신뢰성응용연구 신뢰성기술
제10권, 제2호. pp.107-122, 2010

플로우차트 기반 안전무결성수준 평가 절차

김기영*·고병각**·장중순*·천성일***

아주대학교 산업공학과*·한국산업기술시험원**·전자부품연구원***

Assessment Procedure of Safety Integrity Level(SIL) Based on Flowchart

Gi-young Kim*·Byeong-gak Ko**·Joong Soon Jang*·Sung-il Chan***

Department of Industrial Engineering, Ajou University*, Korea Testing Laboratory**,
Korea Electronics Technology Institute***

Abstract

Functional safety is the part of the overall safety of a system that depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures, systematic failures, and environmental changes. One of the essential concepts of functional safety is Safety Integrity Level(SIL). It is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In this paper, each element of SIL assessment will be defined. Based on each element, specific process of SIL selection will be established by using flowchart. The flowchart provides a SIL assessment guideline for functional safety engineers. The proposed theory will be verified by applying to a oil refining plant for SIL assessment.

Keywords : Flow Chart(플로우차트), Functional Safety(기능안전성), IEC 61508, Mode of Operation(작동모드), Safety Integrity Level(안전무결성수준)

논문접수일 : 2009년 01월 04일 논문수정일 : 2010년 01월 18일 게재확정일 : 2010년 02월 26일

1. 서론

IEC 61508 전기, 전자, 프로그램 가능한 전자 장치 안전관련 시스템(Electrical/ Electronic/ Programmable Electronic Safety-Related Systems, 이하 E/E/PES) 표준에서 제시되는 기능안전성이란 센서, 논리연산자, 액추에이터로 구성된 전기, 전자, 프로그램 가능한 전자 장치를 이용하여 안전관련 시스템을 작동시키는 안전기능을 의미한다 IEC TR 61508-0(1998). 기능안전성에서 안전기능을 구성하는 요소는 기능성(functionality)과 안전무결성(safety integrity)이다. 위험원을 경감시키거나 방지하기 위하여 어떠한 종류의 안전기능을 구현할 것인지 결정하는 것은 기능성과 관련된 부분이다. 반면 안전기능에 대한 성능 정도는 안전무결성과 관련된 부분이다. 이러한 안전무결성의 성능 정도를 나타내기 위하여 사용하는 척도가 안전무결성수준(Safety Integrity Level, 이하 SIL)이다.

IEC 61508 에서 안전기능은 두 가지 작동모드로 분류하고, 안전성능을 4 수준의 SIL 로 나타낸다. SIL1 은 안전무결성이 가장 낮은 상태이고, 반면 SIL4 는 안전무결성이 가장 높은 상태이다. SIL 이 큰 값을 가질수록 위험원이 고장으로 발현될 가능성이 점점 더 작아야 하므로, 표준에 명시되는 요구사항들은 SIL 이 높을수록 더욱 엄격해지고 관련 항목이 증가한다.

SIL 을 도출하는 것은 제품 또는 시스템의 기능안전성을 평가 및 구현하기 위한 시작 단계이자 필수적인 것이므로 다양한 연구가 실시되었다. Beckman 은 ISA S84 표준을 바탕으로 하여 SIL 을 도출하는 절차에 대한 연구를 실시하였다. 위험 사건의 심각성과 빈도를 바탕으로 전체 Safety Instrumented System(이하 SIS) 을 구성하는 서브시스템인 센서, 논리연산자, 최종 요소에 대한 개별적인 SIL 평가를 실시하고, 이를 바탕으로 최종적으로 전체 SIS 에 대한 SIL 을 도출하는 절차를 명시하였다. 하지만 정량적인 값을 도출할 수 없을 때, 정성적인 방법을 이용하여 SIL 을 도출하는 방법에 대한 절차를 명시하지 않았다. 또한 제시한 절차가 상세하지 못하고 추상적이므로, 실제 적용하기 어려운 문제점을 보유하고 있다 Beckman(1998).

Heel et al. 은 IEC 61508에서 제시하는 전체 안전수명주기를 다양한 기호를 이용하여 플로우차트로 도시하였다. 안전수명주기에서 기능안전성 개념 설정 단계부터 폐기 및 해체 단계까지, 필요한 정보의 흐름과 각 단계에서 안전관련 목표를 달성하기 위한 활동과 문서화의 필요성을 나타내었다. 하지만 해당 연구는 단계별 활동 목적과 결과물만을 명시하고, 각 단계에서 세부적인 절차를 제시하지 않은 문제점이 존재한다. 또한 표준에서 제시된 안전수명주기를 플로우차트로 간단하게 바꾼 것에 불과하며, SIL 평가 등 기능안전성 검증을 위한 세부적인 적용 시 문제점이 존재한다 Heel et al(1999).

Beugin et al. 은 IEC 61508 에서 제시하는 SIL 에 대한 개념이 다양하게 해석되고 적용되므로, SIL 개념은 이해하기 어렵고 모호하다는 문제점을 지적하였다. SIL 에 대하여 저 요구 작동모드와 고 요구 작동모드 또는 연속적인 작동모드를 고려하여 정량적으로 SIL 을 도출할 수 있는 파라미터에 대하여 명시하였고, 정성적인 경우에 SIL 을 도출할 수 있는 방법에 대한 내용을 명시하였다. 이를 바탕으로 교통관련 시스템에 대하여 결함 나무 분석을 이용하여 정량적인 SIL 평가를 실시하였다. 하지만 SIL 을 평가하는 세부적인 절차를 명확하게 나타

