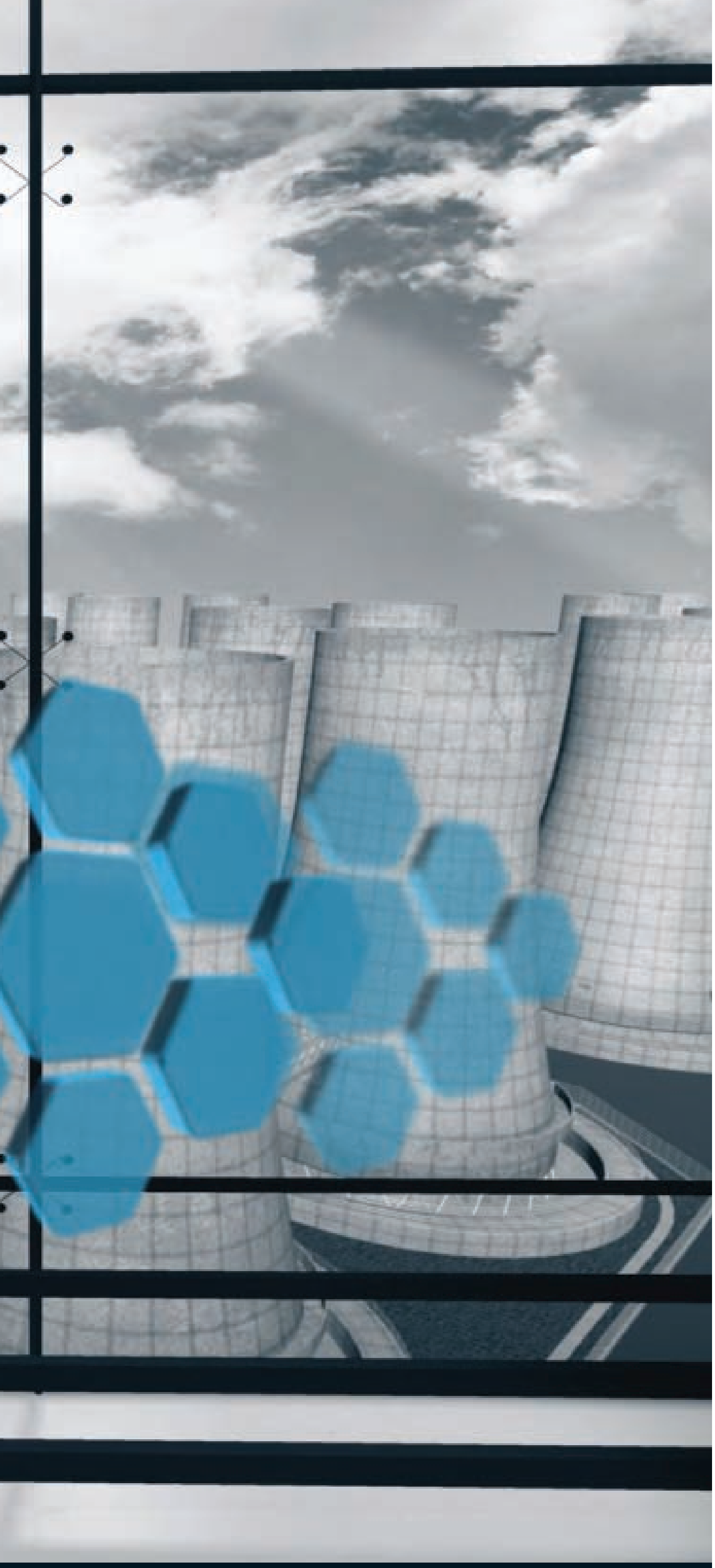
A FUTURE AT



BUCHACHON/123RF STOCK PHOTO

RISK

Nuclear and other forms of power will have difficulty gaining public acceptance until we all have a more complete understanding of the risks involved.

BY ROMNEY DUFFEY

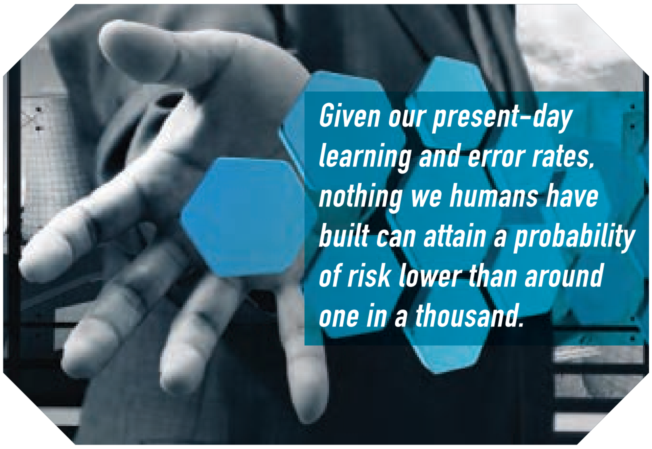
If one is inclined to look for them, the headlines are filled with death and danger from global energy use. In recent years, there have been the meltdowns and explosions at Fukushima, major oil spills in the Gulf of Mexico, gas pipeline fires in California, mine explosions, and other disasters. Less obvious, but no less due to energy use, are the thousands of related everyday casualties: both directly from automobile accidents, airline crashes, train derailments, gas leaks, and coal mining, and indirectly from industrial plant accidents and emissions.

