
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 Boilers
		2	4	99.00 - 99.90%	100 - 1,000	Industrial Boilers
		1	2 - 3	90.00 - 99.00%	10 - 100	Chemical Process

Fig. 1. Safety integrity level correlation with availability and risk reduction factor.

식 (1)에서 정의된 RRF는 SIS에서 사건을 예방하기 위해 또는 잠재위험을 모니터링하기 위해 이용되어지는 요소이다.

또한 SIL에 따른 산업의 분포를 나타내었으며 그중 화학산업은 보통 SIL 2~3등급으로 분류되어있다. Table 1은 이러한 SIL의 무결성을 정성적으로 표현한 것이다.

SIL 등급을 설정하기 위해서는 위험성 평가 방법론에 근거하여 등급을 설정한다. 이러한 위험성 평가 방법론으로는 modified HAZOP, consequence, risk matrix, risk graph, quantitative assessment 와 corporate mandated SIL의 방법론을 포함한다. 위의 위험성 평가 방법론은 SIL 등급 평가의 절차와 지침을 개발하기 위해 필요하다.

Modified HAZOP은 일반적으로 이용하고 있는 정성적 위험성 평가 방법과 비슷하다. 그러나 일반적으로 이용되는 위험성 평가 방법과 다른 점은 Fig. 1에서 제시된 이용가능 상태와 RRF를 고려하여 SIL 등급이 설정되어 있다.

Consequence는 가장 보수적인 위험성 평가 방법 중에 하나이며, SIL에서는 사건의 발생빈도는 고려하지 않았다. Table 2는 SIL 등급에 따른 consequence 등급을 결정하기 위해 사건의 심각도(severity)를 분류해 놓은 표이다.

Table 2. Consequence only decision table.

SIL	Generalized View
4	Potential for fatalities in the community
3	Potential for multiple fatalities
2	Potential for major serious injuries or one fatality
1	Potential for minor injuries

본 연구에서는 위험성 분석을 수행하여 장치가 가지고 있는 이용가능상태(Availability) 또는 이용불능상태(Unavailability)를 평가하여 SIL(Safety Integrity Level) 등급을 설정하였다. 그리고 신뢰도 분석을 수행하여 장치의 중요도(Importance)와 위험성 증가 요소(Risk Increase Factor) 그리고 위험성 감소 요소(Risk Decrease Factor)를 분석하여 새로운 장치의 설치 또는 좋은 신뢰도를 가지는 장치의 교체와 같은 SIS를 적용하여 위험성 분석을 수행한 후 본래 가지고 있던 이용가능 상태와 개선 후에 이용가능 상태를 비교하여 SIL 등급의 변화와 시스템의 중요도 분석을 수행하였다.

II. 신뢰도분석에 근거한 SIS 평가방법

본 연구에서는 신뢰도 분석(reliability analysis)에 근거하여 시스템의 SIS를 평가하고 위험을 감소시키는 방법을 제시하였다. 이 방법은 Fig. 2와 같이 7가지 단계로 이루어진다.

단계 1 : System Description
시스템을 구성하고 있는 장치와 운전조건 및 운전상태, 유지보수 현황 등을 평가한다.

단계 2 : Hazard Evaluation
시스템에 존재하는 잠재위험을 평가하는 단계이다. Modified HAZOP, Consequence Analysis, Risk Matrix, Risk Graph 와 Quantative Analysis 등의 방법을 이용한다.

단계 3 : SIL Determination
단계 2의 결과에 따라 SIL 등급을 평가한다. 이때 평가된 등급이 목표한 SIL 등급(target SIL)을 만족하면 SIS 평가는 종료된다. 그러나 목표한 SIL 등급을 만족하지 못할 경우에는 다음 단계의 분석이 수행되어진다.

단계 4 : Reliability Analysis
신뢰도 분석 단계에서는 시스템에 대한 신뢰도 분석을 수행하여 장치에 대한 중요도, 위험성 증가요소(Risk Increase Factor)와 위험성 감소 요소(Risk Decrease Factor)를 평가하여 안전성 향상 방법을 분석한다.

단계 5 : System Retrofit
신뢰도 분석의 수행 결과로 제시된 시스템의 위험을 감소시키는 방법을 수행한다. 고장률이 낮은 장치로의 교체 또는 다른 안전장치의 설치 및 방호장비 등의 설치하여 시스템을 재 구성하는 단계이다.