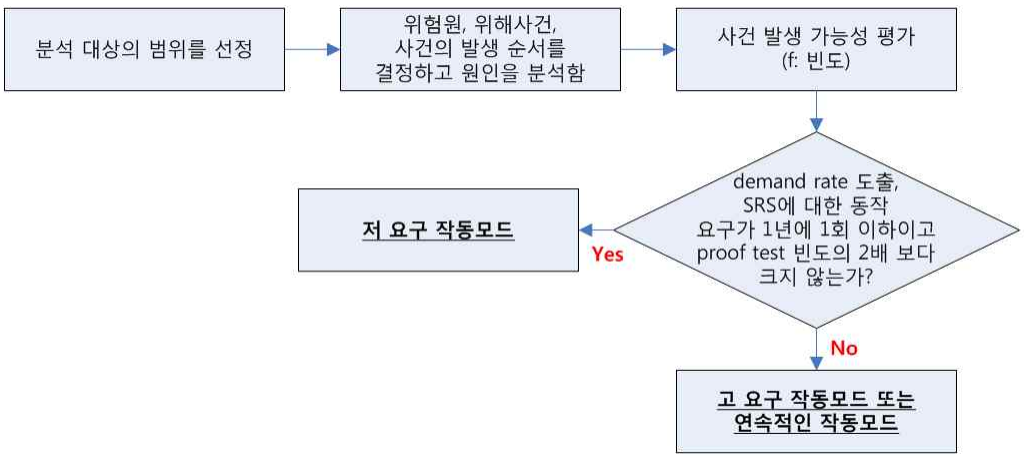
내지 않은 문제점을 보유하고 있다 Beugin et al(2007).
Cruz-campa et al. 은 Hazard and Operability(이하 HAZOP) 을 바탕으로 SIL 을 평가하는 절차를 명시하였다. 위험사건에 대한 결과를 5 수준, 위험사건 발생 빈도를 11 수준으로 분류하여 정량적인 SIL 을 도출하기 위한 가이드를 제시하였다. 설계 단계부터 구현 및 검증 단계까지 고려하여 SIS 에 대한 SIL 을 도출할 수 있는 절차를 5 단계로 제시하였다. 또한, 이미 설치된 SIS 를 special case 로 분류하고, 이에 대한 차별화된 SIL 평가 실시 절차를 5 단계로 제시하였다. 하지만 정성적인 SIL 평가를 위한 절차를 명시하지 않은 단점이 존재하고, SIL 을 도출하기 위한 세부적인 절차가 제시되지 않는 문제점이 있다 Cruz-campa et al(2010).
본 연구에서는 위에서 제시된 문제점을 해결하고 안전 시스템의 신뢰성과 가용성을 높이기 위하여, 기능안전성 설계 및 구현의 바탕이 되는 SIL 을 평가하는 상세한 절차를 제시한다. IEC 61508 표준을 바탕으로 SIL 을 평가하는 요소를 정의하고, 이에 대한 세부적인 절차를 플로우차트를 이용하여 명시하여 요구되는 SIL 도출에 대하여 가이드를 제공한다. 더불어 제시된 절차를 실제 사례에 적용하여 이론의 타당성을 검증한다.

2. 안전무결성수준 평가절차

2.1 위험원 분석과 작동모드

안전관련 시스템의 안전기능에 대한 SIL 을 도출하기 위해서는 먼저 분석하고자 하는 대상에 대한 범위를 선정하여야 하며, 이는 위험원 분석을 실시하기 위한 예비단계 활동이다. 범위를 정의하는 목적은 EUC와 EUC 제어시스템의 경계를 결정하고, 위험원 및 리스크 분석의 적용범위를 명시하는 것이다. 범위를 정의하기 위하여 고려하여야 하는 사항은 위험원과 관련된 물리적인 장비, 외부적인 요인, 관련 세부시스템에 대한 사항, 사고 유발 유형 등이 있다.
대상의 범위가 정의되면 위험원에 대한 분석을 실시한다. 위험원 분석은 SIL 을 도출하기 위하여 매우 중요한 활동이므로 정확한 평가/분석이 필수적이다. 또한 평가된 내용에 대한 명확한 근거가 제시되어야 하고, 관련 근거들이 타당성을 보유해야 한다. 분석 결과 및 근거는 주로 문서 또는 데이터베이스에 저장된다 지식경제부 기술표준원(2006). 위험원 분석을 실시하는 대표적인 기법은 Preliminary Hazards Analysis(이하 PHA), HAZOP, Failure Mode and Effect Analysis(이하 FMEA), What if 등이 있다. 올바른 위험원 분석을 위하여 현재 주어진 정보, 기법들의 장단점, 결과물 등을 고려하여 적절한 위험원 분석방법을 선택하여 실시한다 Hyatt(2009).
위험원 분석은 도출하고자 하는 결과에 따라 실시하는 활동의 범위가 매우 다양하다. 단순히 위험원을 식별하는 활동으로 정의할 수 있지만, 위험원을 식별하고 사건발생 순서를 도출하여 그에 대한 정량적/정성적인 평가를 바탕으로 대책을 강구하는 모든 활동을 포함하는 것으로

정의할 수 있다. 본 연구에서 실시하고자 하는 위험원 분석은 대상에 대한 위험원 및 위험 사건을 고려하여 이를 예방 및 경감시키기 위한 1 차적인 대책을 도출하는 활동을 포함한다. 더불어 위험원 분석으로 식별된 위험 사건들이 어느 정도의 빈도로 발생하고 있는지에 대한 평가를 포함한다. 이러한 분석을 실시하기 위하여 대상 부품의 고장률, 구축된 데이터베이스, 예측 기법 등의 정보를 이용한다.



<그림 1> 작동모드 도출 절차

IEC 61508 표준에 근거하여, 위험 사건의 발생 빈도 도출 가능여부와 빈도의 정량적인 값을 바탕으로 2 가지 작동모드로 분류할 수 있다. 위험원 분석 과정에서 작동모드를 결정하기 위하여 demand rate, 동작요구 빈도, 증명시험 빈도를 고려하여야 하며 구체적인 내용은 다음과 같다.

- 주어진 데이터를 바탕으로 demand rate 의 도출이 가능한가?
- 안전관련 시스템에 대한 동작요구가 1 년에 1 회 이하인가?
- 안전관련 시스템에 대한 동작요구가 증명시험 빈도 2 배 보다 크지 않은가?

위의 3 가지 항목을 모두 만족하면, 저 요구 작동모드와 관련된 기능을 수행하는 제품 또는 시스템으로 분류할 수 있다. 하지만 위의 항목 중 단 하나라도 만족시키지 못한다면 고 요구 작동모드 또는 연속적인 작동모드로 운영되는 것으로 분류하여야 하며 세부적인 절차는 <그림 1> 과 같이 나타낸다.
저 요구 작동모드에 해당되는 제품으로는 장치산업에 사용되는 안전밸브를 대표적인 예로 들 수 있다 [14]. 평소에는 작동하지 않지만 압력이 급격히 증가하는 이상 상태가 발생하게 되면 밸브를 개폐하여 위험 사건이 발생하는 것을 방지할 수 있는 기능을 실시하는 것이다. 고 요구 작동모드 또는 연속적인 작동모드는 지속적인 작동과 제어를 요구하는 시스템이나 장치에 사용되는 것이다. 그 예로는 프로그램 가능한 전자 장치를 이용하는 차량의 전기적 제동장치, 열차의 속도에 대한 연속적인 제어장치가 있다 Smith and Simpson(2004). 위의

두 값은 차원이 다른 값이지만 IEC 61508 에서는 동일한 SIL 이라는 척도를 사용하여 표현하고, 정량적인 값의 범위는 아래의 <표 1> 과 같다 IEC 61508(1998a).

