Learning from failures

Angela Saini

Today's complex energy systems are bound to fail under extreme or unexpected conditions. Preparing for these rare events and containing the damage is an essential part of managing such occurrences.

It is usually in the extremes, say if we lose a job or fall sick, that our characters are truly tested. This is something humans have in common with machines: The real measure of us both is not just in years of survival but in the way we respond to disaster. And that is certainly the case for the nuclear industry following the earthquake and tsunami that hit the Fukushima Daiichi power plant in Japan this spring.

Of the 440 reactors in safe operation around the world, this is the one to have become the focus of debate on the future of atomic energy. Although China and India may need to press ahead with their ambitious plans for new reactors to match growing energy demand, the failure at Fukushima has prompted all countries to revisit safety standards and forensically pick apart the debris of the disaster to figure out what lessons can be learned, how to prevent future failures, how to improve design and materials, and how to respond effectively to accidents that happen despite elaborate procedures for risk mitigation.

Catastrophic failures can have many causes. Some come from human failings or shortcuts taken to save costs or time, perhaps making routine operation more efficient. Other catastrophic failures stem from engineering or materials failures, sometimes seemingly mundane ones. The cause of the explosion of the Space Shuttle Challenger in 1986, for example, lay partly in its rubber O-rings, which should have sealed gases inside the rocket boosters but went brittle in freezing cold weather. This meant that one particular joint could not withstand the dynamic load it was subjected to during the flight. Similarly, the Norwegian oil rig Alexander L. Kielland capsized in 1980 because of a fatigue fracture that originated in a six-millimeter weld. Materials weaknesses such as these—as well as oxidation, corrosion, and creep—seem simple enough to prevent in hindsight, but in these extreme cases, it took disasters to spot them.

Energy technologies inherently contain risk due to the necessity of managing high energy densities, complex processes, and extreme heating and cooling. Some risks are dramatic and insidious like those of nuclear reactors. Some are apparent like those of mining coal or deep sea oil drilling. Some are invisible like the emission of pollutants and carbon dioxide from fossil fuel combustion. According to Michael Golay, a professor of nuclear science and engineering at the Massachusetts Institute of Technology, the major difference at Fukushima Daiichi is that the accident was precipitated not by humans, but by a natural event—which is rare. "Usually when you're looking at technological disasters, the lessons are that somebody failed, that someone was careless in some important area. In the case of Fukushima, those lessons don't apply. That doesn't mean that things won't be learned, but they won't be the more obvious ones," said Golay.

One of the most important lessons from both the disaster in Fukushima and the BP Deepwater Horizon oil spill in the Gulf of Mexico last year is that the post-accident response could be improved. Even if all safety procedures are fully in place and followed and lessons have been learned from the past, it is still not feasible to build completely full-proof systems against the unexpected. "Technological disasters are here to stay. We should focus as much attention on managing a disaster

A picture taken from a helicopter on March 16, 2011 of an explosion caused by a build-up of hydrogen in the Fukushima Daiichi Unit 3 nuclear power station in Japan. Although the reactor's primary containment vessel was not damaged, the explosion injured 11 people. *Credit*: Tokyo Electric Power Co.

https://doi.org/10.1557/mrs.2011.139 Published online by Cambridge University Press

as minimizing its occurrence," explained V.S. Arunachalam of the Center for Study of Science, Technology and Policy in Bangalore, India. In each case, there did not seem to be enough planning to cope with the chain of failures.

An effective way of coping with the confusion and bad decisions that can sometimes be made in the wake of an accident is to prepare "what if" scenarios in advance for all possible eventualities, however unlikely they may be. This scenario planning needs to go hand in hand with expertise on the ground, so it is also important to have a team of professionals on hand that is available to reliably ask and answer "what if" questions the moment a disaster happens.

