Reflections after The Great Japan Earthquake
Woody

Having been a resident of Japan for almost 10 years, and the manager of risk consulting for two companies which deal with nuclear power, I would like to share with you all my observations.

First, it is necessary to understand Japanese culture. Please take off your "western glasses" and try to understand as a Japanese person would, especially those in the government and those with public responsibility. Do not be judgmental. Be understanding.

In Japan, telling the truth sometimes takes a second seat to not upsetting those superior to one's position. Many times, in all industries, a maintenance person will report that everything is fine, even when it is not. I know of a situation where the periodic testing of a diesel generator failed, but was not reported. "Why?" you may ask. The notions of obligation (to one's superiors) and responsibility (not to upset the *status quo*) take precedence over the truth. For a person to be wrong, to make a mistake, is a grave social and professional error in Japan. In this case, the maintenance personnel would have to admit to his superior, who would have to admit to his superior (*ad infinitum*) that the backup power did not pass the test.

Many incidents have happened at Japanese nuclear power plants that have not been reported to the government or to the public in a timely manner, even when such reporting is required by regulations and law, such as the small releases at the Kashiwazaki NPP after the large seismic event there in 2007; after the Monju accident in 1995, the extent of the fire was covered up by releasing altered videos; and the recent incidents of falsified maintenance records at the Kansai plants have only added to the public distrust of nuclear power.

So trying to understand the exact truth of these incidents at the NPPs, from any of the news media or government press releases, is futile.

And we, as nuclear professionals, must be concerned with other aspects of this situation to insure what remaining support for the nuclear industry by the public remains intact. The loud voices of the (un-) (little) informed on television, radio, and print affect public perceptions much more than the truth, as politicians and public figures well know. We cannot afford to be calm voices of reason. The public cares little for scientific truth.

Moreover, meltdowns, partial or otherwise, or a significant release of radionuclides, are of little importance. What is important is that we have had an accident. The public and politicians will pass judgment accordingly.

So here are my ideas as to where we must take action, if indeed nuclear power is to have a future.

Safety to the Public. Was the decision by TEPCO to inject seawater into the reactor made quickly enough? Did TEPCO hesitate on injection because of the damage which would have been done to the reactor? Which was considered more important: the health of a 40 year-old plant with 50 year-old technology, or the health of the public? One must always act on the side of safety to insure life, even at the cost of property, if nuclear technology is to be accepted.

Perhaps the operators acted too slowly to prevent overheating, including procedures that might have required the venting of small amounts of steam and radiation, rather than risk a complete meltdown. Fear among the Japanese regulators over public reaction to such small releases may have delayed operators from acting quickly: responsibility to the regulators to not get the regulators in trouble with the public.

Japanese have a tendency to only do things if they can be done in a perfect manner: fear of being wrong. They will wait to act, instead of taking an action in a less than optimal manner. The Japanese search for perfection often leads workers, managers, and politicians to freeze in inaction or to hide the true situation.

Crisis Management. While superb evacuations plans were in place for earthquake, tsunami, and nuclear accident, there were no plans in place for a simultaneous occurrence of all three, even though these three rare events are not independent. It is well known that seismically induced station blackout is a dominate accident sequence. Emergency planners should have been made aware of this fact.

The buzz word for this is "risk communication". Usually this refers to communication between those in-the-know with the public or the politicians. In this case it is communication between those doing the risk assessment and the emergency planners, who probably did not consider that emergencies are usually a confluence of rare events, hitherto un-thought-of sequences of the unexpected.

Understanding Rare Events. NPPs are extremely well-run, well-tested systems. What happened in Japan with a 9.0 seismic event and tsunami of such force were indeed rare events. But here are some observations, first made by Herb Hecht with respect to software systems, which apply here:

1. In well-tested systems, rarely executed code has a higher failure rate than frequently executed code;
2. consequences of rare event failures in well-tested systems are more severe than those of other failures;
3. given that there are failures in a well-tested system, significantly more of the failures are caused by rare events;
4. inability to handle multiple rare conditions is a prominent cause of failure in well-tested systems.

In short, we have tested out all of the light stuff and what we are left with are rare accidents with severe consequences in any well-tested software system.

How does this apply to other well-tested, vigilantly maintained systems, with well trained staff and enlightened management, good operating procedures in place; do Herb Hecht's observations about software systems apply to a nuclear facility? I believe that they do.

In an NPP, by exceptional planning, maintenance, reliability of equipment, human factors, emergency training, and organizational development skills, the facility is kept in safe operations. The known and the easy problems are vanquished. What are left are the rare events. So if there is a failure, chances are the failure is rare event.

Moreover, Herb Hecht's study makes the following observation: all of the software which failed from three rare events, also failed, perhaps less severely, from two rare events, and three-quarters of the software which failed from two rare events, also failed, perhaps less severely, from one rare event.

What this means at an NPP is that if unwanted events and their consequences are actively guarded against, and equipment is vigilantly maintained, barriers in place, and staff prepared to prevent these events, and if indeed symptoms of unwanted events begin to occur, then there is a good chance that if we are on a failure path, it is the start of a severe accident scenario. Perhaps more failures will occur to compound the situation and form a scenario which may have never been thought of, or previously dismissed as being improbable, and there are no procedures, nor experience nor training to aid in recovery. Chances are that this is not a simple or known situation; the first rare event failure has a good probability of being a harbinger of a severe accident scenario.

Public Communication. While the explosion at Fukushima Daiich #1 occurred at 15:30 on Saturday, the government did not announce the explosion until almost 17:30. The announcement that there had been no large release of radionuclide did not occur until after 20:30. The public perception, here in Japan, was completely, again, that the government and TEPCO have not been telling the truth in a timely manner. Needless to say, Japanese people have an aversion to things nuclear, and truth aversion by superiors only adds to the disaster.

The PSA. In Japan, the PSA is usually done by the reactor vendor. This is quite different than many other countries. Also, the PSA is not disclosed, and will never be disclosed, especially the basic data used (failure rates, seismic frequencies and fragilities, etc.). For example, the seismic data for the JNFL Rokkasho-mura fuel reprocessing plant will not be released by the firm which did the seismic study, even to JNFL. We will never know if the Fukushima failure sequence which began with station blackout caused by a seismic event also considered loss of backup systems caused by the seismically induced tsunami, definitely a common cause initiating event (earthquake/tsunami). In any case, the PSAs must be peer reviewed by independent entities and the data which are the basis must not be held private. One PSA professional, in charge of the PSA at a well known Japanese NPP, actually told me that the CDF was 1e-9 at his plant ... a nice number for his management, but a little dubious for a risk professional.

Seismic, Seismic, Seismic. In a meeting in April, 2010, with a top official from the Japanese regulator, we asked what the most important risk problem was for Japanese NPPs. He said, "There are three problems: (1) Seismic, (2) Seismic, and (3) Seismic. Does anything more need to be said?