Three Nuclear Disasters and a Hurricane:
Some Reflections on Engineering Ethics

Michael Davis
Illinois Institute of Technology, USA

Abstract

The nuclear disaster that Japan suffered at Fukushima in the months following March 11, 2011 has been compared with other major nuclear disasters, especially, Three Mile Island (1979) and Chernobyl (1986). It is more like Chernobyl in severity, the only other 7 on the International Nuclear Event Scale; more like Three Mile Island in long-term effects. Yet Fukushima is not just another nuclear disaster. In ways important to engineering ethics, it is much more like Katrina’s destruction of New Orleans than like any nuclear disaster. It is (primarily) a consequence of a natural disaster, the enormous earthquake and tsunami that wrecked much of northeast Japan. One lesson of Fukushima, one shared with Katrina, concerns the different roles engineers have at different stages in an engineering project (planning, designing, management, and operations). In the planning stage, engineers seem to have relatively little power to affect certain early large-scale trade-offs between public safety and public welfare. Another lesson may be the importance of not leaving complex technical systems untended. The events that made the disasters at Three Mile Island and Chernobyl inevitable lasted only a few minutes or hours; the events that made the disasters in New Orleans and Fukushima inevitable were spread over several days. Fukushima avoided a more serious disaster because the plants were not abandoned in the way New Orleans was. A third lesson concerns our ideas of heroism, especially our sense that heroism is sometimes one’s duty. An engineer’s duty sometimes includes protecting others from harm even at the risk of the engineer’s life.

Keywords: Chernobyl, Fukushima, Katrina, Three Mile Island, precautionary principle

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 pre-mature 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.
to be interested in what scientists or technologists have in common, I have focused on what distinguishes one discipline from another, for example, what distinguishes chemists from engineers (Davis 2002). I have found that the principal way to study professions, especially the profession of engineering, is, in short, not a philosopher, historian, or sociologist of technology (though scholars in those fields sometimes find my work useful). I thereby received the invitation from Japan was a quarter-century of thinking (and writing) about engineering. (For those unfamiliar with my work on engineering, the place to start is Davis 1998.)

Though certainly a nuclear disaster, Fukushima is not just another nuclear disaster. In ways important to engineers, the place to start is Davis 2002). I have found that the principal way to study professions, especially the profession of engineering, is, in short, not a philosopher, historian, or sociologist of technology (though scholars in those fields sometimes find my work useful). I thereby received the invitation from Japan was a quarter-century of thinking (and writing) about engineering. (For those unfamiliar with my work on engineering, the place to start is Davis 1998.)

Interpretations are, of course, open to objection but, without interpretation, facts merely pile up, becoming in time an unmanageable heap. There is no understanding without interpretation. But interpretation relying on changing facts is necessarily the sort of time-stamped enterprise philosophers are inclined to avoid—and I would have avoided it if the invitation from Japan. There is not much that a philosopher can do about a disaster such as that at Fukushima—except help those seeking to understand it and thereby help to prevent similar disasters. I felt the Japanese that much. This paper’s title promises “reflections” on Fukushima, not systematic or definitive understanding. Reflections are what one gets when, focusing thought on ordinary events, one connects observations that happen to see, connections that seem to jump out of the dark. Reflection is a source of hypothesis rather than proof, as a mixture of steam and water passed through them. The operators then shut down the pumps, believing that the mechanical failures were compounded by the cooling systems untended. 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 limiting the harm as well as for fixing the underlying problem, even if limiting the harm involves risking their lives. To see what I mean, let us consider these 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. Perrow 1984 also describes Three Mile Island as a “normal accident”. While I agree that it was a “normal accident” in his sense, my use of that term is somewhat different. I mean that the accident was a product of what engineers normally do rather than a product of incompetence, negligence, corruption, or other unusual conduct (such as experimentation).

During the night of March 27-28, 1979, workers were engaged in routine cleaning of a blockage in one of Reactor 2’s eight condensate polishers (filters for the secondary cooling loop). At 4 am, the pumps feeding the polisher stopped. We still do not know the cause of the stoppage. When a bypass valve failed to open, condensate flowed into the secondary system through the failed valve. These also shut down. No longer receiving water, the steam-driven generators stopped and the reactor automatically carried out an emergency shutdown. Within eight seconds, control rods were inserted into the core to halt the nuclear chain reaction. The reactor nonetheless continued to generate heat (a byproduct of normal decay). Because steam was no longer being automatically carried out an emergency shutdown. Within eight seconds, control rods were inserted into the core to halt the nuclear chain reaction. The reactor nonetheless continued to generate heat (a byproduct of normal decay). Because steam was no longer being

Why Compare These Four Disasters?