Not every accident garners the same reaction. The shrug that's given to a gas leak or a car crash implies that the risks of existing within modern society are tolerated *and* even ultimately beneficial in some way. But this implicit acceptance exists only until the risks are no longer *perceived* to be safe or environmentally acceptable,

Romney Duffey is a physicist and expert on risk analysis and founded DSM Associates in Idaho Falls after retiring as principal scientist at Atomic Energy of Canada Ltd. Duffey is an ASME Fellow and a former chair of ASME's Nuclear Engineering Division.

irrespective of the actual potential presence of future harm, danger, or exposure.

Certainly, the risk from energy systems, energy production, and energy use is low. But societies do not have a unified and universal measure of what constitutes acceptable risk. The attitude to risk varies with the activity, history, technology, and the regulatory or legal framework. This is already well known and documented in the study of risk analysis and is unlikely to change towards some more rational basis. Clearly related to self-preservation, personal experience, and our perceptions, most people accept some necessary everyday risks, such as driving a car, ignore others like living in an earthquake-prone area, pursue some by, say, buying stocks, and reject others like not jumping off a cliff.



Given our present-day learning and error rates, nothing we humans have built can attain a probability of risk lower than around one in a thousand.

The risk from nuclear energy use poses special questions, as its potential radiation threat is unseen and not very well understood by the public. This is rather like electricity itself, which in its earliest days was even perceived as some unknown threat or hazard. Should the risk from an energy source be compared to natural disasters such as floods or earthquakes? Or to the risks of other technologies? Or to some legal or societal norm or standard?

Up to now, nuclear technology risk has been accepted under the general heading of “adequate health and safety protection for the public.” Attempts to define the “boundaries” or regions between acceptable/tolerable and unacceptable/intolerable risks have traditionally been based on the consequences—namely of the numbers of deaths, injuries, releases, or equivalent or actual costs, and the frequency of how often these events may occur. The regions and the boundary are both difficult to define, let alone implement.

Relative risk has been suggested by some as a measure of acceptability. One could compare the number of deaths from a nuclear accident to deaths from lightning strikes, or multiply the probability of an accident by its consequences to get an indicator.

Because of human errors and blunders, actual events occur that exceed these nominal limits, causing outcry, recrimination, inquiries, negative press, and even more regulations. Such rare events or “black swans” are so unexpected that often we do not prepare for them. So it is difficult to define a clear boundary while acknowledging the real uncertainties due to the finite significant probability of a rare event.

In recent years, this sort of unaccounted-for risk has been most closely associated with the world of finance; financial assets were created and sold by banks without a full understanding of how they might fail. Risky assets were reclassified as safe, used as the underpinning for other assets which were then repackaged as safe investments. Because of the poorly understood nature of the risks involved, it only took a relatively small number of financial reversals to wreak havoc on the global economy.

Superficially, the trends and outcomes from rare events in energy systems and technologies worldwide are different from the risks involving massive financial defaults, crises, and losses. But all technological and transactional systems share the common involvement of human learning and risk-taking when goods, products, and services are involved. The same issues of planning and preparedness against the unknown risk or rare event is the objective of risk assessment and safety management in the nuclear, aircraft, and oil and gas industries, as well as in the financial and military sectors. And we may apply the same method of simply finding an estimate for the probability of any size loss as a function of the risk exposure in order to determine the required dynamic response and management actions to reduce—or at least contain—the consequences.

Preparedness for the unexpected is necessary, and is often termed barriers, procedures, or firewalls. We as engineers can never be certain that an unexpected accident will not occur in spite of our best efforts at safety improvement and risk reduction, because we as engineers can never be certain that an accident will not occur. It’s better to have one hundred well-thought-out plans of action that are never implemented than to fall back weakly on the old excuse that “no one could have predicted” a catastrophe.

Zero risk is an impossibility. But to reduce the risk of an accident as much as possible, it’s first necessary to characterize it as completely as possible. The field of risk analysis has some useful mathematical tools for doing that.

