Articles

The Concept of Probability in Safety Assessments of Technological Systems

GEORGE APOSTOLAKIS

Safety assessments of technological systems, such as nuclear power plants, chemical process facilities, and hazardous waste repositories, require the investigation of the occurrence and consequences of rare events. The subjectivistic (Bayesian) theory of probability is the appropriate framework within which expert opinions, which are essential to the quantification process, can be combined with experimental results and statistical observations to produce quantitative measures of the risks from these systems. A distinction is made between uncertainties in physical models and state-of-knowledge uncertainties about the parameters and assumptions of these models. The proper role of past and future relative frequencies and several issues associated with the elicitation and use of expert opinions are discussed.

PROBABILISTIC RISK ASSESSMENT (PRA) OR PROBABILISTIC safety assessment (PSA) is a method that has evolved during the last 20 years. Its aim is to produce quantitative estimates of the risks associated with complex engineering systems such as nuclear plants, chemical process facilities, waste repositories, and space systems. The identification of the most likely failure scenarios and the major sources of uncertainty is an essential part of PSA.

Despite the considerable advances that have been made and the widespread use of PSA in some fields, there are still controversies and misunderstandings surrounding its use. Engineers and physical scientists are asked to deal with methods that require considerable use of subjective judgment, and, because they are unaccustomed to such mixing of "objective" facts with "subjective" judgments, they are left with the feeling that the whole exercise lacks scientific rigor. The few engineers who have taken courses on probability and statistics in their college days find that their notion of probability as the limit of a relative frequency is challenged by the requirements of a PSA for a real system and by the fact that major accidents are rare.

The purpose of doing a PSA is to make decisions regarding the safe operation of a facility. Expected utility theory provides the framework within which decisions can be analyzed in a formal manner and in accordance with several reasonable principles (*1, 2*). We can consider the decision problem as consisting of four major elements: (i) structuring the problem, (ii) quantifying uncertainties, (iii) quantifying preferences, and (iv) making the decision (choosing among alternatives). The first element (problem-structuring) lays the foundation upon which one performs further analysis by building models for the physical world and developing alternative courses of action. The second element requires the introduction of probabilities and their calculus. The preferences (third element) are expressed in terms of utilities and, finally, the decision criterion is the maximization of the expected utility (fourth element). A person who follows this procedure in decision-making and whose probabilities comply with the theory of probability is a coherent decision maker (*1–3*).

For major societal decisions that involve many decision makers (or, more accurately, many stakeholders), formal decision theory breaks down. Because this theory guarantees coherence of the probability assignments and preferences of a single decision maker, two decision makers may be individually coherent and still be unable to agree and reach the same decision. In these situations the last two elements of the decision problem, that is, the quantification of preferences and the maximization of expected utilities, are replaced by ad hoc decision-making criteria that are widely debated and, ultimately, imposed by the regulatory authority. The proposed containment requirements for radioactive waste repositories (*4*), various criteria for nuclear power reactors (*5*), and criteria for chemical facilities (*6*) are such ad hoc decision-making criteria.

Problems with multiple stakeholders also arise in the process of quantifying the uncertainties. For rare events, such as those investigated in safety assessments, the evaluation of probabilities requires the exercise of considerable judgment. Probability theory guarantees that an individual making an assessment will be coherent but cannot force consensus between two different analysts. They may each be coherent and they may still disagree. (Some researchers postulate that, given the same information, scientists should agree on their inferences; if the purpose of such a tenet is to encourage dialogue and the dissemination of information, there can be no argument against it. However, in order to accept this tenet as a scientific principle, one would have to define criteria that would determine under what conditions several individuals have the same information, and this is a nearly impossible task.) In spite of these limitations, probability theory is still the only rational way that is available to us for handling uncertainty.

The Conditional Model of the World

The first step in doing a PSA is to structure the problem, which means to build a model for the physical situation at hand. We refer to this as the model of the world. [The "world" is defined as "the object about which the person is concerned" (*7*, p. 9); we may

The author is professor of Engineering and Applied Science in the Mechanical, Aerospace, and Nuclear Engineering Department, University of California, Los Angeles, CA 90024.

occasionally refer to it as the "model" or the "mathematical model."] It is built on a number of model assumptions and on a number of parameters whose numerical values are required.

An essential part of problem structuring in most PSAs is the identification of accident scenarios (event sequences) that lead to the consequence of interest, for example, system unavailability, the release of hazardous materials, and so forth. Many methods have been developed to aid the analysts in such efforts, for example, failure modes and effects analysis, hazard and operability analysis, fault tree analysis, and event tree analysis (*8*). These analyses consider combinations of failures of the hardware and operator actions during maintenance as well as during accidents, fires, and natural phenomena, such as earthquakes and tornadoes. Their product is the set of causes or consequences, or both, of postulated failures of systems or components.