The nuclear disaster that Japan suffered at Fukushima has been compared with other major nuclear disasters, especially Three Mile Island (1979) and Chernobyl (1986). It is more like Chernobyl in immediate destructiveness, the only other 7 on the International Nuclear Event Scale (the upper limit of which is 7). It is more like Three Mile Island in probable long-term effects (though Fukushima’s long-term effects are likely to be substantially worse than Three Mile Island’s). To date, Chernobyl seems to have directly killed thirty-one reactor site employees, twelve workers, and 2,000 people in Pripyat, and to have ruined perhaps a 100,000 square km of farmland. Over 300,000 people in Chernobyl lost their homes to contamination. (All information about Chernobyl here and below is drawn from Wiki, “Chernobyl”, a source valuable both because it is easily accessed and regularly updated.)

In contrast, the radiation released from the Fukushima plant, though significant, will, it seems, leave little long-term contamination, except at the plant itself and in a plume perhaps fifty km beyond. At least six workers have exceeded lifetime legal limits for radiation and more than three hundred have received significant radiation doses. Estimates of future cancer deaths due to accumulated radiation exposures in the population living near Fukushima have ranged from none to a non-peer-reviewed “guesstimate” of a thousand. No one died in the explosions at the plant or from subsequent radiation exposure (though 23 people killed themselves in evacuation of hospitals in the exclusion zone may have caused as many as forty-five more deaths). The earthquake, tsunami, rather than the nuclear accident, seems to be responsible for the few employees severely injured or killed at the plant. (Fukushima Daiichi.)

The discussion of Fukushima below relies not only 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 more like Three Mile Island in probable long-term effects (though Fukushima’s long-term effects are likely to be substantially worse than Three Mile Island’s). To date, Chernobyl seems to have directly killed thirty-one reactor site employees, twelve workers, and 2,000 people in Pripyat, and to have ruined perhaps a 100,000 square km of farmland. Over 300,000 people in Chernobyl lost their homes to contamination. (All information about Chernobyl here and below is drawn from Wiki, “Chernobyl”, a source valuable both because it is easily accessed and regularly updated.)

In contrast, the radiation released from the Fukushima plant, though significant, will, it seems, leave little long-term contamination, except at the plant itself and in a plume perhaps fifty km beyond. At least six workers have exceeded lifetime legal limits for radiation and more than three hundred have received significant radiation doses. Estimates of future cancer deaths due to accumulated radiation exposures in the population living near Fukushima have ranged from none to a non-peer-reviewed “guesstimate” of a thousand. No one died in the explosions at the plant or from subsequent radiation exposure (though 23 people killed themselves in evacuation of hospitals in the exclusion zone may have caused as many as forty-five more deaths). The earthquake, tsunami, rather than the nuclear accident, seems to be responsible for the few employees severely injured or killed at the plant. (Fukushima Daiichi.)

The discussion of Fukushima below relies not only 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 more like Three Mile Island in probable long-term effects (though Fukushima’s long-term effects are likely to be substantially worse than Three Mile Island’s). To date, Chernobyl seems to have directly killed thirty-one reactor site employees, twelve workers, and 2,000 people in Pripyat, and to have ruined perhaps a 100,000 square km of farmland. Over 300,000 people in Chernobyl lost their homes to contamination. (All information about Chernobyl here and below is drawn from Wiki, “Chernobyl”, a source valuable both because it is easily accessed and regularly updated.)
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 "attitudinal" reports). Of course, 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 steam turbine and residual steam pressure to generate electricity to run the main coolant pumps while the generator was being restarted. But, of course, the analysis had to be confirmed properly. This, of course, was the approved procedure. The approved procedure called for Reactor 4's power output to be gradually reduced to 700-1000 MW. The minimum level established in the procedure (700 MW) was achieved about an hour before the experiment began. However, because of the natural damping effect of the core's neutron absorber, reactor power continued to decrease, even without further operator action.

As the power dropped to approximately 500 MW during the experiment, the role 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 without inserting the reactor control 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 damping of the reactor core by the activated zirconium. The graphite core absorbed neutrons at a high rate. To counteract this unwanted high-absorption, the operators withdrew additional control rods from the reactor core.