<표 1> 작동모드와 안전무결성수준(SIL)

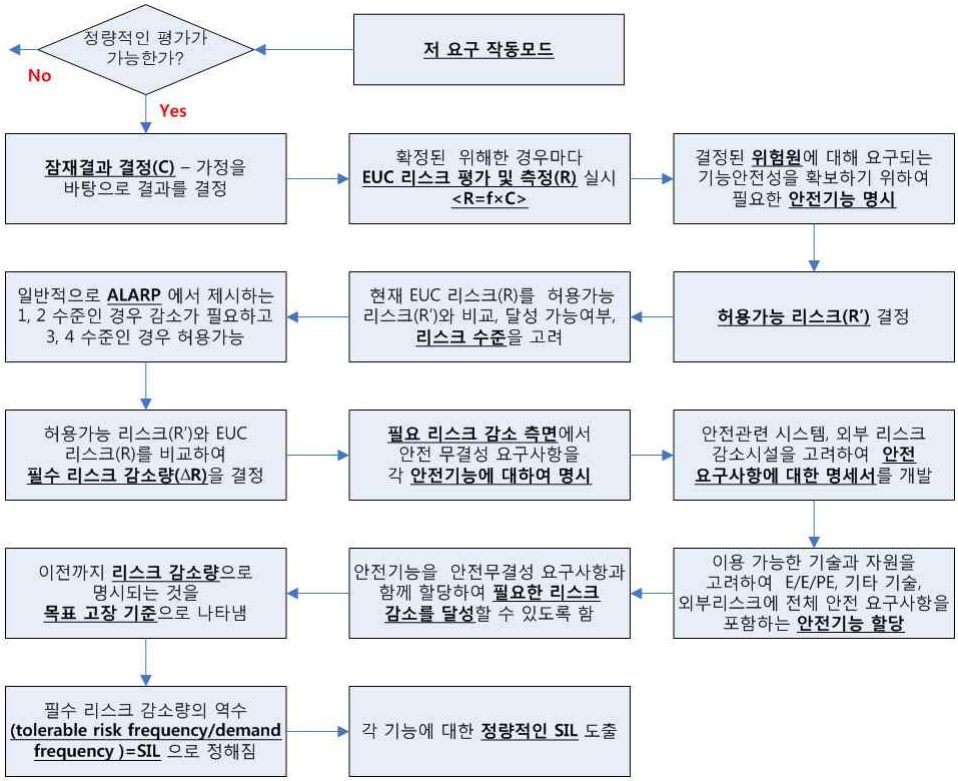
안전무결성수준 (SIL)	고 요구 작동모드 또는 연속적인 작동모드	저 요구 작동모드
4	$\geq 10^{-9}, < 10^{-8}$	$\geq 10^{-5}, < 10^{-4}$
3	$\geq 10^{-8}, < 10^{-7}$	$\geq 10^{-4}, < 10^{-3}$
2	$\geq 10^{-7}, < 10^{-6}$	$\geq 10^{-3}, < 10^{-2}$
1	$\geq 10^{-6}, < 10^{-5}$	$\geq 10^{-2}, < 10^{-1}$

2.2 정량적인 분석 방법

작동모드가 저 요구 작동모드로 결정된다면 SIL을 도출하기 위한 절차는 <그림 2> 와 같고, 관련 파리미터는 작동요구 시 평균 고장확률(Average Probability of Failure on Demand, 이하 PFD)이 사용된다 IEC 61508(1998a). 저 요구 작동모드의 경우, SIL 도출을 위한 정량적인 평가 가능 여부에 대한 확인이 먼저 필요하다. 정량적인 평가가 가능한 경우에는 다양한 정량적인 데이터를 기반으로 SIL 을 도출할 수 있지만, 정량적인 평가가 불가능한 경우에는 리스크 그래프나 심각도 매트릭스와 같은 정성적인 방법을 사용하여 SIL 평가를 실시한다 IEC 61508(1998c). 정량적인 평가가 가능한 경우에는, 안전관련 시스템과 외부 리스크 감소 시설이 존재하지 않았을 때 위해사건의 발생 상황을 가정하여 그 결과의 영향으로 인한 잠재 결과를 결정한다. 이러한 결과는 인명, 재산, 시간 등을 고려하여 정량적으로 표현되어야 한다.

결과와 빈도가 확정된 위해한 경우에 대하여 EUC 리스크 평가 및 측정을 실시한다. 여기에서 리스크는 위험사건의 발생확률인 빈도와 가정된 상황 하에서 도출된 정량적인 잠재 결과의 곱으로 표현된다. 리스크는 이러한 기본적인 개념을 바탕으로 도출되는 것이므로 앞에서 실시한 위험원 분석에 의해 이미 잠정적으로 도출되었다고 할 수 있다. IEC 61508 에서 리스크는 SIL 을 도출하기 위한 출발점에서 제시되는 기본적인 개념으로 정량적인 값을 가지며, 정성적인 개념을 나타내는 위험원과 명확히 구별되는 개념이다.

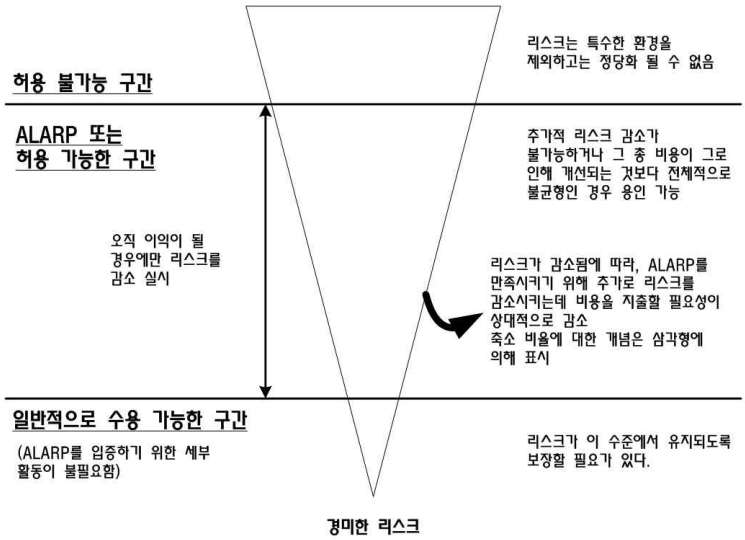
다음 절차로 다양한 분야를 고려하여 허용 가능한 리스크(R′)를 결정하여야 한다. 해당 항목으로는 안전규제 권한에 의한 지침, 관련 당사자들의 논의/합의, 산업분야의 표준과 지침, 국제적 논의/합의, 독립적/현실적/전문적/과학적 자문, 법적 요구사항, 고객의 안전 및 환경 기준, 금전적인 측면 등이 있다. 구체적인 예를 들면 손상의 심각성, 위험에 노출되는 사람의 수, 노출 빈도, 노출의 지속성 등의 정량적인 요소들이 있다. 자동차 산업분야의 경우, 차량을 구성하는 전장부품에 대하여 고 요구 작동모드 또는 연속적인 작동모드 SIL3 를 권장한다. 이러한 경우는 다양한 요인을 고려하지 않아도 해당 산업 분야에서 관행을 따르는 경우라 할 수 있다 Smith and Simpson(2004).



