Taking Action to Prepare Society for Catastrophic Risks

B. John Garrick
Roger L. McCarthy
Taking Action to Prepare Society for Catastrophic Risks

B. John Garrick1
Roger L. McCarthy2

B. John Garrick Institute for the Risk Sciences
University of California, Los Angeles
September 2015

1Founder, UCLA B. John Garrick Institute for the Risk Sciences and retired CEO and Chairman of PLG, Inc.
2Senior Fellow, UCLA B. John Garrick Institute for the Risk Sciences, Principal of McCarthy Engineering, and formerly CEO and Chairman of Exponent, Inc.
Will human beings make it through the next century?

It’s not a frivolous question. Barring a cataclysm that would make the question irrelevant, the answer is “yes.” The real question is how much unnecessary suffering are we going to endure?

Catastrophic risks are not something that most people seriously think about. The human race has all too often addressed disasters only after they happen. There are always more immediate concerns, and the public is becoming increasingly inured to predictions of disaster caused by everything ranging from Y2K to pandemics that never materialize. Unfortunately, disaster fear is fueled by news media hyperbole and entertainment industry fantasies, so potential catastrophes are sensationalized to the detriment of their rational consideration. Even the three simultaneous core meltdowns at Fukushima during the Great East Japan Earthquake of 2011 produced nothing close to the China syndrome or any other apocalyptic casualty scenario popularly associated with nuclear energy.

The stark reality is the human race is at catastrophic risk, more than ever before. Besides threats that have always been with us – and, sadly, always will be – such as plagues, mass warfare, or natural disasters, we are living in an ever denser and thus more fragile urban concentrations, as the 2004 and 2011 tsunamis and the 2005 Hurricane Katrina so painfully illustrated. We also have much greater interconnection, as SARS (severe acute respiratory syndrome) also painfully illustrated. More dense urban population centers provide greatly increased leverage for these long known natural catastrophes to create mass casualties.

In addition, burgeoning technologies have the potential for creating catastrophic events. Advances in artificial intelligence, nanotechnology, biological engineering, and even particle physics are occurring at an exponentially growing rate, with implications that are breathtaking, and certainly with some unintended and unknown consequences. Fueled by Moore’s law3 in computer power and by the expansion of Internet access to virtually the entire world, these and other technologies present challenges that are serious now and could become catastrophic in the not-too-distant future. Unfortunately, popular culture has too often caused this field to be occupied with holocaust fantasies of everything from plagues (too many zombie movies to count), to earthquakes (innumerable, but most recently “San Andreas”) and takeovers by computers/robots (n+1 “Terminator” movies), etc. Asteroids? Genetically modified organisms? Aliens? Let’s not go there. Making catastrophe the subject of so much fiction with little technical accuracy measurably impacts the public perception of catastrophic risk (Satpathy and Smith, Undated) and thus makes more challenging the rational quantification and serious scientific consideration of such risks.

DEFINING CATASTROPHE

Technically, what is a catastrophe? In the book, “Quantifying and Controlling Catastrophic Risks” (Garrick, et al., 2008) catastrophe is defined as an event that results in 10,000 or more fatalities, but there probably should not be such a specific threshold. Nor should fatalities be used as the only measure of damage for defining catastrophic risks. Fundamentally, a catastrophe is an event that creates human suffering on a massive scale, and people can suffer more by not dying. Rather than a threshold number for fatalities, the definition of catastrophe should include events that have the potential for widespread suffering, and these include events that create widespread injury, destruction, population displacement, contamination, environmental damage, and significant health effects. This definition now includes extraordinary natural events and engineered system failures having the potential to release large quantities of toxic and hazardous materials that can reach highly populated areas. Examples are chemical (e.g., Bhopal) and petroleum production and processing facilities, and nuclear power plants.

We’ve got to think about credible catastrophic risks now – many of which are not a question of if, but only when – if we don’t want to be at their utter mercy in the future as we have been too often in the past. We need to rank catastrophic risks since we can’t afford to completely mitigate every one; we need to analyze the cost/benefit tradeoffs of mitigation efforts; and we need to make rational decisions about how to manage mitigation efforts and their consequences to get the maximum bang for our buck. Now is the time for the systematic and scientific evaluation of these potential threats and what we know, or don’t know, about them, as well as what we are going to do, or not do, about them. More specifically, what planning and cost-effective measures are we going to do now to reduce some or most of the loss and suffering when the threats occur? By the time they are upon us, it is too late.

If we’re wise enough to do this, the risk sciences will play a key role. The B. John Garrick Institute for the Risk Sciences has been established at the University of California, Los Angeles (UCLA) to help facilitate that role, particularly with respect to our efficient preparation for potentially catastrophic events.

---

3Moore’s law has to do with the time it takes to double the number of transistors per square inch on integrated circuits. The estimated doubling time has varied over the years, with the most recent value being announced by Intel as approximately 2.5 years.
THE RISK SCIENCES

What are the risk sciences (i.e., the sciences of risk)?

To fully understand what we mean by the risk sciences we need to be explicit on what we mean by risk. For now we simply use the Merriam-Webster dictionary definition of risk: “The possibility that something bad or unpleasant (such as an injury or a loss) will happen.” Later we will specialize the definition, and provide an example of an analytical framework for quantifying the risk of a nuclear power plant.

Of course, risk has different meanings to different individuals and institutions. To the insurance community, risk is applied on the basis of past experience to the potential financial loss associated with lives, health, assets, products, and operations. Financial risk is the core issue of both the insurance business and Wall Street. Public health risk generally relates to the harmful effects that can come to individuals or populations and their environment. Risks to public health and safety and the environment are the Garrick Institute’s major areas of focus.

The Institute’s strategy is to emphasize activities that have the highest payoff in terms of avoiding or minimizing catastrophic human health and safety consequences, including reducing the likelihood or impact of possible but highly unlikely existential events as well as events that could lead to catastrophic reduction in the population of the human species. With such an emphasis comes the need to embrace methods of analysis that account for either limited or no recorded experience with the events being considered; that is, there has to be much greater reliance on the uncertainty sciences to bring credibility to the risk investigations. While catastrophic risks are the near term emphasis of the Garrick Institute, benefits are also expected on how to cope with lesser risks. One goal of the Institute is to create a general theory of quantitative risk assessment that can be applied to essentially any kind of risk.

Focusing on catastrophic risks and attempting to prioritize our efforts to address them introduces many challenges having to do with public perception and risk communication. One of those is the use of credible risk measures or attributes or damage states. A risk measure has to do with the event itself, containing some form of damage (consequence) indicator, and how that event is numerically represented. Since real catastrophes usually involve some combination of fatalities, injuries, environmental and property damage, toxic substance exposure, and undesired system states, in most cases it is necessary to use multiple risk measures to fully represent the risk of a complex system. An example is given later where nine risk measures were employed to characterize the risk of a large nuclear power plant. The good news is that methods currently exist to track multiple risk measures simultaneously.