The development of scenarios introduces model assumptions and model parameters that are based on what is currently known about the physics of the relevant processes and the behavior of systems under given conditions. For example, the failure modes of equipment during given earthquakes, the calculation of heat fluxes in a closed compartment where a fire has started, and the response of plant operators to an abnormal event are all the results of conceptual models that rely on assumptions about how a real accident will progress. These models include parameters whose numerical values are also assumed to be available (for example, in the case of fires, the heat of combustion of the burning fuel, the thermal conductivity of the walls of the compartment, and so forth); that is, observable or measurable quantities. A simple example involves the Darcy equation for ground-water flow in saturated media

$$q = -K\frac{\partial h}{\partial x} \tag{1}$$

where q is the specific discharge in the x direction, h is the hydraulic head, and K is the hydraulic conductivity.

Equation 1 is the model of the world in this example. Its parameter is K, and the use of this model is conditional on the assumption that the numerical value of the hydraulic conductivity is known. In a realistic calculation, Eq. 1 is part of a system of coupled differential equations modeling the convective-dispersive transport of radionuclide chains that form the model of the world. Their solution requires computer codes such as the Sandia Waste Isolation Flow and Transport code (*9*).

We can generalize the above example and write the solution of the conditional model of the world as $G(\phi|M, H)$, where ϕ is the vector of input parameters (for example, the hydraulic conductivity of Eq. 1), M is the set of model assumptions that define the model, and H is the entire body of knowledge and beliefs of the modeler. [A closed-form expression may not be available, as is the case with computer codes, where $G(\phi|M, H)$ is understood to be the solution that is produced numerically by the code.] This notation makes explicit that the solution of the model is a function of the model parameters, the values of which must be given, and is conditional on the model assumptions and on the modeler's current state of knowledge.

We are now ready to discuss the uncertainties associated with the conditional model of the world. The state-of-knowledge uncertainties are the numerical values of the parameters and the model assumptions of the conditional model of the world.

State-of-Knowledge Uncertainties

The model of the world assumes that the numerical values of its parameters are known and that its model assumptions are true. Since there is usually uncertainty about these conditions, we introduce the state-of-knowledge (subjective) probability density function (PDF) $\pi(\phi, M|H)$, which expresses our beliefs regarding the numerical values of ϕ and the validity of the model assumptions. The lognormal distribution is used frequently in safety studies for the parameters. The PDF for a variable K is given by

$$\pi(k|\mu, \sigma) = \frac{1}{\sqrt{2\pi}\,\sigma k}\exp\left[-\frac{(\ln k - \mu)^2}{2\sigma^2}\right] \tag{2}$$

where $0 < K$; $-\infty < \mu < +\infty$, $0 < \sigma$. (K denotes the uncertain variable, and k denotes the value of this variable). Specifying the numerical values of the parameters μ and σ determines the lognormal distribution. It is the positive skewness of this distribution that plays an important role in the decision to use it as the state-of-knowledge PDF for the hydraulic conductivity of a waste repository site (*9*). It is stated that "viable candidate sites will probably have conductivities near or below the low end of the range, and the choice of a lognormal distribution ensures several values" (*9*, p. 29).

The subjective interpretation of the concept of probability tells us that probability is a measure of degree of belief (*1–3*). The primitive notion is that of "more likely"; that is, we can intuitively say that event A is more likely than event B. Probability is simply a numerical expression for this likelihood (additional assumptions are needed for the rigorous definition of probability). When we say that event A has probability 0.6, we mean that A is more likely than every event whose probability is less than 0.6. A set of probabilities that complies with the theory of probability is a coherent set. (It is interesting to note that the standard axioms of the mathematical theory of probability are satisfied by subjective probabilities; we are simply adopting an expanded theory that starts with the primitive notion of likelihood.)

This interpretation of probability is not based on relative frequencies and does not require many identical trials. It would be awkward to use relative frequencies for events such as the truth or falsehood of model assumptions. For example, in some instances we know that an accident will progress in one of two ways, say A or B, but we do not know which one, and we express our belief in terms of a probability. The probability $p(A)$ is not to be interpreted as the limit of the relative frequency of occurrence of A in many repetitions of the accident. We know that either A or B will always occur, so this relative frequency interpretation is inappropriate.

