The Asia-Pacific Journal: Japan Focus
n-depth critical analysis of the forces shaping the Asia-Pacific...and the world.

Nuclear Energy and Risk
May. 06, 2011

核エネルギーと危険性

How was “risk” to the Fukushima Daiichi nuclear power plant calculated? Could risk projections run by successive cabinets and the Nuclear and Industrial Safety Agency predict internal cover-ups of safety defects or plant-owner TEPCO’s shelving of arguments by scientists and anti-nuclear activists that securing the plant against tsunami up to 5.7 meters, a number that now seems woefully small given the 15 meter wave that struck on March 11, was inadequate?

Fukushima politicians such as Ito Tatsuya claim to have repeatedly warned TEPCO representatives about tsunami risks, only to have their petitions for more robust safety measures ignored.

In 2000, a General Electric International employee working with TEPCO blew the whistle on irregularities in safety reports. TEPCO admitted to a widespread cover-up of cracks in core shrouds.

While not a TEPCO incident, the 1999 Tokaimura accident claimed the lives of two workers at a uranium reprocessing facility in Ibaraki Prefecture. Employees were found to have been given inadequate training and safety precautions were circumvented. Hundreds of emergency personnel and residents were exposed to high levels of radiation.

On April 19, M.V. Ramana, a prominent physicist at the Nuclear Futures Laboratory and the Program on Science and Global Security, Princeton University, published a critical take on risk assessment in the atomic energy industry in the Bulletin of the Atomic Scientists. The article highlights some of the systemic problems that led to the Fukushima crisis and warns about remaining blind spots:

Beyond our imagination: Fukushima and the problem of assessing risk

BY M. V. RAMANA | 19 APRIL 2011

Article Highlights

- Severe accidents at nuclear reactors have occurred much more frequently than what risk-assessment models predicted.
- The probabilistic risk assessment method does a poor job of anticipating accidents in which a single event, such as a tsunami, causes failures in multiple safety systems.
- Catastrophic nuclear accidents are inevitable, because designers and risk modelers cannot envision all possible ways in which complex systems can fail.

The multiple and ongoing accidents at the Fukushima reactors come as a reminder of the hazards associated with nuclear power. As with the earlier severe accidents at Chernobyl and Three Mile Island, it will take a long time before the full extent of what happened at Fukushima becomes clear. Even now, though, Fukushima sheds light on the troublesome and important question of whether nuclear reactors can ever be operated safely.

Engineers and other technical experts have two approaches for making nuclear reactors safe: The first is to design the reactor so that it is likely to recover from various initiating failures -- lowering the probability that the damage will spread, even in the absence of any protective actions, automatic or deliberate. The second approach, used in addition to the first, is to incorporate multiple protective systems, all of which would have to fail before a radioactive release could occur. This latter approach is known as "defense-in-depth," and it is often advertised as an assurance of nuclear safety. The World Nuclear Association, for example, claims that "reactors in the western world" use defense-in-depth "to achieve optimum safety."

Within this perspective, accidents are usually blamed, at least in part, on a lack of properly functioning safety systems, or on poor technical design. For example, analysts typically traced the catastrophic impacts of the Chernobyl accident to the reactor's lack of containment and its behavior when being operated at low power. Similarly, in response to the current Fukushima accidents, many analysts have focused on the weaknesses of the reactors' Mark 1 containment system.

Unfortunately, focusing on individual components -- rather than the system as a whole -- gives analysts a false sense of security. Here's how their thinking goes: For each safety system, there is only a small chance of failure at any given time, so it's exceedingly unlikely that more than one safety system will fail at the same moment. A severe accident can't happen unless multiple safety systems fail simultaneously or sequentially. Therefore, a severe accident is exceedingly unlikely.

Unfortunately, there are occasions when multiple safety systems do fail at the same time -- and these occur far more frequently than analysts assume. This is what happened at Fukushima. Accidents can also happen when the failure of one safety component triggers failures in other components. And in some cases, individual components work properly but the system as a whole fails. An example is the Mars Polar Lander accident of 1999, when the lander's software -- working as designed -- interpreted transient signals as confirmation that the space vehicle had touched down. The software then turned off the descent engines prematurely, causing the vehicle to crash on Mars' surface. Such failure modes are hard to model within the mechanistic framework adopted by most safety analysts.

