This paper began with an invitation from Japan a month after the disaster at Fukushima I Nuclear Power Plant began on March 11, 2011. The paper was to be presented six months later (October 30) — at a conference where I was already scheduled to present a paper on the use of imaginary cases in ethics (Davis, 2012). The disaster was still very much the province of journalism. Its outlines certainly lacked the stability of history. Of course, even history, though it generally seems stable, is not entirely so, being subject to dispute here and there and to radical revision every now and then. At first, Fukushima’s facts changed almost daily — if by “facts” we mean those descriptive propositions about which there is general agreement. After a while, the changes were less frequent and more a matter of addition than correction. Today, a year after I began work on the paper, the outline of the disaster seems settled. Dispute now concerns only details, such as how much land, if any, will have to be abandoned for some years, how many premature deaths are to be expected because of radiation released during the disaster, and so on. At some point, I had to stop worrying about the facts and report my reflections. I stopped worrying about the facts on October 15, 2011. Since then, I have changed “a fact” only when a reader or auditor pointed out that it was no longer fact.

I am an oddity in science and technology studies (STS) because I focus not on science and technology but on scientists and technologists. Indeed, I do not write about “scientists” in general or “technologists” in general but about specific professions, for example, chemists or engineers. While most STS scholars seem...
Third Nuclear Disasters and a Hurricane Michael Davis
Journal of Applied Ethics and Philosophy Vol. 4

The nuclear disaster that Japan suffered at Fukushima in 2011 is the importance of not leaving complex technical systems unattended. Engineering systems do not work long without engineers. A fourth lesson may concern the way engineers should respond, and typically do respond, to engineering disasters. They should take responsibility for managing the harm as well as for helping to identify the problem, even if limiting the harm involves risking their lives. To see what I mean, let us consider four disasters in greater detail, beginning with the first.

Three Mile Island

Three Mile Island was a “normal accident”, that is, it began with ordinary failures of equipment and practice within a plant itself operating normally.

Daiichi

Daiichi suffered a partial meltdown. To date, Chernobyl seems to have directly killed thirty-eight reactor site and workers, to have injured or killed at the plant. (Wiki, “Fukushima Daiichi”)

Dai-ni

Dai-ni”. For details, see Wiki, “Fukushima II.

Dai-ri

Dai-ri). For details, see Wiki, “Fukushima II.

The discussion of Fukushima below relies not on this source but also on Wiki, “Fukushima I.

Though I shall hereafter refer to “Fukushima”, it is in fact Fukushima I (Fukushima Dai-ichi) that I shall be referring to. There is also a Fukushima II (Fukushima Dai-ni). For details, see Wiki, “Fukushima II.

Though certainly a nuclear disaster, Fukushima is not just another nuclear disaster. In ways important to engineers, it is much more like Katrina’s destruction of New Orleans than like any other nuclear disaster. It is (primarily) a consequence of a natural—or, at least, much larger—disaster, the enormous earthquake and tsunami that wrought so much harm for much of the world. On March 11, 2011, killing about 28,000 people, Fukushima has many lessons to teach, especially if we compare it with these other disasters. Here I shall focus on four lessons:

The first concerns the different roles engineers have at different stages in an engineering project, especially the relative powerless of engineers to affect certain early large-scale trade-offs between public safety and public profit. A second lesson may be that in some mechanical cause of the coolant-loss meltdown that followed. The mechanical failures were compounded by the failure of plant operators to recognize the situation as a loss-of-coolant accident for more than two hours. (One cause of their failure seems to have been an indicator light blocked from view.) That initial failure led an operator to override the reactor’s automatic emergency cooling system manually. With the relief valve still open, the quench tank that collected the discharge from the release valve overflowed, causing the containment building’s sump to fill and sound an alarm at 4:11 am (eleven minutes after the initial release of alarm, along with higher than normal temperatures on the discharge line and unusually high pressures and in the containment building, clearly indicated that there was a loss of coolant. An emergency, the operators did not respond to these indications. At 4:15, the quench-tank relief diaphragm ruptured and radioactive coolant began to leak out into the general containment building. This coolant was pumped from the containment building sump to an auxiliary building, outside the main containment, until the sump pumps were stopped at 4:39 am.