The risk sciences involve, in one way or another, almost every other scientific and engineering discipline. Fundamentally, the risk sciences are rooted in logic, economics, and plausible reasoning. In assessing a threat, the first questions are: What is the likelihood of such an event, and how serious would the damage be? But that’s just for starters.

In application, the risk sciences can involve almost any other discipline, from human behavior, medicine and biology to all kinds of engineering, game theory, environmental and earth sciences, and physics. Risk analysis is a powerful tool, with an almost unlimited range of applications.

The humanities are also involved, because if risk analysis is to have any impact, there must be effective, credible communication, and it must be clear enough to be broadly persuasive. Left to their own intuition, without information and education, most people make bad decisions about risk, only made worse by the media and entertainment industry depictions. Unfortunately, people worry more than they should about very serious but very unlikely risks, such as a large meteor striking the earth, and less about the chance that the Yellowstone Caldera will erupt, which is also highly unlikely in any given year, but is believed to have a much shorter and more predictable recurrence interval. This is misguided, because events with apocalyptic consequences are not equally probable, even if they are extremely unlikely to occur in any given year. And what we can do about them is even more disparate. People often obsess over certain small but scary risks, such as sharks, airplane crashes, or nuclear accidents, while ignoring far more powerful potential killers, such as automobiles, bad nutrition, or maybe . . . Middle East Respiratory Syndrome (MERS). With better communication and education, our limited resources – our money and brainpower – can be better directed.

This is exciting and deeply important work. The risk sciences can provide context for virtually all the resource allocation we do as a civilization, from our scholarly work to our most dangerous systems and our approach to nature. They can help us deal in a logical way with climate, warfare, government, and law. As we race forward with a variety of radical new technologies, the risk sciences could help to influence this work in a more productive, and hopefully less risky, way.

The Garrick Institute will promote better understanding of the risk sciences, will aid in the development of the risk sciences, and will further the application of the risk sciences to a variety of catastrophic threats. The Institute’s activities will be limited only by the imagination, but it’s expected that they will include collaborations with internationally distinguished groups, education programs, symposia and technology exchange, methods development, risk assessment applications, and independent reviews of risk related activities.
QUANTIFYING THE RISKS

A common goal of all of the institutes and organizations engaged in the risk field is to increase the awareness of the risks to society, especially those risks having the potential for catastrophic consequences. The need is for the development of technologies that will enhance our fundamental understanding of the risks, including the quantification of their likelihood of occurrence. While there is a growing level of knowledge about what might be referred to as the physics of most of the catastrophic events we face, there are methods and applications for quantifying the risks and making transparent what is prudent and necessary to manage them.

Perhaps the biggest challenge in risk analysis is how to numerically represent a rare catastrophic event with unaccountably complex consequences, since these occurrences are often beyond anyone’s memory. Developing probabilities of the magnitude and timing of a catastrophic event is the goal. For a catastrophic event for which there is limited information, event frequency is generally the preferred risk measure. People are generally comfortable with the use of frequency, or perhaps its inverse – a recurrence interval (e.g., the 100-year flood that seems to occur every decade or so). And while frequencies don’t specifically indicate the “when” of catastrophic events, they do provide insights on the recurrence interval or how often to expect events. More importantly, frequency assessment provides a means of putting a number on what is known about the event. While there is less mystery with the concept of a frequency than there is with a probability, there is still the matter of uncertainty in the frequency and how to represent that uncertainty. The solution to this problem is to introduce the concept of probability of frequency. That is, represent the uncertainty in the frequency with a probability distribution based on the totality of the supporting evidence.

For our purposes, probability is defined as the credibility of a hypothesis, based on the totality of the supporting evidence. The scale of the probability is 0 to 1 with 0 being complete certainty that the event will never occur and 1 being that the event will occur with certainty. Defining probability and the probability of frequency in this manner facilitates its use in quantifying the risk of systems for which there is limited information. Obviously, the Garrick Institute will seek refinements on risk measures and the definition of the input parameters.

The probability-of-frequency idea makes transparent the uncertainties involved in catastrophic risk prediction. This approach to measuring risk has largely put to rest the notion that probabilities cannot be developed for rare events. They can. And developing these probabilities will be a major initiative of the Garrick Institute. The probabilities may reflect more uncertainties than desired, but can still provide an important calibration of just how good our state of knowledge is about an event. It makes transparent the analysts’ representation of the evidence and provides a basis for measuring the value added of continued research.

One potential catastrophic risk where quantitative methods have made some inroads is the threat associated with a nuclear power plant core meltdown. While the evidence is strong that Western nuclear plant accidents do not really represent global threats, thanks to Chernobyl with its lack of containment, they are perceived as having the potential for a catastrophic event. The U.S. nuclear power industry and regulators have evolved in how they assess the risk of a nuclear power plant accident. This evolution has put a great deal of focus on quantifying the “likelihood” of accidents, an indicator often missing in safety assessments of complex systems.

The spinoff from the nuclear power risk assessments and similar work in the aerospace and other industries have fueled considerable movement towards risk-informed and risk-based accident assessments in such other fields as the chemical, petroleum, and transportation industries; defense, medicine, food safety, natural events and the general processing and handling of toxic and hazardous materials. Thus, there are signs of progress in assessing and managing technological risk. Offsetting these gains is the uncertainty of the risks associated with new cyber, bio, and nanotechnologies. Because of the limited human experience with these technologies, there is a tendency to think that even if their risks had the potential for catastrophic consequences, they would be so rare as to not warrant serious and priority consideration.

The fact that the sciences are new and their risks may indeed not be rare simply does not register with the general population and our leaders. The conclusion that catastrophic consequences from new sciences or technologies are extremely unlikely is without scientific evidence.

We simply don’t know what we don’t know about the risks of the emerging new sciences. Serious and rigorous investigation may reveal their likelihood to be far greater than such rare natural events as large asteroids impacting earth. While quantitative risk assessment is now routinely being applied to selected complex systems such as nuclear power plants, the catastrophic and at least potentially existential risk of the new sciences is largely void of significant in-depth scientific investigation; the possible exception being the rare-event analyses of natural events that are considered in a comprehensive risk assessment of nuclear power plants. Society tends to give priority to events directly experienced, even though the much less frequent events about which no movies have been made may have far greater catastrophic impacts. In most cases, catastrophic risks have extremely long recurrence intervals, providing the misleading comfort that “it won’t happen in my lifetime.”

The good news is there is increasing interest in being more quantitative about risk. The growing number of texts and major reports on risk is evidence of this interest. Examples referenced are Alkowitiz, 2008; Bernstein, 1996; Fullwood, 2000; Garrick, 2008; Haines, 1998; Helton, 2014; Lewis, 1990; McCormick, 1981; and Molak, 1997. Risk assessment of engineered systems in particular has greatly matured over the
past 50 years under such names as probabilistic risk assessment, probabilistic safety assessment, and quantitative risk assessment. While there is an active community engaged in the risk field and there is growing evidence of its benefits, there are impediments to society receiving the full benefit of a more aggressive development of the risk sciences. Though there can never be complete assurance as to the safety of complex facilities like nuclear plants and chemical and petroleum facilities, a robust understanding will reduce the risk as low as is practicable.