The uncertainty of the risk of any event, whether a giant global tsunami or a local gas leak, is given by its probability or chance. Through observations of events as different as power outages, insurance claims, and stock market losses, it’s been found that the probability density function leading to a loss often varies according to a well-known empirical power law:

$$f(\varepsilon) = K/h(\varepsilon)^{q+1}$$

The terms in that formula are: ε as the measure of the accumulated experience or risk exposure, h as the magnitude of the loss, and K as a constant. The term in the exponent, q, typically varies between 2 and 3 based on the outcome of studies of actual events.

In principle, the q value represents the potential loss magnitude dependency on the "shape" function of risk exposure. In this case, the risk exposure, ε, is actually also a function of the loss, $h(\varepsilon)$. Since, by definition, $f(\varepsilon) = dp/d\varepsilon$, the probability of any outcome with damage or loss of at least h is then given by integration of $f(\varepsilon)$ as:

$$p(\varepsilon) = K/n\, h^q$$

Simply put, the greater the damage or loss, the lower the probability. But the probability also depends on the risk exposure and the number of prior outcomes or events. This form of relation, known as a standard Pareto or inverse "power law," underestimates the risk or probability for rare events when extrapolated beyond the set of observations it's based on, due to the "fat tail" from the influence of inevitable human risk-taking and uncertainty.

The well-known bathtub curve is a combination of two similar, but opposite effects: the results of learning from experience, which decreases the likelihood of accident, and the problems arising from extrapolating beyond the limits of our operational experience, which drives up risk. The minimum risk is at the bottom of the bathtub—the crossover point when the downside and upside probabilities are equal.

Equating these present and future loss risk probabilities, this minimum risk occurs at a risk exposure, ε_{mo}, given by

$$\varepsilon_{mo} = (n/k\lambda_m)^{1/2}$$

where for rare events, $n \approx 1$, with the learning or risk reduction rate, k, and the minimum attainable outcome or loss rate, λ_m. Equating the risk exposure or experiences at the crossover when the probabilities are equal, the minimum achievable risk is a probability,

$$p_{mo} = 1- \exp(\lambda_m /k)^{1/2}$$

Expanding the exponential provides a useful expression for the minimum probability,

$$p_{mo} \approx (\lambda_m /k)^{1/2}$$

That working approximation gives results that are numerically indistinguishable in accuracy for rare events or low failure or event rates.

These new results suggest that the minimum attainable risk exposure and probability are solely and uniquely a function of two known and physically based parameters. Fortunately—or unfortunately—from global data for energy systems and from other multiple industries for millions of accidents and events, we already know estimates or ranges for the values for systems with human involvement. Prior universal studies of systems with human involvement, which include financial markets, transactions, and firms as well as industrial systems, the typical values are a learning constant of $k \sim 3$, and a minimum attainable loss rate or frequency of $\lambda_m \sim 5 \times 10^{-6}$ per unit of risk exposure.

These two universal parameters show that the risks are dominated by the human contribution—things such as mistakes, errors, risk-taking, inexperience, and so on—rather than independent mechanical failures. The average interval between global financial crises and busts also agrees with these estimates. For the first, rare, or any subsequent event where n equals 1, $p_{mo} \sim 1.29 \times 10^{-3}$, corresponding precisely to the intercept values for a full theoretical solution.

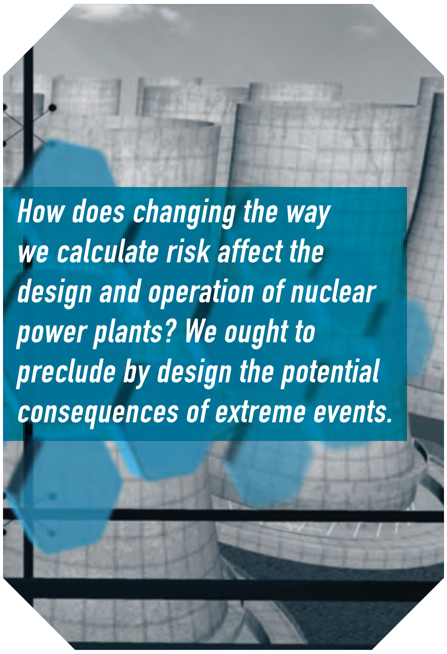
To step back from the mathematics, the plain English version is this: Given our present-day learning and error rates, nothing we humans have built, whether it's a banking system, a transportation system, or an energy system, can attain a probability of risk lower than around one in a thousand. What does a one-in-a-thousand risk look like? The probability of the events that destroyed the reactors at Fukushima—namely, a large tsunami or "natural" hazard occurring once a millennium—is on the order of one in a thousand. The probability of large, uncontrolled leaks due to the blowout of an offshore drilling rig, such as occurred on the *Deepwater Horizon*, is also on the order of one in a thousand, perhaps slightly lower.