After almost eighty minutes of slow temperature rise, the primary loop’s four main pumps began to suffer damage as a mixture of steam and water passed through them. The operators then shut down the pumps, believing that natural circulation would provide the coolant movement, but steam in the system (itself the product of rising temperature) prevented coolant flow through the core. At the coolant stopped circulating, it increasingly turned to steam. Just a few minutes later, in a moment of trouble, the coolant level fell so low that the top of the reactor core was exposed to the steam. Intense heat then caused a reaction between the steam in the reactor core and the nuclear fuel-rod cladding. That reaction burned off the cladding and damaged the fueled pellets. The pellets then released more radioactivity into the reactor coolant, producing hydrogen gas that caused a further explosion in the containment building in the aftermoon.

At 6 am (two hours after the incident began), there was a change of shift in the control room. A new arrival noticed that temperature readings were high and holding tanks were too high and used a backup valve to shut off the coolant venting through the relief valve. But, by then, about 120,000 liters of coolant had already leaked from the primary loop and filled the containment building. At 7 am (almost three hours after the incident began) did contaminated water reach radiation-activated alarms. By then, the radiation in the primary coolant water was around three-hundred times higher than usual. The plant was seriously contaminated and the reactor’s core had suffered a partial meltdown.

The Nuclear Regulatory Commission (NRC) may be the most extensive investigation of the disaster, a typical engineering response. Its report ended with recommendations for changes in controls, quality assurance, maintenance, operator training, management,
and communication of important safety information. There was no finding of negligence or more serious wrongdoing having caused the disaster, no suggestion that major redesign of nuclear plants was needed, and no proposal to rethink the place of nuclear energy in the generation of electricity. (Rogovin 1980, pp. 89-93, focused mainly on changes in emphasis and procedures at the NRC; Kemeny 1979, pp. 61-73, focused on "attitudes and practices"). These reports do, however, contain much criticism of other aspects of how Three Mile Island operated.

Chernobyl

Chernobyl was not a normal accident. Its cause was an engineering experiment which, though successful, lacked proper approval. That is not to say that the experiment was unjustified, fundamentally improper, or indeed abnormal.

Even when not actively generating power, nuclear reactors require cooling to remove heat produced by the natural decay of nuclear fuel. Chernobyl's pressurized water reactors (different in design from Three Mile Island's) used water flowing at high pressure to remove waste heat (about 28,000 liters of water an hour). After an emergency shutdown, the core could still generate a significant amount of residual heat. If not removed, the heat could cause core damage (as it did at Three Mile Island). If the power grid failed, power to run the plant's cooling system might be unavailable from outside for far too long.

Chernobyl's reactors had three backup diesel generators. Each generator required fifteen seconds to start up but took over a minute to attain the speed required to run one of the main coolant pumps. Chernobyl's engineers judged this one-minute power gap unacceptable. Too much can happen in a nuclear reactor in a minute when the cooling system is not working. Analysis indicated that one way to bridge the one-minute gap was to use the mechanical energy of the generator that powered the water pumps to turn the generator's shaft, and thereby to pick up loads. The turbine generator supplied the power for the four main circulating pumps as it coasted down. The experiment was all but complete forty seconds later. But, as the connections to the plant's cooling system might be unavailable from outside for far too long.

The experiment began just after 1:23 am on April 26, 1986. The experiment was designed to test the assumption that the control rods would depressurize the reactor in a much shorter period of time than had been previously hypothesized. The experiment mistakenly inserted the control rods too far, nearly shutting down the reactor. Control-room personnel soon decided to restore the power and exited with the reactor rods, but several minutes elapsed between the extraction and the time that the power output began to increase and stabilize at 160 - 200 MW. The extraction withdrew the majority of control rods to the rods’ upper limit, but the rapid reduction in the power during the initial shutdown and subsequent operation at less than 200 MW led to increased dumping of the reactor core by the automatic emergency protection system. Only the director of the plant approved it (and even his approval did not follow standard procedures). The experiment therefore briefly increased the reactor rate in the lower half of the core. A few seconds after the start of the shutdown, there was a massive power increase, the core overheated, and seconds later this overheating produced the first explosion. Some of the fuel rods fractured, blocking the control-rod columns and causing the control rod dampening effect of the core’s neutron absorber, reactor power continued to decrease, even without further operator action.

