KOSHA GUIDE

E - 149 - 2015

제어시스템에서의 안전무결성등급(SIL) 결정에 관한 지침

2015. 11

한국산업안전보건공단

안전보건기술지침의 개요

o 작성자 : 주식회사 류앤컴퍼니 류보혁

o 제·개정 경과

- 2015년 11월 전기안전분야 제정위원회 심의(제정)

o 관련규격 및 자료

- IEC 61508 시리즈: Functional safety of electrical/ electronic/ programmable electronic safety related systems(1998. 12, First Edition)
- KS C IEC 61508 시리즈(프로그램 가능한 전자장치 안전관련 시스템의 기능안전성)
- IEC 61511-3: Functional Safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels(2003. 3, First Edition)
- KS C IEC61511-3(프로세스산업을 위한 계측제어시스템의 기능 안전 - 제3부: 위험성 및 위험 분석의 응용지침)

o 기술지침 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈페이지(www..kosha.or.kr)의 안전보건기술지침 소관분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료, 법규 등에 관하여 최근 개정본이 있을 경우에는 해당 개정본의 내용을 참고하시기 바랍니다.

공표일자 : 2015년 12월 7일

제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
E - 149 - 2015

제어시스템에서의 안전무결성등급(SIL)결정에 관한 지침 제안개요

I. 제정이유

이 지침은 사업장에서 사용하는 전기·전자 프로그래머블 안전시스템으로 구성된 제어시스템의 신뢰도 확보에 관련된 안전무결성등급(SIL) 결정에 필요한 사항을 정함을 목적으로 함

II. 제정(안)의 주요내용

1. 이 기술지침은 다음의 기존 기술지침을 통합한 제정(안)임
   - X-20-2012 안전무결성등급(SIL) 산정에서의 인적안전 구분에 관한 지침
   - X-21-2012 안전무결성등급(SIL) 산정에서의 사업장 환경피해 구분에 관한 지침
   - X-22-2012 안전무결성등급(SIL) 산정에서의 사업장 재산피해 구분에 관한 지침
   - X-23-2012 안전무결성등급(SIL)의 분석 작업표 작성방법에 관한 지침
   - X-24-2012 안전무결성등급(SIL)의 산정에 관한 지침

2. 이 기술지침의 주요 내용은 다음과 같음
   - 안전관련 시스템의 구성
   - 안전무결성등급 결정
   - 인적안전/환경피해/재산피해 무결성등급 산정절차
   - 안전무결성등급의 분석 작업표 작성방법에 관한 지침

3. 주요 수정, 변경 내용은 다음과 같음
   - 목적 및 적용범위 등을 통합하고 수정함
   - 기술지침에서 사용되는 용어에 대해 정리하고 이를 보완함

KOSHA GUIDE
E - 149 - 2015

제어시스템에서의 안전무결성등급(SIL)결정에 관한 지침

1. 목적

이 지침은 사업장에서 사용하는 전기·전자 프로그래머블 안전시스템으로 구성된 제어시스템의 신뢰도 확보에 관련된 안전무결성등급(SIL) 결정에 필요한 사항을 정함을 목적으로 한다.

2. 적용 범위

이 지침은 제어시스템의 안전무결성등급(safety integrity level, SIL) 결정하는 경우에 적용한다.

3. 용어의 정의

(1) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

(가) “안전무결성(safety integrity)”이라 함은 안전관련 시스템이 주어진 시간동안 모든 운전상태에서 요구되는 안전기능을 만족스럽게 수행할 수 있는 확률을 말한다.

(나) “전기·전자 프로그래밍전자장치(electric/Electronic/Programmable electronic devices)”라 함은 전기·전자 프로그램이 가능한 전자기술을 기반으로 한 장치를 말한다.

(다) “프로그래밍 전자장치(programmable electronic devices, PED)”라 함은 하드웨어, 소프트웨어 및 입출력 장치로 구성된 컴퓨터 기술을 기반으로 한 전자장치를 말한다.

(라) “안전시스템(safety system)”이라 함은 운전설비의 안전상태를 유지하도록 안전기능을 수행하는 전기 전자 프로그램 가능형 시스템, 다른 기술로 구성된

시스템 또는 외부의 위험감소 설비 등을 말한다.

(마) “안전무결성등급(safety integrity level, SIL)”이라 함은 전기 전자 프로그램 가능형 전자장치로 구성된 안전시스템에서, 기능안전의 안전무결성 요건(safety integrity requirements)을 명시한 별개의 등급(1～4)을 말하며 그 중 등급 4가 가장 높고 등급 1이 가장 낮다.

(바) “기능안전(functional safety)”이라 함은 운전설비 또는 운전제어 시스템의 일부인 전기 전자 프로그램 가능형 안전시스템, 다른 기술로 구성된 안전시스템 또는 외부의 위험감소 설비가 올바르게 동작하도록 하는 기능과 관련된 안전을 말한다.

(사) “필요한 최소 위험 감소(necessary minimum risk reduction, NMRR)”라 함은 안전무결성등급을 결정하는데 필요한 위험 감소 추정치를 말한다.

(아) “위험 그래프 방법론(risk graph methodology)”이라 함은 IEC 61508-5를 기준하여 인적안전, 환경피해, 재산피해의 안전무결성등급 값을 구한 후에 요구수준 안전무결성등급(required SIL)을 결정하는 방법론을 말한다.

(자) “위험 변수(risk parameter)”라 함은 결과, 빈도와 노출시간, 유해위험 회피가능성, 원하지 않는 사고발생의 가능성 등의 변수들을 말한다.

(차) “안전무결성등급 분석 작업표(SIL classification worksheets)”라 함은 요구수준 안전무결성등급을 산정하기 위하여 공정의 위험성 분석 등을 기술하는 작업양식을 말한다.

(카) “제어안전시스템(safety instrumented system, SIS)”이라 함은 하나 또는 그 이상의 제어안전기능을 사용하는 계장시스템을 말하며 제어안전시스템(SIS)은 센서, 논리시스템, 최종 구성요소의 조합으로 이루어진다.

(타) “제어안전기능(safety instrumented function, SIF)”이라 함은 기능안전에 필요한 명시된 안전무결성등급의 안전기능으로, 계장안전의 보호기능 또는 계장안전의 제어기능을 말한다.

(2) 그밖에 이 지침에서 사용하는 용어의 정의는 이 지침에서 특별히 규정하는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙 및 산업안전보건기준에 관한 규칙에서 정하는 바에 따른다.

4. 안전관련 시스템의 구성

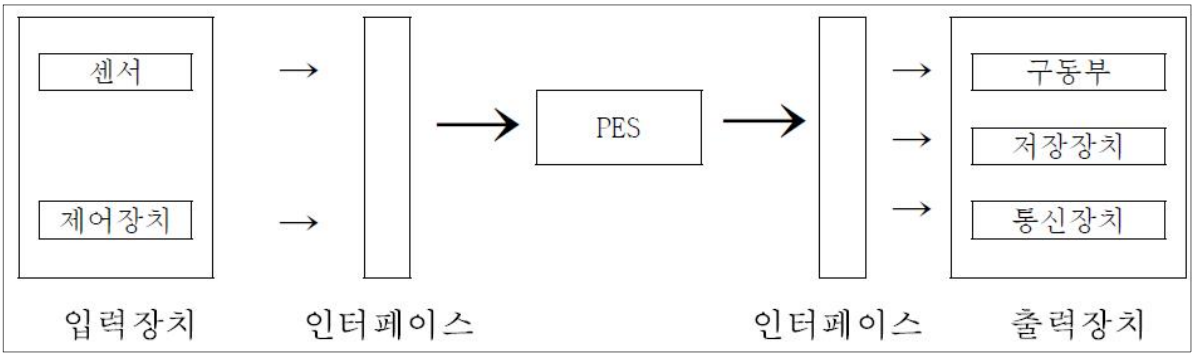
이 지침에서 안전기능을 수행하는데 이용되는 전기·전자프로그램어블 전자장치시스템의 안전수명을 정하는데 필요한 절차, 방법 등은 다음과 같다.