단계 6 : SIL Re-evaluation
단계 5에서 제시한 안전성을 향상시키는 방법을 수행하여 재 구성된 시스템에 대한 SIL 등

급을 다시 평가하는 단계이다. 이때 분석된 SIL 등급이 목표한 SIL 등급을 만족하면 SIS 평가는 종료된다. 하지만 SIL 등급이 설정된 등급을 만족하지 못할 경우 단계 3으로 돌아가 위의 과정을 반복 수행하여 SIL 등급을 평가한다.

단계 7: Stop

만족하는 SIL 등급이 설정되었을 때 SIS 평가를 종료하는 단계이다.

III. 신뢰도 분석(Reliability Analysis)

신뢰도 분석은 중요도 분석(Importance Analysis), RDF(Risk Decrease Factor), RIF(Risk Increase Factor), 불확실성 분석(Uncertainty Analysis) 그리고 민감도 분석(Sensitivity Analysis)등의 분석방법을 모두 포함한다. 중요도 분석과 민감도 분석은 장치가 시스템에 어느 정도 기여도를 가지고 있는지 분석하는 방법이다. 불확실성 분석은 최종

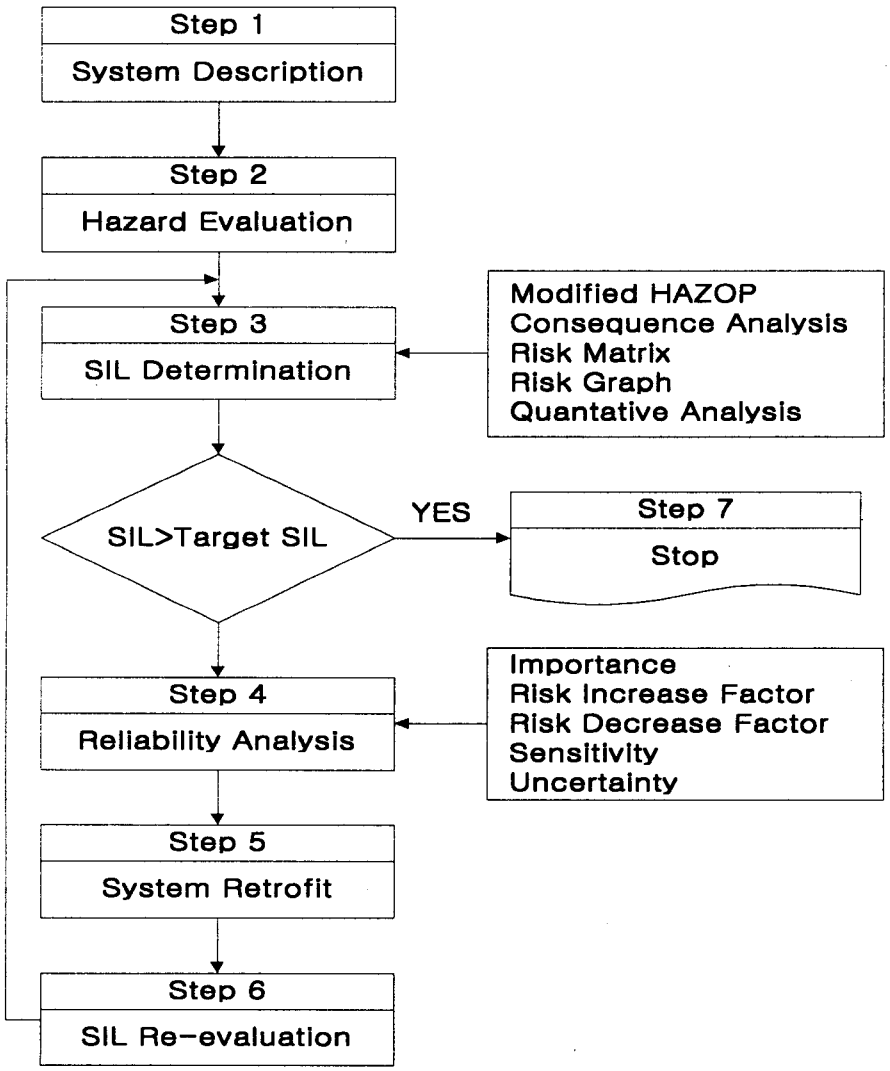

Fig. 2. Procedure of the SIS evaluation method based on reliability analysis.

