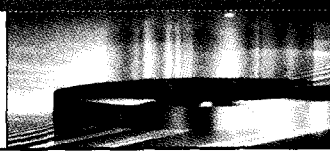


# 안전의 의미



글 · 정 국 삼 / 충북대학교 안전공학과, 교수  
e-mail · kschung@chungbuk.ac.kr

이 글에서는 안전을 과학 및 공학의 한 분야로서 하나의 학문 체계로 구축·정립함에 있어서의 이해를 돕기 위하여 안전(또는 위험)의 의미와 취급 내용에 대하여 간단히 기술한다.

안전이라는 단어는 '안전보증위원회'로부터 '원자력의 안전'에 이르기까지, 실제로 광범위한 분야에서 이용되고 있다. 물론, 여기에서는 공학의 분야에서의 안전에 한정하고 있지만, 이에도 제품안전에서부터 안전교육에 이르기까지 또한, 오래전부터 안전성냥, 안전유리 및 안전모 등 여러 곳에 사용되고 있는 것이다.

따라서, 안전을 과학 및 공학의 중요한 한 분야로서 하나의 학문체계로 정립하여 두기 위해서는 '안전(또는 안전성)'이라는 개념의 엄밀한 규정 즉, 안전에 대한 엄밀한 정의 및 고찰이 필요한 것으로서 여기에서는 이에 대한 이해를 돕기 위하여 안전의 기본적인 의미와 다루어지는 내용에 대하여 간단히 기술하여 보고자 한다.

## 안전의 의미

안전은, 간단한 뜻으로는 위험의 반대 개념으로, '위험하지 않은 것'이라고 해석할 수 있을 것이다. 그런데, 위험은 하나하나 지적될 수 있어도, 안전은 그것에 어떠한 위험도 존재하지 않는다고 하는 부정형으로 표현되는 개념이어서, 안전을 구체적으로 지적하기 곤란한 것이 안전의 정의를 어렵게 하고 있다.

여기에서는, 공학 분야의 정의로서 인간이 만든 '물건', 즉 시스템이나 기계 및 제품 등이 위험하지 않은 것을 의미하고 있는 것으로

한정하여 생각하기로 한다. 물론, 이들을 사용하는 경우뿐만 아니라 만드는 경우도 포함하고 있는 것으로 한다. 그렇다면, 위험하지 않은 것은 위험으로부터 무엇을 지키는 것인가? 물론, 지키는 대상은 분명히 '사람'이다. 직접적이든 간접적이든 간에 '사람에게 상해를 주지 않는 것'이 안전의 제1인 것이다.

그러면, '물건'(이후, 대표하여 시스템이라 부르기로 한다)은 어떠한 경우에 '사람에게 상해를 주는 것'일까? 그 원인은 ① 시스템 자체의 결함(고장, 설계 miss, 소프트웨어의 bug 등), ② 인간의 잘못(human error)(깜빡miss, 예견 가능한 오사용, 고의 등)을 생각할 수 있으며, 그 외에도 ③ 자연재해, 환경의 열화, 과부하 등을 고려할 필요가 있는 경우도 있다.

위에서와 같은 것이 원인으로 시스템에 장애가 발생하여, '사람에게 상해를 주는 것'의 경우, 일반적으로 사고가 일어났다고 한다.

그런데, 어느 시스템에서 이제까지 사고가 일어난 적이 거의 없다고 하여 그 시스템은 안전하다고 하는 것이 타당한 것인가? 사고가 일어나지 않게 수단을 강구하였기에 안전하다고 하는 '입증되고 있는 안전'과 지금까지 사고가 거의 일어나지 않았기 때문이라는 '경험적 또는 확률적인 안전'과의 사이에는 커다란 차이가 있다. 본래, 전자의 경우와 같이, 구조로서 안전을 집어넣게 하여, 그것이 입증되어 질 때만 비로소 그 시스템은 안전하