4.1 일반사항

(1) 안전기능 시스템은 안전에 영향을 미치는 시스템으로써 이에는 컴퓨터와 같은 프로그래밍 전자장치가 일반적으로 사용된다.

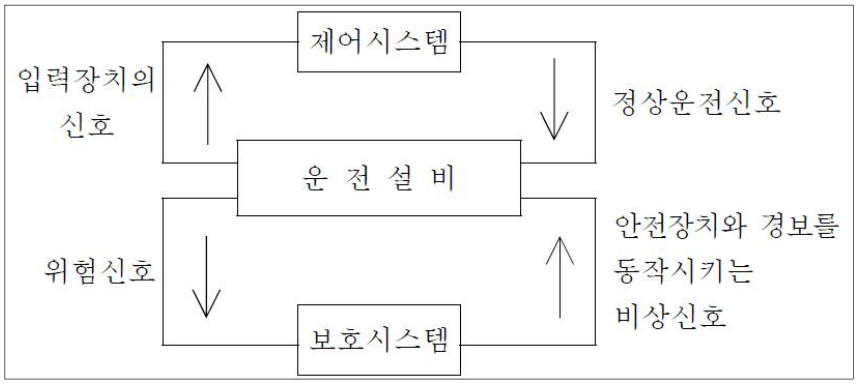
(2) 프로그래밍 전자시스템(Programmable Electronic System, PED)은 컴퓨터를 기본으로 하는 부분적인 시스템을 말하며, 프로그래밍 전자시스템을 갖춘 기계설비의 프로그래밍 전자시스템이 안전과 관련된 시스템의 정지기능을 갖는 경우에는 일반적으로 안전시스템이 된다. 안전시스템의 기능안전에 관한 상세내용은 프로그램 가능형 안전시스템의 기능안전 확보에 관한 안전가이드(KOSHA GUIDE E-12-2009)를 참조한다.

(3) 프로그래밍 전자시스템(PED)은 <그림 1>과 같이 데이터 하이웨이(data highway)나 기타 통신선을 통해 기기의 센서 및 기타 입력장치로부터 기기의 동작부나 기타 출력장치로 연결된다. 원칙적으로 안전시스템을 운전하는 작업자의 작업방법도 고려하여야 하나, 일반적으로 생략되는 경우가 많다.



<그림 1> 프로그래밍 전자시스템(PED)의 구조

(4) 일부 안전기능 시스템에서는 <그림 2>와 같이 제어시스템(control system)과 보호시스템(protection system)으로 이원화되어 사용될 수 있다. 제어시스템은 설비가 정상적으로 운전되도록 하는 시스템이고, 보호시스템은 고장조건을 취급하거나, 위험상황의 피해 최소화를 위한 출력을 발생하거나, 또는 위험한 사고를 예방하기 위한 시스템이다.



<그림 2> 제어시스템과 보호시스템

(5) 프로그래밍 전자시스템의 핵심은 프로그램이 가능한 전자부품이며, 이는 다른 프로그램을 사용하거나 지시 시퀀스를 바꾸게 되면 다른 시각 또는 다른 운전방식으로 작업을 수행할 수 있다.

(6) 프로그래밍 전자시스템의 강점은 다양한 활용에 있으나, 프로그램인 소프트웨어는 안전시스템의 매우 중요한 요소이므로 이의 품질은 매우 중요하다. 이에 대한 내용은「프로그램 가능형 안전시스템의 소프트웨어 안전을 위한 가이드(KOSHA GUIDE E-24-2009)」를 참조한다.

4.2 안전무결성 등급의 결정

안전무결성등급의 결정 및 방법은 5항에서, 인적안전분야는 6항, 환경피해분야는 7항, 재산피해분야에 대해서는 8항에 각각 기술한다.

5. 안전무결성 등급 결정

5.1 안전무결성 등급의 기준 및 적용

(1) 위험과 운전분석(hazard and operability, HAZOP) 등 정성적 위험성평가에서 확인된 모든 사고 시나리오에 대해 제어안전기능의 필요여부를 판단하고, 각 제어안전기능에 대하여 규명된 안전무결성등급의 값을 부여하여야 하므로 안전무결성등급 검토는 원칙적으로 위험과 운전분석(HAZOP) 등 정성적 위험성평가 후에 수행하는 것이 바람직하다.

(2) 안전무결성등급 검토는 화학플랜트의 비상정지시스템(ESD system)과 같이 안전과 관련된 제어계통을 대상으로 수행한다.

5.1.1 인적안전의 기준 및 적용

안전무결성등급 위험목표기준(risk target criteria)의 구분을 위하여 인적안전에 대한 안전무결성등급을 산정하는 기술적 내용을 제시한다.

5.1.2 환경피해의 기준 및 적용

안전무결성등급 위험 목표기준의 구분을 위하여 인적안전에 대한 안전무결성등급을 산정하는 기술적 내용을 제시한다.

5.1.3 재산피해의 기준 및 적용

안전무결성등급 위험 목표기준의 구분을 위하여 재산피해에 대한 안전무결성등급을 산정하는 기술적 내용을 제시한다.

5.2 안전무결성등급의 산정

(1) 제어안전시스템과 관련한 시나리오에서 요구수준 안전무결성등급(SIL)은 안전무결성등급 분석 작업표 상에 기입한 인적안전 안전무결성등급, 환경피해 안전무결

성등급, 재산피해 안전무결성등급의 값들과 동일하거나 낮도록 산정 한다.

(2) 요구운전방식(demand mode of operation)에서 제어안전기능의 목표평균 고장확률에 대한 안전무결성등급은 <표 1>을 참조한다.

(3) 일반적으로 정유플랜트, 석유화학 및 화학플랜트, 가스플랜트, 발전플랜트, 제철플랜트 등에서의 제어계통 설계기준은 “안전무결성등급 3” 이상을 요구하며, 아울러 기기공급업자(vendor)로부터 제3자 인증(certificate)을 요구하기도 한다.

<표 1> 안전무결성등급:고장고장확률(probability of failure on demand)(IEC 61511-1 참조)

요 구 운 전 방 식[1]		비 고
안전무결성등급	목표평균 고장확률[2]	
4	10^{-5}이상 ~ 10^{-4} 미만	
3	10^{-4}이상 ~ 10^{-3} 미만	
2	10^{-3}이상 ~ 10^{-2} 미만	
1	10^{-2}이상 ~ 10^{-1} 미만	

주1: 요구운전방식(Demand mode of operation)에서 안전시스템을 구축하기 위한 운전의 요구횟수는 1년에 1회 이하이고 성능검사(proof-test)의 요구횟수는 1년에 2회 이하이어야 한다.
2: 여기에서 고장확률이란 제어시스템 내에 사용된 부품(parts or components) 및 관련 프로그램의 고장 확률을 포함한다.

(4) 안전무결성등급 3은 제어기기의 고장확률이 1천분의 1 미만이면서 1만분의 1 이상의 신뢰도를 말한다. 즉, 제어기기의 신뢰도가 99.9 % 이상이면서 99.99 % 미만인 것을 의미한다.

(5) 바람직한 안전무결성등급 검토를 위하여는 각각의 제어계통에 대한 요구수준 안전무결성등급을 산정한 후에 이를 검증하는 과정을 수행 한다.

(6) 요구에서 안전무결성등급에 따른 각각의 위험감소목표는 <표 2>와 같다.