As the power dropped to approximately 300 MW during the experiment, four of the engineers conducting the experiment mistakenly inserted the control rods too far, nearly shutting down the reactor. Control-room personnel soon decided to restore the power and exit with the reactor rods, but several minutes elapsed between the extraction and the time that the power output began to increase and stabilize at 160 - 200 MW. The extraction withdrew the majority of control rods to the rods’ upper limit, but the rapid reduction in the power during the initial shutdown and subsequent operation at less than 200 MW led to increased dumping of the reactor core by the automatic emergency protection system. Only the director of the plant approved it (and even his approval did not follow standard procedures). The experiment therefore briefly increased the reactor rate in the lower half of the core. A few seconds after the start of the shutdown, there was a massive power increase, the core overheated, and seconds later this overheating produced the first explosion. Some of the fuel rods fractured, blocking the control-rod columns and causing the control rod dampening effect of the core’s neutron absorber, reactor power continued to decrease, even without further operator action.

As the power dropped to approximately 300 MW during the experiment, four of the engineers conducting the experiment mistakenly inserted the control rods too far, nearly shutting down the reactor. Control-room personnel soon decided to restore the power and exit with the reactor rods, but several minutes elapsed between the extraction and the time that the power output began to increase and stabilize at 160 - 200 MW. The extraction withdrew the majority of control rods to the rods’ upper limit, but the rapid reduction in the power during the initial shutdown and subsequent operation at less than 200 MW led to increased dumping of the reactor core by the automatic emergency protection system. Only the director of the plant approved it (and even his approval did not follow standard procedures). The experiment therefore briefly increased the reactor rate in the lower half of the core. A few seconds after the start of the shutdown, there was a massive power increase, the core overheated, and seconds later this overheating produced the first explosion. Some of the fuel rods fractured, blocking the control-rod columns and causing the control rod dampening effect of the core’s neutron absorber, reactor power continued to decrease, even without further operator action.

Fukushima

The disaster at Fukushima fits neither of these patterns. The accident was not normal or the result of an engineering experiment. It was also not the result of operator negligence, incompetence, or misconduct. The Fukushima accident was an unprecedented, man-made disaster. Any Japanese had experienced in 1400-years of recorded history (http://en.wikipedia.org/wiki/List_of_earthquakes_in_Japan, accessed April 25, 2011). The quake was followed by an enormous tsunami. That double disaster would have happened even if the Fukushima nuclear power plant, one of the twenty-five largest in the world, had never existed. The nuclear disaster is a byproduct of that larger natural disaster.

At the time of the quake, 2:46 pm, Reactor 4 had been de-fueled while 5 and 6 were in cold shutdown for planned maintenance. The remaining three reactors shut down automatically when the reactors shut down, the plant’s own generation of electricity ceased, eliminating one source of electricity used to run cooling and control systems. One of two connections to the national electrical grid also failed. That loss of power started up thirteen on-site emergency diesel generators. These would ordinarily have provided enough power to operate the reactors’ control and cooling systems until the lost connection to the national grid could be restored. Had the earthquake been the only disaster to hit the Fukushima plant on March 11, there would have been little to discuss here. The tsunami changed that.

The plant was protected by a seawall designed to withstand any tsunami up to 5.7 meters, but the great wave that struck forty-one minutes after the quake was fifteen-meter-high. It flooded the entire plant, including generators and electrical switchgear in reactor basements. It also broke the remaining connection with the national electrical grid. All conventional power for cooling had been lost. Only one backup remained: emergency batteries, able to run some of the monitoring and control systems for up to eight hours. Replacement batteries and mobile generators were soon dispatched to Fukushima, but collapsed bridges, debris-strewn roads, and similar obstacles delayed them. The first replacements did not arrive until 9:00 pm (six hours after the first call went in).

