Bulletin of the Atomic Scientists

IT IS 6 MINUTES TO MIDNIGHT

Feature

Bulletin of the Atomic Scientists
67(6) 44–52

DOI: 10.1177/0096340211426395
http://thebulletin.sagepub.com

Fukushima and the inevitability of accidents

Charles Perrow

Abstract

Governments regulate risky industrial systems such as nuclear power plants in hopes of making them less risky, and a variety of formal and informal warning systems can help society avoid catastrophe. Governments, businesses, and citizens respond when disaster occurs. But recent history is rife with major disasters accompanied by failed regulation, ignored warnings, inept disaster response, and commonplace human error. Furthermore, despite the best attempts to forestall them, "normal" accidents will inevitably occur in the complex, tightly coupled systems of modern society, resulting in the kind of unpredictable, cascading disaster seen at the Fukushima Daiichi Nuclear Power Station. Government and business can always do more to prevent serious accidents through regulation, design, training, and mindfulness. Even so, some complex systems with catastrophic potential are just too dangerous to exist, because they cannot be made safe, regardless of human effort.

Keywords

accident warnings, industrial disasters, normal accidents, probability, regulatory failure, risk

The March 11, 2011 disaster at the Fukushima Daiichi Nuclear Power Station in Japan replicates the bullet points of most recent industrial disasters. It is outstanding in its magnitude, perhaps surpassing Chernobyl in its effects, but in most other respects, it simply indicates the risks that we run when we allow high concentrations of energy, economic power, and political power to form. Just how commonplace— prosaic, even—this disaster was illustrates just how risky the industrial and financial world really is.

Nothing is perfect, no matter how hard people try to make things work, and in the industrial arena there will always be failures of design, components, or procedures. There will always be operator errors and unexpected environmental conditions. Because of the inevitability of these failures, and because there are often economic incentives for business not to try very hard to play it safe, government regulates risky systems in an attempt to make them less so. Formal and informal warning systems constitute another method of dealing with the inherently risky systems of industrial society. And society can always be better prepared to respond when accidents and disasters occur.

But for many reasons, even quality regulation, close attention to warnings, and careful plans for responding to disaster cannot eliminate the possibility of catastrophic industrial accidents. Because that possibility is always there, it is important to ask whether some industrial systems have such huge catastrophic potential that they should not be allowed to exist.

Regulations

Nuclear safety is problematic when nuclear plants are in private hands because private firms have the incentive and, often, the political and economic power to resist effective regulation. That resistance often results in regulators being captured in some way by the industry. In Japan and India, for example, the regulatory function concerned with safety is subservient to the ministry concerned with promoting nuclear power and, therefore, is not independent. The United States had a similar problem that was partially corrected in 1975 by putting nuclear safety into the hands of an independent agency, the Nuclear Regulatory Commission (NRC), and leaving the promotion of nuclear power in the hands of the Energy Department. Japan is now considering such a separation. It should make one. Since the accident at Fukushima, many observers have charged that there is a revolving door between industry and the nuclear regulatory agency in Japan—what the *New York Times* called a "nuclear power village"—compromising the regulatory function.

Of course, even in Europe, where for-profit firms have less power, there are safety problems that have needed more effective oversight. But by and large, European nuclear plants, which are generally part of a state-run industry, appear to be safer than the privately owned, poorly regulated nuclear plants in the United States, Japan, and other countries.

Systemic regulatory failure—as opposed to simple error—is tricky to identify accurately. After an accident in a risky industry, it is always possible to find some failure of a regulatory agency. Everything, after all, is subject to error, in regulatory agencies as well as chemical or power plants. To say that regulation failed on a system-wide basis, one must have strong evidence of agency incompetence or collusion.

The Union Carbide chemical plant in Institute, West Virginia, is my favorite example of regulatory incompetence; in this case, it was a matter of regulators seeing what they were apparently predisposed to see. Shortly after a Union Carbide pesticide plant in Bhopal, India, leaked methyl isocyanate gas in December 1984, killing thousands, the Occupational Safety and Health Administration (OSHA) inspected the company's West Virginia plant and gave it a clean bill of health. What happened in Third World India could not happen in the United States, it was said.

Nine months later, an accident quite similar to Bhopal occurred at the plant, though the gas released was not as toxic and the wind was in a favorable direction, so only some 135 people were hospitalized (Perrow, 2011: 179–180). OSHA looked again and, predictably, found "an accident waiting to happen" and cited the plant for numerous violations, despite its clean bill of health nine months before. There was a trivial fine and a Union Carbide promise to store only the small amounts of the toxic gas actually needed for production.