Undoubtedly the Garrick Institute faces challenges in fulfilling its mission. One is the lack of a generally accepted risk assessment methodology in terms of breadth and depth. Another is industry and its associated regulators lacking the vision and motivation to put the assessments into practice. In the nuclear industry, where even limited scope assessments have reaped many benefits, there lacks a total buy-in to performing full-scope risk assessments. The Fukushima nuclear meltdowns (NAS, 2014) demonstrated the inadequacies of limited-scope risk assessments while adding clarity to what in fact should constitute a more complete risk assessment. The meltdowns made clear that risk models must be greatly expanded in scope to be complete. This applies across the industrial spectrum, even though some scopes are more complete than others.

The question is why regulators and industry are reluctant to conduct the necessary full-scope studies to quantify the risks. The answer often given is that the studies are too expensive and they require a level of skilled staffing that is difficult to establish and maintain. This argument has lost a lot of its impact, given the estimated $250 billion recovery cost of the Fukushima event. After all, there is a high likelihood that the event could have been avoided by more fully considering the risks involved; risks that were beyond the design basis of the plants, but judged to be acceptable. There was in fact hard evidence of the risk of the event that led to the Fukushima economic disaster, evidence not properly taken into account (Nelson, 2015; NAS, 2014).

The needs of the risk sciences are clear and take two forms: improving the technology (science and engineering) and increasing the implementation (systems and site-specific applications). Both are part of the mission of the Institute. The risk sciences and how they are engineered hold the key to coping with and managing the risks of an increasingly complex society. Continuous research and development activity is necessary to overcome the perceived and actual shortcomings of the methodology. Issues of scope include the consideration of internal threats (system failures and human error); external threats (floods, earthquakes, severe storms, etc.); accounting for the interaction of replicated adjoining facilities and processes at the same site, should they exist; and the impact of threats to infrastructure, accident mitigation and recovery, particularly with respect to site accessibility. Issues of depth include better representation of system degradation phenomena and safety system logic and reliability, as well as quantification of the uncertainties.

A major problem has been the lack of a dedicated, continuous and permanent residence for research and development of the risk sciences. The sources have been fragmented and temporary. There is also the need for educating researchers, educators, and practitioners. The Garrick Institute has been established to fill such needs, to be a repository for archiving risk information, and to be active in broadening the acceptance and use of the risk sciences for the good of society.

FACTORS BEYOND RISK

Of course, decisions are not made on the basis of risk alone. Other attributes have to be considered such as costs, benefits and preferences. And these attributes can be decomposed into component parts to facilitate any desired spectrum of risk measures. Consider the simple decision diagram of Figure 1.

At the point of a decision for this model we have chosen to assess the various outcomes on the basis of costs, benefits, and damage. Each option is characterized by a triplet of probability curves. Utility values are then assigned to each triplet as a whole, accounting for such other decision measures as “preferences” and something the decision analysts call “affect” (Isen, 2001). The intention is that the most desirable outcome is the one having the largest utility.

When it comes to decisions that can be a basis for policy on what should be done to protect society and the environment from catastrophic events, or mitigate their impact to the extent affordable, a formal decision analysis is a prudent path forward as long as the risk measures are rigorously determined and can withstand the challenge of scientific scrutiny. The task of the risk scientist is to generate the curves representing the uncertainties in each of the option indicators – in this example costs, benefits,
Taking Action to Prepare Society for Catastrophic Risks

and risks. The task of the decision analyst is to interpret the set of curves through some form of utility theory or weighting procedure that factors in other attributes that may be desired. Neither the risk analyst nor the decision analyst actually makes the decision—it’s left up to others to do, and in a democratic society that is often the citizenry through the various branches of government. Of course, one cannot expect a citizenry that is ill-informed to make good risk decisions. A critical part of the Garrick Institute’s mission is tackling the ever-present communication challenge of scientific risk analysis.

There are two general categories of catastrophic risks, natural and anthropogenic (i.e., the “unnatural” ones created by man). Super earthquakes, volcanoes, and asteroid impacts are examples of natural threats. Pollution, technological accidents, war and terrorism are examples of anthropogenic threats. Of course, there are combinations of the two where a natural disaster can trigger the catastrophic failure of an engineered system, such as was the case in Fukushima.

Threats to society and the environment have always existed. The real question is whether we are making progress on managing them. To be sure our quality of life has improved over the millennia and the burden of survival has greatly diminished, resulting in longer life expectancies. However, it is not clear that we live in a world of diminishing societal and environmental risk, particularly with respect to catastrophic and existential risks. While quality of life, including life expectancy, has increased quite dramatically, so too has population and societal advances that provide more options of things that can go wrong on a bigger scale, some of which can be catastrophic in nature. In other words, the advances we have made to protect society from famine, disease, the elements, and wild beasts have been offset by the development of weapons of mass destruction, urbanization, economic interdependence, and new technologies not well understood in terms of their risk. Examples of such technologies are nanotechnology, genetically engineered biological species, artificial intelligence, and super-intelligent computers and robots that are given increasing amounts of control over complex systems and weapons ranging from airplanes to nuclear reactors. Some will say that the risks from the Internet should be a priority, as well, because of its international pervasiveness and vulnerability to abuse. The bottom line is we have made much progress on routine risks such as those related to diet, health care, lifestyle, and protection from the elements, but have increased at least the potential (and often unknown) risk of those events for which we have little direct experience, even though there is compelling evidence of their existence.

Risk science has become a popular activity, as measured by the great number of risk centers there are at leading universities (garrickfoundation.org). When it comes to the specialty area of catastrophic risk, there too is a growing list of institutions and focus groups. Posner’s book (Posner, 2004) provides strong evidence of the need to address catastrophic risks and characterizes them not only in terms of their physical and health impacts, but the need for cost-benefit analysis to make the priorities more transparent. In the United Kingdom two institutes have been founded, one at the University of Oxford (The Future of Humanity Institute) and the other at the University of Cambridge (The Center for the Study of Existential Risk) for the explicit purpose of increasing our fundamental understanding of the threats facing the inhabitants of our planet. Nick Bostrom of Oxford has been one of the most active spokesmen of existential risk (Bostrom, 2013; Bostrom, 2002). Martin Rees of Cambridge has studied and written extensively on both catastrophic risk and existential threats (Rees, 2003).