The arrival of the replacement batteries and mobile generators did not end the crisis, however. They had to be installed. The normal connection points were in flooded natural oils. There was also difficulty finding suitable cables. Work to connect batteries and generators was still continuing twenty-four hours after the quake when there was an explosion in Reactor 1’s building. The side walls of the reactor building roof collapsed, and debris covered much of the floor and machinery.

The roof of the building was designed to provide ordinary weather protection, not to withstand an explosion or to act as containment for the reactor. In the Fukushima reactors, the primary containment surrounded the reactor’s pressure vessel. The top floor had no roof, but only water filled pools for storing new fuel ready to be craned into the reactor and used fuel ready for disposal.

This first explosion was probably caused when...
hydrogen collected under the roof. Exposed fuel rods became very hot and reacted with steam, oxidizing the cladding and releasing hydrogen. The hydrogen would have leaked upward. Safety devices normally burn such hydrogen before it reaches explosive concentrations. These systems seem to have failed when the electrical power did.

Reactor 1’s containment survived the explosion. There were no major leaks or escape of radioactive material, although there was an increase in radiation following the explosion. The explosion at Reactor 1 injured four workers. But this was only the beginning. Hydrogen gas was also collecting at the other five reactors. Over the next few days, hydrogen explosions destroyed the upper cladding of the buildings for Reactors 3 and 4 and the containment inside Reactor 2. Several fires broke out at Reactor 4. In addition, spent-fuel rods stored in the spent-fuel pools of Reactors 1-4 began to overheat as the water level dropped. Fear of radiation leaks led to evacuation of all non-essential persons within a twenty-kilometer radius of the plant.

In short, the Fukushima plant was overwhelmed by forces from outside well beyond what it was designed for. Without heroic efforts by plant staff, some of whom may have died in the process, an explosion of exposure to radiation, the Fukushima disaster might have become at least as devastating as Chernobyl. Even with those heroic efforts, several weeks passed before the plant could be said to be under control. One generation at Reactor 6 was restarted on March 17 (six days after the quake) allowing some cooling at Reactor 5 and 6, the least damaged. Connection to the power grid was restored to parts of the plant on March 20, but machinery for Reactors 1-4—damaged by flooding, fires, and explosions—could not be restarted for several months. Only in late April did all cooling in the reactors reach safe temperatures.

The Fukushima plant could have been designed to withstand the natural disaster that occurred. A breakwater three times the height of the actual breakwater could have protected the plant against the tsunami (assuming it survived the quake); the plant might have been located far enough away from the ocean to be safe from even such large waves. Even if building foundations might have been made waterproof, and so on. Even some less expensive arrangements might have improved what happened considerably. For example, storing more batteries on site would have allowed the cooling and control systems to function longer without repair or resupply, weeks instead of hours. But all of these changes would have been more (or less) expensive, raising the price of electricity the plant produced. Typically, engineers, though consulted, do not make such decisions. Government regulators, senior management, or public opinion typically decide, for example, whether to protect against a 500-year, 1,000-year, or 10,000-year quake.

Katrina

When it struck New Orleans on August 29, 2005, Katrina was a category 3 hurricane, a large storm but no larger than storms that strike the Gulf Coast almost every year. The top hurricane season is 5. Like Katrina, this was nonetheless unusually destructive because it moved so slowly that anything in its path was subject to heavy rains and high winds for many hours. The rain and high winds were worse for Task Force IPET (IPET) issued its (draft) Final Report. IPET was an independent team of more than one-hundred-fifty international and national experts from more than fifty different government organizations, universities, and private companies. The U.S. Army Corps of Engineers commissioned IPET a few weeks after Katrina hit New Orleans. It was to analyze how the levee system performed. Though many questions of detail remain unsettled, this nine-volume report, is (more or less) the last word on both the causes of the Katrina disaster and means of preventing similar disasters in the future.