Calculating Risk

Most people conceive of risk as multidimensional, encompassing several characteristics of the hazard -- such as its catastrophic potential, its controllability, and its threat to future generations. Technical analysts, on the other hand, have a narrow conception of risk, viewing it as a mathematical product of the likelihood of an adverse occurrence, and the consequence of that occurrence. To quantify risks at complex systems such as nuclear power plants, analysts rely on a mathematical method known as probabilistic risk assessment. (Some call this method probabilistic safety assessment or probabilistic safety analysis.) The probabilistic risk assessment method conceives of accidents as resulting from one of many combinations of a series of failures, and computes the probability of a severe accident resulting from these. As described by the US Nuclear Regulatory Commission (NRC), probabilistic risk assessment involves multiple steps, including identifying initiating events (such as a pipe breaking) that could lead to hazardous outcomes (such as core damage), estimating how often each of these initiating events is expected to occur, and identifying failures that could allow the initiating event to proceed to a hazardous outcome.

The results of these risk assessments are used by different sets of people in different ways. The nuclear industry, for example, uses them to guide operational and maintenance decisions. Regulators, on the other hand, use them to tailor regulations, partly in response to pressure from the nuclear industry. Like the NRC, Japan's Nuclear and Industrial Safety Agency, which extended Fukushima Daiichi's operating license by 10 years just a month before the accident, has adopted a "probabilistic approach to regulation."

The most misleading and politically controversial uses of risk assessments, however, are claims about the frequency of severe accidents at various reactors. For example, the French nuclear company Areva asserts that with its EPR (formerly called European or Evolutionary Pressurized Reactor), now under construction in Europe and China, "the probability of an accident leading to core melt, already extremely small with the previous-generation reactors, becomes infinitesimal." In its application to the United Kingdom's safety regulator, Areva estimates an average of one core-damage incident per reactor in 1.6 million years. Likewise, Westinghouse claims that its AP1000 reactor offers "unequalled safety," in part because the company's probabilistic risk assessment calculated that the core melt frequency is roughly one incident per reactor in 2 million years. Older reactors in the US are estimated to have higher frequencies; for example, the NRCcalculated an average of about one incident in 10,000 years for the Peach Bottom reactor in Pennsylvania, which is a boiling water reactor with a Mark 1 containment like the reactors at Fukushima Daiichi.

Reality Check

There are both empirical and theoretical reasons to doubt these numbers. A 2003 study on the future of nuclear power carried out by the Massachusetts Institute of Technology points out that "uncertainties in PRA methods and data bases make it prudent to keep actual historical risk experience in mind when making judgments about safety." What does history tell us? Globally, there have been close to 15,000 reactor-years of experience, with well-known severe accidents at five commercial power reactors -- three of them in Fukushima. However, as Thomas Cochran of the Natural Resources Defense Council explained in his recent testimony to the US Senate, depending on how core damage is defined, there are other accidents that should be included. The actuarial frequency of severe accidents may be as high as 1 in 1,400 reactor-years. At that rate, we can expect an accident involving core damage every 1.4 years if nuclear power expands from today's 440 commercial power reactors to the 1,000-reactor scenario laid out in the MIT study. In either case, though, our experience is too limited to make any reliable predictions.

Theoretically, the probabilistic risk assessment method suffers from a number of problems. Nancy Leveson of MIT and her collaborators have argued that the chain-of-event conception of accidents typically used for such risk assessments cannot account for the indirect, non-linear, and feedback relationships that characterize many accidents in complex systems. These risk assessments do a poor job of modeling human actions and their impact on known, let alone unknown, failure modes. Also, as a 1978 Risk Assessment Review Group Report to the NRC pointed out, it is "conceptually impossible to be complete in a mathematical sense in the construction of event-trees and fault-trees ... This inherent limitation means that any calculation using this methodology is always subject to revision and to doubt as to its completeness."