<그림 2> 저 요구 작동모드 SIL 도출 절차

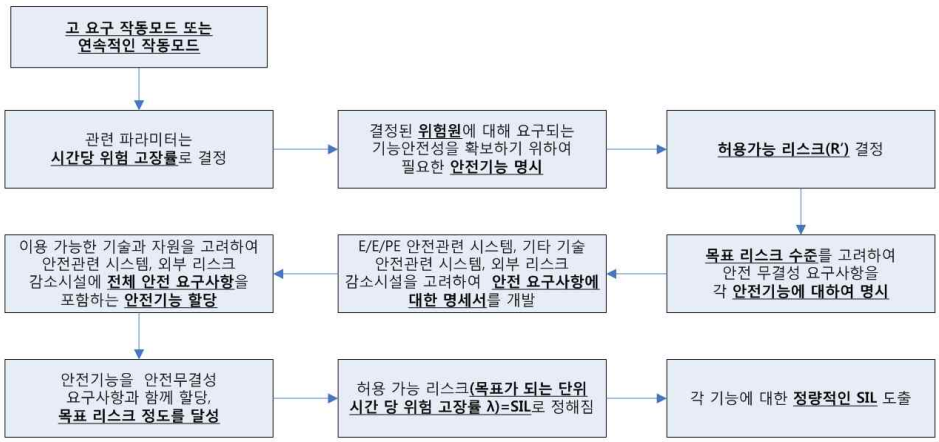
앞 단계에서, 가정된 사건의 정량적인 결과와 빈도를 바탕으로 평가된 현재 EUC 리스크(R)와 목표로 설정된 허용 가능한 리스크(R′)에 대하여 비교를 실시한다. 목표로 설정된 허용 가능 리스크의 달성 가능여부를 고려하여 감소시켜야 할 리스크의 수준을 도출한다. 리스크 감소를 위하여 ALARP 이 IEC 61508 에서 제시되며, 이는 As Low As Reasonably Practicable 의 약자로 현실적으로 달성 가능한 리스크 감소 수준과 관련된 내용을 담고 있다. <그림 3> 은 ALARP 에 대한 개념을 나타내며, 리스크와 관련된 구간은 크게 3 가지로 구분할 수 있다. 가장 위 부분이 허용 불가능한 수준의 리스크를 보유하는 구간, 중간 부분이 ALARP 또는 허용 가능 구간, 제일 아래 부분이 일반적으로 수용 가능한 구간을 나타내는 것이다 IEC 61508(1998c).

위에서 설명한 리스크 감소를 기본으로 허용 가능 리스크(R′)와 현재 EUC 리스크(R)를 고려하여 필수 리스크 감소량 ΔR= R-R′ 을 결정한다. 결정된 필수 리스크 감소량을 바탕으로 하여 안전무결성 요구사항을 각 안전기능에 대하여 명시한다. 이 때 주의사항은 E/E/PES, 기타 기술 안전관련 시스템, 외부 리스크 감소시설을 고려하여 안전 요구사항에 대한 명세서를 개발하여야 한다는 것이다. 다음 단계로 이용 가능한 기술과 자원을 고려하여 E/E/PES, 기타 기술 안전관련 시스템, 외부 리스크 감소시설에 전체 안전 요구사항을 포함하는 안전기능을 할당한다. 안전기능 할당 시, 안전무결성 요구사항과 함께 할당하여 필요한 리스크 감소를 달성할 수 있도록 한다.



<그림 3> ALARP 과 리스크 감소

이전 단계까지 리스크 감소량으로만 명시되었던 정량적인 값을 목표 고장 기준인 SIL 로 표현한다. 저 요구 작동모드에서 어떠한 사건이 발생할 확률은 요구의 빈도와 요구 시 기능 고장 발생 확률의 조합으로 표현된다. 이러한 경우 SIL 을 선택하기 위하여 PFD 또는 PFD 와 역수 관계를 가지는 리스크 감소 인자(Risk Reduction Factor, 이하 RRF)를 척도로 사용한다 Beugin et al(2007). 다시 말하면, PFD 또는 1/RRF 의 정량적인 수치를 바탕으로 해당 값에 대한 SIL 을 도출하는 것이다. 이러한 값들은 차원이 존재하지 않는 확률 값이라는 특징을 지니고 있다.



<그림 4> 고 요구 또는 연속적인 작동모드 SIL 도출 절차

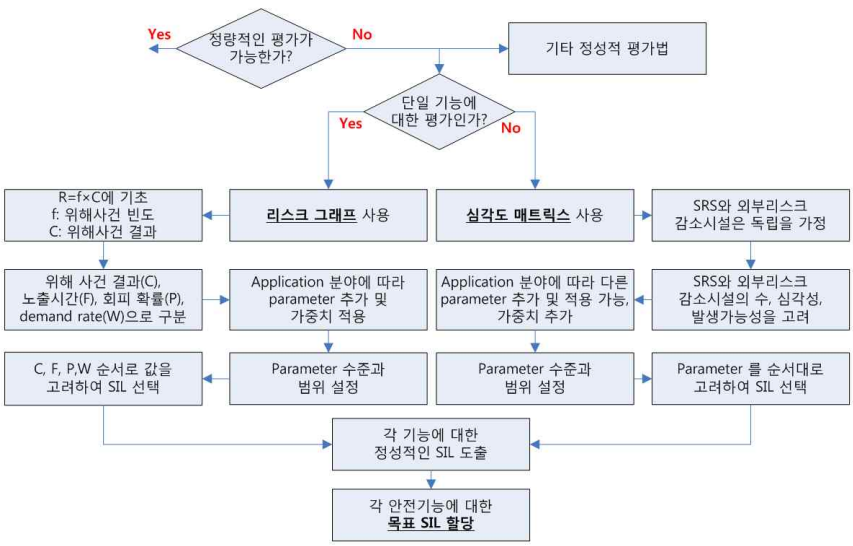
작동모드가 고 요구 작동모드 또는 연속적인 작동모드로 결정된다면 SIL 을 도출하기 위한 기본 파라미터는 시간 당 위험고장 확률(Probability of a Dangerous Failure per Hour,

이하 PFH)로 결정된다 IEC 61508(1998a). 먼저 식별된 위험원에 대한 기능안전성을 확보하기 위하여 요구되는 안전기능을 결정한다. 다음으로 허용 가능한 리스크(R′)를 결정한다. 허용 가능한 리스크는 다양한 분야를 고려하여 도출하여야 하며 그 방법은 저 요구 작동모드의 경우와 상이하지 않으므로 세부적인 내용은 생략한다.