IPET reports a “system” that grew up piecemeal, only in part under the control of the Corps of Engineers, the government agency officially in charge of waterways. In some places, the system failed because a levee or other barrier was not high enough, often because of unanticipated subsidence rather than original design error. In other places, the system failed because, though high enough, the barriers were not designed for the forces to which they were in fact subject (an unusually slow-moving storm). Design of floodwalls along three canals was “particularly inadequate”. A series of incremental decisions, even small, about how the structures actually constructed “systematically increased the inherent risk in the system without recognition or acknowledgment” (IPET 2006, I-2). Many of the failures in the system would not have occurred had implementation of plans for reconstruction not been delayed for almost twenty-five years by inadequate funding, new laws governing the environment, and simply inefficient cost control. For some important “decisions”, there was no decision-maker at all. The decisions were a mere byproduct of poor communication, poor information, poor coordination, or some combination of these.

The most important lesson IPET drew from its analysis is unsurprising: The way to avoid similar disasters is to use larger safety factors (“conservative design”: 3 instead of 1.5 for buildings, 5 instead of 3 for concrete barriers) and giving good materials (“higher quality, less erodible”). (IPET 2006, I-3).

The flood control system now replacing the one Katrina overwhelmed is considerably more expensive than the old one. For example, the Corps has been replacing the five-meter pilings holding canal walls in place with pilings that would go down fifteen and a half meters (three times as deep). The Corps agreed that the use of I-walls along the canals would increase its impact even with the support of a simple earthen levee) was a mistake. It is replacing the canal’s I-walls with heavily-braced T-walls locked down by twenty-one meter H-piles angled out in two directions. The use of simple, thick walls was also judged a mistake. The Corps is now “armoring” all levees where they seem vulnerable to overtopping, that is, covering them with something water will not soak through. There is also a campaign to increase the width of the levees (by widening the channels) to prevent it from raising the water level too high too quickly, or in other words, to reduce the changes in design that government was unwilling to pay for without a major disaster and may yet lose interest in paying for before the work is complete.

Conclusions

We can, I think, distinguish four sorts of engineering decision in these four case studies: planning, designing, management, and operations. (In a different context, I would include “disposal” in this list. I do not include it here only because none of these disasters concerns disposal as such, though Fukushima’s problems were due, in part, to fuel rods waiting disposal.)

By planning, I mean such decisions as whether to build a levee at all, where to put it, and the upper limit of its budget. For such decisions, engineers are most important for vetoing certain options, for example, a location because the risk of earthquake makes safe construction too expensive. They are also important for suggesting alternatives, for example, conservation or a gas-fired plant rather than a nuclear plant. Engineers are not (at least, not in most cases) “problem solvers”. One important function they have is helping to define problems—or redefine them when it becomes clear that the client or employer has not asked the right questions.

But, for any large undertaking such as a nuclear plant or flood control system, engineers are generally only one party in a complex social decision in which the other parties include employer, government officials, experts of various sorts (such as geologists), bankers, and civil society (“or the public”). Perhaps the most important contribution engineers can make to planning is developing minimum standards for evaluating and responding to specific risks and benefits of the technology in question.

By designing, I mean the actual drafting of specifications. Floor plans on necessities to construct or modify the technological artifact in question. Once planning has set limits, engineers are generally only concerned to ensure that the work is complete.

By management, I mean the actual drafting of specifications. Floor plans on necessities to construct or modify the technological artifact in question. Once planning has set limits, engineers are generally only concerned to ensure that the work is complete.

By operation, I mean the actual drafting of specifications. Floor plans on necessities to construct or modify the technological artifact in question. Once planning has set limits, engineers are generally only concerned to ensure that the work is complete.
a nuclear plant that will fail slowly rather than quickly or cool rather than heat up if left alone. Only when a planning limit is too strict do engineers have a reason to restart the planning process, for example, by suggesting that the budget be raised to provide an adequate margin of safety.