A specific example of a program aimed at protecting society from catastrophic risk is NASA’s Safeguard program (http://www.neo.jpl.nasa.gov) for surveying near-earth objects. This program tracks potentially threatening asteroids, one of the major means by which a catastrophic or existential event could occur. Volunteer groups such as The Future Watch (http://www.thefuturewatch.com) have rallied interest in catastrophic events and the need for action. The Future Watch website states it is “to be a resource for citizens and policy makers across the world” interested in seeing more done on controlling catastrophic risks. The book “Quantifying and Controlling Catastrophic Risks” (Garrick, et al., 2008) sketches four case studies having to do with the catastrophic potential of severe storms, asteroid impacts, an abrupt climate change scenario, and a cyber and physical attack of a hypothesized national grid. Numerous individual researchers have addressed most of the threats that have been identified as having the potential for global or catastrophic consequences.

CURRENT STATUS OF QUANTITATIVE RISK ASSESSMENT

It’s too ambitious for this paper to assess the status of the risk sciences as that would practically mean assessing the status of science and technology as a whole – clearly not a practical undertaking. It is possible to examine briefly the current status of quantitative risk assessment, that part of the risk sciences that is counted on to pull the various disciplines together to answer the basic risk questions.

Most of the work in quantitative risk assessment has focused on the risk of major industrial facility accidents where large inventories of toxic or hazardous materials could be released. Apostolakis (Apostolakis, 1990) discusses the specific issue of using probability and formal risk assessment methods in the safety assessment of technological systems. In general, rigorous quantitative risk assessment methods have not been explicitly applied to assess the risk of stand-alone natural events, although considerable work has been done to understand their consequences.
The nuclear power community has been the frontrunner in moving towards the use of quantitative – that is probabilistic – methods of risk assessment (Garrick, 2014). This brief examination into the status of quantitative risk assessment is weighted toward the methods being used where quantitative risk assessments are in fact being practiced. An important reason for weighting the comments in this manner is that nuclear safety experts also have been incorporating the probabilistic risk of natural events into their risk models as possible triggering events for plant accidents. To be sure there is one area where there is need for much more research and analysis, particularly regarding the integration of the two basic types of events, internal and external.

Since risk can be thought of in terms of scenarios, likelihoods and consequences, it is valuable to examine the status of quantitative risk assessment accordingly.

Scenarios

A general approach to structuring scenarios has emerged in the quantitative risk assessment field. Logic models such as event trees and fault trees have advanced to a reasonably mature level, including the software for their processing. While advances have been made, there are opportunities for improvement with respect to the scope or completeness of the scenario set used as a basis for the risk models. For example, the failure at the Fukushima nuclear power plant dramatically demonstrated the limitations of the risk scenarios that were the design basis of the plant. Although external events such as earthquakes and severe storms have always been a consideration in nuclear plant risk assessments, experience indicates the need for more rigor and integration of external events into the basic risk models. Another external factor that must be more integrated is the impact of multiple units on the same site, especially when shared systems are involved (e.g., off-gas systems, control rooms, and emergency systems). The impact of severe natural events on the site and general infrastructure needs much greater visibility in the scenarios. Cyber-attacks and space weather (e.g., geomagnetic disturbances of the electric grid) are also examples of threats that are not hypothetical and should be examined more thoroughly in risk scenarios.

The scenario sets must include the progressions of accidents to facilitate the timely orchestration of corrective and recovery actions. Matching accident and upset condition symptoms with the most effective corrective and recovery procedures and actions is an area requiring continued research. Key information in this regard is the timing and sequencing of events leading to the symptom. There has been considerable research on transitioning the event tree/fault tree scenarios into dynamic representations of the sequences (Amendola, 1988). A particular pioneering formulation of dynamic methods, known as the “Theory of Continuous Event Tree,” stands out for its generality and mathematical rigor (Devooght and Smidts, 1992). Simulations and dynamic analyses are possible paths forward for advancing the models.

Other needed improvements of the scenario sets include more detailed representations of safety system software and modern digital instrumentation and control systems. Experience indicates that for selected scenarios a more fundamental understanding of basic phenomena and processes associated with the progression of an accident must be developed to facilitate recovery and better enable their representation in the risk scenarios. A major need is more comprehensive treatment of the role of human performance leading to, during, and following severe accidents. As discussed in the next section, greater consistency and rigor is needed to quantify the uncertainties in the process and system state variables that are the drivers for the risk measures.

In regard to natural events such as severe storms, earthquakes, tsunamis, and asteroid impacts, a strategy of developing risk-based response and recovery scenarios for different categories of events is generally lacking. Quantification of the scenarios would provide guidance on those conditions most expected and for which there needs to be the greatest amount of preparation to minimize the consequences. In fact, scenarios for both industrial accidents and natural disasters would greatly benefit from more emphasis on response and recovery. Response and recovery risk assessments from disastrous events are areas where there has been very limited application of quantitative analysis. The idea is to minimize the real scenarios for which there are no procedures to guide recovery. Such applications could provide major benefits in terms of saving lives and protecting the environment.

Likelihoods

The likelihoods of scenarios are based on the processing of evidence that may exist in a variety of forms. The principal logic engine for processing evidence is Bayes theorem, the theorem that explicitly answers the question of how a given hypothesis changes with new information. With the emphasis on rare event phenomena, it is critical that uncertainty be a fundamental part of the representation of likelihood. This is particularly true when attempting to quantify catastrophic risks over such a wide range of frequencies of occurrence; frequencies covering recurrence intervals from 102 to 108 years, that is, from rare anthropogenic and natural events to existential events.

The uncertainty sciences have been greatly bolstered by the growing activity in the risk sciences, particularly with respect to catastrophic events of very low frequencies. Two broad categories of uncertainty have been defined – aleatory and epistemic.
Aleatory uncertainty has to do with the natural randomness, that is, the probability of frequencies of basic events associated with the process or model. Aleatory uncertainty is an inherent property that generally can only be addressed by changing the process or model. Epistemic uncertainty has to do with knowledge uncertainties about the process or model. Such knowledge is the uncertainty in the parameters making up the risk measure, the integrated and propagated uncertainty in the risk measure itself, and model uncertainty, including the completeness of the model or scenario set.

Parameter uncertainty analysis is a mature discipline utilizing the basic principles of Bayesian probability and statistics. There are major opportunities for improvements, particularly with respect to software and computer aids. And it is true that too few information management systems include high-quality classification, collection, and information-processing programs. Still, more often than not, more data and information exists than is generally used. The problem is that it takes time and money to dig it out, although progress on “big data” technologies and the ever-growing digitization of information is steadily lowering this hurdle. Even in the absence of more formal methods of information processing, much more can be done to better support the probabilities associated with catastrophic events. The major problem in many cases is simply an unwillingness to use the more rigorous methods.