Then, about the time the experiment ended, there was an emergency shutdown of the reactor. The shutdown started when someone pressed the button of the reactor's emergency protection system. (We do not know whether the button was pushed as an emergency measure, by mistake, or simply as a routine method of shutting down the reactor upon completion of the experiment.) Because of a flaw in the design of the graphite-tip control rods, the operator began to move the control rods. The operator then moved a neutron-absorbing material to slow the reaction. The emergency shutdown therefore briefly increased the reaction rate in the lower half of the core. A few seconds later, the steam turbine and residual steam pressure to generate steam would reduce the ability of the coolant to absorb neutrons, increasing the reactor's output of heat. The increased heat would cause yet more water to become steam, further increasing heat. During almost the entire period of the experiment, the automatic control system successfully counteracted this destructive feedback loop: the production of steam would reduce the ability of the coolant to absorb neutrons, increasing the reactor's output of heat. The increased heat would cause yet more water to become steam, further increasing heat. During almost the entire period of the experiment, the automatic control system successfully counteracted this destructive feedback loop, inserting control rods into the reactor core to keep the temperature down.

If conditions had as planned, the experiment would almost certainly have been carried out safely. The Chernobyl disaster resulted from attempts to boost the reactor past its pre-determined safe limits, the core overheating. Because of the natural damping effect of the core's neutron absorber, reactor power continued to decrease, even without further operator action.

As the power dropped to approximately 500 MW during the experiment, the role 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 without inserting the reactor control 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 damping of the reactor core by the activated zirconium. The graphite core absorbed neutrons at a high rate. To counteract this unwanted high-absorption, the operators withdrew additional control rods from the reactor core.

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 maintenance breakdown, the management and communication failures, and the emergency protection system were all specific and unintentional. The workers at Fukushima did not expect a nuclear accident. They were not de-fueled while 5 and 6 were in cold shutdown for planned maintenance. The remaining three reactors shut down automatically when they detected a neutron-absorbing material to slow the reaction. The emergency shutdown therefore briefly increased the reaction rate in the lower half of the core. A few seconds later, the steam turbine and residual steam pressure to generate steam would reduce the ability of the coolant to absorb neutrons, increasing the reactor's output of heat. The increased heat would cause yet more water to become steam, further increasing heat. During almost the entire period of the experiment, the automatic control system successfully counteracted this destructive feedback loop, inserting control rods into the reactor core to keep the temperature down.

If conditions had been as planned, the experiment would almost certainly have been carried out safely. The Chernobyl disaster resulted from attempts to boost the reactor past its pre-determined safe limits, the core overheating. Because of the natural damping effect of the core's neutron absorber, reactor power continued to decrease, even without further operator action.

As the power dropped to approximately 500 MW during the experiment, the role 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 without inserting the reactor control 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 damping of the reactor core by the activated zirconium. The graphite core absorbed neutrons at a high rate. To counteract this unwanted high-absorption, the operators withdrew additional control rods from the reactor core.

When the experiment ended, there was an emergency shutdown of the reactor. The shutdown started when someone pressed the button of the reactor's emergency protection system. (We do not know whether the button was pushed as an emergency measure, by mistake, or simply as a routine method of shutting down the reactor upon completion of the experiment.) Because of a flaw in the design of the graphite-tip control rods, the operator began to move the control rods. The operator then moved a neutron-absorbing material to slow the reaction. The emergency shutdown therefore briefly increased the reaction rate in the lower half of the core. A few seconds later, the steam turbine and residual steam pressure to generate steam would reduce the ability of the coolant to absorb neutrons, increasing the reactor's output of heat. The increased heat would cause yet more water to become steam, further increasing heat. During almost the entire period of the experiment, the automatic control system successfully counteracted this destructive feedback loop, inserting control rods into the reactor core to keep the temperature down.

If conditions had been as planned, the experiment would almost certainly have been carried out safely. The Chernobyl disaster resulted from attempts to boost the reactor past its pre-determined safe limits, the core overheating. Because of the natural damping effect of the core's neutron absorber, reactor power continued to decrease, even without further operator action.