고 요구 작동모드 또는 연속적인 작동모드는 저 요구 작동모드와는 상이하게, SIL 을 도출하기 위하여 현재의 리스크 정도를 평가하는 절차가 존재하지 않는다. 고 요구 작동모드 또는 연속적인 작동모드의 경우에는 demand rate 를 추정할 수 없기 때문에 현재의 리스크 정도를 도출할 수 없다. 그러므로 평가된 현재의 리스크를 목표로 설정된 허용 가능 리스크 수준과 비교 후, 필수 리스크 감소량을 도출하는 활동도 포함되지 않는다. 단지 허용 가능한 리스크(R′) 만을 도출하여 이에 상응하는 SIL 을 달성하고자 하는 것이다.

이 후, SIL 도출 단계 역시 저 요구 작동모드의 경우와 매우 유사하거나 동일하므로 생략한다. 허용 가능 리스크 정도를 고려하여 안전무결성 요구사항을 각 안전기능에 대하여 명시하고 E/E/PES, 기타 기술 안전관련 시스템, 외부 리스크 감소시설을 고려하여 안전 요구사항에 대한 명세서를 개발한다. 다음으로 이용 가능한 기술과 자원을 고려하여 E/E/PES, 기타 기술 안전관련 시스템, 외부 리스크 감소시설에 전체 안전 요구사항을 포함하는 안전기능을 할당한다. 안전기능 할당 시, 안전기능을 안전무결성 요구사항과 함께 할당하여 목표 고장 기준을 달성할 수 있도록 한다.

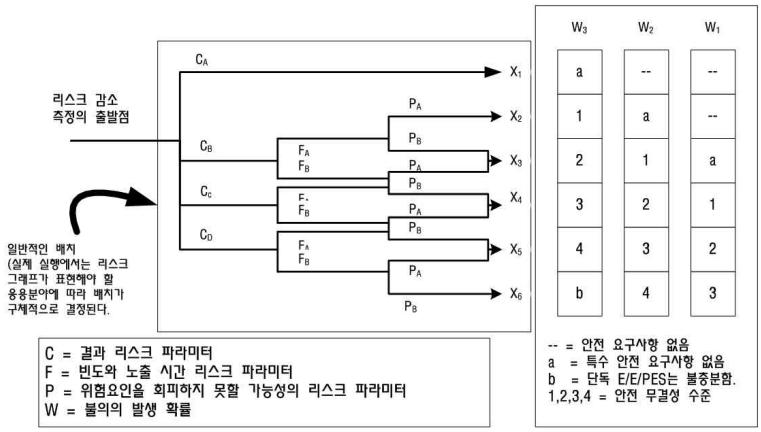
이전 단계까지는 허용 가능 리스크로만 명시되는 정량적인 값을 목표 고장 기준인 SIL 로 표현한다. 고 요구 작동모드 또는 연속적인 작동모드에서 사건이 발생할 확률은 고장률 λ 를 바탕으로 도출하며 대안적인 척도로는 기능에 대한 평균 고장 시간(Mean Time to Failure, 이하 MTTF)이 있다. 만약 고장이 발생하는 형태가 지수분포를 따른다고 가정하면 MTTF 와 λ 는 역수 관계를 가진다. 고 요구 작동모드 또는 연속적인 작동모드는 허용 가능 리스크와 단위시간에 대한 고장률 λ/t 값을 고려하여 도출된 정량적인 값인 PFH 을 바탕으로 SIL 을 결정한다.



<그림 5> 정성적인 SIL 도출 절차

2.3 정성적인 분석 방법

저 요구 작동모드에서, 정량적인 SIL 평가가 불가능한 경우에는 정성적인 SIL 평가를 실시한다. 정성적인 평가 방법으로는 리스크 그래프, 심각도 매트릭스가 존재하고, 반-정성적인 방법으로는 safety layer matrix, calibrated risk graph, 장치 산업에서 많이 사용되는 LOPA 등이 있다 Smith and Simpson(2004). IEC 61508 표준에서는 대표적인 정성적인 평가 방법으로 리스크 그래프와 심각도 매트릭스를 제시하므로, 본 연구에서는 두 기법에 대하여 상세히 설명한다. 두 기법의 분석 절차는 <그림 5> 와 같고, 평가 대상이 되는 안전기능의 수를 기준으로 분류할 수 있다. 평가대상이 되는 안전기능이 하나인 경우는 리스크 그래프를 사용할 수 있지만 평가하고자 하는 안전관련 기능이 2 개 이상인 경우는 심각도 매트릭스를 사용하여야 한다 IEC 61508(1998c).

