Union of Concerned Scientists
Citizens and Scientists for Environmental Solutions

Fukushima: Lessons Learned? Public Policy: Regulation, Enforcement, and Reform

The tragedy at the Fukushima Dai-Ichi nuclear plant in March 2011 is the latest in a series of surprising non-surprises. Its design protected vital equipment from damage caused by large earthquakes. Its site was protected against tsunamis by a seawall nearly 15 feet tall. Onsite emergency diesel generators protected against loss of the normal power supply. Batteries protected against loss of this backup power supply. Severe accident management procedures protected against multiple system failures. Yet an earthquake and the tsunamis it generated defeated all the protection layers to cause significant damage to three reactor cores and challenge several spent fuel pools. Tens of thousands of people who endured the earthquake and tsunami had to abandon their homes and disrupt their lives due to the nuclear plant disaster. As Yogi Berra said, "It's déjà vu all over again." There are very few unanticipated disasters and unforeseen hazards. Most disasters occur because existing safety precautions against known hazards proved inadequate. For example:

- In 2010, a blow-out preventer failed to prevent a blow-out at the Deepwater Horizon oil-drilling rig in the Gulf of Mexico.

- Levees failed to protect New Orleans in August 2005 from Hurricane Katrina.

- Global positioning systems and channel markers failed to prevent the Exxon Valdez from running onto Bligh Reef in Alaskan waters in March 1989 and spilling over 250,000 barrels of oil.

- O-rings that had failed during more than a handful of prior shuttle launches failed to protect space shuttle Challenger from exploding shortly after take-off in January 1986.

- And, of course, being deemed "unsinkable" afforded Titanic little protection following its collision with an iceberg in April 1912.

Neither TEPCO – Fukushima's owner – nor the Japanese government considered the plant to be under-protected or overly vulnerable the day before disaster struck. BP considered its Deepwater Horizon platform to be a manageable risk. The U.S. Corp of Engineer believed New Orleans to be adequately protected against most hurricanes. Exxon thought its three-year old oil tanker had state-of-the-art safety measures. NASA felt Challenger was go for launch. And the White Star line was so confident about Titanic's seaworthiness that a senior manager was aboard for the inaugural crossing of the Atlantic.

www.ucsusa.org
Two Brattle Square · Cambridge, MA 02238-9105 · TEL: 617.547.5552 · FAX: 617.864.9405
1825 K Street NW · Suite 800 · Washington, DC 20006-1232 · TEL: 202.223.6133 · FAX: 202.223.6162
2397 Shattuck Avenue · Suite 203 · Berkeley, CA 94704-1567 · TEL: 510.843.1872 · FAX: 510.843.3785
One North LaSalle Street · Suite 1904 · Chicago, IL 60602-4064 · TEL: 312.578.1750 · FAX: 312.578.1751

Our review of past nuclear plant disasters in specific and other disasters in general identified two commonly recurring causes: (1) failure to comply with established safety protocols, and (2) insufficient margins when hazards exceeded those assumed in establishing the safety protocols.

The Challenger disaster was largely caused by safety protocols not being met. At that time, the space shuttle featured large external fuel tanks constructed by bolting segments together. Each flange connection had two pliant o-rings intended to provide a tight seal. Only one o-ring was necessary to provide this seal; the second added an independent layer of protection. On nine prior shuttle launches, flames had damaged an o-ring. In some cases, flames burned completely through that o-ring to damage the second o-ring. The safety protocol required each o-ring to function. However, o-ring failures were tolerated because the second o-rings had not failed—until Challenger blew up shortly after take-off. Challenger's second o-ring failed for the same reason the first one failed—flames damaged them both. O-ring failures indicated a design weakness violating the two independent safety barrier protocol, but that weakness was tolerated until the Challenger was lost. Only then were the external fuel tanks re-designed to eliminate the need for o-rings.

Fukushima demonstrated the results when safety protocols provide inadequate protection against actual hazards. Its 15-feet tall seawall provided scant protection against a 45-feet tall tsunami wave. That inadequacy would have been survivable had it not been for similar inadequacies. The 8-hours of battery capacity provided limited protection against power outages lasting 9 days. And its emergency procedures were transformed into long lists of equipment workers could not use due to the lack of electrical power.