Probabilistic risk assessment models do not account for unexpected failure modes during many accidents. At Japan's Kashiwazaki Kariwa reactors, for example, after the 2007 Chuetsu earthquake some radioactive materials escaped into the sea when ground subsidence pulled underground electric cables downward and created an opening in the reactor's basement wall. As a Tokyo Electric Power Company official remarked then, "It was beyond our imagination that a space could be made in the hole on the outer wall for the electric cables."

Yet when it comes to future safety, nuclear designers and operators always seem to assume that they know what is likely to happen. This is what allows them to assert that they have planned for all possible contingencies. Or, as the chairman of the Indian Atomic Energy Commission asserted in the aftermath of Fukushima, nuclear reactors [in India] are "one hundred percent" safe.

Common-Cause Failures

If there is one weakness of the probabilistic risk assessment method that has been emphatically demonstrated at Fukushima, it is the difficulty of modeling common-cause or common-mode failures. From most reports it seems clear that a single event, the tsunami, resulted in a number of failures that set the stage for the accidents. These failures included the loss of offsite electrical power to the reactor complex, the loss of oil tanks and replacement fuel for diesel generators, the flooding of the electrical switchyard, and perhaps damage to the inlets that brought in cooling water from the ocean. As a result, even though there were multiple ways of removing heat from the core, all of them failed. The probabilistic risk assessment method does try to incorporate common-cause failures, but this

is not always satisfactory. For example, the probabilistic risk assessment for the EPR calculates the frequency of core damage following a total loss of offsite power to be one incident per reactor in 12 million years. This low number is a result of assuming that failures other than offsite power loss occur essentially at random and independently of each other. But at Fukushima the same event that knocked out external power also caused the failure of other systems for cooling the core.

Fukushima also demonstrated one of the perverse impacts of using multiple systems to ensure greater levels of safety: Redundancy can sometimes make things worse. At Fukushima, as with most reactors around the world, zirconium cladding surrounded and protected the fuel. But when the cooling systems stopped working, the zirconium cladding overheated. Hot zirconium interacted with water or steam, producing hydrogen gas. When this hydrogen came into contact with air in the containment building, it caused an explosion that reportedly damaged the suppression pool beneath the reactor, another protective system. In other words, in complex systems such as nuclear reactors, redundancy may have unexpected and negative consequences for safety, as scholars including Charles Perrow and especially Scott Sagan have pointed out in the past.

Accidents are Inevitable

The multiple problems with the probabilistic risk assessment method suggest that any conclusions about overall accident probabilities derived from its use are far from dependable. Perhaps the only robust conclusion one can draw is that no two major accidents are alike. Historically, severe accidents at nuclear plants have had varied origins, progressions, and impacts. These have occurred in multiple reactor designs in different countries. This means, unfortunately, that while it may be possible to guard against an exact repeat of the Fukushima disaster, the next nuclear accident will probably be caused by a different combination of initiating factors and failures. There are no reliable tools to predict what that combination will be, and therefore one cannot be confident of being protected against such an accident. These problems cannot be resolved simply by constructing reactors with newer designs, ones that have been deemed safer on the basis of probabilistic risk assessment calculations that predict lower accident frequencies.

If probabilistic risk assessments were just esoteric exercises performed by nuclear engineers for internal consumption, there would not be much reason to be concerned with their lack of reliability except that they create overconfidence among those designing and operating reactors. The problem is that the small numbers produced by this exercise, widely seen as involving complicated calculations, have the effect of what might be termed false or misplaced concreteness, especially on policy makers and the general public. This is profoundly misleading and was most tragically revealed in the Chernobyl accident. Just three years earlier, B. A. Semenov, the head of the International Atomic Energy Agency's safety division, had written about the RBMK reactor design used at Chernobyl: "The design feature of having more than 1,000 individual primary circuits increases the safety of the reactor system -- a serious loss-of-coolant accident is practically impossible." The similarity between this assertion and claims about the safety of nuclear reactors currently being built is striking.

The lesson from the Fukushima, Chernobyl, and Three Mile Island accidents is simply that nuclear power comes with the inevitability of catastrophic accidents. While these may not be frequent in an absolute sense, there are good reasons to believe that they will be far more frequent than quantitative tools such as probabilistic risk assessments predict. Any discussion about the future of nuclear power ought to start with that realization.