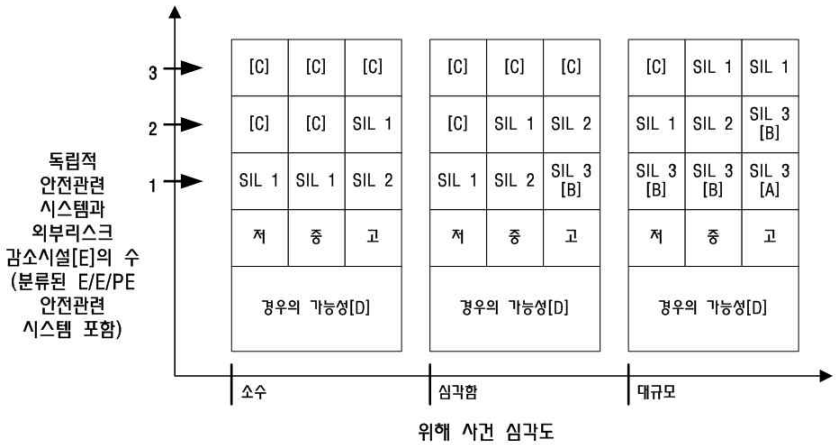


<그림 6> 리스크 그래프

정성적인 평가 방법 중 하나인 리스크 그래프는 정량적인 분석 방법과 동일하게 위험 사건의 발생빈도와 위험 사건의 심각도를 모두 고려하여 리스크에 대한 평가를 실시한다. 위험 사건 발생의 심각도를 고려하기 위하여 결과의 심각성-C, 사건의 노출시간-F 를 파라미터로 사용한다. 또한 위험 사건의 발생빈도를 바탕으로 SIL 을 도출하기 위하여 사건을 회피하지 못할 확률-P, demand rate-W 를 파라미터로 사용한다. <그림 6> 과 같이 제시된 리스크 그래프는 해당 파라미터를 순서대로 선택하며 제품 또는 시스템에 대한 정성적인 평가를 실시하고 SIL 을 도출하게 되면 절차는 종료된다. 정성적인 기법은 정량적인 분석과 달리 위해 사건이 발생하는 경우의 영향과 빈도를 정확하게 수치적으로 표현하지 못하는 단점이 존재하므로 각각의 파라미터를 몇 개의 수준으로 나누고, 이를 바탕으로 분류하여 평가를 실시한다 [14].

또 하나의 정성적 기법인 심각도 매트릭스는 하나의 안전관련 기능이 아닌 다양한 안전관련 기능에 대하여 동시적이며 정성적인 평가를 실시하고자 하는 경우 사용될 수 있다. 심각도 매트릭스를 사용하기 전, 안전관련 시스템과 외부리스크 감소시설은 서로 독립적인 기능을 수행한다는 것이 먼저 가정되어야 한다. 만약, 안전관련 기능들에 대한 안전무결성 요구사항이

서로 다르고, 안전기능들 간의 구현 독립성이 충분하지 않다면, 상대적으로 가장 높은 SIL 에 적용하는 안전관련 요구사항들을 전체 E/E/PES 에 적용하여야 한다.
심각도 매트릭스에서 SIL 을 도출하기 위하여 먼저 독립적인 안전기능의 수를 결정한다. 표준에서 제시하는 심각도 매트릭스는 <그림 7> 과 같고, 최대 3 가지 독립적인 안전기능을 고려하여 평가가 가능한 형태를 지니고 있다. 다음 절차로 위해 사건의 심각도를 결정하고 사건 발생 가능성을 고려하여 SIL 을 결정한다. <그림 7> 은 사건의 심각도와 발생 가능성 모두 3 수준으로 나누어 SIL 을 선택하고자 하는 예이다. 위의 순서를 바탕으로 SIL 을 도출하고 이를 각 안전기능에 대하여 할당하여 SIL 도출 절차를 종료할 수 있다.



<그림 7> 심각도 매트릭스

정성적인 SIL 도출 방법은 각 산업 분야의 특이성을 반영하여 적용하여야 하므로 분야마다 다른 형태를 가진다. 그러므로 리스크 그래프나 심각도 매트릭스를 구성하기 위하여 필요한 파라미터의 수와 수준은 경우에 따라 상이한 형태를 나타낸다. 때문에 이러한 정성적인 기법을 이용한 SIL 평가 시, 가장 중요한 것은 어떠한 파라미터를 선정하고 어느 정도 수준으로 분류할 것인지 결정하는 것이다. 수준을 나눌 때 한 수준을 정의하는 정량적인 값의 범위와 파리미터에 어떠한 방법으로 가중치를 부여할 것인지 결정하는 것 또한 매우 중요한 문제이므로 주의하여야 한다.

3. 사례연구

본 장에서는 위에서 플로우차트를 이용하여 제시된 SIL 평가 절차에 따라 실제 대상 시스템의 안전기능에 대한 SIL 평가를 실시하는 사례를 제시하고자 한다. 사례연구를 실시하고자 하는 대상은 정유를 실시하는 화학 플랜트이다. 본 사례연구에 사용된 세부적인 데이터는 해당 기업의 보안 사항이므로, 관련 내용을 제시하는 것을 생략한다. 해당 화학플랜트에서 SIL

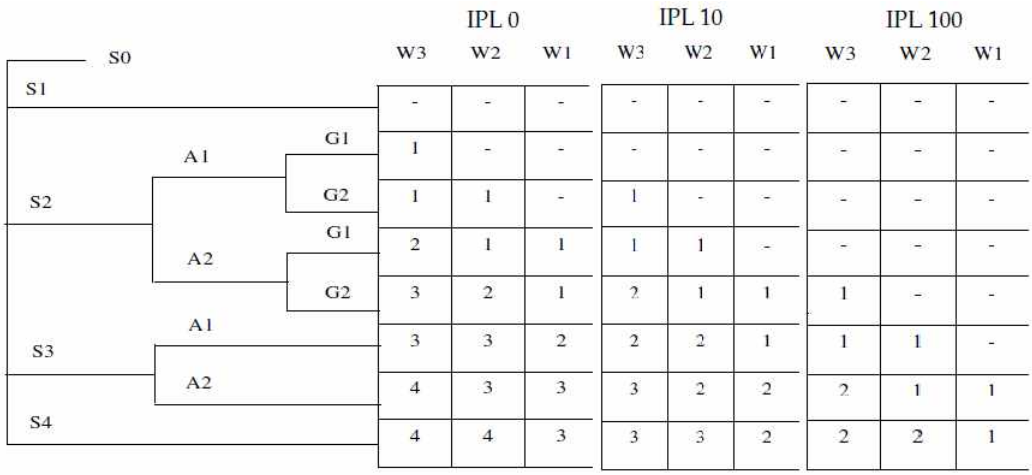
평가의 대상이 되는 안전기능은 정량적인 평가를 위한 데이터가 충분히 존재하지 못하여 리스크 그래프를 이용한 정성적인 평가 방법을 이용하여 실시하고자 한다.

사례연구의 대상이 되는 시스템에 대한 SIL 을 평가하기 위하여, 먼저 안전 기능에 대한 정의를 바탕으로 분석 대상의 범위를 명확히 한다. 분석대상이 되는 시스템은 다양한 기능을 실시하는 시스템이며, 수행하는 기능 중 대표적인 것은 조작기능, 통제기능, 프로세스 제어 기능, 기계관련 보호 기능, 응급장비 절연 기능, 화재 및 가스 시스템 등이 존재한다. 분석 대상의 범위를 선정하는 것은 이러한 다양한 시스템의 기능에 대하여 정의하고, 이 중 안전관련 기능과 비 안전관련 기능을 분류하는 것이다. 이를 바탕으로 분석하고자 하는 기능이 무엇이며 그 범위가 어느 정도인지를 명확히 한다. 다양한 기능 중 기능안전성과 관련된 기능과 그렇지 않은 기능으로 분류하여 분석 대상의 범위를 선정하고, 기능안전성과 관련된 기능에 한정하여 SIL 평가를 실시한다.