Returning to the example of hydraulic conductivity, we recognize that the uncertainty about its values stems from not knowing the characteristics of the site (this is usually the case for "generic" studies). As more information is gathered about the site and its hydraulic properties, the subjective distribution must be adjusted to reflect the corresponding state of knowledge. It should be evident that relative frequencies have no place in this example. The selection of a repository site (and, consequently, the hydraulic conductivity value) has nothing to do with large numbers of "trials."

The Unconditional Solution of the Model

We are now in a position to produce an unconditional solution of the model of the world by finding the weighted average of the solution of the conditional models where the weights are the probabilities of the parameter values and the assumptions. For a discrete set of n models, which is likely to be the case, we write

$$\bar{G} = \sum_{i=1}^{n}\left[\int G_i(\phi_i|M_i, H)\,\pi_i(\phi_i|M_i, H)\,d\phi_i\right] p(M_i|H) \tag{3}$$

where $G_i(\phi_i|M_i, H)$ is the solution of the ith conditional model and

$\pi_i(\phi_i|M_i, H)$ is the PDF of the parameter vector ϕ_i of the ith model. The factor $p(M_i|H)$ is the analyst's probability that the ith model (set of assumptions) is true.

Uncertainties in the Model of the World

Many important phenomena in safety assessments cannot be modeled by deterministic expressions like Eq. 1; for example, the occurrence times of earthquakes of given magnitudes cannot be predicted. Various stochastic models have been proposed in the literature to calculate the probability of some event of interest. A simple model that calculates the probability of r events occurring in a period of time t uses the Poisson distribution

$$h(r \text{ events in } t|\lambda, t, M, H) = \frac{e^{-\lambda t}(\lambda t)^r}{r!} \quad (4)$$

The principal model assumption is that the interarrival times (that is, the times between successive events) are independent. The constant rate λ of occurrence of the events is the only parameter that may be uncertain, thus requiring a state-of-knowledge distribution $\pi(\lambda|M, H)$. Distributions that appear in the model of the world, such as Eq. 4, are sometimes called frequency or statistical distributions by PSA practitioners, so that they can be distinguished from state-of-knowledge distributions.

Our example of the hydraulic conductivity provides an excellent illustration of the subjective nature of these models and how practical considerations create the need to modify the conditional model of the world and, consequently, the subjective distributions of its parameters and model assumptions. The model of Eq. 1 in the context of the overall model for ground-water flow, is a simple one. It ignores stochastic variability and allows for state-of-knowledge uncertainties only. The hydraulic conductivity may display large scatter across a site due to spatial variations of rock properties (*10*). To model this phenomenon, we abandon the previous simple model and we expand the conditional model of the world to include spatial uncertainties. The hydraulic conductivity is now a function of space $K(x)$. (For simplicity, we consider the one-dimensional case only.)

A possible model of the world is now the following set of equations

$$q(x) = -K(x)\frac{\partial h}{\partial x}$$

$$\gamma = \ln k \quad (5)$$

$$f(\gamma_1, \gamma_2|\mu, \sigma, \rho)$$

$$\rho(x_1 - x_2) = e^{-|x_1 - x_2|/\lambda}$$

where

$$f(\gamma_1, \gamma_2|\mu, \sigma, \rho) = \frac{1}{2\pi\sigma^2\sqrt{1-\rho^2}} \exp\left[\frac{(\gamma_1-\mu)^2 - 2\rho(\gamma_1-\mu)(\gamma_2-\mu) + (\gamma_2-\mu)^2}{2\sigma_2(1-\rho^2)}\right] \quad (5a)$$

The first equation in this new model is the Darcy equation, Eq. 1. The second expression is simply the definition of the logarithm of the hydraulic conductivity. The third expression, given explicitly as Eq. 5a, is the bivariate normal distribution for the logarithm of the hydraulic conductivity evaluated at two points in space, x_1 and x_1. The bivariate distribution is shown for simplicity; for many spatial points, the appropriate multivariate normal distribution would be used. The fourth expression in the set of Eqs. 5 is the model for the spatial variability of the correlation coefficient ρ that appears in the bivariate normal distribution (*11*). The other two parameters μ and σ are defined similarly to those appearing in Eq. 2. In addition to the assumptions behind the Darcy equation, this mathematical model includes two new assumptions: that the values of the logarithm of the hydraulic conductivity at any two points in space are distributed according to the bivariate normal distribution and that the correlation coefficient of this distribution is an exponential function of the distance between these two points. The bivariate normal distribution is the model for the uncertainty, that is, the spatial variability of the hydraulic conductivity, that is part of this expanded conditional model (in our terminology, it is a frequency distribution). The state-of-knowledge model will involve multivariate distributions for the parameter vector (μ, s, l), as well as for the corresponding model hypotheses.

