In the wake of Japan's developing nuclear crisis, people have begun questioning the future of US nuclear policy. Here is Sen. Lieberman, cautiously arguing for a review of nuclear power safety:

> I think it calls on us here in the U.S., naturally, not to stop building nuclear power plants but to put the brakes on right now until we understand the ramifications of what's happened in Japan.

One somewhat obvious conclusion from the situation in Japan is that their risk assessment of their nuclear reactors was deeply flawed. Risk is commonly defined as the probability of an accident occurring times the expected loss. Another way to think about risk is as probability times exposure.

In Japan, exposure is lessened because Japan is a developed country with resources to respond to a crisis. But exposure is heightened because of the dangers of widespread radiation contamination, the duration of such contamination, and the proximity of the reactors to population centers. Nuclear accidents are low-probability events, but exposure can be catastrophically high due to the dangers of a Chernobyl-like poisoning of the environment. And so even minimal probability events must be taken seriously.

This brings us to the probability of cooling system failure, the second element of the risk equation. David Lochbaum, a nuclear engineer with Union of Concerned Scientists, had this to say about the probability of what we are now seeing in Japan:

> The real situation they found themselves in is not really planned for. Those plants are designed to be highly resistant to damage by earthquakes, and as immune as possible to tsunami. The problem was the one-two punch. We design against these sorts of things in isolation, and the combination is a little beyond what they would have anticipated.

If Mr. Lochbaum is correct, this suggests a serious oversight on the part of risk planners for these nuclear plants. The combination of a tsunami and earthquake is hardly an unforeseen possibility; that is why we have a tsunami warning system in the Pacific. But I would also argue that the "cause" of the reactor failures in Japan owe more to a failure in designing independent safety systems than with any failure to imagine an earthquake-tsunami combination.

Theories of accidents in large-scale systems typically argue that complex, tightly coupled systems will produce interactions that can defeat safety devices. Furthermore, safety goals can be compromised through a combination of bounded rationality and group interests, such as profit pressures. In other words, small errors can propagate into large errors (tight coupling) and errors can interact in unexpected ways (interactive complexity). Safety systems meant to decrease the probability of a serious accident can have the opposite effect if the systems are interdependent. But creating truly independent or redundant safety systems have economic resources.

The failure of cooling systems at three separate reactors at Fukushima may become a model example for accident theory. This New York Times description highlights the interdependent nature of the system meant to protect the Fukushima plant from accidental meltdown:

> The central problem arises from a series of failures that began after the tsunami. It easily overcame the sea walls surrounding the Fukushima plant. It swamped the diesel generators, which were placed in a low-lying area, apparently because of misplaced confidence that the sea walls would protect them. At 3:41 p.m. Friday, roughly an hour after the quake and just around the time the region would have been struck by the giant waves, the generators shut down. According to Tokyo Electric Power Company, the plant switched to an emergency cooling system that operates on batteries, but these were soon depleted.

There were multiple systems to power the cooling system: powerline, diesel generators and battery power. The tsunami/earthquake combination, however, took out both the generators and the powerline. The generators depended on the sea walls. The batteries are short-term; they depend on getting the powerlines or diesel back online quickly.

After the failure of the battery system, Tokyo Electric installed a mobile generator. Still, "controlled containment venting" was necessary, which suggests that the battery-controlled cooling mode was not designed for long-term use. This controlled venting failed, with a resulting explosion. (The NY Times suggests that the venting may have in fact set off the explosion, which if true, illustrates the the complexity of this system.)

In another example of the complexity of this system, the high pressure inside the overheated reactors was preventing efforts to inject cooling seawater into the reactor. A faulty valve had stopped working, preventing the vents from releasing the radioactive steam. In turn,

the increased pressure prevented workers from injecting seawater into the reactor.

The Japanese nuclear crisis has taught us that these supposed redundant systems of failure for the reactor are not necessarily redundant nor independent. And these types of nuclear reactors are complex, tightly coupled systems prone to the interactive, cascading failures commonly described by accident theory.

One final note: besides redundancy, another way to prevent failure is the use of an inherent fail-safe design. Pebble bed reactors are one such example. These reactors contain spheres of uranium covered by a graphite material with hard shell. As the pebbles heat up, they expand (the “Doppler broadening” effect). This expansion lessens the likelihood of fission events, causing the temperature to naturally fall over time. When designed properly, these reactors can power down safely without coolant or human interaction. Germany, China and South Africa have all explored this technology at some point, but China is the only one of the three with a current development program. The U.S. DOE has also considered a similar design for its “Next Generation Nuclear Plant.“