Union Carbide soon resumed massive storage of methyl iscocyanate. Bayer subsequently took over the plant and, in 2008, an explosion killed two workers and threatened to release 4,000 gallons of the deadly gas. Subsequent investigation by the US Chemical Safety Board again found an accident waiting to happen. OSHA appears not to have noticed that its strictures on the amount of storage were violated.

Regulations will always be imperfect. They cannot cover every exigency, and, unfortunately, almost anything can be declared the cause of an accident. One can also make the case that too much regulation interferes with safe practices, as nuclear plant operators have always claimed in the United States. But the overregulation complaint is undermined by the following anecdote: A few years ago, the NRC sharply increased the number of inspections of nuclear power plants following some embarrassing near-misses. A then-powerful US senator, Pete Domenici of New Mexico, a recipient of large campaign donations from the industry, called in top NRC officials and threatened to cut the agency's budget in half if it did not reduce the number of inspections (Mangels, 2003). The NRC reduced its inspections. I doubt that anything similar could take place in Europe.

Regulatory capture is widespread in many risky US industrial systems and often subtle—but not always. In the Interior Department's Materials Management Service, for example, representatives of the oil industry and regulators who were supposed to be overseeing oil exploration exchanged sexual favors and drugs. This intramural partying was disclosed just before the BP-leased *Deepwater Horizon* oil rig blew up in the Gulf of Mexico, resulting in the largest oil spill of its kind, making the regulatory failure especially dramatic.

Charges of regulatory failure were also levied in the 2010 Massey Energy coal mine disaster in West Virginia, which killed 29; the explosion at BP's Texas City, Texas, refinery in 2005, which killed 15 and injured at least 170; and BP's massive oil pipeline break in 2006 in Prudhoe Bay, Alaska.

There are many forms of regulatory failure. Regulations on the books can lie dormant by the common consent of regulators and industry. A worker at the Millstone nuclear power plant in Connecticut kept warning management that the spent fuel rods were being put too quickly into the spent storage pool and that the number of rods in the pool exceeded specifications. Management ignored him, so he went directly to the NRC, which eventually admitted that it knew of both of the forbidden practices, which happened at many plants, but chose to ignore them. The whistleblower was fired and blacklisted.

Rather than completely ignore regulations, a captured regulatory agency may just lower the standards it uses. The NRC has consistently lowered standards for emergency electric power supplies in US nuclear plants. And in the wake of the Fukushima disaster, the government of Japan is lowering standards for allowable doses of radiation.

Regulations are only as good as their enforcement, and here the evidence is fairly uniform: Enforcement is generally lax and often all but nonexistent. Workers at Fukushima reported that they had advance warnings of inspections, and inspectors regularly winked at violations. The record of the NRC is

similar in the United States; for example, when utilities complained about the standards for fire prevention at nuclear plants in recent years, the regulators lowered the standards.

Even when safety inspections find violations, there is no guarantee that the regulated firm will be moved to change its practices. In many cases, the fines levied are too small to be a deterrent. After BP's huge spill in Prudhoe Bay, the company was fined less than its profits for one day of operation. After the Texas City refinery explosion, the *New York Times* reported that OSHA had levied a record fine of $87 million against the firm. According to BP, it made a profit of about $14 billion in 2009, meaning the fine amounted to about six-tenths of a percent of its profit for the year. An official of OSHA subsequently testified to the agency's weakness and the power of the petrochemical industry by noting that the size of the fines levied did not deter; firms repeated the same glaring mistakes despite their costs, ignored warnings, and harassed workers who warned of wrongdoing.

Warnings

Even if a risky system is only loosely regulated, a point will come when warnings are loud enough to attract attention. Catastrophes are expensive; no one wants them. The overall experience with warnings about global warming, however, should caution against expecting warnings to be too effective. A well-funded but factually challenged campaign to deny that climate change is the result of human activity has managed to ice the climate-warming warnings of a consensus of thousands of the world's top climate scientists.

Not surprisingly, we also do not find that warnings of looming industrial and financial disasters have much impact. At Fukushima, the regulatory authorities required a seawall that was a bit taller than the largest tsunami that locale had experienced in the last 1,000 years. So the danger was, indeed, recognized. But the seawall design was based on probabilistic thinking, not thinking about what is possible, and the seawall was horribly inadequate to the 2011 tsunami.