<표 2> HAZOP & SIL 워크시트의 예

설계의도	요구 시나리오	요구 시 실패 결과 정도	현재 설치된 안전장치		관련 사항	리스크 그래프 파라미터				
			독립 보호층 (IPLs)	리스크 감소인자 (RRF)		S	A	G	W	SIL
물 배출구를 통한 LPG 방출 방지	요구되는 것보다 A 밸브를 과도하게 개방하는 오작동이 발생	수위가 낮아지고 대기 중 LPG의 누출로 인한 화재/폭발의 위험원이 존재함	없음	0	발생할 것으로 예상되는 화재/폭발은 제한된 지역에 영향을 미칠 것으로 예상됨	S2	A1	G2	IPL0 W1	SIL1

분석대상의 범위가 결정되면 위험원 및 위해사건에 대한 분석을 실시한다. 본 사례에서는 위험원 및 위해사건 분석을 위하여 <표 2> 와 같은 양식의 HAZOP & SIL 워크시트를 사용한다. HAZOP & SIL 워크시트의 앞부분에서 제시되는 항목인 설계의도, 요구 시나리오, 요구 시 실패 결과 정도에 대한 정성적인 분석을 실시한다. 정성적인 척도를 정량적으로 전환하는 절차가 필수적으로 요구되며, 이는 <표 3> 에서 제시되는 기준을 바탕으로 실시한다. 도출된 정량적인 분석 결과를 이용하여, 위험원 및 위해사건의 demand rate 와 잠재 위험원이 발생한 경우에 대한 정량적인 결과 값을 얻는다. 본 사례에서 정량적인 데이터에 대한 분석 결과, 다양한 안전기능을 위한 여러 요소들이 중첩되어 구성되기 때문에, 안전관련 시스템에 대하여 요구되는 빈도정도가 1년에 1회 이하이다. 더불어 증명시험의 빈도의 2배보다 작은 값을 가지기 때문에, 저 요구 작동모드로 해당 안전기능에 대한 작동모드를 결정한다.



<그림 8> 5개 파라미터를 고려한 리스크 그래프

작동모드로 저 요구 작동모드를 결정한 후 대상 시스템에 대하여 정량적인 평가의 가능 여부에 대한 판단이 필요하다. 본 사례는 정량적인 평가를 가능하게 할 만큼의 정확하고 충분한 데이터가 존재하지 않으므로 정성적인 평가를 실시한다. 정성적인 평가를 실시함에 있어 각각의 단일 기능에 대한 평가를 실시하므로 <그림 8> 과 같은 형태를 지니는 리스크 그래프를 이용하는 방법을 선택한다.

<표 3> 리스크 그래프 파라미터

요구빈도(W)	W1 = 낮음 (0.1회 미만/ 1년)
	W2 = 보통 (0.1 이상 1회 미만/ 1년)
	W3 = 높음 (1 이상 10회 미만/ 1년)
요구 시 안전기능이 작동하지 않았을 때 인명 피해의 잠재적인 정도(S)	S0 = 인명 피해 없음
	S1 = 영구적이지 않은 가벼운 부상 정도
	S2 = 1명이 사망, 심각한 부상 정도
	S3 = 여러 사람이 사망하는 정도
	S4 = 대참사의 발생, 많은 희생자 발생
요구 시 위험 지역에서 존재 정도(A)	A1 = 거의 없음 ~ 빈번함
	A2 = 빈번함 ~ 연속적임
위험을 회피할 확률(G)	G1 = 어떠한 조건에서 가능함
	G2 = 대부분 불가능함
독립 보호층 (IPLs)	IPL0 = 존재하지 않음
	IPL10 = 독립 보호 기능층이 존재
	IPL100 = 강한 독립 보호 기능층이 존재

본 사례에서 SIL 을 평가하기 위하여 사용되는 파라미터는 크게 5 가지로 분류하며 <표 3> 과 같다. 각각의 파라미터에 대하여 요구빈도(W)는 3 수준, 요구 시 안전기능이 작동하지 않았을 때 인명 피해의 잠재적인 정도(S)는 5수준, 요구 시 위험 지역에서 존재 정도(A)와 위험을 회피할 확률(G)는 2 수준, 독립 보호층(IPLs)는 3 수준으로 분류한다.

각각의 수준을 선택하는 대략적인 기준은 <표 3> 에서 주어진다. 리스크 그래프를 사용하여 SIL 평가하기 위해 먼저 HAZOP 실시 후 얻어진 위해사건의 정량적인 결과와 위해사건의 빈도 정도를 이용하여 파라미터 W 와 S 의 값을 할당한다.
대상 시스템의 안전기능에 대한 SIL 을 평가하기 위하여 <표 3> 에서 제시하는 기준만을 이용하는 것은 어려움이 존재한다. 그러므로 제시된 <표 3> 보다 세부적이며 개별적인 응용분야 또는 시스템에 따라 세부적인 기준 및 파라미터에 대한 가중치를 부여한 세부적인 분류기준을 사용한다. <표 4> 에서 <표 7> 까지는 대상 시스템의 안전기능에 대하여, 제시되는 5개의 파라미터에 대한 평가를 실시하여 SIL 을 도출하기 위한 세부적인 기준을 나타내는 것이다. 이를 바탕으로 수정된 파라미터 수준과 범위를 이용하여 대상 시스템에 대한 SIL 평가를 실시한다.

<표 4> IPL 에 대한 정량화 규칙

Independent Protection Layer	Risk Reduction Factor
압력 완화 장치	100
SRS - SIL1	10
SRS - SIL2	100
SRS - SIL3	1000
평균적으로 높은 압력하의 운영자의 반응	0
단일 체크 밸브	0
위험한 시나리오에 대하여 설계된 이중 체크 밸브	10
완화가 가능한 초기 사건 발생에 대비한 방벽(환경적인 사건만을 위한 IPL)	100

<표 5> 요구빈도에 대한 정량화 규칙

Scenario	사건발생빈도(회/년)	요구빈도(W)
제어 루프 고장	> 0.1	W2
분석 장치 고장	> 1	W3
펌프 고장 손실(OREDA)	0.79	W3 / W2
용적 식 펌브 트립(OREDA)	1.1	W3
원심 압축기 트립(OREDA)	2.1	W3
단일 기계적 펌프 실 누출	0.1	W2
이중 기계적 펌프 실 누출	0.01	W1
전기적 전원의 손실	0.1	W2
일반 유틸리티 고장	0.1	W2
열 교환 튜브 누출	0.01	W1 or W2

SIL 평가를 실시하기 위하여 사용되는 워크시트는 앞에서 이미 제시된 <표 2> 의 양식을 사용하며, 각 항목에 대한 평가를 바탕으로 “물 배출구를 통한 LPG 방출 방지” 기능에 대한 SIL 평가를 실시한 예를 제시하고 있다. 만약 5개의 파라미터 중 하나의 값이라도 도출할 수 없다면 해당 기능에 대한 SIL 은 도출할 수 없으며, 안전관련 기능이 아닌 기능에 대해서는 SIL 에 대한 값을 부여하지 않는다. 최종적으로 각 기능에 대하여 SIL 을 할당하여 전체 프로세스를 종료한다.