There is no preferred or established protocol for quantifying model uncertainties. An often used approach is to compare different models and attempt to bound the range of the resulting uncertainty on the basis of the differences in the results. Thus, continuing research on quantifying model uncertainty is needed (Mosleh, et al., 2009). Scenario or model completeness uncertainty is more a matter of being confident that the scenario set covers all the important threats to a system or all the important evidence impacting the likelihood of a natural event. The question often raised is, what about the scenarios you don’t think of? Regulators and oversight organizations tend to answer this question by saying, “That’s why we require additional in-depth analysis on safety margins and defense.” But the real problem has more to do with a willingness to consider a more complete scenario set than it has to do with using conservatism in covering the so-called “unknowns.” For example, there was evidence on the event that led to the Fukushima meltdown, it just wasn’t included in the scenario set that was the basis for the design; not including it was considered an acceptable risk. The way to achieve completeness is to develop more comprehensive scenario sets to serve as the basis for the risk assessments and the design.

The most important output of a comprehensive quantitative risk assessment of extremely rare catastrophic events, besides the assessment of the damage incurred, is the quantification and importance ranking of the primary contributors to the risk. For rare events, where there is little evidence about their occurrence frequency, uncertainty is the primary contributor.

To illustrate how quantifying the uncertainties in the contributors enables better resolution of their importance, consider the following two examples. The first example is for the case where – on the basis of point estimates (no uncertainty considered) – two contributors turn out to be approximately equal in their contribution to risk. Based only on the point estimates, the contributors would be assigned equal priority. Now, suppose we quantify the uncertainties of the two contributors and find that there is a major difference in our state of knowledge about them even though their central tendency parameters (means and medians) are about the same, as illustrated in Figure 2. With quantitative information about the uncertainties, we would be foolish to rank the two contributors equally, as Contributor 2 is a much greater risk than Contributor 1.

Another important and often encountered case is illustrated in Figure 3. Suppose a point estimate analysis indicates that Contributor 2 is far less of a contributor than Contributor 1. The difference is that we know much more about Contributor 1 than we do about Contributor 2, not an uncommon situation. Quantifying our state-of-knowledge results in a probability, perhaps small, that Contributor 2 can in fact be a greater risk than Contributor 1. Obviously, it is very important to know what that probability is when it comes to establishing priorities and making decisions.

This kind of transparency in regard to the uncertainties of the contributors can only be achieved through their quantification. Quantifying the contributors is like turning up the microscope on the truth about their importance. It is not the truth, but is closer to it, which is the type of information needed to develop meaningful strategies to mitigate contributors to risk. Obviously such resolution of the uncertainties becomes less important with increasing evidence of the event.
Consequences

Quantitative risk assessments are distinguished not only by the probabilistic character of the risk measure, but the multiple measures sometimes needed for completeness in the characterization of the risk of a single site, facility, or event. Examples of risk measures, sometimes referred to as damage states, are fatalities, injuries, property damage, physical system damage, environmental impacts, and economic consequences such as recovery, replacement, and evacuation costs. An appropriate set of risk measures provides insights into other, more subtle, measures such as the degree of suffering imposed on an affected population. There are always some errors, simplifications and uncertainties in the models, but these can be explicitly addressed for each risk measure. The nuclear power industry, the most experienced practitioner of quantitative risk assessment, choose to use core damage frequency and a large early release of radionuclides as their contemporary risk measures. Current U.S. regulations do not require any offsite risk measures to be quantified. Clearly, the opportunity exists to upgrade the set of risk measures that are generally employed, even for nuclear plants, to more comprehensively represent the risk. It is believed that the most important upgrade is to include fatality risk in the set. The concern about adopting fatality risk is its negative implications, but it is believed that the benefits of knowing the fatality risk outweigh any psychological negatives.

The use of multiple risk measures that include fatality risk for nuclear plants is not without a precedent. Some early nuclear plant risk assessments (for example, PLG, et al., 1981; PLG, et al., 1982) performed by industry and guided in part by the U.S. Nuclear Regulatory Commission’s Reactor Safety Study (USNRC, 1975) did quantify offsite risk measures. In fact, nine risk measures were included: core damage frequency, release frequencies, plant damage state frequencies, early fatalities, thyroid cancer cases, injuries, latent cancer fatalities, radiation exposure, and property damage and evacuation costs. In addition, the contributors to the risk measures were ranked in terms of their risk importance. The U.S. nuclear power community eliminated metrics associated with fatality risk and other measures about the time (late 1980s) the USNRC started issuing policy and guidance documents on the use of probabilistic risk assessments and, as noted earlier, eventually settled on core damage frequencies and radionuclide releases for measuring risk. It is not clear what changes will be made, if any, as the nuclear industry transitions from limited scope risk assessments to more complete models.

Many believe that society has become sufficiently sophisticated to be able to accept fatality risk as a risk measure. During the last 50 years or so the world population has become increasingly exposed to more formal risk information in such fields as weather forecasting, medical procedures, and financial investments. Media and entertainment industry focus, while often misleading, also increases societal familiarity with the concept of risk. Thus, accurate communication of the risk of rare catastrophic events represents more of a challenge than events for which there is lifetime or real experience.

TARGET RISKS

One way to identify the most important target risks for the Garrick Institute to examine is to canvas world scholars who are trying to raise public consciousness about catastrophic risks. Fortunately, the Edge Foundation (edge.org) seeks to do this. Edge presents annually the response of selected scholars to a profound question concerning catastrophic risk. The 2013 question was, “What Should We Be Worried About?” (Brockman, 2014), which is very relevant to the topic of catastrophic risk. The disciplines of experts who are surveyed include “…biology, genetics, computer science, neurophysiology, psychology, cosmology, and physics.” The scope of their worry list is expansive and can only be grasped by a serious study of the referenced book. The worry list includes what is described as the knowns, the known unknowns, and the unknown unknowns. Examples of each category are, respectively, nuclear war, cyberwarfare, and narcissistic leaders. One of the contributors to the Brockman book, Max Tegmark, sums it up well: “What we should be worried about is that we’re not worried.”

While such deep thought scenarios as considered by Brockman (2014) are of interest to the Institute, they are not necessarily the bull’s eye of the target risks. The Garrick Institute emphasis will be on those risks that can have catastrophic consequences and whose likelihoods have not been rigorously assessed. Also of priority are risks where there is evidence that severe consequences are more likely than is commonly perceived by our leaders and decision makers. In terms of damage, most are in the regional category rather than global, but global consequences as well as existential risk will be within the scope of the Institute. In particular the Institute, while interested in and wanting to contribute to the existential risk discussion, is primarily targeting that part of the risk spectrum just below existential risk, but above the risks we know a lot about; risks that could lead to extensive fatalities and environmental damage.

There are good reasons for applying the risk sciences to catastrophic risks below the existential level. One is the prospect of having an immediate impact in terms of saving lives and protecting the environment. Another is that this class of events is where most of the contemporary risk assessment methods have evolved, and it is thus the best starting point for the development of ways to deal with even greater risks including those in the existential class, especially with respect to their better definition, classification, and quantification.