결과에 대한 불확실성을 평가하기 위해 수행되어진다. [4]

신뢰도 분석을 수행하여 새로운 SIS 장치의 설치 또는 고장률이 낮은 SIS 장치로의 교체를 평가한다. 신뢰도 분석에서 각각의 장치가 가지는 중요도를 기본으로 하여 위험성 감소요소(Risk Decrease Factor)와 위험성 증가요소(Risk Increase Factor) 분석한다.

위험성증가 요소는 Risk Achievement Worth로도 알려져 있으며, 위험성 증가요소는 중요도를 측정하고자 하는 사건이나 계통이 이용불능사태라고 가정할 때의 위험성 증가효과를 나타내는 중요도로서 현재의 위험성에 대한 증가된 위험성과의 비율로서 다음과 같이 표현할 수 있다.

$$RIF = \frac{Q_{TOP}(Q_i = 1)}{Q_{TOP}} \qquad (2)$$

여기서,

Q_{TOP} : 정상사상이 발생할 확률

$Q_{TOP}(Q_i=1)$: 설비 i가 확실한 고장을 일으킬 때의 정상사상 발생확률

어떤 사건이나 계통에 대하여 위험성 증가요소가 크게 나타나면 그 사건이나 계통이 이용불능상태에 대한 설비의 위험도가 크게 증가하는 것을 뜻한다. 따라서 위험성 증가요소로 나타낸 중요도 순위는 신뢰도 보증 프로그램, 시험 및 보수 등의 우선 순위 결정에 사용된다.

위험성감소 요소는 Risk Reduction Worth로도 알려져 있으며, 위험성 감소요소는 중요도를 측정하고자 하는 사건이나 계통이 완전히 이용 가능 상태라고 가정할 때의 위험성 감소효과를 나타내는 중요도로서 감소된 위험성에 대한 현재의 위험성과의 비율 혹은 차이로서 다음과 같이 나타낸다.

$$RDF = \frac{Q_{TOP}}{Q_{TOP}(Q_i = 0)} \qquad (3)$$

여기서,

Q_{TOP} : 정상사상이 발생할 확률

$Q_{TOP}(Q_i=0)$: 설비 i가 확실한 신뢰도를 가질 때의 정상사상 발생확률

어떤 사건이나 계통에 대하여 위험도 감소가치가 크게 나타나면 그 사건이나 계통이 완전한 이용 가능시 설비의 위험도가 크게 감소하는 것을 뜻하고 있으므로 위험성 감소가치로 나타낸 중요도 순위는 설계개선 부분의 우선순위 결정에 사용한다.

각 사건이나 계통에 대한 중요도분석, 위험성 증가요소와 위험성 감소요소 분석결과로부터 시스템이나 설비에 대한 위험성에 대하여 다음과 같은 설비, 시스템의 개선방법 및 유지 · 보수 방법 등을 제시 할 수 있다.

- 위험성 감소요소가 큰 부분에 대하여 우선적으로 설계 개선을 하는 것이 효과적이다.
- 위험성 증가요소가 큰 부분에 대하여는 절차서 개선, 정기검사, 보수, 및 운전요원 훈련 등을 강화하여야 한다.
- 위험성 감소요소와 위험성 증가요소가 모두 낮은 부분에 대하여는 별도의 특별한 조치가 필요 없고 현재의 설계상태 및 유지 · 보수 상태를 유지한다[5].

Ⅳ. 사례연구

본 연구에서 제시한 신뢰도 분석에 근거한 SIL 평가 방법을 검증하기 위해서 간단한 동력전달 시스템을 예제로 사용하였다. 이 예제 시스템은 구성요소가 5개이며 간단한 결함수 목을 가지고 있다.