<표 2> 안전무결성등급: 목표 위험 감소(target risk reduction)(IEC 61511-1 참조)

요 구 운 전 방 식		비 고
안전무결성등급	목표 위험 감소	
4	10^4 이상 ~ 10^5 미만	
3	10^3 이상 ~ 10^4 미만	
2	10^2 이상 ~ 10^3 미만	
1	10 이상 ~ 10^2 미만	

주 1. 요구운전방식(demand mode of operation)에서 안전시스템을 구축하기 위한 운전의 요구횟수는 1년에 1회 이하이고 성능검사(proof-test)의 요구횟수는 1년에 2회 이하이어야 한다.
2. 참고로 ISA-S84.01(Application of safety instrumented systems for the process industries)에 따른 안전무결성등급에 대한 제어안전시스템의 성능요구사항은 <표 3>과 같다.

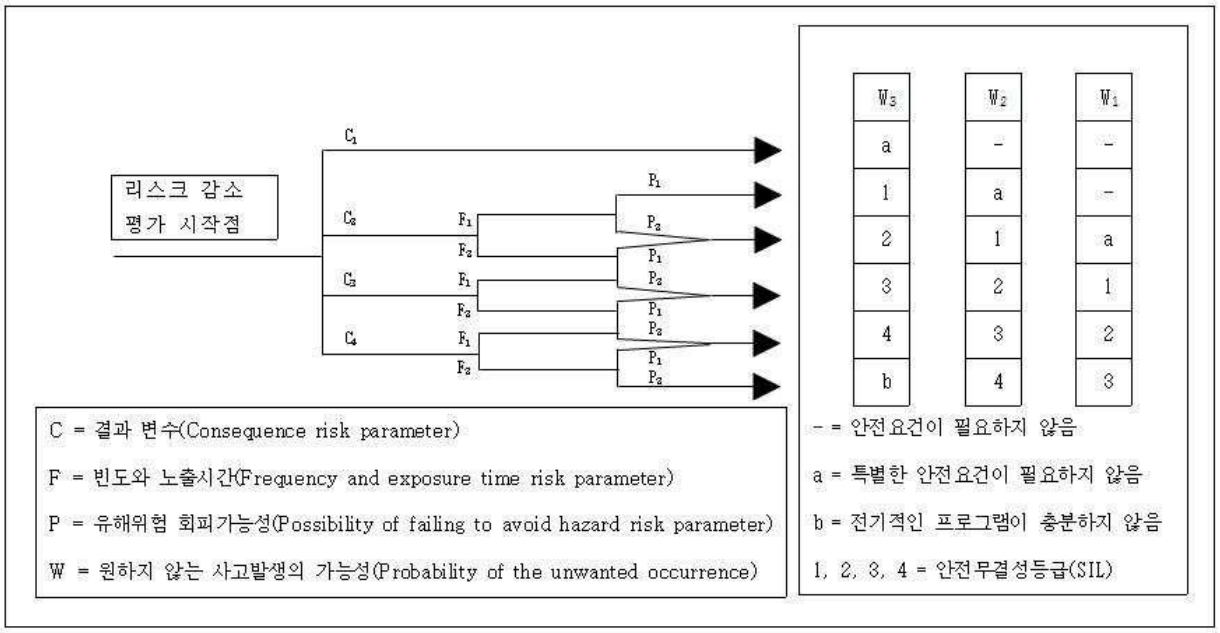
<표 3> ISA-S84.01에 따른 안전무결성등급의 성능요구사항(ISA-S84.01 참조)

안전무경성등급	1	2	3
제어안전시스템 성능요구사항	안전 가용도 범위(Safety availability range)		
	0.9 ~ 0.99	0.99 ~ 0.999	0.999 ~ 0.9999
	고장확률(PFD) 평균 범위(Average range)		
	10^{-1} ~ 10^{-2}	10^{-2} ~ 10^{-3}	10^{-3} ~ 10^{-4}

주: ANSI/ ISA S84.01:
1) Application of Safety Instrumented Systems for the Process Industries
2) US National Standard
3) OSHA 'recognised' under 29 CFR (Process Safety Management of Highly Hazardous Chemicals, etc.) (1910.119)

6. 인적안전무결성등급 산정절차

인적안전 안전무결성등급 값은 <그림 3>의 위험 그래프 방법을 이용하여 결정하되. 이에 대한 위험 변수는 <표 4>와 같이 결과(C), 빈도와 노출시간(F), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)을 참고한다.



<그림 3> 인적안전에 대한 위험 그래프 방법론

(1) 결과 위험 변수(C)에 대한 설명

결과 위험 변수(C)는 인명에 대한 사고피해의 등급으로서 경미한 사고는 C1, 다수의 중상 또는 사망사고 1명은 C2, 사망 2인 이상 사고는 C3, 다수가 사망한 사고는 C4 등급으로 구분하며 사고피해를 예측한 데이터를 참고하여 선정한다.

(2) 빈도와 노출시간 위험 변수(F)에 대한 설명

빈도와 노출시간 위험 변수(F)는 위험요인 지역에 노출되는 빈도의 등급으로서 매우 희박하게 노출되는 경우 F1, 빈번히 노출되는 경우에는 F2 등급으로 구분하여 선정한다.

(3) 유해위험 회피가능성 위험 변수(P)에 대한 설명

유해위험 회피가능성 위험 변수(P)는 위험요인에 회피할 수 있는 정도를 결정하는 등급으로서 위험상황에 대하여 회피가능하거나 사전에 경고가 가능한 경우 P1 등급, 위험상황에 대하여 회피가 불가능하거나 사전에 경고가 불가능한 경우에는 P2 등급으로 구분하며 다음의 고려조건을 참고하여 선정한다.

(가) 공정운전(즉, 숙련자 또는 비숙련자에 의한 운전 시 관리감독을 받는지 또는 관리감독을 받지 않는지)
(나) 위험요인 사상의 진행률(예: 급작스럽게, 빠르게 또는 느리게)
(다) 위험 인식의 용이성(예: 즉각적인 발견, 기술적인 혹은 비기술적인 측정에 의한 감지)
(라) 위험요인 사상의 회피(예: 대피로의 가능성 또는 조건부 회피)
(마) 실제 안전경험(동일한 제어 하의 기기 또는 이와 유사한 제어 하의 기기에 대한 경험의 유무)

(4) 원하지 않는 사고 발생의 가능성 위험 변수(W)에 대한 설명

원하지 않는 사고발생의 가능성 위험 변수(W)는 안전시스템이 추가로 설치되지 않았을 경우 사고발생 정도를 결정하는 등급으로서 사고발생 건수가 연간 0.1건 미만일 경우 W1, 사고발생 건수가 연간 0.1건 이상 1건 이하일 경우 W2, 사고발생 건수가 연간 1건을 초과하여 10 이하일 경우 W3 등급으로 구분하며 아래의 고려조건을 참고하여 선정한다.

(가) 사고발생확률은 위험감축장비는 구비하였으나 안전시스템이 추가로 설치되지 않았을 경우 발생 가능한 사고빈도를 추정함.
(나) 제어 하의 기기 시스템의 사용경험 또는 이와 유사한 경험이 없다면, 사고발생확률 추정은 계산방법에 의하며 그 확률은 최악의 예상치를 적용함.