Some Japanese experts had done possibility analysis. They pointed to historical records of a huge tsunami in the year 869; three huge tsunamis on the Pacific Ring of Fire, along which Japan lies, in the last 100 years; and a geological record of relentless collision between two tectonic plates underneath Japan. Before 2011, these experts were largely ignored.

Japan has 53 nuclear power plants drawing cooling water from the ocean. Before Fukushima, 14 lawsuits charging that risks had been ignored or hidden were filed in Japan, revealing a disturbing pattern in which operators underestimated or hid seismic dangers to avoid costly upgrades and keep operating. But all the lawsuits were unsuccessful.

A representative in the Japanese parliament in 2003 warned that the nuclear plants were not sufficiently protected; a seismology professor at Kobe University resigned in protest from a nuclear safety board in 2006 due to a lack of attention to earthquake and tsunami risks. Even though there had been a 30-foot tsunami in 1993 on Japan's west coast from a much smaller 7.8 earthquake, the former head of the Toyko Electric Power Company (Tepco) said

that that the risk of a tsunami never crossed his mind when he was president of that firm. He obviously did not have a possibilistic mind set.

But warnings can be slippery and hard to use effectively, regardless of the attitudes of the people being warned. Too often warnings are imprecise, which was why Condoleezza Rice, as national security adviser at the time of 9/11, dismissed the warnings of a terrorist attack using airplanes. The warnings did not specify the time and place. Many warnings are, in fact, so general as to be useless, e.g., "nuclear power is dangerous" or "radical Moslems will strike the United States."

There is the problem that warnings are often seen as mere obstructionism. This was the view of a representative for a Japanese utility who brushed away the possibility that two backup electrical generators would fail simultaneously. He said that worrying about such possibilities would "make it impossible to ever build anything."

Warnings may also be false, especially if based upon information that has little credibility, as with the weapons of mass destruction that Iraq was supposed to have. Many seemingly credible warnings never materialized, e.g., that President Barack Obama would not live through his first year in office. Florida coast residents are said to have stopped paying much attention to hurricane warnings after there were two evacuations for storms that didn't make landfall in the state.

And to be sure, there are major accidents that occur without warning, including the Three Mile Island nuclear incident and some chemical plant accidents, such as the toxic releases from Union Carbide's West Virginia plant. But these no-warning events are few. Credible warnings before major accidents are much more common.

The most credible ones are specific and in-house: The night before the launch of the space shuttle *Challenger*, engineers wanted to delay it because of the cold, saying, "We have never launched at this temperature, and cold affects the O rings." Before the re-entry that burned up *Columbia*, a technician on the shuttle's launch team tried to get pictures of the extent of the damage caused by chunks of insulation that had fallen off a fuel tank during the lift-off. Before the *Deepwater Horizon* was destroyed in a fiery blowout, Halliburton managers warned BP officials that there were not enough stabilizing rings installed on the drill pipe to continue drilling safely. Before BP's Prudhoe pipeline leaked, workmen placed hand-painted signs in the parts of the pipeline that did the most shaking, warning people to stand back because it might rupture (it did, but in an isolated area, and the break was not discovered for some days). Testimony has revealed that Massey managers regularly told supervisors to ignore warnings of dangerous concentrations of methane.

The warning at Texas City a few days before the plant blew was less specific than these others, but more ominous. At a company safety meeting, a slide was shown that simply said, "This is not a safe plant to work in." It was the view of management at the plant; they were unable to maintain the plant in safe conditions because of budget cuts and production pressures by top management.

Other warnings are more general and long range, but significant anyway. Scientists had regularly warned that the

erosion of the wetlands protecting New Orleans was making it more vulnerable to hurricanes. They were more specific about the negative consequences of building a new ship canal that did, as predicted, channel Katrina's storm surge directly into the city.

There were multiple warnings in the United States before the 2008 economic meltdown. They came from some directors of impacted firms and from many risk managers and department heads, worried about the risks of their highly profitable mortgage business. They also came from government regulatory agencies, including the Securities and Exchange Commission, and watchdog agencies such as the Government Accountability Office; from bills proposed in Congress; from chief executives of financial firms not at direct risk; from financial gurus; and from journalists at leading magazines such as the *Economist*. There were also some 7,000 news stories containing the phrase "the housing bubble" from 2000 to 2006, meaning there were seven years of warnings before that bubble burst late in 2007.