As the power dropped to approximately 500 MW during the experiment, the role 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 without inserting the reactor control 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 damping of the reactor core by the activated zirconium. The graphite core absorbed neutrons at a high rate. To counteract this unwanted high-absorption, the operators withdrew additional control rods from the reactor core.
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, but the plant was not designed with the necessary explicit concentrations. These systems seem to have failed when the electrical power did.

Reactor 1’s containment survived the explosion. There was no indication 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 Reactor 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 die from 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.

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 of the Hurricane Katrina levees 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 in some places than others. In some places, the system failed because a levee or other barrier to water 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 engineering decisions had led to disastrous initial plans that were not good enough. By planning, I mean such decisions as whether to build above or below some particular water level. 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 (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 earthen levees 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 or quickly wear away. These are expensive solutions. They are also important for suggesting alternatives, for example, conservation or a gas-fired plant rather than a nuclear plant. Engineers are not, of course, the only ones who are solving problems. One important function they have is helping to define problems—or re-define them when it becomes clear that the client or employer has not asked the right questions.

By planning, I mean the actual drafting of plans for reconstruction not being completed due, in part, to fuel rods waiting disposal.) But, for any large undertaking such as a nuclear plant or flood control system, engineers are generally only one part 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 are only one necessary task. But, for any large undertaking such as a nuclear plant or flood control system, engineers are generally only one part 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.

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 above or below some particular water level. The Corps is now “armoring” all levees where they seem vulnerable to overtopping, that is, covering them with something water will not soak through or quickly wear away. These are expensive solutions. They are also important for suggesting alternatives, for example, conservation or a gas-fired plant rather than a nuclear plant. Engineers are not, of course, the only ones who are solving problems. One important function they have is helping to define problems—or re-define 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 part 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.
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. The operation 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 exposed fuel rods to enter the core. While operators can be reprimanded, and their acts reversed, they are, while acting as operators, completely in control of the plant.

The discussion of the three nuclear disasters is how quickly things can go wrong. What goes wrong in a nuclear plant does not, of course, go wrong for just one reason. Because engineers typically design nuclear plants with a large safety factor, several systems must fail before anything goes seriously wrong. But, given the complexity of a nuclear plant, it is reasonable to expect something to go wrong now and then because even with proper maintenance and inspection, technical systems sometimes fail unexpectedly. That being so, it is also reasonable to expect (given the laws of statistics) that all of the independent systems will fail together at some point. It is an empirical reminder that even a low-probability event will, given a large enough population, become highly probable.

If we look at our four disasters, two —Three Mile Island and Chernobyl—seem unrelated to any ordinary planning or design failure. Of course, with a higher budget, the Three Mile Island plant might have had more working backups for its cooling system; Chernobyl might 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 asked whether he or she actually expected 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—that 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 doubt, adopt some version of the precautionary principle that has its roots in the (usually) justified 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) shall, all else equal, do our utmost to 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 parallel to the precautionary principle (though its 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 unknown 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 million—six Sigma). No product of engineering is (strictly speaking) “failure proof” (all things considered).

Most, perhaps all, nuclear power plants now in operation are far from failure of their fuel, all in violation of their planning principle suggested above (at least when the calculation of probability takes into account that human beings will operate the plant). The analogy with gamblers’ games is again useful. For we 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 250,000 directly—over 10 million through resulting disease and famine (Wiki, “Banqiao”). Three Mile Island itself is only a hundred miles or so from the site of the “Johnstown Flood”, which killed more than 2,200 people, the result of prudence in planning. For the time at least, we may face a choice among dangerous friends. We can only minimize the risk of disaster, not avoid it.

Two features that neither Fukushima nor Katrina should have. Three Mile Island and Chernobyl (the 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 unknown 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

How many of (what the media called) “workers” at Fukushima were engineers? I believe there is no evidence that either from news sources or from contacts in Japan. My visits to nuclear plants in the United States suggest that most of those working at Fukushima would have been engineers (say, 90%) with the remainder divided about evenly between scientists and technicians. The grand total of 6,100 was probably about 6,000 (often, to be sure, a tiny failure rate, such as 3.4 defects per million—six Sigma). No product of engineering is (strictly speaking) “failure proof” (all things considered).
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 Alpern 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 Ethics, the Technical University, University-Eindhoven, The Netherlands, May 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

A Pluralist Ethical Decision-making Procedure
Valentin Muresan
University of Bucharest, Romania

Abstract
This paper claims that the use of several moral tests to assess the ethics of a new policy is unavoidable. All the efforts 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

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).