By management, I mean overseeing the operations of a plant, including choosing, training, and directing operators. Management is not technical—and is therefore not the domain of the engineers. But, for nuclear plants or flood control systems, the managers will typically be engineers. For engineers, part of technical management is remaining alert to possible improvements in staff, procedures, and equipment. So, for example, a manager who noticed that operators at Three Mile Island often missed readings on an important gauge because equipment blocked their view of it should recommend, or order, that the control board or control room be redesigned to improve the view.

By operations, I mean actually doing what is necessary for the plant or other technical artifact to work. While engineers do not, in general, operate plants, they do constitute most of the operators in a nuclear plant. So, for example, at Chernobyl, they pushed the button that caused the 90-inch dampening rods to go into the core. While operators can be reprimanded, and their acts reversed, they are, while acting as operators, completely in control of the plant. So, if they push the button, the resulting event is (technically) not a precautionary principle (though its effect, that of improved plant safety, might be).

How safe is “safe enough” is at least as much a social decision as an engineering decision. But it is an engineering decision in part. For small risks, engineers may well make the final decision. Even concerning the largest risks, engineers will be consulted and their opinion given considerable weight. No decision-maker was ever willing to order engineers on the spot directly to have the decision (more or less figuratively) blow up in her face.

Engineers generally evaluate risk by multiplying the harm’s (net) disvalue by the harm’s probability. This method of risk analysis works reasonably well for small harms. The method does not, I think, work at all well for the largest harms—those that, even if highly improbable, would be intolerable if realized—such as destruction of the earth or even the sort of devastation Chernobyl produced. For such intolerable harms, engineers should, I think, adopt a precautionary principle. But in this case, the precautionary principle has its use in engineering. The precautionary principle says: if we (society at its rational best) would reject any plausible benefit in exchange for suffering that harm, we (that part of society making the decision) should, all else equal, rule out any design that risks that harm (however small the probability—so long as it is finite). Since this principle applies when we know both the harm in question and its probability, it is technically neither a precautionary principle (though it is spirit is much the same). It is, in this respect, more like advice frequently given to gamblers betting in games of chance with known odds (“Don’t bet more than you can afford to lose”). Precautionary principles are about dealing with uncertainty. (See, for example, Andorno, 2004.)

The precautionary principle I am proposing is only about dealing with highly improbable probabilities. Yet it is, or at least should be, an important principle in engineering. Failure is part of engineering. While engineers have a very low tolerance for failure of any kind, even in subsystems that are not “safety sensitive”, I have yet to hear of any complicated system (even one as simple as a mechanical pencil) for which engineers have not calculated a failure rate (often, to be sure, a tiny failure rate, such as 3.4 defects per billion (six Sigma)). No product of engineering is (strictly speaking) “failure proof” (all things considered).

Most, perhaps all, nuclear power plants now in operation have been built in violation of a planning principle suggesting above (at least when the calculation of probability takes into account that human beings will operate the plant). The analogy with gambling may not be perfect, but it is close enough. For we have always have the option of doing something much safer, such as going to the theater or buying government bonds. For nuclear energy, our choices today are more difficult. Fossil-fuel plants together (though not individually) threaten us with a world too hot to live in. Hydro-electric dams flood lowlands when they fail and are often not available as an alternative to nuclear power. Failing hydro-electric dams may have killed many more people than nuclear power-plant accidents have (depending on how deaths are calculated). Just one dam failure, that of the dam at Banqiao, China, in 1975, seems to have killed at least 150,000 and quite likely over 450,000 through resulting disease and famine (Wike, “Banqiao”). Three Mile Island itself is only a hundred miles or so from the center of the Johnstown, Pennsylvania, flood, which killed more than 2,200 people, the result of a dam failing in 1889 (Wike, “Johnston Flood”). In contrast, no one died at Three Mile Island and statistical deaths worldwide to be expected from the radiation that escaped is much smaller.