Indeed, according to a book by a respected journalist (Sorkin, 2011), the newly appointed secretary of the treasury in the Bush administration, Henry Paulson, delivered warnings about a dangerous mortgage bubble at his first cabinet meeting in 2006. He proposed that investment banks be regulated much as commercial banks were, but Goldman Sachs, where Paulson had just served as president, and other major investment banks that dominated Wall Street would not hear of it. Credible warnings were dense, but the profits the firms were making drowned them out.

Coping

So how do organizations cope with disasters once one occurs? The record here is just as dismal as with regulation and warnings.

There are vastly more cases of creative coping from citizens than from organizations. The true first responders to disaster—co-workers, neighbors, passersby—have almost always performed splendidly, as with the completely self-organized flotilla that evacuated thousands from lower Manhattan in the 9/11 crisis. And in a few cases, governmental agencies and private firms do successfully cope with disaster.

Though failed space flights do not have the catastrophic potential of the other systems I have mentioned (they affect only a handful of people), they are complex and risky. The rescue of the crippled *Apollo 13* capsule is a prime case of skill and innovation in dealing with and overcoming a failure. There are many outstanding examples of coping by airplane pilots, though, again, the potential loss of life in these cases is relatively small. The response of President Lyndon Johnson's administration to the 1964 Alaskan earthquake—at 9.2 magnitude, the biggest ever in North America—is a model of what can be done by government to help victims and rebuild a city. But examples of creative coping by organizations are rare.

The poster child for official failure to cope with disaster is the response to Hurricane Katrina, the subject of so many books and articles that I will not dwell upon it (although it should be noted that the US Coast Guard performed extremely well and the unofficial response by citizens and private firms

was often innovative and effective). In the case of Fukushima, there was official denial and secrecy, refusal to accept outside help, the failure to evacuate citizens at risk, and an attempt by the prime minister to halt the cooling of the damaged reactors by seawater shortly after the process had been started (fortunately, the plant manager lied, saying he had stopped using seawater even as he continued to use the ocean to cool the crippled plants, thus preventing a far worse catastrophe).

At Bhopal, plant officials initially denied any chemical release and then said it was not dangerous, even as they themselves were fleeing upwind of the toxic fumes. The Soviet Union refused to admit there had been an accident at Chernobyl, even after the Swedish nuclear agency had concluded that the radioactive materials they were detecting had to come from Chernobyl. Worse yet, the USSR waited two days before evacuating the town next to the plant. BP officials *and* American officials consistently minimized the damage of the oil spill in the Gulf of Mexico and kept reporters and scientists away from the scene. Little of the equipment oil companies are required to have on hand in case of a big spill was present when the Exxon Valdez ran aground. Similarly, Massey Energy didn't have equipment available to handle a mine explosion.

Crises may bring out the best in citizens. But, in some cases, they often raise the rate of routine errors made by distressed, tired managers and workers. At Fukushima, workers desperately trying to assemble a huge tank that would remove radioactive substances from the salt water being poured over the damaged reactor and its spent fuel pool saw the system fail on its first trial—because a valve had been installed backward. Workers at the Fort Calhoun Nuclear Power Plant near Omaha were surrounded by a flooding Missouri River with dikes close to being topped. They assembled an emergency berm to protect the vital electrical system. It was a 15-foot-wide, eight-foot-high plastic doughnut filled with water, a literal example of defense in depth. But someone backed a truck into it, and all the water poured out onto the soggy plant grounds.

This litany of regulatory failures, failures to heed warnings, and commonplace failures is independent of normal accident theory. That theory says that even if we had excellent regulation and everyone played it safe, there would still be accidents in systems that are highly "interactively complex," and if the systems are tightly coupled, even small failures will cascade through them. The theory is useful for its emphasis on system complexity and tight coupling; these concepts play a huge role in analyzing the failures of any source in risky systems. In the financial meltdown, for example, the mounting complexity of the overall system allowed fraud and self-dealing to go undetected, and the tight coupling of many systems allowed the failures to cascade.

In my work on "normal accidents," I have argued that some complex organizations—such as chemical plants, nuclear power plants, nuclear weapons systems, and, to a more limited extent, air transport networks—have so many nonlinear system properties that eventually the unanticipated interaction of multiple failures may create an accident that no designer could have anticipated and no operator can understand.