“`All models are wrong, but some are useful” - George E. P. Box (1919 – 2013)
It is convenient to classify the risks in some orderly fashion to facilitate their ranking. Posner (Posner, 2004) presents catastrophic risks using the following classifications: natural disasters, scientific accidents, other unintended man-made catastrophes, intentional catastrophes, and basically an “other” category. Bostrom breaks down the existential risks into such colorful categories as: “bangs, crunches, shrieks, and whimpers.” The “bangs” to “whimpers” range of existential risks goes from total extinction of intelligent life to situations where a “posthuman civilization arises but evolves in a direction that leads gradually but irreversibly to either the complete disappearance of the things we value or to a state where those things are realized to only a minuscule degree of what could have been achieved.” Bostrom has also published more formal classifications of risk.

Much of the catastrophic risk of the last century was due to humans, particularly concentrated in wars and revolutions. Much of the catastrophic risk of the current century has come from nature. Thus, both have to be analyzed for their future management. Future potentially catastrophic man-made risks include exhaustion of natural resources (particularly fresh water), overpopulation, nanotechnology, bioterrorism, nuclear war, nuclear accidents, industrial accidents, transportation accidents, cyber terrorism, climate change, and pandemics. Natural catastrophic events include asteroids, super volcanoes, earthquakes, and climate change. Note that climate change is listed in both categories as it is clear that severe climate changes have naturally taken place without any impact from humans, and will do so again. The extent to which the climate change cycle we are now in is anthropogenic versus natural continues to be debated.

As these and other threats are more rigorously assessed, it is likely that the list will change in types of events and importance. It is evident that the human-driven risks are the most dynamic and challenging because of emerging science and technologies that are not well understood in terms of their threat to society.

**THE PATH FORWARD**

We must identify the most threatening regional and global catastrophic events, and quantify the risks involved. As Richard Posner keeps asking: “What are the catastrophic risks, and how catastrophic are they?” The answers will not always be intuitive. Better quantification will tell us what we know and what we don’t know about a risk, including how the uncertainties can be reduced. Advanced computational methods will be critical to this process.

We must look to the science and technology associated with the threat being considered. This involves the physical, chemical, and earth sciences; it certainly involves engineering; and it may have to involve something else altogether. Existing risk models are not always sophisticated enough to give us a proper understanding of the threat to be mitigated. We do better with industrial accidents – where there are often strong economic incentives to get it right – than we do with natural phenomena.

Finally, a successful path forward not only involves posing the right questions and applying the right science and technology, but also creating a culture where those closest to the point of the threat are passionately invested in improving public safety and protection of the environment. The concern is that the combinations and permutations of the “what-can-go-wrong” scenarios for complex systems, be they natural or anthropogenic, are just too rooted in the system-specific or phenomenological details to think that a general or generic set of government rules and regulations can possibly assure safety. Those in immediate charge of the system or phenomena at the point of the threat have to bridge the inevitable gap between the applicable rules and regulations and the system-specific knowledge necessary to protect the public and the environment. Compliance management is the law, but it is not the answer. If there is a lack of the vision necessary at the point of control to go the extra lengths in assessing and managing the risks involved, there will surely be catastrophic events that could have been avoided, or there will be suffering associated with them that could have been dramatically reduced.
Quantitative risk assessment is considered the best measuring stick of the advances that have been made in the risk sciences. It is the integrator of the various disciplines for the purpose of answering the question, what is the risk? Of course, the answer to that question really involves answering three subsidiary questions: What can go wrong, how likely is it if it does go wrong, and what are the consequences? This brings us to the need to introduce a more quantitative and specialized definition of risk than the dictionary does in order to form the technical foundations for assessing and analyzing risk. The basic framework for analyzing risk that has been widely adopted is based on the “set of triplets” definition (Kaplan and Garrick, 1981). This definition represents risk in terms of scenarios, consequences, and likelihoods. In particular, risk is defined as

\[ R = \{ <S_i, L_i, X_i> \} \]

where, \( R \) is the risk of the system, process, event, or activity of interest, \( S_i \) is the risk scenario (a description of something that can go wrong), \( L_i \) is the likelihood of that scenario happening, and \( X_i \) represents the consequences of that scenario if it does happen. The angle brackets \( <> \) enclose the risk triplets, the curly brackets \( \{ \} \) are math-speak for “the set of,” and the subscript “c” denotes “complete,” meaning that all scenarios, or at least all of the important ones, must be included in the set. The body of methods used to identify the scenarios \( (S_i) \) constitutes an evolving “theory of scenario structuring” (Kaplan, et al., 2001). Quantification of the \( L_i \) and \( X_i \) is based on the available evidence. Bayes theorem is the basis for processing the evidence (Kaplan, 1986).

In accordance with this “set of triplets” definition of risk, the actual quantification of risk consists of answering the following three questions:

1. What can go wrong? \( (S_i) \)
2. How likely is that to happen? \( (L_i) \)
3. What are the consequences if it does happen? \( (X_i) \)

The first question is answered by describing a structured, organized, and complete set of possible risk scenarios. As above, we represent scenarios by \( S_i \). The second question requires us to calculate the “likelihood,” \( L_i \), of each of the scenarios, \( S_i \). Each such likelihood, \( L_i \), is expressed either as a “frequency,” a “probability,” or a “probability of frequency” curve to characterize the uncertainty in the scenario. As noted earlier, probability of frequency is the preferred way of expressing likelihood, as it embodies both the notion of frequency and probability.

The third question is answered by describing the “damage states” or “end states,” \( X_i \), resulting from these risk scenarios. These damage states are also, in general, uncertain. Therefore these uncertainties must also be quantified as part of the risk assessment process. Indeed, it is part of the philosophy to quantify all the uncertainties in all the parameters in the risk assessment.

Some authors have added questions to the definition of risks such as “What are the uncertainties?” “What corrective actions should be taken?” and “What are the contributors?” The uncertainty question is embedded in the interpretation of “likelihood.” The question about corrective actions is interpreted here as a matter of decision analysis and risk management, not risk assessment. The question about contributors is a matter of importance ranking the scenarios and decomposing them into contributors, which is part of the process of implementing the risk triplet framework and protocol.

To implement the triplet definition of risk, the key activities are the development of the “what can-go-wrong” scenarios, the quantification of the likelihoods of the scenarios, and the determination of the endstates of the scenarios that drive the consequences. Of course, there is much that goes on in the way of engineering analysis and physical processes to get to the scenarios, just as there is much that goes on in processing the evidence to get to the likelihoods.

The calculation of likelihoods primarily evolved in the fields of mathematics and mathematical physics, and has a history of several hundred years. On the other hand, the discipline of formally structuring scenarios is much more recent and was developed primarily by engineers involved in designing and analyzing complex systems evolving from 20th century technology. For example, the disciplines of reliability analysis and reliability engineering have made a significant contribution to the development of integrated models of engineered systems, including the development of a variety of logic structures for displaying interdependencies of components, subsystems and systems.