Since the conditional model now contains probability distributions, its solution will also be in the form of a probability distribution. It is, therefore, necessary to abandon the expression $G(\phi|M, H)$ that represented the solution of the model without uncertainties and to introduce $h(A|\phi, M, H)$ as the conditional probability distribution of the event of interest A that results from solving the conditional model of the world. When A is a discrete event, $h(A|\phi, M, H)$ is understood to be a probability mass function [a trivial example is afforded by Eq. 4, where A is the event (r events in t)]. When A is a continuous variable, $h(A|\phi, M, H)$ is understood to be a PDF (as an example, the solution of Eqs. 5 will be the PDF of the specific discharge q, which will be A in this case.) The unconditional solution is derived similarly to Eq. 3, that is,

$$\bar{h}(A|H) = \sum_{i=1}^{n}\left[\int h_i(A|\phi_i, M_i, H)\,\pi_i(\phi_i|M_i, H)d\phi_i\right] p(M_i|H) \quad (6)$$

A similar situation is encountered in PSAs for nuclear power plants. A simple model for the failure time of a component is the exponential distribution with PDF as follows

$$f(t|\lambda, M) = \lambda e^{-\lambda t} \quad (7)$$

with $\lambda > 0$ and $t > 0$. This model of the world is conditional on the failure rate λ (not to be confused with the correlation length of Eq. 5) and on the assumption that this rate is constant. The lognormal distribution (Eq. 2) is the state-of-knowledge distribution that is widely used for the failure rate, a practice that has been established by the pioneering Reactor Safety Study (RSS) (*12*). The RSS has developed such lognormal distributions for a number of components; the principal source of uncertainty is considered to be "plant-to-plant variability," the variation of performance caused by the different conditions that prevail at various plant sites.

As data concerning the failures of equipment from various plants are gathered, the need arises to account explicitly for the plant-to-plant variability. If the parameters of the lognormal distribution for λ are allowed to vary, the lognormal distribution becomes part of the conditional model of the world; that is, it becomes a frequency distribution (*13*). Comparing this case to the hydraulic conductivity example, we recognize that it is the desire to account explicitly for the spatial variability of K that creates the need to move the lognormal distribution to the conditional model of the world, whereas in the failure rate case it is the desire to account explicitly for the plant-to-plant variability of λ. The similarity of the two cases stops there, however, as the failure rate case does not use multivariate distributions, such as that of Eq. 6 (*13*).

These examples illustrate the kinds of subjective judgments that are required of analysts and also show how practical needs can generate adjustments to the model of the world. These adjustments (for example, treating the lognormal distribution of the hydraulic

conductivity or of the equipment failure rate as part of the model of the world and not as a subjective parameter distribution) are allowed because probability is fundamentally the same concept regardless of whether it appears in the model of the world or in the subjective distributions for the parameters. There is only one kind of uncertainty stemming from our lack of knowledge concerning the truth of a proposition, regardless of whether this proposition involves the possible values of the hydraulic conductivity or the number of earthquakes in a period of time. The distinction between the conditional model-of-the-world probabilitie, for example, Eq. 4, and the probabilities for the parameter $\pi(\lambda|\mu, s)$ in the same example is merely for our convenience in investigating complex phenomena. Probability is always a measure of degree of belief. While we will discuss the proper role of relative frequencies later, it is important at this time and in light of the confusion that persists in practice to clearly state that there is only one logical and workable interpretation of probability and it is that of degrees of belief.

The Role of Relative Frequencies

When the model of the world does not contain uncertain quantities, relative frequencies are irrelevant. The parameters of the model are usually parameters with physical interpretations, and the only justification for repeated observations is the presence of measurement errors. In the absence of such errors, a single observation can remove the state-of-knowledge uncertainty and determine precisely the value of the parameters.

When the model of the world contains uncertain quantities such as the occurrence times of earthquakes or the failure times of equipment, Bayes's theorem tells us how past observations influence our current state-of-knowledge distributions.

In order to understand the proper role of relative frequencies, we must consider the issue of how new evidence E changes our current state of knowledge. The only condition that is imposed on us is to update our probabilities according to the rules of the theory of probability. The rule of conditional probabilities gives the conditional probability of an event A given that we have received evidence E

$$p(A|E) = p(A)\frac{p(E|A)}{p(E)} \tag{8}$$

Equation 8 shows how the prior probability $p(A)$, the probability of A prior to receiving E, is modified to give the posterior probability $p(A|E)$, subsequent to receiving E. The likelihood function $p(E|A)$ demands that we evaluate the probability of this evidence assuming that the event A is true. Equation 8 is the basis of Bayes's theorem, which is so fundamental to the subjectivistic theory that this theory is sometimes referred to as Bayesian theory.