<표 6> 발생 가능성이 있는 사건에 대한 정량화 규칙

누출 정도	일반탄화수소		쉽게 발화되는 물질	
	발화 확률	RRF	발화 확률	RRF
미미한 누출 / 실 누출(<0.5 ton)	0.01	100	0.1	10
주요 누출(0.5~5 ton)	0.1	10	1	0
대형 누출(>5 ton)	1	0	1	0

<표 7> 노출 및 회피에 관한 파라미터

요구시간에 위험지역에서 존재		위험원을 피할 가능성	
A1	부재	G1	위험원이 수동 작업의 결과로 가정되는 경우
A2	위험원이 수동 작업의 결과로 가정되는 경우	G2	부재

4. 결론 및 향후 연구

본 논문에서는 IEC 61508 표준을 바탕으로 SIL 을 평가할 수 있는 세부적인 절차를 제시하고 이에 대한 사례연구를 통한 검증을 실시하였다. 먼저 demand rate 의 도출 가능여부와 도출된 값, 증명시험의 간격을 기준으로 저 요구 작동모드와 고 요구 작동모드 또는 연속적인 작동모드로 분류하여 정량적인 SIL 을 평가하는 세부적인 절차를 제시하였다. 저 요구 작동모드의 경우는 SIL 평가를 위하여 현재 해당 기능의 리스크 평가를 실시하고 목표 리스크를 설정하였다. 이를 바탕으로 감소시켜야 하는 리스크의 양을 도출하고, 이 값을 RRF 라 하고 리스크 감소의 개념을 적용하였다. 저 요구 작동모드에서 SIL 평가를 위한 파리미터 PFD 는 RRF 에 대하여 역수 관계를 가지므로 이를 이용하여 최종적인 SIL 을 도출하였다. 하지만 고 요구 작동모드 또는 연속적인 작동모드에서는 단위시간당 고장률을 고려한 값을 목표 값으로 설정하여 SIL 을 도출하는 차이점이 존재함을 언급하였다.

저 요구 작동모드의 경우, demand rate 에 대하여 정량적으로 정확한 수치 도출이 불가능한 경우에는 정성적인 평가를 통하여 SIL 을 도출해야 한다. IEC 61508 표준에서 정성적인 평가 방법은 리스크 그래프와 심각도 매트릭스를 이용하는 두 가지 방법이 제시된다. 평가 대상이 되는 안전기능의 수를 고려하여 두 가지 방법 중 하나를 선택할 수 있다. 단일 안전기능에 대한 평가인 경우는 리스크 그래프를 사용하고 다수의 안전기능인 경우는 심각도 매트릭스를 사용한다. 심각도 매트릭스를 사용하는 경우에는 각 안전기능에 대한 독립성이 먼저 가정되어야 한다.

본 연구에서 SIL 평가를 위한 세부적인 절차에 대하여 문헌상의 내용과 실제 현업에서 실시하는 내용을 고려한 사례 연구를 실시하였다. 실제 사례연구를 통하여 문헌이나 이론에서 제시되는 내용을 바탕으로 산업현장의 경험적인 측면에 기초한 활동을 고려한 SIL 평가 절차에

대한 제시 및 검증을 실시하였다. IEC 61508 이라는 규격 자체가 특정 분야의 규격이 아닌 다양한 분야에 공통적인 가이드를 제공할 수 있는 광범위한 표준이므로 해당 절차를 적용할 때 각 분야의 특성을 고려한 수정이 필수적이라는 것을 본 사례연구를 통하여 확인할 수 있었다.

본 연구에서 제시되는 SIL 평가 프로세스에 관하여 사례연구를 통한 검증은 정성적인 평가에만 한정되어 실시되었다. 때문에 제시되는 정량적인 SIL 평가 절차에 대한 세례연구를 통하여 제시된 평가절차의 적절성 여부를 검증하는 활동이 필요할 것이다.

참고문헌

[1] 지식경제부 기술표준원(2006), "KS A IEC 61882 위험운전성(HAZOP)- 연구 적용지침", 한국표준협회.

[2] Hector Javier Cruz-Campa and M. Javier Cruz-Gomez(2010), "Determine SIS and SIL Using HAZOPS", Process Safety Progress, vol.29, p.22~31.

[3] IEC TR 61508-0(1998), Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 0: Functional safety and IEC 61508.

[4] IEC 61508(1998a), "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 1: General Requirements.

[5] IEC 61508(2000), Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 2: Requirements for Electrical / Electronic / Programmable Electronic Safety-Related Systems.

[6] IEC 61508(1998b), Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 3: Software Requirements.

[7] IEC 61508(1998c), Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 5: Examples of Methods for the Determination of Safety Integrity Levels.

[8] J. Beugin, D. Renaux and L. Cauffriez(2007), "A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems", Reliability Engineering and System Safety, vol.92, p.1686~1700.

[9] K.A.L. Van Heel, B. Knegterting and A. C. Brombacher(1999), "Safety Lifecycle Management : A Flowchart Presentation of the IEC 61508 Overall Safety Lifecycle Model", Quality and Reliability Engineering International, vol.15, p.493~500.

[10] Kirkwood, D. and Tibbs, B.(2005), "Developments in SIL determination", IEE Computing and Control Engineering, vol.16(3), p.21-27.

[11] Lawrence Beckman(1998), "Determining the required safety integrity level for your process", ISA Transactions, vol.37, p.105-111.

[12] Night Hyatt(2009), "Guidelines for Process Hazards Analysis, Hazards Identification and Risk Analysis", DYADEM.

[13] Smith, David J. and Simpson, Kenneth G. L.(2004), "Functional Safety: A Straightforward Guide to Applying IEC 61508 and Related Standards", Butterworth-Heinemann.

[14] The UK Offshore Operators Association(1999), "Guidelines for Instrumented-Based Protective Systems", Issue No.2.