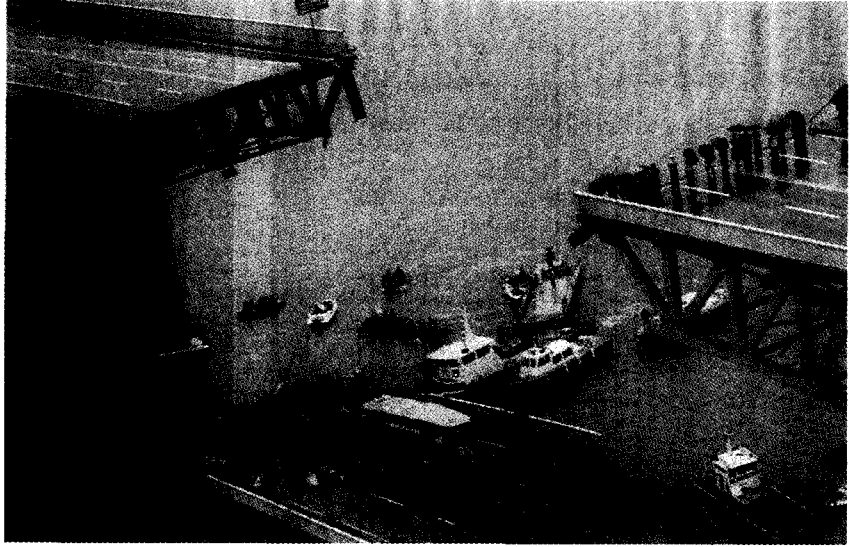
다고 할 수 있다.

이와 같이, 어느 '시스템이 안전하다' 함은, '그 자체 속에 고장 등의 결함이 있어도, 또한 인간 측에 잘못이 있어도, '사람에게 상해를 주지 않음'의 구조로 되어 있고, 그것이 입증되고 있는 것'으로 정의할 수 있다. 이러한 의미에서 안전모, 안전화, 또는 안

전면도기와 같이, 쉽게 '안전○○'이라고 하는 용어들의 사용은 피하여야 할 것이다. 이상은, 정성적 및 이념적인 관점에서의 확률론적인 안전의 정의이다.

한편, 기계안전 등의 공학 분야에서는 품질의 하나의 측면으로서, '안전(또는 안전성)'은 '사람에의 위해 또는 손상의 위험성이 허용 가능한 수준에 머물러지고 있는 상태' 또는 '받아들일 수 없는 위험으로부터의 해방'으로 정의되고 있다.

그리고 '위험(또는 위험성)'은 '주어진 상황 하에서 상해(자산 또는 환경상의 피해의 결과로서 직접 또는 간접적으로 인체가 받는 물리적 상해)의 발생확률과 상해의 크기와의 조합(곱)'으로 정의되고 있다. 따라서 안전은, 위험 측의 고장의 발생확률과 상해의 크기라고 하는 양의 개념을 이용한 정량적 및 현실적인 관점에서의 확률론적인 정의로 되어 있다. 이 안전의 정의에는, 받아들일 수 있



서울 성수대교 붕괴사고('94. 10. 21.)

는 위험의 존재를 처음부터 허용하고 있는 것은 현실적으로 타당한 정의라고 말할 수 있다. 그러나 안전을 실현하는 구조로 언급하는 것이 아니고 단지 위험의 평가에 따라 정의하는 것과, 위험을 어디까지 허용하는 가는 자의적으로, 해석의 여지가 있다고 하는 두 가지 관점에서 논의의 여지가 남아 있다.

이상, 두 가지 안전의 정의, 즉 정성적, 이념적의 확률론적인 정의와 정량적, 현실적의 확률론적인 정의를 소개하였지만, 양자의 관계에 대하여 해석하기 위해서는 좀더 구체적이고 안전에 대한 고찰이 필요할 것이다. 참고로, 컴퓨터 및 통신관계의 분야에서는, 안전은 security(비밀보장)의 것을 의미하는 것이기에 주의를 요하여야 한다.

## 안전의 공학적 취급

공학에서 안전을 취급하는 경우에는, 사람

에 따라 다른 개념으로는 처리할 수는 없다. 그러므로 일반적 개념에 가능한 한 가까운 객관량(예를 들면, 예상 빈도 또는 발생 빈도)으로써 안전성(또는 위험성)을 정의하고, 객관량으로써 안전성을 취급하는 것까지를 공학의 범위로 하여야 할 것이다. 즉, 조건을 주었을 때 안

전성이 얼마나 되는가를 구하거나, 안전성을 주었을 때 이를 만족하는 제반 조건을 구하는 것일 것이다. 따라서, 안전성을 사람이 어떻게 받아들이는 가는 심리학의 문제에서, 안전성을 얼마나 정하는 가는 정치의 문제에서, 그리고 안전성을 세상 사람들이 어떻게 받아들이고 어떻게 행동하는 가는 사회학의 문제에서 다루어져야 할 것이다. 물론 안전공학을 논할 때는 이들의 문제에도 관심을 갖고 처리를 하여야 하지만, 범위만은 명확히 하고, 공학의 범위 내에서 먼저 다루어져야 할 것이다.