Returning to Eq. 6, we use the idea of Eq. 8 to update the probabilities of the models and their parameter distributions as follows (*14*)

$$p(M_i|E) = \frac{\int h_i(E|\phi_i, M_i)\pi_i(\phi_i|M_i)d\phi_i}{\sum_{i=1}^{n}[\int \pi(\phi_i|M_i)h_i(E|\phi_i, M_i)d\phi_i]p(M_i)} p(M_i) \tag{9}$$

and

$$\pi_i(\phi_i|M_i, E) = \frac{h_i(E|\phi_i, M_i)}{\int \pi_i(\phi_i|M_i)h_i(E|\phi_i, M_i)d\phi_i} \pi_i(\phi_i|M_i) \tag{10}$$

Comparing Eqs. 8 and 9, we recognize that

$$p(E|M_i) = \int h_i(E|\phi_i, M_i)\pi_i(\phi_i|M_i)d\phi_i \tag{11}$$

This integral is the probability of the evidence assuming that the ith model is correct. (Note that, for simplicity, in Eqs. 9–11 we have dropped H, since it appears everywhere.)

Equation 10, which updates the parameter distributions of the ith model assuming that this model is the right one, is the form of Bayes's theorem that is usually found in standard textbooks (*15*).

In the case of "perfect knowledge," all of the uncertainty regarding models and parameters has been eliminated and the subjective distributions of the parameters are determined by relative frequencies. However, the uncertainty that is part of the conditional model of the world is still present. For example, we still do not know when the next earthquake will occur, even though we know the value of the rate of occurrence. Similarly, the time of the next radioactive decay cannot be known, even though both the model (exponential) and its parameter (decay constant) are known for a given species.

The preceding discussion referred to the proper use of past observations. The question now is what the values of future relative frequencies are going to be. The laws of large numbers tell us that we should expect these frequencies to be close to the corresponding probabilities. For example, given that we know the rate λ and that the assumption that it is constant is true, we can calculate the probability of r earthquakes occurring in an interval $(0, t)$ using Eq. 4. If we now consider a great many such intervals for which the same rate is valid, we expect the relative frequency of such intervals where r earthquakes occur to be close to the probability of Eq. 4. This is a consequence of the theory of probability and is not a definition of probability.

This result is useful in practice when future relative frequencies will, in fact, be observed within some reasonable time. In safety assessments, however, we are typically dealing with rare events, and the laws of large numbers are not of any particular usefulness. What matters is whether a given nuclear power plant or a given repository of hazardous wastes will harm people or the environment in a given period of time. Our decisions concerning the safe operation of such facilities are based on probabilities that quantify our knowledge about possible failures of these unique facilities during these specific time periods. Relative frequencies at this level can only be parts of thought experiments. Even if long historical records have led us to assess the numerical values of the parameters of the models with high accuracy, as discussed in the preceding comment, we are still using probabilities for well-defined unique events of the future, that is, in the degree-of-belief sense.

The ideas that we have discussed, which are based on a pure Bayesian viewpoint, have been presented in practice in various forms and to various degrees of accuracy. In one form, uncertainties that appear in the conditional model of the world, or Type 1 uncertainties, are considered to be the result of the stochastic variability of some random variable. The case of no random variables is considered limiting (*16*). This is consistent with our framework, although the model of the world is more general in that it does not need to contain random variables. Another source proposes to adopt the classical (relative frequency–based) interpretation for the irreducible uncertainties in the "building blocks of the PSA" (that is, the conditional model of the world) and the subjectivistic interpretation for the reducible uncertainty about parameter values and the validity of models (*17*). In our framework, probabilities, regardless of where they appear, are always measures of degrees of belief. The relationship between future frequencies and probabilities is properly understood within the laws of large numbers.

The proper use of the parameters of distributions that appear in

the conditional model of the world, in particular the rate of the exponential distribution or of the Poisson distribution, has been debated in the literature. For example, in the nuclear power safety arena, almost all accidents are discussed in terms of their rate of occurrence per year. Even probabilistic safety criteria have been formulated in terms of the rate of nuclear reactor core damage or of major release of radioactivity. Of course, it may happen that decisions based on rates may be inconsistent with decisions based on expected utilities [a related example demonstrates inconsistencies between decisions based on expected values and on the conditional model of the world with point values for the parameters (*18*)]. This extraordinary attention to rates has led some researchers (*19, 20*) to emphasize that these rates are fictional parameters, and that they should not be tied to relative frequencies. On the other extreme, it has been asserted that these rates can be measured (at least in principle) and that the purpose of a PSA is the identification of accident scenarios and their rates (*21*). To emphasize the difference between probability and frequency, the term "frequency" is used exclusively for these rates. The state-of-knowledge probability distributions of the parameters are called "probability-of-frequency" curves (*21*).