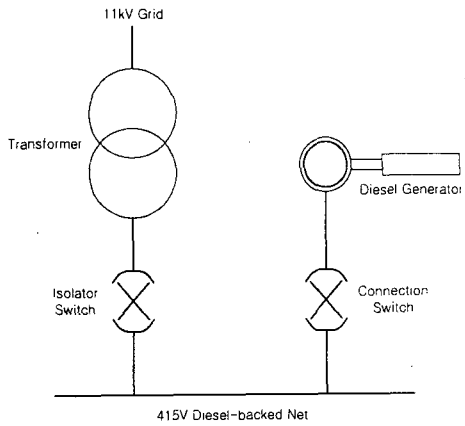

Fig. 3. Diagram of 415V Diesel BUS.

단계 1 : System Description

Fig. 3은 415V Diesel BUS에 동력을 전달하는 과정을 간단하게 표현한 그림이다. 415V BUS는 isolator switch와 변압기를 통하여 외

부 power grid에 연결되어져 있다. 415V BUS는 외부 power grid가 고장이 발생하였을 경우 diesel generator에 의해 동력이 공급되어지도록 설계되었다. diesel generator에서 415V bus로 동력을 전달하기 위해서는 connection switch가 필요하다. 또한 isolator switch는 diesel generator로부터 동력이 공급되는 동안에 외부 power grid로부터 415V bus를 차단하는 역할을 한다.

단계 2 : Hazard Evaluation

위에서 제시한 시스템에 대하여 415V BUS에 동력이 전달하지 않는 경우를 정상사상으로 설정하여 정량적 위험성 분석을 수행하였다. Fig. 4는 415V BUS 시스템의 결함수목(fault tree)이다. 정상사상으로는 415V BUS에 동력이 전달되지 않는 경우로 설정하였다. 기본사상으로는 외부 power grid의 고장(EXT GRID REPAIR), 접촉불량으로 인한 절연스위치의 고장(ISO-A), 부주의로 인한 스위치의 접촉불량(ISO-D), diesel generator의 고장(DIESEL) 그리고 스위치 접촉실패(CON-A) 다섯 가지로 분석되었다.

단계 3 : SIL Determination

분석된 결과를 평가하여 시스템이 가지고 있는 이용가능상태 또는 이용불능상태를 평가하여 SIL 등급을 설정하였다. Table 3은 415V BUS에 대한 최소 단절군 분석을 수행한 결과이다. Table 3에서 diesel generator이 시스템에 가장 중대한 영향을 주는 기본사상으로 분석되었다. 정상사상의 확률 값은 5.91×10^{-3}으로 계산되었다. 그러므로 415V BUS의 이용가능상태는 99.40%로써 이는 SIL 등급 2등급이라는 것을 Fig. 1에서 알 수 있다.

Table 3. Minimum cut sets.

No	Probability	%	Event 1	Event 2
1	2.45E-01	41.43	DIESEL	ISO-D
2	1.86E-02	31.36	DIESEL	EXT GRID REPAIR
3	7.46E-03	12.63	CON-A	ISO-D
4	5.67E-02	9.59	CON-A	EXT GRID REPAIR
5	5.67E-02	9.59	EXT GRID REPAIR	ISO-A