Reliability analysis uses block diagrams to describe how components in a large system are connected. From these block diagrams, Watson at Bell Laboratories (Watson, 1961) developed the fault-tree technique based on switching algebra and telecommunication theory, which he applied to the Minuteman Missile launch control system, and which Boeing and the nuclear industry later adopted and computerized. These diagrams, in combination with switching algebra and probability theory, have provided a powerful tool for displaying and quantifying the “fault paths” of systems, subsystems, components, human actions, procedures, etc.
The advantage of these techniques in the field of safety analysis, as opposed to just reliability, began to be recognized in the 1960s. E.R. Farmer of the United Kingdom proposed a new approach to nuclear power plant safety based on the reliability of consequence-limiting equipment (Farmer, 1964). Under the direction of Garrick, Holmes and Narver, Inc., a U.S. engineering firm was contracted by the then U.S. Atomic Energy Commission to perform a series of studies on nuclear reactor safety and reliability. The final report (Homes and Narver, 1967) in the series advocated, with examples, the need for much greater use of advanced systems engineering methods of modeling the reliability of safety systems. The authors made explicit reference to the use of logic tools, such as the fault-tree methodology noted earlier. At about the same time, a PhD thesis was published that proposed a methodology for probabilistic, integrated systems analysis for analyzing the safety of nuclear power plants (Garrick, 1968). Numerous other investigators and organizations engaged in the development of probabilistic methods of risk assessment.

The breakthrough in quantitative risk assessment (or probabilistic risk assessment, as it is most often labeled in the nuclear field) of technological systems came in 1975 with the publication of the Reactor Safety Study by the U.S. Atomic Energy Commission under the direction of N.C. Rasmussen of the Massachusetts Institute of Technology (USNRC, 1975) and Saul Levine, Director of Research, U.S. Nuclear Regulatory Commission. This project, which took three years to complete, marked a turning point in the way people think about the safety of complex facilities and systems. The Reactor Safety Study provided a basis for a wide range of applications for risk assessment, not only for nuclear power plants and other technological systems (e.g., chemical and petroleum facilities, transportation systems, and defense systems), but also for environmental protection, health care, and food safety.

In addition to fine-tuning fault tree analysis for safety applications, the Reactor Safety Study introduced another extremely important graphic tool to facilitate the structuring of scenarios, the event tree, which has its roots in decision theory. Fault trees and event trees, in combination, provided a critically important one-two punch in structuring scenarios. An event tree starts with an initiating event and proceeds to identify succeeding events, including branches that eventually terminate in possibly undesired consequences. An event tree, therefore, is a cause-and-effect representation of logic.

A fault tree starts with the end-state or undesired consequence and attempts to determine all of the contributing system states. Therefore, fault trees are effect-and-cause representations of logic. An event tree is developed by inductive reasoning while a fault tree is based on deductive reasoning. A key difference is that a fault tree is only in “failure space,” while an event tree includes both “failure and success space” and can be structured as a linear vector space which facilitates the use of linear algebra. The choice between the two is a matter of circumstances and preference, and they are often used in combination; the event tree provides the basic scenario space of events and branch points, and the fault tree is used to add casual depth and quantify the “split fractions” at the branch points.

The Reactor Safety Study inspired many first-of-a-kind risk assessments in the commercial nuclear power industry that led to major advances in the application of quantitative risk assessment. Important examples are the full scope probabilistic risk assessments of the Zion and Indian Point nuclear power plants sponsored by the plants’ owners and operators. New methods were introduced in those assessments that have become standards of many quantitative risk assessment applications (PLG, et al., 1981; PLG et al., 1982). The methods included the treatment of uncertainty, a framework of risk assessment embedded in the set of triplets’ definition of risk (Kaplan and Garrick, 1981), common-cause failure analysis, importance ranking of risk contributors, models for calculating source terms, and improved dispersion models for calculating offsite health effects.

These and other studies, for example, Philadelphia Electric, 1981 and USNRC, 1990, have evolved into a contemporary theory of structuring scenarios that is part science and part art. Elements of the theory include a set of principles having to do with issues of completeness and the general structure of scenarios.

The requirements for developing a set of scenarios capable of answering the questions of the risk triplet include (1) completeness of the set in terms of its impact on consequences, (2) the direct involvement of subject matter experts on the system being analyzed, and (3) analysts and technology capable of accounting for the many combinations and permutations of what can go wrong during different normal and abnormal states of the system. The likelihood question is a matter of the supporting evidence and the ability to truthfully represent the uncertainties in the risk measures. Likelihood requires a formal interpretation. Generally that interpretation is to adopt the frequency of events as the risk measure, realize that there is uncertainty in such frequencies, and then use the available evidence and only the evidence to construct a probability distribution over that frequency. As noted earlier, this interpretation is referred to as the probability of frequency.

Although the scope, depth, applications, and boundary conditions of quantitative risk assessments vary widely, they all follow the same general steps:

1. Define the system being analyzed, emphasizing the intended operating states.
2. Identify and characterize the sources of danger, that is, the hazards associated with the system (e.g., stored energy, toxic substances, hazardous materials, radiation, physical damage, sabotage, terrorism, equipment failure and their combinations).
3. Develop “what can go wrong” scenarios considering both internal and external events to establish the possible levels of damage and consequences.
4. Adopt risk metrics that reflect the likelihoods of different levels of damage and quantify the scenarios based on the totality of relevant evidence. Present the results in a form that makes the uncertainties transparent, that is, quantify the uncertainties.

5. Assemble the scenarios according to damage levels and cast the results into the appropriate risk curves, tables, and descriptions, including the importance ranking of the contributors to risk.

6. Interpret the results to inform the risk-management process.

These steps can be thought of as a protocol for answering the three fundamental questions of the risk triplet.

**APPLYING THE RISK TRIPLET FRAMEWORK**

The triplet definition of risk is the basic framework for illustrating the structure of a risk model. The framework is based on scenarios, likelihoods, and consequences. Figure 4 shows the relationship between the system being assessed, the threats to the system, and the structuring of the scenarios that indicates the vulnerability of the system.

Among the tasks in developing the scenarios are (1) familiarization and analysis of the system to determine what constitutes the success states for each stage of the system, among other issues (2) determination of the appropriate set of initial conditions and initiators that can disrupt or disturb the normal state of the system, and (3) performance of a vulnerability assessment of the system by structuring a set of risk scenarios and damage states corresponding to each operating stage or phase. With a structured set of scenarios for each phase or mode, then it is a matter of assembling the individual models at the appropriate pinch points (interfaces) to form an integrated model.

The individual scenarios are quantified based on the supporting data. The quantification process involves the use of Boolean expressions to represent the scenarios and Bayes theorem to transform the frequencies of the individual failure events in the scenarios, based on the supporting evidence, into representations of the scenarios. Repeating this process for each stage results in the quantification of the input and output variables needed to assemble the stages into a complete system model.

Numerous computer codes are capable of processing scenarios into an integrated statement of the risks. In this sketch of a model we use the tools of linear and matrix algebra to assemble the stages (Kaplan, et al., 1983). The stages for this illustration are the response of the plant to the various possible threats, containment, and the site.