Although it is true that these rates, like all parameters of models, are intermediate quantities that are eventually averaged out as shown in Eq. 3, they are no more fictional or less useful than other rates, such as the hydraulic conductivity or the speed of a car. In other words, they are quantities that can be assessed, and what we know about them is expressed by our state-of-knowledge distribution. In the case of radioactive decay constants, this distribution is very narrow (for a given radionuclide) and, because we are confident that our model is correct and we realize that we cannot influence the values of these constants, we consider them as physical properties of the radionuclides. The situation is very different for the rates of major technological accidents because we have considerable uncertainties regarding both models and numerical values of their parameters. It would be unreasonable to consider these rates as physical constants, mainly because we can influence them, for example, by making the systems safer. The proper role of these parameters in a decision problem is summarized in Eqs. 3 and 6.

Expert Opinions

The judgment of analysts is prevalent in PSA. Because the events or phenomena of interest are usually very rare, thus lacking significant statistical or experimental support, the opinions of experts acquire great significance. Engineering judgment, which is another, more traditional, name for expert opinion, has always played an important role in engineering work but now the use of judgment is made very visible and formal. The framework that we have discussed allows us to see where the analysts' judgment is utilized and how. Objections have been raised to the use of these models in PSAs for major technological systems (*22, 23*), but no PSA has been performed to date that does not use subjectivistic methods [although very few analysts (*24, 25*) state explicitly that they are using Bayesian methods]. "The bottom line is that the quality and quantity of more-or-less relevant available data for use in a PSA is almost never of the precise form and format required for using classical statistical methods" (*26*, p. 401).

Physical scientists and engineers do not object to the theoretical foundations of Bayesian probability theory, but they are uncomfortable with the extensive use of judgment that PSAs require (*27*). The problems related to the elicitation and use of judgment have been recognized and investigated (*28–30*).

An assessor of probabilities must be knowledgeable both of the subject to be analyzed and of the theory of probability. The normative "goodness" of an assessment requires that the assessor does not violate the calculus of probabilities, and that he or she does make assessments that correspond to his or her judgments. The substantive "goodness" of an assessment refers to how well the assessor knows the problem under consideration (*31*). It is not surprising that frequently one or the other kind of "goodness" is neglected, depending on who is doing the analysis and for what purpose. The fact that safety studies usually deal with events of very low probability makes them vulnerable to distortions that eventually may undermine the credibility of the analysis.

Direct assessments of model parameters, like direct assessments of the event rates, should be avoided, because model parameters are not directly observable (they are "fictional"). The same observation applies to moments of distributions, for example, the mean and variance.

Intuitive estimates of the mode or median of a distribution are fairly accurate, whereas estimates of the mean are biased toward the median (*32*). This has led to the suggestion (*33*) that "best" estimates or "recommended" values, which are often offered by engineers, be used as medians. In assessing rare-event frequencies, however, the possibility of a systematic underestimation or overestimation ["displacement bias" (*29*)], even of the median, is very real.

Assessors tend to produce distributions that are too narrow compared to their actual state of knowledge. In assessing the frequency of major accidents in industrial facilities, it is also conceivable that this "variability bias" (*29*) could actually manifest itself in the opposite direction; that is, a very conservative assessor could produce a distribution that is much broader than his or her state of knowledge would justify.

Probability assessments tend to be more representative of the analysts' state of knowledge when formal methods are used. Even when formal methods are used, however, one should be cautious when very low probabilities and frequencies are produced. The completeness of an analysis that yields very low numbers is always an issue. For engineered safety systems, skepticism is expressed about probabilities of failure smaller than 10^{-5} per demand when these numbers are not supported by strong statistical evidence. It is suggested that human error probabilities smaller than 5×10^{-5} are "unlikely to exist" (*34*). In a more general context, frequencies smaller than 2.5×10^{-10} per year are considered meaningless (*35*). For geological events, frequencies less than 10^{-11} per year correspond to events that are virtually impossible if one uses the age of the earth as a yardstick (*36*). All of these numbers are reference points, not rigid bounds.

