Chapter 2

SAFETY DEFINITIONS AND TERMINOLOGY

9/7/2019

> "The real trouble with this world of ours is not that it is an unreasonable world, nor even that it is a reasonable one. The commonest kind of trouble is that it is nearly reasonable, but not quite. Life is not an illogicality; yet it is a trap for logicians. It looks just a little more mathematical and regular than it is; its exactitude is obvious, but its inexactitude is hidden; its wildness lies in wait."
>
> G. K. Chesterton

2.1 INTRODUCTION

The meanings of terms used in safety analysis depend on the contexts and the traditions of the different academic disciplines and the technical areas in which they are used. Quantifying these terms can be done using the tools of *probability theory* if they can be considered as random variables that lend themselves to measurements and observations.

If we need to quantify the meanings of linguistic variables, *possibility theory* rather than probability theory is the adequate tool to use for quantifying these variables which lend themselves to numerical simulation, modeling or expert interpretation.

A combination of random and linguistic variables constitutes an information quantum and can be adequately quantified for monitoring, control and decision-making purposes in terms of *coupled probability-possibility theory*.

2.2 SAFETY AND RISK

"Accident" is an undesired event that causes damage or injury. In the medical profession the term "injury" is preferred to "accident." In the medical profession, "accident" thus means an event that results or could result in "injury."

Different categories of accidents can be considered:

1. An accident with a direct consequence, such as a chemical explosion.
2. An accident resulting in an increased probability or possibility for injury or damage. An example would be the increased cancer risk from exposure to chemicals or to radiation.
3. Accidents resulting in degeneration such as the continuous occupational exposure to gases, chemicals, or noxious substances.
4. Accidents resulting from sabotage events caused by willful action. This includes acts of terrorism against civilians and noncombatant individuals or groups of individuals.

"Incident" is an undesired event that may cause damage or injury. The term: "near-accident" is often used to describe an "incident."

The word "transient" is also used to describe an "incident."

"Hazard" is a probable or possible cause of an accident. It could be an object or a situation, which constitutes a threat of loss. This loss could be economical, monetary, injuries, disease, morbidity or death.

"Risk" is the possibility or probability of an undesired consequence. It is often considered a function of probability and consequence. Sometimes it refers to the likelihood per unit time of injury, illness or death to people. It is also used when the outcomes are uncertain or not well defined. Some definitions of objective risk from the perspective of statistics are:

1. The probability of loss.
2. The size of the possible loss.
3. A function consisting of the product of the probability and the size of the loss.
4. The variance of the probability distribution of all possible consequences of a risky course of action.
5. The semi-variance of the distribution of all consequences, taken over negative consequences only, and with respect to some reference value.
6. A weighted linear combination of the variance and the expected value of the distribution of all possible consequences.

"Perceived risk" is, from the psychological perspective, a risk judgment that is an intuitive value judgment, which expresses a diffuse negative evaluation of a decision alternative. It could be a general feeling that a certain situation is undesirable.

"Safety" becomes then, not the opposite of risk as sometimes perceived, but its inverse. This can be expressed mathematically by defining safety as inversely proportional to the risk, or:

$$Safety \;\; \alpha_{\ell} \;\; \frac{1}{Risk} \qquad (1)$$

The proportionality sign in the previous equation, if a proportionality constant C is introduced, can replace the equality symbol:

$$Safety = \frac{C}{Risk} \qquad (2)$$

This expresses the notion that a high level of risk implies a low level of safety. A low risk value implies high safety.

2.3 RISK AND UNCERTAINTY

The difference between risk and uncertainty is that risk has a price. One can establish the probability of a loss, and price it. Life insurance, as an example, is a pricing mechanism for risk.

However one cannot price uncertainty. It must be incorporated in its different forms in the modeling and the calculation process of risk.

2.4 SECURITY AND SURETY

"Security" and "Surety" are composite information quanta, which describe the degree by which a desired safety or a risk level are achieved. For instance, one could measure the degree by which the following security or surety level is attained:

$$\text{Security} = \text{detection rate } \textit{is} \text{ high,} \tag{3}$$

$$\text{Surety} = \text{failure rate } \textit{is} \text{ tolerable.} \tag{4}$$

In general, an information granule g, can be defined as:

$$g \triangleq (X)\, is\, (Y) \tag{5}$$

where X is a measurable or observable quantity or random variable subject to the laws of probability theory, and Y is a linguistic variable quantifiable by simulation, modeling or expert opinion and subject to the laws of possibility theory.