The matrix approach to assembling the stages or modules for this illustration is portrayed in Figure 5.
The diagram shows four segments of a QRA study: the initiating events model, the plant model, the containment model, and the site or "consequence" model. The interfaces between the models, the "pinch points," are established by defining input/ output "states" for each model. These are called respectively, "initiating events," "plant states," "release categories," and "damage levels."

The results of the initiating event model are summarized in a row vector, $\mathbf{\Phi}_i$, whose elements, $\Phi_{ij}$, are the frequencies of the various initiating events. The vector may be viewed as partitioned into events inherent to the plant and events or threats external to the plant such as earthquakes, tsunamis, and severe storms:

$$\mathbf{\Phi}_i = \Phi_{i1}, \Phi_{i2}, \Phi_{i3}, \ldots$$

| ← internal → | ← fires → | ← earthquakes → | ← wind → | etc.

The results of the plant model are summarized in a "plant matrix," $\mathbf{M}$, whose $i$, $j$th element, $m_{ij}$, is the fraction of initiating events of type $i$ which results in a plant state $j$. Similarly, the results of the containment event tree work are summarized in a containment matrix, $\mathbf{C}$, whose typical element, $c_{ij}$ is the fraction of occurrences of plant state $j$ which results in a release of type $k$.

The site matrix, $\mathbf{S}$, summarizes the results of the site specific consequence calculations, using an appropriate atmospheric dispersion and uptake model, together with a health effects model. The element $s_{ij}$ is the fraction of releases of category $k$ which results in level of damage $l$ or greater. A different $\mathbf{S}$ matrix is produced for each type of damage considered.

With the results of the individual models summarized this way, the assembly of the results may be viewed as a matrix multiplication operation. Thus, the vector
defines $\mathbf{\Phi}_i M$ as the elements, $\Phi_{ij}$, the frequencies of occurrence of the various plant states.

Similarly

contains the frequencies, $\Phi_{jl}$, of the various release categories. Finally the vector

contains the frequencies, $\Phi_{jl}$, with which the levels of damage, $l$, are exceeded. This vector may be plotted as a risk curve. The most common form is a complementary, cumulative distribution function, Figure 6, often referred to as frequency of exceedance curves. This form of the results presents the frequency as a function of the consequence, with probability as the parameter of the model. With uncertainty included at all stages of the calculation, the elements, $p_l$, of $\mathbf{\Phi}_i$ are themselves probability curves, expressing our state of knowledge about the frequency with which accidents resulting in damage level $l$ occur. In this case $\mathbf{\Phi}_i$ may be plotted as a family of risk curves.

To illustrate how to read Figure 6 suppose $P_1$ has the value 0.95 and we want to know the risk of an $X_1$ consequence. According to the figure, we are 95% confident that the frequency of an $X_1$ consequence or greater is $\Phi_{12}$. An often used method of communicating uncertainty in the risk of an event is to present the risk in terms of a confidence interval. To illustrate how to read Figure 6 in terms of a confidence interval, let $P_1$ have the value of 0.05, $P_3$ the value 0.95, $\Phi_{1}$ the value of 1 in 10,000, $\mathbf{\Phi}_{2}$ in 1,000, and $\mathbf{\Phi}_{3}$ the value of 10,000 fatalities. Given that $P_3$ minus $P_1$ is 0.90 the appropriate language is we are 90% confident that the frequency of a 10,000-fatality consequence or greater varies from one every 10,000 years to as much as one every 1,000 years.

Figure 7 is the form generally used to represent the risk of a specific event, for example, the core damage frequency of a nuclear power plant. If the area under the curve between $\Phi_{1}$ and $\Phi_{2}$ of Figure 7 is 90% of the area under the whole curve, this indicates that we are 90% confident that the frequency range is between $\Phi_{1}$ and $\Phi_{2}$.

The form of the results includes not only the identification, quantification, and importance ranking of the contributors to risk, but also the sensitivity of different risk measures to different contributors. For example, consider Figure 8. Figure 8 is a result from an actual risk assessment of a nuclear power plant and graphically illustrates the contribution and sensitivity of selected external events to the core damage frequency of a specific plant. It also shows the contribution of the internal events as a group.
The results from this model not only take the form of the risk curves of Figures 6 through Figure 8, but also a variety of tables and charts that supplement and interpret the information provided by the curves. These results are facilitated by the explicit diagnostic capabilities of the matrix formalism. For example, combining Equations 2, 3 and 4 we obtain

$$\emptyset^f = \emptyset^1MC$$  \hspace{1cm} (5)  

$$\emptyset^f = \emptyset^1MCS$$  \hspace{1cm} (6)  

$$\emptyset^f = \emptyset^1CS$$  \hspace{1cm} (7)  

Thus $MC$ can be seen as the transition matrix from initiating events to release categories. $MCS$ is the transition from initiating events to damage levels, and $CS$ from plant states to damage levels. These matrices thus show the likelihood of going from an output state of one model to any output state of a downstream model.

If the row matrix $\emptyset^1$ is written in diagonal form, i.e.:

$$\emptyset^1_D \hspace{1.5cm} \emptyset^1_D \hspace{1.5cm} \emptyset^1_D \hspace{1.5cm} \emptyset^1_D$$

then the matrix

$$\emptyset^1_D M$$

shows the actual (not conditional) frequencies with which states $j$ occur as a result of events $i$. Similarly

$$\emptyset^1_D MC$$

shows the frequency each initiating event contributes to each release category. Similar interpretations apply to

$$\emptyset^1_D MCS, \emptyset^1_D CS, \emptyset^1_D S$$

In particular, the matrix method for interfacing the models makes visible what aspects of risk are coming from which source. This feature of the approach permits importance ranking of contributors to risk from a variety of sources.

In establishing the output states for each model, the key idea is to define the states in such a way that the downstream portion of the scenario depends only on the fact that that given state has been reached, and not on the details of the path by which that state was reached. This then allows a “pinching off” of the scenarios at that state; all scenarios reaching that state are from that point on effectively identical. From a computational standpoint this is very advantageous, as the stages can be computed simultaneously.

In order to accomplish this, the pinch-point characterization, i.e., the definition of states at that point, must capture the information from the preceding models that is of key importance to the subsequent model. This is shown in Figure 5 for the plant states; i.e., for the pinch point between the plant model and the containment model. Of course, considerable analyses to parametrically define the plant and containment conditions represented by the various input and output states must accompany this approach. Such parameters have a significant impact on the containment response and on the release of radionuclides.

The point of this example is to be explicit about what characterizes quantitative risk assessment, aka probabilistic safety assessment or probabilistic risk assessment. The characteristic features are the risk scenarios, likelihoods, and consequences, and their appropriate assembly into bottom line risk results. The context of the results includes the uncertainties in the scenarios and the bottom line representations of the risk measures such as system damage, environmental impact, and human health effects. Finally, the contributors to the risk are ranked in their importance to facilitate making the right decisions on how to manage the risk.