<표 4> 인적안전에 대한 위험 데이터

위험 변수	등급 분류		비 고
결과변수 (Consequence risk parameter, C)	C_1	경상	
	C_2	다수의 중상 또는 사망 1명	
	C_3	사망 2인 이상	
	C_4	사망 다수	
빈도와 노출시간 (Frequency of, and exposure time in, thw hazardous zone, F)	F_1	매우 희박함	
	F_2	빈번함	
유해위험 회피가능성 (Possibility of avoiding the hazardous event, P)	P_1	회피 가능	1. 고려조건 1) 공정운전(즉, 숙련자 또는 비숙련자에 의한 운전 시 관리감독을 받는 지 혹은 관리감독을 받지 않는지) 2) 위험요인 사상의 진행률(예: 급작스럽게, 빠르게 또는 느리게) 3) 위험 인식의 용이성(예: 즉각적인 발견, 기술적인 혹은 비기술적인 측정에 의한 감지) 4) 위험요인 사상의 회피(예: 대피로의 가능성 또는 조건부 회피) 5) 실제 안전경험(동일한 제어 하의 기기 또는 이와 유사한 제어 하의 기기에 대한 경험의 유무)
	P_2	회피 불가능	
원하지 않는 사고발생의 가능성 (Probability of the unwanted occurrence, W)	W_1	낮음(연간 0.1건 미만)	2. 사고발생확률은 위험감축장비는 구비하였으나 안전시스템이 추가로 설치되지 않았을 경우 발생 가능한 사고빈도를 추정함 3. 제어 하의 기기 시스템의 사용경험 또는 이와 유사한 경험이 없다면, 사고발생확률 추정은 계산방법에 의하며 그 확률은 최악의 예상치를 적용함
	W_2	중간(연간 0.1건 이상 1건 이하)	
	W_3	높음(연간 1건 초과 10건 이하)	

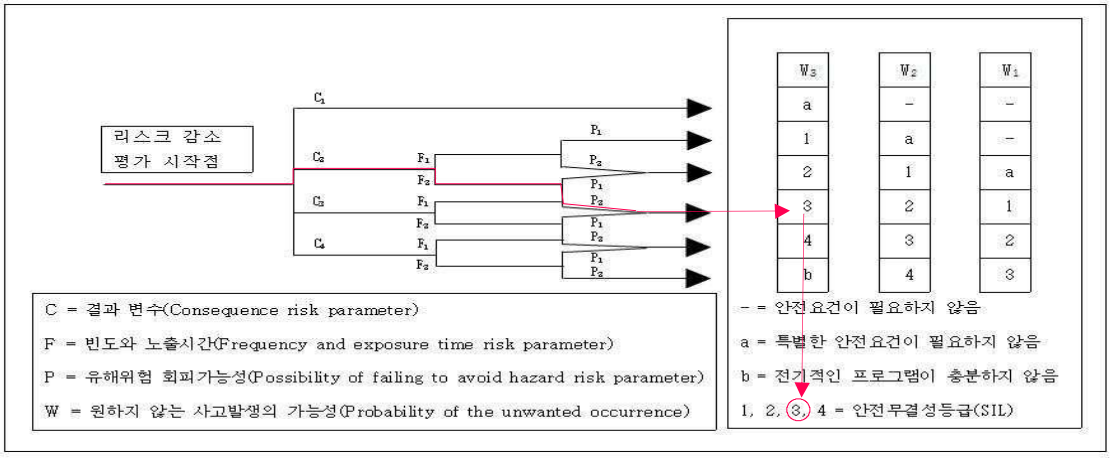
(5) 인적안전에 대한 안전무결성등급 산정방법

(가) 인적안전에 대한 위험 변수인 결과 변수(C), 빈도와 노출시간 (F), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)에 대하여 각각의 등급에 따라 부록의 <그림 4>에서 보는 바와 같이 시작점에서 출발하여 우선적으로 결과 변수(C) 등급에 따라 C1, C2, C3, C4 등급 중 하나를 결정하고 빈도와 노출시간(F), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)을 각각의 등급에 따라 결정하여 필요한 최소 위험 감소(necessary minimum risk reduction)를 구한다.

(나) 그 다음에 최종적으로 <그림 3>에서 명시한 바와 같이 필요한 최소 위험 감소(NMRR)인 '-', 'a', 'b', '1', '2', '3', '4'에 상응하는 인적안전 안전무결성 등급을 산정한다.

(6) 인적안전에 대한 안전무결성 산정의 예

인적안전에 대한 안전무결성등급을 산정하는 예는 아래 <그림 4>, <표 5>와 같다. 예를 들어, 결과 변수(C)는 C2, 빈도와 노출시간(F)은 F2, 유해위험 회피가능성(P)은 P2, 원하지 않는 사고발생의 가능성(W)은 W3등급일 경우 아래 <그림 4>과 같이 시작점에서 출발하여 C2 → F2 → P2 → W3의 필요한 최소 리스크 감소(NMRR)인 '3'을 결정하면 '3'은 <그림 4>에서 명시한 바와 같이 인적안전 안전무결성등급 3으로 산정한다.



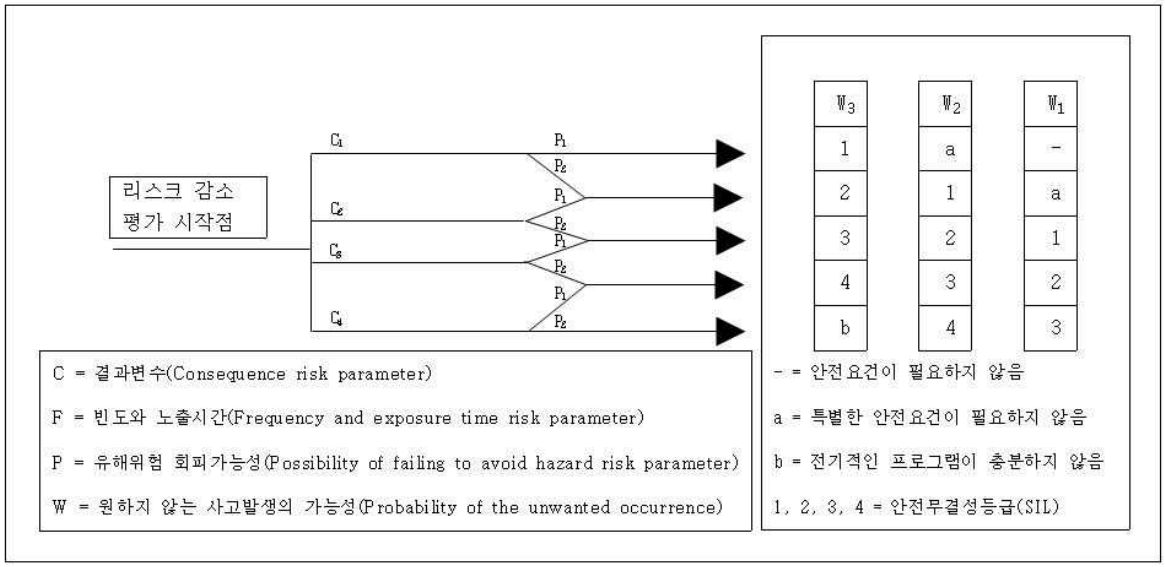
<그림 4> 인적안전에 대한 안전무결성 등급 산정 방법

<표 5> 등급분류에 따른 인적안전 안전무결성등급 산정

위험 변수	등급 분류	비고
1) 결과 변수(Consequence risk parameter, C)	C_2	
2) 빈도와 노출시간(Frequency of, and exposure time in, the hazardous zone, F)	F_2	
3) 유해위험 회피가능성(Possibility of avoiding the hazardous event, P)	P_2	
4) 원하지 않는 사고발생의 가능성(Probability of the unwanted occurrence, W)	W_3	
5) 필요한 최소 위험 감소(Necessary minimum risk reduction, NMRR)	3	
6) 인적안전 안전무결성등급	SIL 3	

7. 환경피해 안전무결성등급 산정 절차

환경피해에 대한 위험 변수는 <표 6>과 같이 결과 변수(C), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)으로 구성되어 지며, 이 값들을 사용하여 <그림 5>의 위험 그래프 방법론을 통해 인적안전 안전무결성등급 값을 산정한다.