Nowhere has wind and geothermal met the demand for electricity in an industrial country. And so on. Even wind and geothermal have nothing like the history of prudence in planning: if we (society at its rational best) would reject any plausible benefit in exchange for suffering that harm, we (that part of society making the decision) should, all else equal, rule out any design that risks that harm (however small the probability—so long as it is finite). Since this principle applies when we know both the harm in question and its probability, it is technically neither a precautionary principle (though it is spirit is much the same). It is, in this respect, more like advice frequently given to gamblers betting in games of chance with known odds (“Don’t bet more than you can afford to lose”). Precautionary principles are about dealing with uncertainty. (See, for example, Andorno, 2004.)

The principle I am proposing is only about dealing with highly improbable probabilities. Yet it is, or at least should be, an important principle in engineering. Failure is part of engineering. While engineers have a very low tolerance for failure of any kind, even in subsystems that are not

Could have been designed with T-walls rather than I-walls, Fukushima could have had a higher breakwater; Chernobyl could have had a better design for its dampening rods; and Three Mile Island could have had a control board that was even stronger like such as sight lines. And, of course, after these disasters, engineering designs made—or, in the case of Fukushima—will make—such improvements. Engineers generally learn from their failure, and even making repairs, even making repairs, they seem to have prevented an even worse outcome. Fukushima, the canals in New Orleans may have had a concrete containment for its reactor or a better way of controlling core temperature. But that will always, or at least almost always, be true. Engineering is about making things “safe enough” rather than “absolutely safe”.

How safe is “safe enough” is at least as much a social decision as an engineering decision. But it is an engineering decision in part. For small risks, engineers may well make the final decision. Even concerning the largest risks, engineers will be consulted and their opinion given considerable weight. No decision-maker was ever willing to order engineers on the spot directly to have the decision (more or less figuratively) blow up in her face.

Engineers generally evaluate risk by multiplying the harm’s (net) disvalue by the harm’s probability. This method of risk analysis works reasonably well for small harms. The method does not, I think, work at all well for the largest harms—those that, even if highly improbable, would be intolerable if realized—such as destruction of the earth or even the sort of devastation Chernobyl produced. For such intolerable harms, engineers should, I think, adopt a precautionary principle. But in this case, the precautionary principle has its use in engineering. The precautionary principle says: if we (society at its rational best) would reject any plausible benefit in exchange for suffering that harm, we (that part of society making the decision) should, all else equal, rule out any design that risks that harm (however small the probability—so long as it is finite). Since this principle applies when we know both the harm in question and its probability, it is technically neither a precautionary principle (though it is spirit is much the same). It is, in this respect, more like advice frequently given to gamblers betting in games of chance with known odds (“Don’t bet more than you can afford to lose”). Precautionary principles are about dealing with uncertainty. (See, for example, Andorno, 2004.)

The principle I am proposing is only about dealing with highly improbable probabilities. Yet it is, or at least should be, an important principle in engineering. Failure is part of engineering. While engineers have a very low tolerance for failure of any kind, even in subsystems that are not.
other engineers may not be able to make the necessary changes immediately because of budget or schedule, or at all because changes that they have already made bar the improvement in question. Engineers may also find an alternative way to achieve the same end. For these reasons (and perhaps others), nuclear plants, however alike at birth, tend to grow into noticeably different individuals, much as biological plants do.

Some people, especially philosophers, seem to think of those who stayed on at Fukushima — those who, for example, worked in the dark in cold waist-high radioactive water to restart the generators — as engaged in “supererogatory” conduct, that is, as engaged in conduct above and beyond what morality requires. The engineers I have discussed this with seem to view the conduct as heroic but required (supposing the “workers” in question to be engineers). An engineer who left when needed would have acted unprofessionally; he would have failed as an engineer even if he left to save his life or look after his family. Engineering sometimes requires heroism (a significantly higher standard than proposed in Alpert 1983) — or so the engineers I have talked with about this seem to think.