### Fail Safe

위험은 하나하나 지적되지만, 안전에 있어서는 어렵다고 말하였는데, 실제, 안전에 관하여도 분명히 안전하다고 명확히 지정되는 경우가 있다. 그것은, 기계 및 열차의 경우에서 말하면, '정지한 것' 또는 '정지하여 있는



프랑스 드골공항 터미널 붕괴사고('04. 5. 24.)

것'이다. 전원이 끊어져있어 작동하지 않으면 기계에 다치는 경우는 없고, 달리고 있지 않으면 열차에 치이는 경우도 없다. 분명히 '안전'이라고 말할 수 있는 상태이지만 아쉽게도 여기에서는 본래의 기능을 발휘하고 있지는 않다. 따라서, 본래의 기능을 발휘하면서 동시에 안전한 것이 안전시스템의 본래의 목적인 것이다. 즉, 안전에는 실제로 두 종류의 것이 있는 바, 본래의 기능을 발휘하고 있지 않지만 안전한 상태인 정지안전과 본래의 기능을 발휘하고 있으면서 동시에 안전한 상태인 기계적 안전이 있다.

신호로 말하면, 적신호는 정지안전이고, 청신호는 기능적 안전을 나타내고 있다.

'정지안전이 존재하고 있는 시스템에서, 시스템 내에(당연히 안전장치 자체도 포함하여) 고장 등이 발생하여 정상 기능을 유지할 수 없게 되면, 언제나 정지안전에 고정하도록 즉, 안전 측의 장해밖에 발생하지 않도록 구

조적으로 구성된 시스템'이 fail safe system이다. Fail safe system에서는, 기능적 안전이든가 정지안전이든가의 두 가지 상태만 취할 수 있게 보증되어 있다. 정지안전이 존재하는 경우에는, 안전확인형이라는 시스템 구성과 비대칭 고장(비대칭 잘못) 소자를 이용하는 것에 의해, fail safe system을 실현시켜 주고 있음을 보여주고 있다.

그런데, 언제나 정지되면 안전이라고 하는 정지안전의 상태가 존재한다고만은 할 수 없다. 날고 있는 비행기와 같이 정지안전을 보여줄 수 없는 경우 및 컴퓨터 시스템과 같이 비대칭 잘못을 보증할 수 없는 경우에는, 기능적 안전을 어떻게 신뢰도 높게 실현하는가 하는 신뢰성에 의존하는 것밖에 없다. 장애가 생기면 위험측의 장애의 발생 가능성은 배제할 수 없어, 가능한 한 정상적인 동작을 유지하여 장애에 이르지 않도록 신뢰도 높게 만드는 것밖에 없다. 이것은 신뢰성을 바탕으로 하여 안전성을 실현하는 방법이다. 시스템을 신뢰도 높게 구성하는 방법에는, 구성부품의 신뢰도를 높이는 방법(fault avoidance)과 다중계 등의 용장성 기술에 의해 시스템 전체의 신뢰도를 높이는 방법(fault tolerance)이 대표적인 것이다.

참고로, 신뢰성과 안전성과의 차이에 대하여 간단히 언급하기로 한다. 신뢰성은 시스템의 본래 기능을 유지하는 능력이고, 안전성은 안전을 유지하는 능력인 것이다. 따라서, 신뢰성의 목적은 시스템 본래의 기능이고, 안전성의 목적은 안전 그것에 있다. 일반적으로, 신뢰성이 높으면 안전성도 높다고 하는 관계에 있지만, 신뢰성을 낮추어도 안전성을 올릴 수 있는 경우가 있다. 안전이 확인될 때까지는 비행기는 날 수 없고, 고장이 생기면 열차를 멈추게 하는 본래의 기능은 발휘하고 있지

않지만(=신뢰성은 낮음) 사람에게 상해를 주지 않음(=안전성은 높음)인 것을 생각하면 양자간에는 깊은 관계가 있지만, 본질적으로는 다른 개념인 것임을 알 수 있다.

## 안전성의 평가

기계는 절대로 고장이 없다고 하는 것은 있을 수 없고, 인간도 절대로 잘못하지 않는다고 하는 것은 있을 수 없다. 더구나, 자연재해도 언제나 예측할 수 있다고는 할 수 없는 것이다. 그렇기에, 이 세상에는 절대적인 것은 있을 수 없다고 생각된다. 따라서, fail safe에 구성된 것에서도 절대로 안전하다고 주장할 수는 없다. 수십 년에 한 번의 확률로 사고가 일어난다고 하여 절대로 안전하다고 하는 등의 주장은 논리적 모순이다.