<그림 5> 환경피해에 대한 위험그래프 방법론

(1) 결과 위험 변수(C)에 대한 설명

결과 위험 변수(C)는 환경에 대한 사고피해의 등급으로서 소량누출 피해는 C1, 사업장 내부 누출피해는 C2, 사업장 외부로 누출피해가 발생하였으나 빠른 방제가 가능한 경우는 C3, 사업장 외부로 지속적으로 누출피해가 발생하는 경우는 C4 등급으로 구분하며 아래의 고려조건을 참고하여 선정한다.

(가) 밸브나 플랜지에서 보통의 누출, 소규모 액체 유출 또는 지하수에 영향이 없는 소규모 토양오염
(나) 플랜지 개스킷 블로우 아웃(blow-out)이나 압축기 밀봉(seal)의 파열에 의한 단위공정 외부로 매우 불쾌한 증기운(vapor cloud)의 이동
(다) 식물, 동물에 일시적 피해를 야기하는 증기 또는 분무상태(aerosol)의 누출, 강 또는 바다로 액체 유출
(라) 식물, 동물에 지속적 피해를 야기하는 증기 또는 분무상태(aerosol)의 누출.
(마) 고체의 낙진(먼지, 촉매, 그을음, 화산재) 또는 지하수에 영향을 주는 액체 누출

(2) 빈도와 노출시간 위험 변수(F)에 대한 설명

빈도와 노출시간 위험 변수(F)는 점유(occupancy)의 개념을 적용하지 않아 사용하지 않는다.

(3) 유해위험 회피가능성 위험 변수(P)에 대한 설명

유해위험 회피가능성 위험 변수(P)는 위험요인에 회피할 수 있는 정도를 결정하는 등급으로서 위험상황에 대하여 회피가능하거나 사전에 경고가 가능한 경우 P1 등급, 위험상황에 대하여 회피가 불가능하거나 사전에 경고가 불가능한 경우에는 P2 등급으로 구분하며 다음의 고려조건을 참고하여 선정한다.

(가) 공정운전(즉, 숙련자 또는 비숙련자에 의한 운전 시 관리감독을 받는지 혹은 관리감독을 받지 않는지)
(나) 위험요인 사상의 진행률(예: 급작스럽게, 빠르게 또는 느리게)
(다) 위험 인식의 용이성(예: 즉시 발견, 기술적 또는 비기술적 측정에 의한 감지)
(라) 위험요인 사상의 회피(예: 대피로의 가능성 또는 조건부 회피)
(마) 실제 안전경험(동일한 제어 하의 기기 또는 이와 유사한 제어 하의 기기에 대한 경험의 유무).

(4) 원하지 않는 사고 발생의 가능성 리스크 변수(W)에 대한 설명

원하지 않는 사고발생의 가능성 리스크 변수(W)는 안전시스템이 추가로 설치되지 않았을 경우 사고발생 정도를 결정하는 등급으로서 사고발생 건수가 연간 0.1건 미만일경우 W1, 사고발생 건수가 연간 0.1건 이상 1건 이하일 경우 W2, 사고발생 건수가 연간 1건을 초과하여 10 이하일 경우 W3 등급으로 구분하며 아래의 고려조건을 참고하여 선정한다.

(가) 사고발생확률은 위험감축장비는 구비하였으나 안전시스템이 추가로 설치되지 않았을 경우 발생 가능한 사고빈도를 추정함.
(나) 제어 하의 기기 시스템의 사용경험 또는 이와 유사한 경험이 없다면, 사고발생확률 추정은 계산방법에 의하며 그 확률은 최악의 예상치를 적용함

(5) 환경피해에 대한 안전무결성등급 산정방법

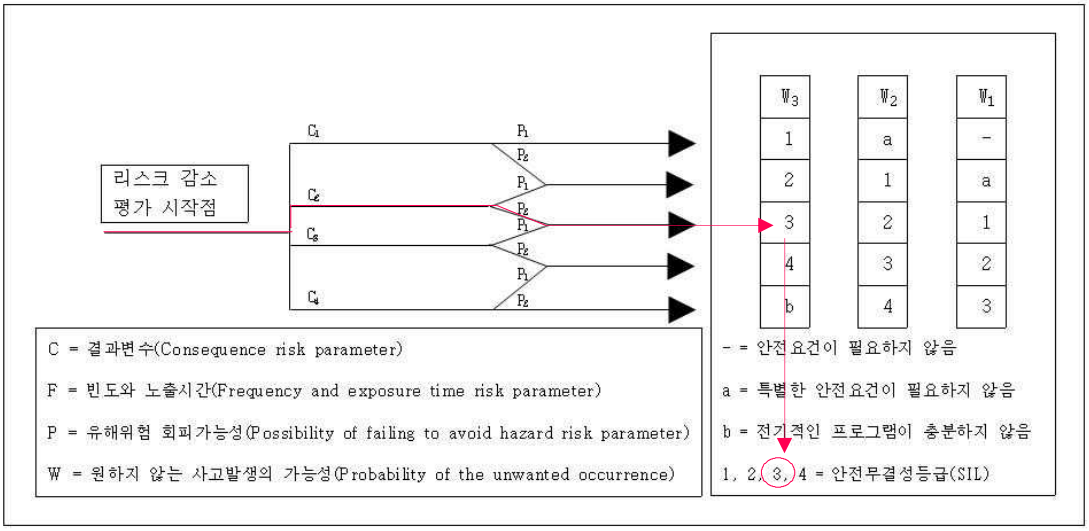
(가) 환경피해에 대한 리스크 변수인 결과 변수(C), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)에 대하여 각각의 등급에 따라 <그림 6>에서와 같이 시작점에서 출발하여 우선적으로 결과 변수(C) 등급에 따라 C1, C2, C3, C4 등급 중 하나를 결정하고 빈도와 노출시간(F), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)을 각각의 등급에 따라 결정하여 필요한 최소 리스크 감소NMRR(necessary minimum risk reduction)을 구한다.
(나) 그 다음에 최종적으로 <그림 5>에서 명시한 바와 같이 필요한 최소 위험 감소(NMRR)인 '-', 'a', 'b', '1', '2', '3', '4'에 상응하는 환경피해 안전무결성 등급을 산정한다.

<표 6> 환경피해에 대한 위험 데이터

위험 변수	등급 분류		비 고
결과변수 (consequence risk parameter, C)	C_1	소량누출	1. 밸브나 플랜지에서 보통의 누출 2. 소규모 액체 유출 3. 지하수에 영향 없는 소규모 토양오염
	C_2	사업장 내부 누출	4. 플랜지 캐스킷 블로우 아웃(blow-out)이나 압축기 밀봉(Seal)의 파열에 의한 단위공정 외부로 매우 불쾌한 증기운의 이동
	C_3	일시적인 사업장 외부 누출	5. 식물, 동물에 일시적 피해를 야기하는 증기 또는 분무상태(aerosol)의 누출 6. 강 또는 바다로 액체 누출
	C_4	지속적인 사업장 외부 누출	7. 식물, 동물에 지속적 피해를 야기하는 증기 또는 분무상태(aerosol)의 누출 8. 고체의 낙진(먼지, 촉매, 그을음, 화산재) 9. 지하수에 영향을 주는 액체 누출
유해위험 회피가능성 (possibility of avoiding the hazardous event, P)	P_1	회피 가능	10. 고려조건 1) 공정운전(즉, 숙련자 또는 비숙련자에 의한 운전 시 관리감독을 받는 지 또는 관리감독을 받지 않는지) 2) 위험요인 사상의 진행률(예: 급작스럽게, 빠르게 또는 느리게) 3) 위험 인식의 용이성(예: 즉각적인 발견, 기술적인 혹은 비기술적인 측정에 의한 감지) 4) 위험요인 사상의 회피(예: 대피로의 가능성 또는 조건부 회피) 5) 실제 안전경험(동일한 제어 하의 기기 또는 이와 유사한 제어 하의 기기에 대한 경험의 유무)
	P_2	회피 불가능	
원하지 않는 사고발생의 가능성 (probability of the unwanted occurrence, W)	W_1	낮음(연간 0.1건 미만)	11. 사고발생확률은 위험감축장비는 구비하였으나 안전시스템이 추가로 설치되지 않았을 경우 발생 가능한 사고빈도를 추정함 12. 제어 하의 기기 시스템의 사용경험 또는 이와 유사한 경험이 없다면, 사고발생확률 추정은 계산방법에 의하며 그 확률은 최악의 예상치를 적용함
	W_2	중간(연간 0.1건 이상 1건 이하)	
	W_3	높음(연간 1건 초과 10건 이하)	