2.5 PERFORMANCE LEVEL

In the definition of the information granule g in Eq. 5, X as random variable is represented by a probability density function (pdf) $p_X(u)$.

Similarly Y is a semantic or meaning associated with it as a fuzzy variable, and is represented by a membership function $\mu_Y(u)$.

For a discrete random variable, the performance level or the degree of truth of the proposition g can be calculated from:

$$PL = \sum_{i=1}^{n} \mu_{Yi}(u) p_{Xi}(u) \tag{6}$$

In the case of a continuous random variable, the summation is replaced as an integral as:

$$PL = \int_{u} \mu_Y(u) p_X(u) du \tag{7}$$

In either case, the performance level PL is the degree of truth of the proposition given by the information granule g, and is in fact the probability of the considered fuzzy event

EXAMPLE

If the fuzzy variable Y = “tolerable” is represented by the discrete membership function defined over the temperature range from 65-75 degrees:

$$\mu_Y = \begin{pmatrix} 1.0 & 1.0 & 1.0 & 0.0 \\ 65 & 70 & 75 & 80 \end{pmatrix},$$

and the following discrete probability density function represents X = “temperature level":

$$p_{X1} = \begin{pmatrix} 0.0 & 0.1 & 0.8 & 0.1 \\ 65 & 70 & 75 & 80 \end{pmatrix},$$

then we can calculate the performance level of the surety:

$$\begin{aligned} g &\triangleq (\text{X is Y}) \\ &\triangleq (\text{temperature level } \textit{is} \text{ tolerable}) \end{aligned}$$

from Eq. 6 as:

$$\begin{aligned} PL &= (1.0x0.0) + (1.0x0.1) + (1.0x0.8) + (0.0x0.1) \\ &= 0.0 + 0.1 + 0.8 + 0.0 \\ &= 0.9 \end{aligned}$$

We can conclude that temperature is tolerable to a degree of 90 percent.

On the other hand if our obtained measurement is described by the probability density function:

$$p_{X2} = \begin{pmatrix} 0.0 & 0.0 & 0.4 & 0.6 \\ 65 & 70 & 75 & 80 \end{pmatrix},$$

this yields the performance level:

$$\begin{aligned} PL &= (1.0x0.0) + (1.0x0.0) + (1.0x0.4) + (0.0x0.6) \\ &= 0.0 + 0.0 + 0.4 + 0.0 \\ &= 0.4 \end{aligned}$$

which implies that the temperature is tolerable only to a degree of 40 percent.

2.6 SAFETY AND SECURITY PERFORMANCE

Several traditional approaches exist to safety and security risk management. The recent approaches use standards blending performance based flexibility and risk assessment. New technology and management systems ensure that the risks are controlled in a dependable manner. However, accidents and incidents still occur and the engineering profession has the responsibility of raising safety ans security to the next higher level.

The steps to the next level are layered controls, effectively learning from accidents, evaluating and correcting process safety, the development of safety and security cultures within organizations and the development of methodologies for anticipating and predicting accidents from the observation of their precursors and thus preventing the occurrence of serious accidents rather than reacting to them.

EXERCISE

1. If the fuzzy variable Y = "tolerable" is represented by the discrete membership function:

$$\mu_Y = \begin{pmatrix} 1.0 & 1.0 & 1.0 \\ 0 & 5 & 10 \end{pmatrix},$$

Calculate the performance level of the security:

g = X *is* Y = Failure rate *is* tolerable,

for the following discrete probability density functions representing X = "failure rate" :

a) $$p_{X1} = \begin{pmatrix} 0.1 & 0.8 & 0.1 \\ 0 & 5 & 10 \end{pmatrix}$$

b) $$p_{X2} = \begin{pmatrix} 0.2 & 0.6 & 0.2 \\ 5 & 10 & 15 \end{pmatrix}$$

c) $$p_{X3} = \begin{pmatrix} 0.3 & 0.4 & 0.3 \\ 10 & 15 & 20 \end{pmatrix}$$

Plot the discrete functions and discuss the obtained results for the security performance levels.