Everything is subject to failure—designs, procedures, supplies and equipment, operators, and the environment. The government and businesses know this and design safety devices with multiple redundancies and all kinds of bells and whistles. But nonlinear, unexpected interactions of even small failures can defeat these safety systems. If the system is also tightly coupled, no intervention can prevent a cascade of failures that brings it down.

I use the term "normal" because these characteristics are built into the systems; there is nothing one can do about them other than to initiate massive system redesigns to reduce interactive complexity and to loosen coupling. Companies and governments can modularize integrated designs and deconcentrate hazardous material. Actually, though, compared with the prosaic cases previously mentioned, normal accidents are rare. (Three Mile Island is the only accident in my list that qualifies.) It is much more common for systems with catastrophic potential to fail because of poor regulation, ignored warnings, production pressures, cost cutting, poor training, and so on.

All of the organizational faults I have noted have their counterpart in daily life. Like organizations and their leaders, people seek wealth and prestige and a reputation for integrity. In the process, they occasionally find it necessary to be deceitful, engaging in denials and coverups, cheating and fabrication. Everyone has violated regulations, failed to plan ahead, and bungled in crises. But people are not, as individuals, repositories of radioactive materials, toxic substances, and explosives, nor do they sit astride critical infrastructures. Organizations do. The consequences of an individual's failures can only be catastrophic if they are magnified by organizations. The larger the organizations, the greater the concentration of destructive power. The larger the organizations, the greater the potential for political power that can influence regulations and ignore warnings.

Modern society is not likely to deconcentrate big organizations and toxic substances, so what can be done? High-reliability theory is correct, of course, to say that government and business can do much more than they do to prevent serious accidents through constant training and mindfulness. More important is system design: Modular systems are less vulnerable than integrated ones, and the toxic and explosive potential is more dispersed in modular systems than in tightly coupled ones. Even more can be done through regulation; highly regulated nuclear power plants in Europe do much better than poorly regulated ones in the United States and Japan. Technical improvements can make systems safer, of course, and we do learn from past disasters. Emergency power facilities are being upgraded at nuclear plants in the United States because of Fukushima.

And the learning is continuous. Before the Three Mile Island incident, some held that during a loss-of-coolant accident in a nuclear plant, there would be a possibility of a zirconium-water reaction that consumes oxygen and frees hydrogen, which is explosive. One nuclear scientist scoffed at such a possibility in a publication, which was released shortly before he was, unfortunately, designated to be the key scientific adviser to Pennsylvania Governor Richard Thornburg during the Three Mile Island accident. (Later, the scientist

was appointed chairman of the NRC.) The scientist was of course wrong. The appearance of hydrogen meant there was hydrogen "burn," as it is called, at Three Mile Island. Fortunately, the hydrogen accumulation was small, and the damage was minimal.

With this march of knowledge, engineers learned to install vents to prevent the explosive accumulation of hydrogen in the reactor buildings of nuclear plants in case of a loss-of-coolant accident. But the vents failed at Fukushima, and hydrogen explosions sent radioactive materials and gasses into the environment. Don't despair, though. Learning from disaster still goes on: US plants have been asked to make sure their vents will open as designed in case of a hydrogen explosion!

It is the commonplace scenario, such as this encounter with zirconium and vents, that needs to be emphasized. Prosaic organizational failures will always be with us, and knowledge is always incomplete or in dispute. Even highly reliable systems are subject to everyday failures, and even if we avoid these, there is always the possibility of normal accidents—rare but inevitable in interactively complex, tightly coupled systems. Some complex systems with catastrophic potential are just too dangerous to exist, not because we do not want to make them safe, but because, as so much experience has shown, we simply cannot.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

Mangels J (2003) NRC cracks down: Industry strikes back. *Cleveland Plain Dealer*, June 25.

Perrow C (2011) *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*. Princeton, NJ: Princeton University Press.

Sorkin A (2011) *Too Big to Fail*. New York: Penguin.

Author biography

Charles Perrow is an emeritus professor of sociology at Yale University and visiting professor at Stanford University. The author of several books and many articles on organizations, he is primarily concerned with the impact of large organizations on society (*Organizing America: Wealth, Power, and the Origins of Corporate Capitalism*, Princeton University Press, 2001), and their catastrophic potentials (*Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, 1999; *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*, Princeton University Press, 2011).