(6) 환경피해에 대한 안전무결성 산정의 예

환경피해에 대한 안전무결성등급을 산정하는 예는 아래 <그림 6>, <표 7>과 같다. 예를 들어, 결과 변수(C)는 C2, 유해위험 회피가능성(P)은 P2, 원하지 않는 사고발생의 가능성(W)은 W3등급일 경우 <그림 6>과 같이 시작점에서 출발하여 C2 → P2 → W3의 필요한 최소 리스크 감소(NMRR)인 '3'을 결정하면 '3'은 <그림 6>에서 명시한 바와 같이 인적안전 안전무결성등급 3으로 산정한다.



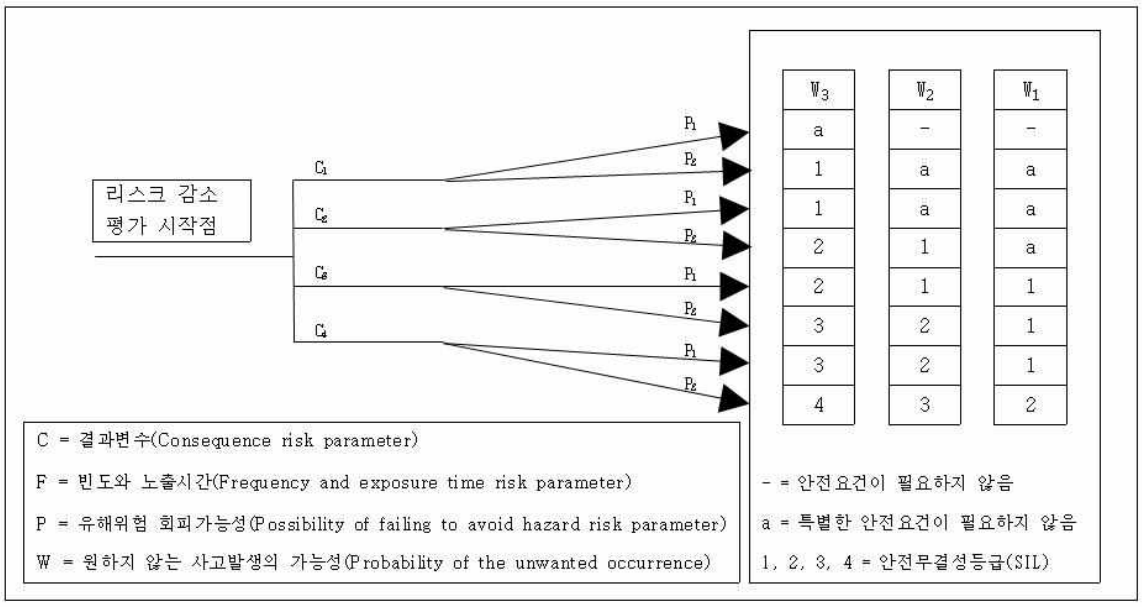
<그림 6> 환경피해에 대한 안전무결성 등급 산정 방법

<표 7> 등급분류에 따른 환경피해 안전무결성등급 산정

위험 변수	등급 분류	비고
1) 결과 변수(consequence risk parameter, C)	C_2	
2) 유해위험 회피가능성(possibility of avoiding the hazardous event, P)	P_2	
3) 원하지 않는 사고발생의 가능성(probability of the unwanted occurrence, W)	W_3	
4) 필요한 최소 위험 감소(necessary minimum risk reduction, NMRR)	3	
5) 환경피해 안전무결성등급	SIL 3	

8. 재산피해 안전무결성등급 산정 절차

재산피해에 대한 위험 변수는 <표 8>과 같이 결과 변수(C), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)으로 구성되어 지며, 이 값들을 사용하여 <그림 7>의 위험 그래프 방법론을 통해 인적안전 안전무결성등급 값을 산정한다.



<그림 7> 재산피해에 대한 위험 그래프 방법론

(1) 결과 위험 변수(C)에 대한 설명

결과 위험 변수(C)는 재산에 대한 사고피해의 등급으로서 6천만원 미만의 피해는 C1, 6천만원 이상 1억2천만원 미만의 피해는 C2, 1억2천만원 이상 12억원 미만의 피해는 C3, 12억원 이상의 피해는 C4 등급으로 구분하며 아래의 고려조건을 참고하여 선정한다.

(가) 1~2일 생산손실 또는 미약한 설비손상
(나) 1주 생산손실 또는 약간의 설비손상
(다) 1달 생산손실 또는 상당한 설비손상
(라) 6개월 이상의 막대한 생산손실 또는 설비손상.

(2) 빈도와 노출시간 위험 변수(F)에 대한 설명

빈도와 노출시간 위험 변수(F)는 점유(occupancy)의 개념을 적용하지 않아 사용하지 않는다.

(3) 유해위험 회피가능성 위험 변수(P)에 대한 설명

유해위험 회피가능성 위험 변수(P)는 위험요인에 회피할 수 있는 정도를 결정하는 등급으로서 위험상황에 대하여 회피가능하거나 사전에 경고가 가능한 경우 P1 등급, 위험상황에 대하여 회피가 불가능하거나 사전에 경고가 불가능한 경우에는 P2 등급으로 구분하며 다음의 고려조건을 참고하여 선정한다.

(가) 공정운전(즉, 숙련자 또는 비숙련자에 의한 운전 시 관리감독을 받는지 혹은 관리감독을 받지 않는지)
(나) 위험요인 사상의 진행률(예: 급작스럽게, 빠르게 또는 느리게)
(다) 위험 인식의 용이성(예: 즉각적인 발견, 기술적인 혹은 비기술적인 측정에 의한 감지)
(라) 위험요인 사상의 회피(예: 대피로의 가능성 또는 조건부 회피)
(마) 실제 안전경험(동일한 제어 하의 기기 또는 이와 유사한 제어 하의 기기에 대한 경험의 유무)

(4) 원하지 않는 사고 발생의 가능성 리스크 변수(W)에 대한 설명

원하지 않는 사고발생의 가능성 리스크 변수(W)는 안전시스템이 추가로 설치되지 않았을 경우 사고발생 정도를 결정하는 등급으로서 사고발생 건수가 연간 0.1건 미만일경우 W1, 사고발생 건수가 연간 0.1건 이상 1건 이하일 경우 W2, 사고발생 건수가 연간 1건을 초과하여 10 이하일 경우 W3 등급으로 구분하며 아래의 고려조건을 참고하여 선정한다.

(가) 사고발생확률은 위험감축장비는 구비하였으나 안전시스템이 추가로 설치되지 않았을 경우 발생 가능한 사고빈도를 추정하다.
(나) 제어 하의 기기 시스템의 사용경험 또는 이와 유사한 경험이 없다면, 사고발생확률 추정은 계산방법에 의하며 그 확률은 최악의 예상치를 적용한다.