Acknowledgments
This article has benefited from discussion of it at: a workshop for philosophy graduate students at the Technical University-Delft, The Netherlands, May 11, 2011 (“The engineer, public safety, and economic constraints”); a seminar for the Department of Philosophy and Ethics, the Technical University-Eindhoven, The Netherlands, May 13, 2011 (“The Fukushima Nuclear Disaster: Reflections”); a talk for the Department of Philosophy and Religion, University of North Texas, Denton, October 13, 2011 (“The Fukushima Nuclear Disaster: Some Issues of Engineering Ethics”); a plenary session of Sixth International Conference on Applied Ethics, Hokkaido University, Sapporo, Japan, October 30, 2011; and the Annual Meeting of the Association for Practical and Professional Ethics, Cincinnati, Ohio, March 3, 2012, as well as from comments of several reviewers for this journal.

References

Dealing with the moral value of an action, rule or public policy cannot be reduced to a verdict resulting from the application of traditional tests based on the major ethical theories, despite the fact that handbooks still unanimously support this view. The history of ethical test results is more one of surprises than one of predictability. You would expect, for instance, that people who adopt the same moral doctrine do this in order to approach issues in the same way, including the moral assessment of actions. We all believe that this is the main reason it is useful to embrace the same moral creed. Therefore it seems strange to find that several members of the Romanian Parliament, all active supporters of Christian morality, assessed the legalization of prostitution in opposing ways. On the other hand, it is also strange that two people who adopt different ethical theories — precisely because they offer distinct explanations of moral phenomena — can frequently assess actions in the same manner. When a utilitarian and a Kantian — or a follower of Christian ethics and one of Muslim ethics — debate issues, it is somehow surprising to see them judging situations in the same way in most cases, despite the fact they declare themselves to be supporters of opposing ethical beliefs. Are these beliefs really opposing? In general, it appears that use of tests based on distinct or even opposing theories, such as utilitarianism and Kantianism, can result in different verdicts, but in most cases it results in convergent ones (Kantian and utilitarian moral duties are, ultimately, the same). On the other hand, if we dogmatically adopt a single theory and apply the same test repeatedly to the same action we usually get similar results, but some divergent ones also appear (see the cases of divergent utilitarian assessments of the same case given as examples in the textbooks).

Valentin Muresan
University of Bucharest, Romania

A Pluralist Ethical Decision-making Procedure

This paper claims that the use of several moral tests to assess the ethics of a new policy is unavoidable. All the efforts to make credible a methodological monism — by critical or reductionist strategies — have been unsuccessful; moreover, it must be acknowledged that even if there were a single test, when applied successively or by different people it would usually give divergent results. The main aim of the paper is to propose a pluralist procedure of ethical decision-making, using a set of proper ethical tests (such as utilitarian, Kantian, Christian, principlist and casuist) in the frame of an “ethical Delphi” procedure intended to make convergent the supposed variety of verdicts. This pluralist testing process, made by moral experts, is only a fraction of a more complex procedure intended to deliver social sanction for a new moral policy. This longer procedure also shows that the adoption of a new moral policy, rule or law is not only a question of passing a strict ethical test, but also a political (i.e. multi-criteria) decision. In general, the adoption of a new moral rule does not rely solely on an ethical test, but is essentially the outcome of a complicated social agreement. That is why in academic applications of the usual moral tests we do not take a moral decision on a new case, but merely simulate it.

Key words: ethical decision-making, ethical pluralism, ethical Delphi, pluralist model

Decisions about the moral value of an action, rule or public policy cannot be reduced to a verdict resulting from the application of traditional tests based on the major ethical theories, despite the fact that handbooks still unanimously support this view. The history of ethical test results is more one of surprises than one of predictability. You would expect, for instance, that people who adopt the same moral doctrine do this in order to approach issues in the same way, including the moral assessment of actions. We all believe that this is the main reason it is useful to embrace the same moral creed. Therefore it seems strange to find that several members of the Romanian Parliament, all active supporters of Christian morality, assessed the legalization of prostitution in opposing ways. On the other hand, it is also strange that two people who adopt different ethical theories — precisely because they offer distinct explanations of moral phenomena — can frequently