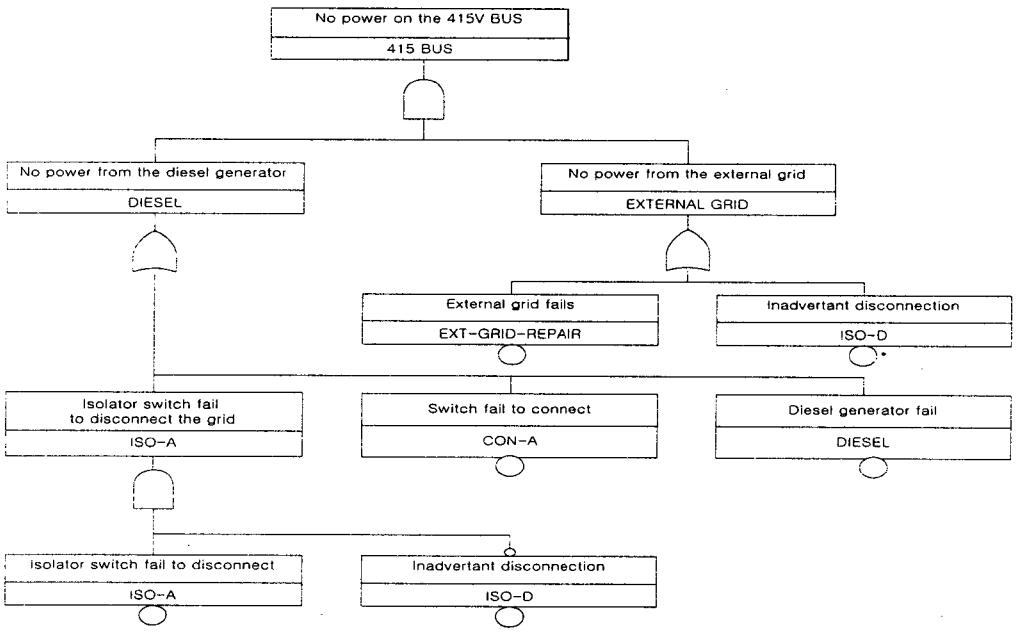

Fig. 4. Fault tree of 415V BUS.

단계 4 : Reliability Analysis

신뢰도 분석을 수행하여 위험성 증가 요소 또는 위험성 감소 요소를 평가하여 시스템을 구성하고 있는 장치나 설비를 대상으로 하여 새로운 안전 장치나 방호 장비의 설치 또는 구성 요소에 대해 고장률이 좋은 장치로의 교체를 통하여 시스템이 가지고 있는 이용가능 상태를 평가하여 기존의 SIL 등급과 변화를 비교하였다.

Table 4는 신뢰도 분석을 수행한 결과를 제시하였다. Table 4에서 시스템에 가장 중요한 영향을 주는 기본사상(basic event)으로는 diesel generator로 분석되었다.

Table 4. Importances for basic event.

No	Basic Event	Nom. Val.	FV	RDF	RIF
1	DIESEL	2.04E-01	7.28E-01	3.15	3.65
2	ISO-D	1.20E-02	5.15E-01	43.3	2.06
3	EXT GRID REPAIR	9.11E-03	4.87E-01	51.1	1.94
4	CON-A	6.22E-02	2.22E-01	3.65	1.21
5	ISO-A	6.22E-02	9.59E-02	2.44	1.11

단계 5 : System Retrofit

RIF와 RDF를 분석하여보면 DIESEL의 경우 RIF가 3.65, RDF가 3.15로서 기존의 diesel generator를 신뢰도가 높은 generator로 교체하는 경우 정상사상의 이용가능상태가 증가한다는 것을 유추할 수 있다.

Table 5는 generator를 고장률이 좋은 것으로 교체한 후에 결함수목 분석을 수행한 결과이다. generator 교체 후 generator가 시스템에 주는 영향은 아주 적은 것으로 분석되었다. generator 교체 후 415V BUS의 이용가능 상태는 99.81% (failure probability = 1.88×10^{-3})로 상승되었지만 SIL 등급에는 변화가 없다. 교체 후 시스템에 가장 중요한 영향을 주는 기본사상으로는 CON-A로 분석되었다.

단계 6 : SIL Re-evaluation

Table 6은 CON-A의 고장률이 좋은 장치로 교체 후 결함수목 분석을 수행한 결과를 제시하였다. generator와 CON-A를 고장률이 낮은 장치로 교체한 후에 415V BUS에 대한 이용가능 상태는 99.94% (failure probability = 5.72×10^{-4})로 상승되었다. 이는 SIL 등급이 2등급에서 3등급으로 향상되었다.

Table 5. Minimum cut sets using the better generator.

No.	Probability	%	Event 1	Event 2
1	7.46E-02	39.65	CON-A	ISO-D
2	5.67E-03	30.1	CON-A	EXT GRID REPAIR
3	5.67E-02	30.1	EXT GRID REPAIR	ISO-A
4	2.45E-02	0.13	DIESEL	ISO-D
5	1.86E-04	0.1	DIESEL	EXT GRID REPAIR

Table 6. Minimum cut sets using the better generator and CON-A.