<표 8> 재산피해에 대한 위험 데이터

위험 변수	등급 분류		비 고
결과변수 (Consequence risk parameter, C)	C_1	피해액 6천만원 미만(5만불 미만)	1. 1~2일 생산손실 또는 미약한 설비손상
	C_2	피해약 6천만원 이상 1억2천만원 미만(5만불이상 10만불 미만	2. 1주 생산손실 또는 약간의 설비손상
	C_3	피해액 1억2천만원 이상 12억원 미만(10만불이상 100만불미만)	3. 1달 생산손실 또는 상당한 설비손상
	C_4	피해액 12억원 이상(100만불 이상)	4. 6개월 이상의 막대한 생산손실 또는 설비손상
유해위험 회피가능성 (Possibility of avoiding the hazardous event, P)	P_1	회피 가능	5. 고려조건 1) 공정운전(즉, 숙련자 또는 비숙련자에 의한 운전 시 관리감독을 받는 지 혹은 관리감독을 받지 않는지) 2) 위험요인 사상의 진행률(예: 급작스럽게, 빠르게 또는 느리게) 3) 위험 인식의 용이성(예: 즉각적인 발견, 기술적인 혹은 비기술적인 측정에 의한 감지) 4) 위험요인 사상의 회피(예: 대피로의 가능성 또는 조건부 회피) 5) 실제 안전경험(동일한 제어 하의 기기 또는 이와 유사한 제어 하의 기기에 대한 경험의 유무)
	P_2	회피 불가능	
원하지 않는 사고발생의 가능성 (Probability of the unwanted occurrence, W)	W_1	낮음(연간 0.1건 미만)	6. 사고발생확률은 위험감축장비는 구비하였으나 안전시스템이 추가로 설치되지 않았을 경우 발생 가능한 사고빈도를 추정함 7. 제어 하의 기기 시스템의 사용경험 또는 이와 유사한 경험이 없다면, 사고발생확률 추정은 계산방법에 의하며 그 확률은 최악의 예상치를 적용함
	W_2	중간(연간 0.1건 이상 1건 이하)	
	W_3	높음(연간 1건 초과 10건 이하)	

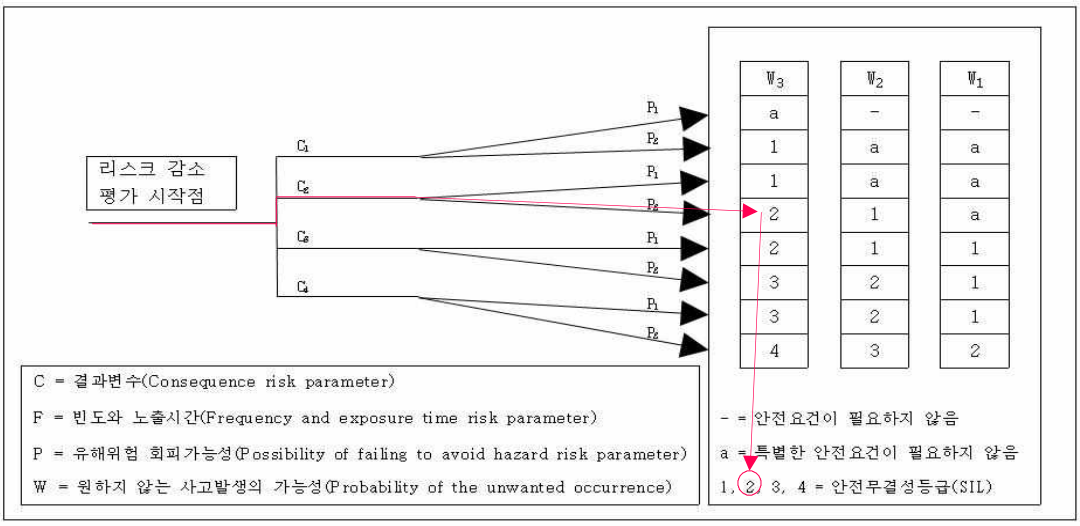
(5) 재산피해에 대한 안전무결성등급 산정방법

재산피해에 대한 리스크 변수인 결과 변수(C), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)에 대하여 각각의 등급에 따라 <그림 8>에서와 같이 시작점에서 출발하여 우선적으로 결과 변수(C) 등급에 따라 C1, C2, C3, C4 등급 중 하나를 결정하고 빈도와 노출시간(F), 유해위험 회피가능성(P), 원하지 않는 사고발생의 가능성(W)을 각각의 등급에 따라 결정하여 필요한 최소 리스크 감소 NMRR(necessary minimum risk reduction)을 구한다.

그 다음에 최종적으로 <그림 7>에서 명시한 바와 같이 필요한 최소 위험 감소(NMRR)인 '-', 'a', 'b', '1', '2', '3', '4'에 상응하는 환경피해 안전무결성등급을 산정한다.

(6) 재산피해에 대한 안전무결성 산정의 예

재산피해에 대한 안전무결성등급을 산정하는 예는 아래 <그림 8>, <표 9>와 같다. 예를 들어, 결과 변수(C)는 C2, 유해위험 회피가능성(P)은 P2, 원하지 않는 사고발생의 가능성(W)은 W3등급일 경우 아래 <그림 8>과 같이 시작점에서 출발하여 C2 → P2 → W3의 필요한 최소 리스크 감소(NMRR)인 '2'를 결정하면 '2'는 <그림 8>에서 명시한 바와 같이 인적안전 안전무결성등급 2로 산정한다.



<그림 8> 재산피해에 대한 안전무결성 등급 산정 방법

<표 9> 등급분류에 따른 재산피해 안전무결성등급 산정

위험 변수	등급 분류	비고
1) 결과 변수(consequence risk parameter, C)	C_2	
2) 유해위험 회피가능성(possibility of avoiding the hazardous event, P)	P_2	
3) 원하지 않는 사고발생의 가능성(probability of the unwanted occurrence, W)	W_3	
4) 필요한 최소 위험 감소(necessary minimum risk reduction, NMRR)	2	
5) 재산피해 안전무결성등급	SIL 2	

9. 안전무결성등급(SIL) 분석 작업표 작성방법

9.1 안전무결성등급 분석 과정

(1) 안전안전무결성등급 분석은 작성된 제어안전시스템에 대하여 IEC 61508 및 IEC 61511을 기준으로 한 위험 그래프 방법론(risk graph methodology)을 사용하여 요구수준 안전무결성등급을 산정하는 과정이다.

(2) 안전무결성등급 구분은 다음과 같은 구성원을 팀으로 하여 실행한다.

(가) 공정전문가(process specialist)
(나) 공정제어기술자(process control engineer)
(다) 생산관리자(operations management)
(라) 안전전문가(safety specialist)
(마) 대상 공정의 운전경험자(person who has practical experience of operating the process under consideration) 등

9.2 안전무결성등급의 위험 목표기준(risk target criteria) 결정

(1) 안전무결성등급 분석에서 위험 등급은 각 분야 전문가들의 회의를 통해 위험 그래프 방법론(risk graph methodology)을 사용하여 결정하며, 다음과 같은 항목을 결정한다.

(가) 공정 위험(결과, 빈도) 반영
(나) 실패확률 및 반영
(다) 인적안전 위험 반영
(라) 환경피해 위험 반영
(마) 재산피해 위험 반영
(바) 허용 위험 반영
(사) 안전무결성등급 결정

(2) 안전무결성등급 결정은 KS C IEC 61508 및 KS C IEC 61511을 참조하여 결정한다.

9.3 안전무결성등급 분석 작업표

안전무결성등급 분석 작업표는 다음과 같은 항목들을 포함하여 작성한다.

(1) 제어안전시스템 번호

제어안전시스템(SIS)의 번호(Tag No. 등)를 기입한다.

(2) 공정배관・계장도 번호

공정배관・계장도(P&ID)의 번호를 기입한다.

(3) 제어안전기능 설명

제어안전기능(SIF)에 대한 설명을 기입한다.

(4) 설계의도

설계자의 설계의도 및 설계사양을 기입한다.