These observations about the accuracy of expert opinions are important when we quantify our own judgment and when we elicit the opinions of experts. In one study (*33*), Bayes's theorem is used to combine statistical evidence concerning equipment failures from a facility with prior distributions for these failure rates. These prior distributions are derived from expert opinion polls (*12, 37*). In some cases, the posterior distribution lies mainly in the tail region of the prior distribution on the high side, suggesting that these expert opinion-based distributions are biased toward low values of the failure rate (a more fundamental problem may be that the experts have been asked to estimate failure rates directly).

The practice of eliciting and using expert opinions became the center of controversy recently with the publication of a major risk study of nuclear power plants (*38*). This study considers explicitly alternate models for physical phenomena that are not well understood and solicits the help of experts to assess $p(M_i|H)$ (Eqs. 3 and 6). Objections have been raised both to the use of expert opinions (with complaints that voting is replacing experimentation and hard science) and to the process of using expert opinions (for example,

the selection of the experts). The latter criticism falls outside the mathematical theory that I have been discussing and is not of interest here; however, the view that voting replaces hard science is misguided. The probabilities $p(M_i|H)$ of Eqs. 3 and 6 are an essential part of the decision-making process. A formal mechanism exists (Eq. 9) to incorporate available evidence into $p(M_i|H)$. Unfortunately, many decisions cannot wait until such evidence becomes available, and assessing $p(M_i|H)$ from expert opinions is a necessity. (Incidentally, such an assessment may lead to the decision to do nothing until experiments are conducted.) The elicitation and use of expert opinions in safety studies and risk management is an area where attention will be focused in the near future (*39–42*).

Conclusions

We have discussed a rational probabilistic framework for the assessment of the risks from technological systems. The question that immediately arises is why this framework is not universally accepted. A major reason must be the lack of a strong statistical background of most engineers (*43*). What complicates matters is that simple, albeit often ad hoc, methods do provide "point" parameter values that are within the uncertainty range that a more rigorous analysis would produce.

Bayesian methods are often identified with the extensive use of personal judgments, the implication being that the methods of relative frequency–based statistics are more objective. Judgment and expert opinions are required because safety assessments must deal with rare events. The issue, therefore, is how to process this judgment and how to combine it with observations and frequencies. To achieve this, one applies the rules of the subjectivistic theory of probability; that is, one must be coherent, which is synonymous with being objective. These methods are not a panacea. For example, the most controversial part of using expert opinions, that is, selecting the experts, is outside the theory and requires processes similar to those for establishing decision-making criteria for major societal issues that involve several stakeholder groups. However, after these opinions have been received, they must be processed coherently, according to the rules that we have discussed.