그래서, 안전의 정도, 즉 안전성의 평가 또는 안전도라고 하는 개념이 불가결하게 된다. 신뢰성의 평가는 본래 행하는 기능을 발휘하는 확률을 의미하는 신뢰도로서 숫자적으로 엄밀히 정의되지만, 안전성에는 사람에 대한 상해의 크기를 어떻게 보는가 하는 가치관이 들어가기 때문에, 위험 측의 장애의 발생 확률만으로는 평가할 수 없다. 그렇기에, 위험의 개념이 필요하게 되는데, 위험이란 각종의 원인으로 시스템에 장애가 발생할 때, 이것이 사람에게 상해를 주는 확률(frequency ; 여기에서는 시스템의 장애가 위험 측의 장애인 확률 및 인간이 여기에 합쳐진 확률, 그리고 인간이 그것을 회피할 수 없는 확률 등도 고려하여 결정된다)과 그 장애가 실제로 발생하였을 때에 얼마나 큰 것(severity)인가의 정도의 조합(곱)으로 정의되고 있다. 그러나 실제로는 엄밀하게 수량적으로 정의하기는 곤란한 것이다.

현실적으로는, 위험을 몇 개의 등급으로 분류하여, 등급 IV(무시 가능 : negligible)이면 문제없이 안전으로 인식하고, 등급 III은 받아들일 수 있는(acceptable) 위험으로 안전한 시스템으로 이해하며, 등급 I은 도저히 받아들일 수 없는(unacceptable) 위험으로 위험한 시스템으로 한다. 그리고 등급 II가 안전한 시스템으로서 허용될 수 있는 (tolerance)가의 여부를, 그 때의 경제적, 문화적, 때로는 정치적인 사회적 요인에 의존하는 것으로 제안하고 있다. 이는 위험의 엄밀한 수량적 정의가 곤란한 것을 고려하면, 어쩔 수 없는 방법으로 생각된다.

기능적 안전만 존재하는 경우 및 소프트웨어를 저장한 컴퓨터에서 안전을 실현하고 자 하는 경우에는, 신뢰성을 근거로 가능한 한 기능적 안전의 실현을 목표로 할 수밖에 없다. 이 때, 이를 안전한 시스템이라고 할 수 있는가의 여부는 여전히 논의의 여지가 있다. 그러나 적어도 정지안전이 존재하여 fail safe로 실현될 수 있음에 도 불구하고 가격, 효율, 지식의 부족 등 때문에 구조적으로 안전을 편입하지 않고 신뢰성에 바탕을 둔 접근만으로, 등급 II 및 등급 III을 갖고 안이하게 안전하다 라고 말하는 것은 아무래도 피하여야 할 것이다.

## 위험의 구분

위험(risk)이란 '위해 또는 손실이 생길 염려가 있는 것'의 의미로 사전에 정의되고 있으며, 이와 같은 문제에 가장 밀접한 관계가 있는 손해보험업계에서는 일반적인 표현으로서 '무언가의 사건의 발생에 관하여 존재하는 불확실성'으로 정의하고 있다. 따라서 위험이라고 하는 개념은 손실 그 자체, 손실의 원인

인 사건, 손실의 확률과는 다른 것이다.

그리고 위험은 발생의 위험(if risk)과 시기의 위험(when risk)으로 나누어 볼 수 있다. 전자의 예인 공장재해는 이의 발생하는가의 여부는 불확실하여 손실 발생의 불확실성이 있다. 후자의 예인 사람의 사망으로 언제 사망하는 가는 불확정하여 시기에 관하여 불확정성이 있는데, 사람은 반드시 사망하기 때문에 발생의 위험은 존재하지 않는다.

그런데, 우리들이 일상적으로 사용하고 있는 위험이라는 단어는, 어느 때에는 발생 빈도(frequency)를 강조하기도, 손해 및 피해 정도(severity)를 문제시하기도 한다.

다만, 개인의 체험이나 성격에 따라 위험의 내용은 매우 달라지지만, 앞에서도 언급 한 바와 같이, 이들 발생빈도와 피해 정도의 곱의 값을 위험의 정도(또는 위험성)로 정의하여, 일상생활에서의 사고에 의한 사회적 위험 (social risk)의 척도로 일반적으로 나타내고 있다.

즉, 일정 기간 중에 발생한 손해나 피해 정도를 나타내는 것으로, 예를 들면, 작년 한 해 동안 국내에서, 교통사고로 8,500명이 사망하였다든가, 산업재해로 경제적인 총 손실액이 12조여 원에 이르렀다 하는 것이다. 이를 한 사람 당의 사회적 위험인 개인적 위험성 (personal risk)으로 하여(사망/년·인) 등의 단위로 위험의 정도를 나타내기도 한다.