(5) 요구 시나리오

사고발생의 시나리오를 기입한다.

(6) 사고발생결과

사고발생의 결과인 인적안전, 환경피해 및 재산피해를 기입한다.

(7) 현재안전조치

각각의 요구 시나리오에 대해 관심 대상의 제어안전기능을 제외한 현재안전조치(Safeguard)를 기입한다.

(8) 결과 변수(consequence risk parameter) : (C)

결과 위험변수를 기입한다.

(9) 빈도와 노출시간(frequency of, and exposure time in, the hazardous zone) : (F)

폭발위험장소(hazardous zone)에 노출되는 빈도와 시간을 기입한다.

(10) 유해위험 회피가능성(possibility of avoiding the hazardous event) : (P)

유해위험(hazardous event)의 회피 가능성을 기입한다.

(11) 원하지 않는 사고발생의 가능성(probability of the unwanted occurrence) : (W)

원치 않는 사고발생의 가능성을 기입한다.

(12) 인적안전

인적안전무결성등급 산정 절차(6항 참조)에 따라 해당하는 값을 기입한다.

(13) 환경피해

환경피해 안전무결성등급 산정 절차(7항 참조)에 따라 해당하는 값을 기입한다.

(14) 재산피해

재산피해안전무결성등급 산정 절차(8항 참조)에 따라 해당하는 값을 기입한다.

(15) 요구수준 안전무결성등급

인적안전 안전무결성등급, 환경피해 안전무결성등급, 재산피해 안전무결성등급 값들 중 가장 높은 안전무결설등급 값을 기입한다.

(16) 안전무결성등급 분석 작업표의 양식은 <표 10>을 기준으로 한다.

(17) 안전무결성등급 분석 작업표의 작성 예는 <부록>을 참조한다.

<표 10> 안전무결성등급 분석 작업표

<table>
<tr><th colspan="6">안전무결성등급 분석 작업표</th><th>비고</th></tr>
<tr><td colspan="4">(1) 제어안전시스템 번호</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(2) 공정배관・계장도 번호</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(3) 제어안전기능 설명</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(4) 설계의도</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(5) 요구 시나리오</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(6) 사고발생결과</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(7) 현재안전조치</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(8) 결과 변수(C)
(consequence risk parameter)</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(9) 빈도와 노출시간(F)
(frequency of, and exposure time in, the hazardous zone)</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(10) 유해위험 회피가능성(P)(possibility of avoiding the hazardous event)</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(11) 원하지 않는 사고발생의 가능성(W)
(probability of the unwanted occurrence)</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">(12)인적안전</td><td colspan="2">(13) 환경피해</td><td colspan="2">(14) 재산피해</td><td>약 자</td><td></td></tr>
<tr><td>C</td><td></td><td>C</td><td></td><td>C</td><td></td><td rowspan="5">C = 결과 변수
(consequence risk parameter)
F = 빈도와 노출시간
(frequency and exposure time risk parameter)
P = 유해위험 회피가능성
(possibility of avoiding hazard risk parameter)
W = 원하지 않는 사고발생의 가능성
(possibility of the unwanted occurrence)
NMRR = 필요한 최소 위험 감소
(necessary minimum risk reduction)</td><td rowspan="5"></td></tr>
<tr><td>F</td><td></td><td>F</td><td></td><td>F</td><td></td></tr>
<tr><td>P</td><td></td><td>P</td><td></td><td>P</td><td></td></tr>
<tr><td>W</td><td></td><td>W</td><td></td><td>W</td><td></td></tr>
<tr><td>NMRR</td><td></td><td>NMRR</td><td></td><td>NMRR</td><td></td></tr>
<tr><td>인적안전안전무결성등급 (SIL</td><td></td><td>환경피해안전무결성등급 (SIL)</td><td></td><td>재산피해안전무결성등급 (SIL)</td><td></td><td colspan="2">(15) 요구수준 안전무결성등급</td><td></td></tr>
</table>

<부록>

안전무결성등급 분석 작업표 예시

안전무결성등급 분석 작업표		비고
(1) 제어안전시스템 번호	XV-0013	
(2) 공정배관·계장도 번호	LKT-105-103-R1	
(3) 제어안전기능 설명	1) 구형탱크 압력 high high 2) 구형탱크 액위 high high 3) 구형탱크 가스 감지 4) 구형탱크 화재 감지	
(4) 설계의도	1) 설정압력: high high 15kgf/cm2g 2) 설정액위: high high 95% 3) 가스 탐지 4) 화재 탐지	
(5) 요구 시나리오	1) 압력 신호 발신기 고장 2) 수위 신호 발신기 고장 3) 가스 탐지기 고장 4) 화재 탐지기 고장	
(6) 사고발생결과	요구 시나리오에 대한 인적안전, 환경피해, 재산피해 발생	
(7) 현재안전조치	1) 압력 신호 발신기 고장: (1) PSV-203/ 205/ 206/ 207 (2) TI-0011/ 0012 2) 수위 신호 발신기 고장: (1) 수위 계기판(LI-0011/ 0012/ 0031) 3) 가스 탐지기 고장: (1) 물분무 시스템 4) 화재 탐지기 고장: (1) 물분무 시스템	
(8) 결과 변수(C) (Consequence risk parameter)	1) 가스 누출에 의한 잠재적 분출화재 위험 2) LPG 넘침(Carry over)에 의한 가스 압축기에 대한 기계적 피해	
(9) 빈도와 노출시간(F) (Frequency of, and exposure time in, the hazardous zone)	매우 희박함	
(10) 유해위험의 회피가능성(P) (Possibility of the unwanted occurrence)	회피 가능함	
(11) 원하지 않는 사고발생 가능성(W) (Probability of the un-wanted occurrence)	낮음(연간 0.1건 미만)	

안전무결성등급 분석 작업표 예시(계속)

<table>
<tr><th colspan="8">안전무결성등급 분석 작업표</th><th>비고</th></tr>
<tr><td colspan="4">(1) 제어안전시스템 번호</td><td colspan="4">XV-0013</td><td></td></tr>
<tr><td colspan="4">(2) 공정배관 계장도 번호</td><td colspan="4">LKT-105-103-R1</td><td></td></tr>
<tr><td colspan="2">(12) 인적안전</td><td colspan="2">(13) 환경피해</td><td colspan="2">(14) 재산피해</td><td colspan="2">약 자</td><td></td></tr>
<tr><td>C</td><td>C_3</td><td>C</td><td>C_2</td><td>C</td><td>C_3</td><td colspan="2" rowspan="5">C = 결과 변수 (consequence risk parameter)
F = 빈도와 노출시간 (frequency and exposure time risk parameter)
P = 유해위험 회피가능성 (possibility of avoiding hazard risk parameter)
W = 원하지 않는 사고발생의 가능성 (possibility of the unwanted occurrence)
NMRR = 필요한 최소 위험 감소 (necessary minimum risk reduction)</td><td rowspan="5"></td></tr>
<tr><td>F</td><td>F_1</td><td>F</td><td>-</td><td>F</td><td>-</td></tr>
<tr><td>P</td><td>P_1</td><td>P</td><td>P_1</td><td>P</td><td>P_1</td></tr>
<tr><td>W</td><td>W_2</td><td>W</td><td>W_2</td><td>W</td><td>W_2</td></tr>
<tr><td>NMRR</td><td>-</td><td>NMRR</td><td>2</td><td>NMRR</td><td>a</td></tr>
<tr><td>인적안전 안전무결성등급 (SIL</td><td>안전요건이 필요하지 않음</td><td>환경피해 안전무결성등급 (SIL)</td><td>SIL 2</td><td>재산피해 안전무결성등급 (SIL)</td><td>특별한 안전요건이 필요하지 않음</td><td>(15) 요구수준 안전무결성등급</td><td>SIL 2</td><td></td></tr>
</table>