The first common cause is the easier one to remedy. Safety protocols have to be met in order to be effective. Period. No ifs, no ands, no buts, and no excuses. Today, roughly half (47) of the U.S. fleet of 104 operating nuclear reactors fail to comply with fire protection regulations adopted years ago. The NRC has stated that fire constitutes 50 percent of the risk of reactor core damage at the average U.S. nuclear reactor. In other words, the fire threat equals all other threats combined. And that analysis assumed that all fire regulations were met—the hazard only increases when reactors operate in violation of the fire protection regulations. The NRC must establish *and enforce* safety regulations.

The NRC's regulations are essentially contracts between the agency, plant owners, and the public. The regulations define the acceptable level of safety. The regulations thus protect plant owners from the NRC requiring more stringent, and more costly, measures than those specified in the regulations. Similarly, the regulations protect the public from the NRC accepting lower safety levels. The NRC cannot tolerate violations of its regulations without breaching its contract with the American public. That's simply wrong.

The second common cause is more difficult to address. Unless safety protocols are established so conservatively as to bound all possible hazards, drawing the line at x carries the associated policy question "What if x plus 1 happens?" A practical way of testing the propriety of safety protocols is to quantify their robustness and reliability. Consider flooding protection at nuclear plants located next to rivers in the United States. Historical information on past floods is reviewed to establish the flooding heights these plants are designed to withstand without nuclear disaster. But what if future rainfall, snow melts, etc. result in even larger floods? Two flood levels could be determined for each nuclear plant: (1) the flood height likely to be experienced at the site based on historical data, and (2) the flood height projected to almost certainly result in disaster. The difference between these two levels represents the safety margin for flooding at that nuclear plant site. In other words, the safety margin defines the robustness of the flooding design. Margin of 2 inches (i.e., a flood only two inches higher than the design protects against results in disaster) might suggest that additional protection is necessary while margin of 80 feet might suggest otherwise. The reliability of the flooding design needs to complement the robustness determination. For example, margin of 2 inches might be tolerated if chance of having such a flood is 1 in 50 billion years. Conversely, margin of 80 feet might be inadequate if the chance of a flood of that severity is only 1 in 10 years. Robust and reliable safety margins provide useful insights on the adequacy of safety requirements.

The best protection against disaster involves the establishment and enforcement of safety requirements that are robust and reliable enough to manage risks from all known hazards. Identifying the margins associated with safety requirements serves to test their robustness and reliability. Even 100 percent compliance with safety requirements is insufficient if credible hazards of slightly greater magnitude are likely to cause disaster.

This approach should be applied to the lessons learned from Fukushima. For example, the NRC's Fukushima task force recommended that all U.S. nuclear plants adopt a three-tiered approach to ensuring adequate power supplies to emergency equipment. For the first 8 hours, the design should provide sufficient power from permanently installed equipment. From that point until 72 hours, the design can rely on temporary equipment like portable pumps and generators if those resources are already onsite and staffing levels required to take all these steps are sufficient. Beyond 72 hours, the design can rely on resources from offsite locations. The NRC must independently audit measures implemented by all plant owners to verify compliance with the agency's safety requirements. And the NRC must complement this compliance check with robustness and reliability tests answering questions like:

- How long a delay deploying temporary measures can be tolerated before reactor core damage occurs?

- How likely is a delay in deploying temporary measures to occur?

- How long a delay in offsite resources arriving can be tolerated before reactor core damage occurs?

- How likely is a delay in the arrival of offsite resources to occur?

The NRC must become able to look Americans in the eyes and say "We've taken every reasonable step to protect you." Right now, the NRC cannot honestly make this claim. If a U.S. nuclear plant experienced a disaster caused in whole or in part by pre-existing fire protection deficiencies or Fukushima lessons not yet implemented, NRC would be as defenseless as Minerals Management Service after Deepwater Horizon from charges that it should have done more. Rather than waiting for that disaster to induce the reforms and fixes, the NRC must act now to consistently and aggressively enforce its safety requirements. After all, it is one thing for the NRC to have identified lessons learned from Fukushima. It is another thing for the NRC to have ensured that all the nuclear reactors have fully and faithfully implemented those lessons. Safety IOUs are worthless. They represent vulnerabilities that NRC knows to exist at operating nuclear plants, but which have not yet been fixed. They are disasters waiting to happen. They are tomorrow's surprising non-surprises.

Presentation by: David Lochbaum
Director, Nuclear Safety Project
Union of Concerned Scientists
www.ucsusa.org

at the Oberlin Shansi symposium conducted March 9-10, 2012 at Oberlin College in Ohio.