No.	Probability	%	Event 1	Event 2
1	5.67E-03	80.7	EXT GRID REPAIR	ISO-A
2	7.46E-02	10.63	CON-A	ISO-D
3	5.67E-03	8.07	CON-A	EXT GRID REPAIR
4	2.45E-02	0.35	DIESEL	ISO-D
5	1.38E-04	0.26	DIESEL	EXT GRID REPAIR

Table 7은 generator 교체 후 신뢰도 분석을 수행한 결과를 제시하였다. Table 7에서 제시된 것처럼 generator는 교체 후 시스템에 중요한 영향을 주지 않는 것으로 분석되었다. 반면에 CON-A가 시스템에 가장 큰 영향을 주는 기본사상으로 분석되었다.

Table 8은 generator와 CON-A 모두를 고장률이 낮은 장치로 교체 후 신뢰도 분석을 수행한 결과이다. Tables 6, 7 그리고 8에서 제시한 중요도 분석결과를 보면 시스템에 중요한 영향을 주는 장치를 교체함으로써 장치가 가지고 있는 중요도를 낮추면서 시스템에 대한 안전성을 향상 시켰다.

단계 7 : Stop the procedure

평가를 종료하고 보고서를 작성한다.

Table 7. Importances for basic event using the better generator.

No.	Basic Event	Nom. Val.	FV	RDF	RIF
1	CON-A	6.22E-02	6.97E-01	11.5	3.30
2	EXT GRID REPAIR	9.11E-03	6.03E-01	64.5	2.51
3	ISO-D	1.20E-02	3.98E-01	33.7	1.66
4	ISO-A	6.22E-02	3.01E-01	5.53	1.42
5	DIESEL	2.04E-04	2.29E-03	11.5	1.00

Table 8. Importances for basic event using the better generator and CON-A.

No.	Basic Event	Nom. Val.	FV	RDF	RIF
1	EXT GRID REPAIR	9.11E-03	8.90E-01	97.3	9.11
2	ISO-A	6.22E-02	8.07E-01	13.2	5.18
3	CON-A	6.22E-03	1.87E-01	30.7	1.23
4	ISO-D	1.20E-02	1.10E-01	10.0	1.12
5	DIESEL	2.04E-04	6.13E-03	30.7	1.01

V. 결 론

본 연구에서는 quantitative assessment 방법인 결함수목 분석법을 이용하여 Safety Integrity Level (SIL)을 평가하고 시스템의 목표한 SIL에 도달하지 못할 경우에 신뢰도 분석과 시스템 retrofit을 통해서 목표한 SIL을 만족시키게 하는 방법을 개발하였다.

신뢰도 분석에 근거한 SIL 평가 방법을 검증하기 위해서 415V BUS에 대해서 위험성 분석을 수행하였으며, 시스템이 가지고 있는 이용가능 상태를 평가하였다. 평가된 이용가능 상태를 기본으로 하여 시스템이 가지고 있는 SIL 등급을 설정하였다. 그리고 시스템의 구성요소에 대하여 신뢰도 분석으로 RDF와 RIF를 평가하여 고장률이 좋은 장치로 교체 또는 다른 안전장치나 방호장비의 설치 등의 Safety Instrument System을 적용하여 시스템의 이용가능 상태와 SIL 등급을 증가시키는 방법을 보여주었다. 415V BUS가 가지고 있는 초기의 이용가능 상태는 99.40%에서 99.94%로 SIL 등급 2등급에서 3등급으로 상승하였다.

본 연구에서 제시한 신뢰도에 근거한 SIL 평가 방법을 적용하면 사고 예방과 손실감소로 일어나는 유지보수 비용의 절감 등을 가져오면 물론 시스템의 신뢰도를 극대화 할 수 있다.

감사의 글

본 연구는 한국과학재단(과제번호 R01- 2001-00409)의 지원으로 수행되었으며, 연구비 지원에 감사드립니다.

참 고 문 헌

[1] Paul Gruhn, P.E., ISA S84--Use and What's Next, 1st Annual Symposium of the Mary Kay O'Connor Process Safety, 1998.

[2] William M. Goble, *Control Systems Safety Evaluation and Reliability*, ISA-The Instrumentation, Systems, and Automation Society, 1998.

[3] Angela E. Summers, Techniques for assigning a target safety integrity level, *ISA Transactions*, 37, 95-104, 1998.

[4] Relcon AB, *Risk Spectrum User's Guide*, 1998.

[5] 진상화, *가스시설에 대한 위험성 평가 및 신뢰도 분석*, 석사학위논문, 건국대학교, 2002.