또한, 사람은 위험이 수반됨에도 불구하고 자발적으로 행하는 능동적 위험과 생활 속에서 발생하는 수동적 위험으로 구분하여 나타내기도 하는데, 스포츠 활동이나 흡연은 전자의 예로서, 생활 속에서 일어나는 자연재해 및 인위재해와 같은 후자의 예보다 '사망/년·인'의 개인적 위험성의 값으로 비교하여 볼 때, 상대적으로 높게 나타나는데, 이는 사람

들 스스로가 무의식적으로 높은 위험을 감수하면서까지 스포츠나 흡연을 즐기고 있음을 알 수 있다.

한편, 위험을 수용 상태에 따라 다음과 같이 세 가지로 구별하여 사용하고 있다.

(1) 실재하는(de facto) 위험 : 위험이 실재하여 공중이 받아들여지고 있는 것으로서 자연재해의 발생 위험이 그 예이다.

(2) 받아들일 수 있는(acceptable) 위험 : 받아들일 수 있는 가치가 있다고 하는 의미를 말한다. 여기에는 그 주체를 전문가/정부의 입장에서 평가와 판정을 행하는 것으로서 공중의 수용(public acceptance : 일명 PA)이 얻어지거나 얻어지지 않거나 한다. 공중이 받아들일 수 없는 경우도 제반 수정책에 의하여 받아들여지고 있는 것도 있다. 이와는 반대로, 전문가/정부의 입장에서 받아들일 수 없는(unacceptable) 위험이라 판정하여도 흡연에 의한 폐암의 위험의 경우와 같이 공중에게 받아들여지고 있는(accepted) 경우도 있다.

(3) 받아들여지고 있는(accepted) 위험 : 이 위험에 대하여 PA가 이미 얻어지고 있는 경우, 이를 받아들여지고 있는 위험을 말하며, 반면에 PA가 얻어지지 않은 경우에는 받아들여지지 않는(unaccepted) 위험이라 한다.

이와 같이 정의하여 보면, 위험의 상태는 de facto, acceptable-accepted, unacceptable-accepted, acceptable-unaccepted, unacceptable-unaccepted risk의 5단계로 나누어 볼 수 있는 것이다. 그런데 위험의 실제의 수준과 공중의 수용성(PA)과의 사이에는 큰 차이가 있는 것으로 나타나고 있다. 예를 들면, 받아들여지고 있는 위험은 연간 사망률이 대략  $10^{-2} \sim 10^{-10}$ 의

범위의 값이고 대부분은  $10^{-4} \sim 10^{-8}$ 의 범위에 있다. 그리고 받아들여지지 않는 위험은 거의  $10^{-2} \sim 10^{-8}$ 의 범위의 값이다. 한편, 전문가/정부의 입장에서 판단하여 평가한 받아들일 수 있는/받아들일 수 없는 위험은 그다지 불합리한 것은 없이 각각 거의  $10^{-4} \sim 10^{-8}/10^{-2} \sim 10^{-5}$ 의 범위를 나타내고 있어, 서로가 일부 중복되는 경우가 있기는 하지만 구별되고 있는 것이다.

## 위험 - 편익법

위험이 비록 크다 하여도 편익이 크면 이를 용인하고자 하는 경향이 있다. 극단적인 예는 중병의 환자의 생명 연장에 위험이 큰 수술 및 처치를 행하는 경우이거나, 또는 말라리아가 창궐한 지역에서의 D.D.T의 사용 등인데, 이와 같이 편익에 따른 위험의 용인은 의지 결정의 그 시점, 그 사회에서의 가치관에 크게 지배되고 있는 것이다. 또한, 위험과 편익과의 비교에는 무엇을 행하거나 또는 행하지 않음으로써 생기는 위험도 포함된다. 미국 및 캐나다에서는 소프트드링크에의 사카린의 사용을 금지하고 있는데, 그 이유는 방광암을 일으키게 한다는 것인데, 그 대신으로 설탕의 사용에 따른 섭취에 의한 수명 단축(비만에 의한)의 위험이 오히려 보다 큰 값(약 100배 이상)을 초래하고 있다는 것이다. 이러한 관점에서 생각하면, 어느 쪽의 위험도 소프트드링크 대신에 물을 마시게 되면 줄일 수 있다고 하는 논리이기에, 결론적으로, 위험의 실제 정도와 공중의 수용성 간에 상관을 구하는 것은 비현실적 일 수 있어, 보다 폭넓게 종합적인 차원에서 영향인자를 검토하여 다루어져야 할 것이다.