It has been pointed out that with both Fukushima and the *Deepwater Horizon*, the loss of life was small compared to everyday accidents. What that assurance misses is that the environmental, political, and social impacts of both accidents were enormous—far greater than the mathematics of risk may have predicted.

What were the major impacts from Fukushima and from *Deepwater Horizon*? Those accidents put people in fear and trepidation of potential harm, even at large distances away, when the actual risk is negligible. There was also societal fear and media reinforcement of possible extensive damage to homes and the environment, which can cause social disruption, trauma, and even evacuations. Of course, these accidents *did* also produce actual economic, financial, and social consequences, with losses in energy production, corporate value, and business markets. And there was a consequential reduction of public confidence in political, industrial, and social institutions.

Fukushima is the most prominent recent example, but it is common that during so-called extreme events, the many physical and procedural barriers that guard against large, uncontrolled environmental releases from an energy system are bypassed, made inoperable, or are proven ineffectual. When the public is exposed to such releases (whether it's radioactive material, toxic sludge, or some other pollutant) it sows fear, uncertainty, and adverse public reaction.

The metric of expected deaths—or probability of release or severe-damage consequence—that is used to define the boundary of acceptable risk doesn't accurately capture the range of outcomes from this kind of "black swan" event. And thus, that metric ought not to be the sole basis for the design.



How does changing the way we calculate risk affect the design and operation of nuclear power plants? We ought to preclude by design the potential consequences of extreme events.

The key outcome from extreme events is the importance of risk assessment and human decision-making during emergencies that challenge the existing design basis. In particular, an overall safety program must go beyond the expected to the unexpected. There needs to be a structured risk review in planning changes during the (many) phases of operations and emergency actions. And adequate knowledge and measurement of accident conditions must be conducted by qualified instruments to ensure informed decisions and correct actions.

It is vital that the designers and operators of nuclear facilities use probabilistic-based analysis as part of the safety case and risk assessment to define and quantify potential event scenarios. Such analyses enable everyone to identify and prioritize the risks from and in management, design, maintenance, and operation; and to assist decision-making for estimating the future risk and consequences of the many phases and aspects of operation. Additionally, such analysis can help define the qualifications, procedures, controls, training, skills, and knowledge needed for risk-critical aspects; and help to provide guidance to management and operators on relative risks and consequent potential losses and define mitigation and safety measures.

Therefore, in light of the multiple and far-reaching consequences of the Fukushima accident, one of the most important roles for probabilistic-based analysis is to define uncertainties so as to ensure employee and corporate safety, to assure environmental preservation, and to attain public and political trust.

The uncertainty of an extreme event happening—and its fiscal costs, political damage, and social consequences—can be defined using probability and consequence measures. But the risk of such an event is not given by the often-used formula, probability times consequence. Nor is it found via the more sophisticated means of defining a negatively sloped risk boundary between acceptable and unacceptable risks. Instead, the best method for finding this risk is by calculating the total integral risk due to all possible exposure to releases, fears, damages, and social and political disruption. We can also derive the exact expression for relative social risk using a social damage relation.

How does changing the way we calculate risk affect the design and operation of nuclear power plants in particular? First, and perhaps most critically, we ought to preclude by design measures and margins the potential consequences of extreme events that lead to severe damage.

Designs, policies, and safety management must address extreme and rare events that may almost defy our imagination. Such technical issues for consideration include: resistance to presently unforeseen failure combinations; preclusion and/or mitigation of core melting; reduction or avoidance of the potential for hydrogen explosions; extensive use of natural circulation for long term cooling; assurance of ultimate heat sinks to ensure continued heat rejection; ability to withstand almost indefinite loss of power; availability of back-up systems for restoring power and cooling; elimination and avoidance of significant offsite radioactive releases in accidents; and comprehensive emergency management and public communication. Based on such comprehensive risk-informed analyses, the systems and designs evolving in the nuclear energy future may indeed be different from those of the past.

In addition, we will need to adopt integrated relative risk as a measure for all technologies with extreme events as a means to quantify social-consequence costs and impacts. Equally important is the creation of a learning environment at all of the operational, regulatory, managerial, political, and social levels to help promote assurance of societal acceptance. The goal is restoration of perceived public and political acceptance and trust.

For too long the nuclear industry has struggled to gain wide public acceptance, in part because it has misunderstood the true nature of the risk nuclear power plants present. If nuclear power is going to play a role in meeting the myriad energy challenges of the 21st century—and I and others strongly believe it must—then the industry has to embrace a risk model that integrates not just potential loss of life but social, economic, and political costs as well. Let it begin now! ■