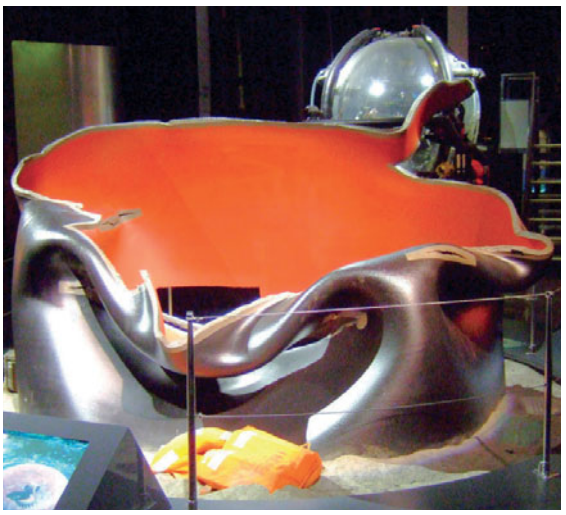
As surgeon and writer Atul Gawande explains in his book, *The Checklist Manifesto* (2009), exhaustive planning may seem unnecessary or simplistic, but evidence has shown that it saves lives. It was exactly this kind of preparation during NASA's Apollo 13 moon mission in 1970, when an oxygen tank exploded and forced an emergency return to Earth, that allowed the craft's crew to return home safely.

The problem for both the materials community and the wider engineering industry, though, is that planning is nowadays more difficult because systems have become so complex and difficult to understand. "The very close coupling of subsystems that makes machines more efficient can also create multiple paths for catastrophic failures," explained Arunachalam. These interlinked systems raise the risk of technological disaster. Along with constraints on knowledge, computational power, resources, and time, they place natural limits on how experts can reasonably be expected to anticipate and respond to failure.

Arunachalam described the problem as "bounded rationality." A classic example is that of the world's first commercial jet airliner, the de Havilland Comet, which suffered three crashes in the space of a few months in 1954. Its problem lay in fatigue of the aluminium alloy structure around the doors and windows—fabrication had been poor and then stress tests were performed incorrectly, which meant that the inspectors who signed off on the plane as airworthy did not have correct information about its true safety.

The Comet airliner first highlighted the phenomenon of low cycle fatigue to metallurgists. It was also proof for the need to be vigilant against the temptation to believe it is possible to design out failure. Russian Prime Minister Vladimir Putin, for instance, announced in the wake of Fukushima that his country's new generation of reactors would be built using an "arsenal of progressive technological means to ensure the stable and accident-free operation of nuclear power plants." But even with computer simulations to model weaknesses and with the reassurance of passive safety features, backup systems, alarms, rigorous materials testing, and duplicate components, there is likely to be a leftover degree of risk.

Mitigating complex risks means constantly thinking the unthinkable. "Even if we could achieve failure-proof designs," said Henry Petroski, a professor of civil engineering at Duke University and the author of *To Engineer Is Human: The Role of Failure in Successful Design* (1985), "which would mean that there would be no accidents or disasters over a prolonged period of time, there would develop great pressures within an industry or regulatory body to relax standards, lower factors of safety, operate beyond experience, and generally move toward less safe conditions."



One of six bracings supporting the Alexander L. Kielland, a Norwegian oil rig that failed in 1980 from a fatigue crack resulting from a poor weld. Of 212 people aboard, only 89 survived the accident. This section of the rig is on display at the Norwegian Petroleum Museum in Stavanger. ©2007 Jarle Vines, some rights reserved.

Indeed, following the oil spill in the Gulf of Mexico, a U.S. National Commission blamed the disaster on a "culture of complacency" that led to a systematic oversight of safety issues. This complacency applies as much to tackling accidents as guarding against failure in the first place.

A final lesson from Fukushima and the Gulf of Mexico is that the work of scientists and engineers during a major disaster often happens in the glare of the media spotlight. So alongside dealing with the technical problems, it is vital to understand and respond sensitively to people's fears. David Ropeik, a consultant on risk perception and the author of *How Risky Is It, Really? Why Our Fears Don't Always Match the Facts* (2010), said that Fukushima provided a lesson in what not to do. "Inconsistent communications between the people who are supposed to protect the population—in this case the company on the one hand and the government on the other—are unsettling because they don't seem to be all on the same page," he explained.

On the 25th anniversary of the Chernobyl disaster in April, just weeks after the catastrophe in Fukushima, United Nations Secretary-General Ban Ki-moon said that nuclear power plants should continue to be sources of peaceful energy. Developing post-accident technologies and thorough disaster planning, as well as keeping an open dialogue with the public, are some of the keys to maintaining this confidence in the energy industry when a failure happens. Incorporating lessons from the past is a key place to start. □

https://doi.org/10.1557/mrs.2011.139 Published online by Cambridge University Press