REFERENCES AND NOTES

1. D. V. Lindley, *Making Decisions* (Wiley-Interscience, New York, ed. 2, 1985).
2. M. H. De Groot, in *Accelerated Life Testing and Expert Opinions in Reliability*, C. A. Clarotti and D. V. Lindley, Eds. (North Holland, Amsterdam, 1988), pp. 3–24.
3. B. De Finetti, *Theory of Probability* (Wiley, New York, 1974), vols. 1 and 2.
4. Code of Federal Regulations, Title 40, Part 191 (Environmental Protection Agency, Washington, DC, 1985).
5. *Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria* (International Atomic Energy Agency, Technical Report IAEA-TECDOC-524 Vienna, Austria, 1989).
6. M. F. Versteeg, *J. Hazard. Mater.* **17**, 215 (1988).
7. L. J. Savage, *The Foundations of Statistics* (Dover, New York, ed. 2, 1972).
8. *Guidelines for Hazard Evaluation Procedures* (The American Institute of Chemical Engineers, New York, 1985).
9. R. M. Cranwell *et al.*, *Risk Methodology for Geologic Disposal of Radioactive Waste: Final Report* [U.S. Nuclear Regulatory Commission, Report NUREG/CR-2452 (SAND81-2573), Washington, DC 1987].
10. R. M. Cranwell *et al.*, *Proceedings of the Nuclear Energy Agency Workshop on Uncertainty Analysis for Performance Assessments of Radioactive Waste Disposal Systems*, Seattle, WA, 24–26 February 1987 [Organization for Economic Cooperation and Development (OECD), Paris, 1987], pp. 18–29.
11. R. A. Freeze *et al.*, *Proceedings of the Conference on Geostatistical, Sensitivity, and Uncertainty Methods for Ground-Water Flow and Radionuclide Transport Modeling*, San Francisco, CA, 15–17 September 1987 (Battelle Press, Columbus, OH, 1989), pp. 231–260.
12. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants* [U.S. Nuclear Regulatory Commission, Report WASH-1400 (NUREG-75/014), Washington, DC, 1975].
13. S. Kaplan, *IEEE Trans. Power Appar. Syst.* **PAS-102**, 195 (1983).
14. A.F.M. Smith, *Statistician* **35**, 97 (1986).
15. D. V. Lindley, *Introduction to Probability and Statistics from a Bayesian Viewpoint*, Part 2, *Inference* (Cambridge Univ. Press, London, 1970).
16. E. Hofer and F. O. Hoffman, *Proceedings of the Nuclear Energy Agency Workshop on Uncertainty Analysis for Performance Assessments of Radioactive Waste Disposal Systems*, Seattle, WA, 24–26 February 1987 (OECD, Paris, 1987), pp. 132–148.
17. G. W. Parry, *Reliab. Eng. Syst. Saf.* **23**, 309 (1988).
18. C. A. Clarotti, *ibid.* **20**, 117 (1988).
19. _____, in *Reliability Engineering*, A. Amendola and A. Saiz de Bustamante, Eds. (Kluwer Academic, Dordrecht, Netherlands, 1988), pp. 49–66.
20. R. A. Howard, *Risk Anal.* **8**, 91 (1988).
21. S. Kaplan and B. J. Garrick, *ibid.* **1**, 11 (1981).
22. R. G. Easterling, *Nucl. Saf.* **22**, 464 (1981).
23. L. R. Abramson, *Risk Anal.* **1**, 231 (1981).
24. Pickard, Lowe, and Garrick, Inc., Westinghouse Electric Corporation, Fauske & Associates, Inc., "Indian Point probabilistic safety study," prepared for the Power Authority of the State of New York and Consolidate Edison Company of New York, Inc. (Pickard, Lowe, and Garrick, Inc., Newport Beach, CA, 1982).
25. Pickard, Lowe, and Garrick, Inc., "Seabrook Station probabilistic safety assessment," prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company (Pickard, Lowe, and Garrick, Inc., Newport Beach, CA, 1983).
26. H. F. Martz and R. A. Waller, *Reliab. Eng. Syst. Saf.* **23**, 399 (1988).
27. Special Issue on the Interpretation of Probability in Probabilistic Safety Assessments, G.E. Apostolakis, Ed., *ibid.* (no. 4).
28. A. Tversky and D. Kahneman, *Science* **185**, 1124 (1974).
29. C. S. Spetzler and C.-A.S. Staël von Holstein, *Manage. Sci.* **22**, 340 (1975).
30. M. W. Merkhoffer, *IEEE Trans. Syst. Man Cybern.* **SMC-17**, 741 (1987).
31. R. L. Winkler and A. H. Murphy, *J. Appl. Meteorol.* **7**, 751 (1968).
32. C. Peterson and A. Miller, *J. Exp. Psychol.* **68**, 363 (1984).
33. G. Apostolakis, S. Kaplan, B. J. Garrick, R. J. Duphily, *Nucl. Eng. Des.* **56**, 321 (1980).
34. A. D. Swain and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications* (U.S. Nuclear Regulatory Commission, Report NUREG/CR-1278, Washington, DC, 1983).
35. C. Starr, R. Rudman, C. Whipple, *Annu. Rev. Energy*, **1**, 629 (1976).
36. P. E. Gretener, *Am. Assoc. Pet. Geol. Bull.* **51**, 2197 (1967).
37. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations* (Institute of Electrical and Electronics Engineers, IEEE Std-500, New York, 1977).
38. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, (U.S. Nuclear Regulatory Commission, Report NUREG-1150, Draft, Washington, DC, 1989).
39. R. M. Cooke, *Reliab. Eng. Syst. Saf.* **23**, 277 (1988).
40. A. Mosleh, V. M. Bier, G. Apostolakis, *ibid.* **20**, 63 (1988).
41. E. J. Bonano, S. C. Hora, R. L. Keeney, D. von Winterfeldt, *Elicitation and Use of Expert Judgment in Performance Assessment for High-Level Radioactive Waste Repositories* (U.S. Nuclear Regulatory Commission, Report NUREG/CR-5411, Washington, DC, 1990).
42. D. V. Lindley, in *Accelerated Life Testing and Expert Opinions in Reliability*, C. A. Clarotti and D. V. Lindley, Eds. (North Holland, Amsterdam, 1988), pp. 25–57.
43. A. Penzias, *Science* **244**, 1025 (1989).

44. Supported by Sandia National Laboratories and by U.S. Nuclear Regulatory Commission grant NCR-04-89-357.