<table>
<thead>
<tr>
<th>Title</th>
<th>Three Nuclear Disasters and a Hurricane: Some Reflections on Engineering Ethics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Davis, Michael</td>
</tr>
<tr>
<td>Citation</td>
<td>Journal of applied ethics and philosophy, 4, 1-10</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2012-08</td>
</tr>
<tr>
<td>DOI</td>
<td>10.14943/jaep.4.1</td>
</tr>
<tr>
<td>Doc URL</td>
<td><a href="http://hdl.handle.net/2115/50468">http://hdl.handle.net/2115/50468</a></td>
</tr>
<tr>
<td>Type</td>
<td>bulletin (article)</td>
</tr>
<tr>
<td>File Information</td>
<td>jaep4-1_micael davis.pdf</td>
</tr>
</tbody>
</table>
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

Editorial Note

The Journal of Applied Ethics and Philosophy is an interdisciplinary periodical covering diverse areas of applied ethics. It is the official journal of the Center for Applied Ethics and Philosophy (CAEP), Hokkaido University. The aim of the Journal of Applied Ethics and Philosophy is to contribute to a better understanding of ethical issues by promoting research into various areas of applied ethics and philosophy, and by providing researchers, scholars and students with a forum for dialogue and discussion on ethical issues raised in contemporary society.

The journal welcomes papers from scholars and disciplines traditionally and newly associated with the study of applied ethics and philosophy, as well as papers from those in related disciplines or fields of inquiry.

Shunzo Majima
Editor-in-Chief

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 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
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 there is no one way to study professions, especially the profession of engineering. I am, in short, not a philosopher, historian, or sociologist of technology (though scholars in those fields sometimes find my work useful). I 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 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 Daiichi”.

The discussion of Fukushima below relies 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”.

Reflection is a source of hypothesis rather than proof, to see, connections that seem to jump out of the dark. 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 interpretation from Japan. There is not much 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 I owed the Japanese that much.

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 an area 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 substantial numbers killed from the evacuation of hospitals in the exclusion zone may have caused as many as forty-five more deaths). The earthquakes or tsunami, rather than the nuclear accident, tends to be responsible for the few employees severely injured or killed at the plant. (Wiki, “Fukushima Daiichi”)

The Nuclear Regulatory Commission (NRC) may offer preventable engineering failures with the release of steam into the environment, 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 “attitudinal” reports). We 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 gap was to use the mechanical energy of the generator that powered the water pumps decreased, the water flow decreased, producing more and more steam bubbles in the core. The reactor was now ready to begin a 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, 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 power generation during the experiment, and once the experiment had started (something inconsistent with 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 300 MW during the experiment, one 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 withdrawing 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 rod’s 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 automatic control rods (135 an unusual feature for any Japan had experienced in 1400-years of recorded history (http://en.wikipedia.org/wiki/List_of_eartqua kes_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 in 15s. 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-meters 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 and control was 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 floodwater near the reactors. 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 were blown away, the 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. Only water filled pools for storing new fuel were ready to be craned into the reactor and used fuel ready for disposal.

This first explosion was probably caused when

Three Nuclear Disasters and a Hurricane Michael Davis

Journal of Applied Ethics and Philosophy Vol. 4

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 shutdown of Reactor 4 was delayed (135 an unusual feature for any Japan had experienced in 1400-years of recorded history (http://en.wikipedia.org/wiki/List_of_eartqua kes_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 in 15s. 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-meters 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 and control was 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 floodwater near the reactors. 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 were blown away, the 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. Only water filled pools for storing new fuel were 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 to waste, but in individual tanks at Fukushima, these systems seem to have failed when the electrical power did.

Reactor 1’s containment survived the explosion. There was no external collapse of Reactors 1 or 2, and the containment and a reactor bay at Reactor 3 had only minor damage. But Reactor 4 was destroyed, with major collapse. This reactor contains more fuel than the other four 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 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 generator 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 evacuations——could not be restarted for several months. Only Reactor 3 had enough water left in the spent fuel pools to cool the reactor core. In short, the plants far enough away from the ocean to be safe from even the massive wave that went over the barriers (for example, the one in 1965 named for hurricane Betsy) were also damaged by massive floods. Even so, Reactor 3 showed more survival from the quake; the plant might have been located far enough away from the ocean to be safe from even the massive wave that went over the barriers. A breakwater designed to withstand the natural disaster that occurred. A breakwater would have allowed the cooling and resupply, weeks instead of hours. But all of these changes happened considerably. For example, storing more water in a levee 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 several times Task Force IPEET (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 ineffective decisions at crucial points when 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 subsequent inefficiencies still beyond the control of the government.

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 margins”) and 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 be much cheaper, 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 i-walls instead of the cost savings 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 so easily wash away or erode. There is, however, no guarantee that 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 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 where 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 anything like the role of “problem solvers”. 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 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 loss on necessary to construct or modify the technological artifact in question. Once planning has set limits, engineers are generally free to work within those limits, for example, to design

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 scale is 5. Katrina 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 several times Task Force IPEET (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 ineffective decisions at crucial points when 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 subsequent inefficiencies still beyond the control of the government.

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 margins”) and 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 be much cheaper, 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 i-walls instead of the cost savings 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 so easily wash away or erode. There is, however, no guarantee that 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 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 where 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 anything like the role of “problem solvers”. 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 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 loss on necessary to construct or modify the technological artifact in question. Once planning has set limits, engineers are generally free to work within those limits, for example, to design
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 a 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 (engineers are 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 buttons that ended up dumping rods into the core. While operators can be reprimanded, and their acts reversed, they are, while acting as operators, completely in control of the plant. Of the three disasters we noted in our 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 seriously 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 that, with time, new and then new, 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 sooner or later. One of the “systems” that may fail at any given time is the human operator — whether because of distraction, fatigue, poor training, misjudgment, or just inattention.

How likely is a catastrophic failure at any moment? Not very. Perhaps only 10⁻²³ at any time. But over many years and many reactors even such small risks add up. One author recently calculated that there are:

450 nuclear power plants in the world. There have been 4 meltdowns in history, one each at Chernobyl and Three Mile Island and two so far at Fukushima, as partial meltdowns count as meltdowns. That is a ~1% failure rate. (Lindsay, 2011)

This calculation means nothing unless the four meltdowns are statistically significant, that is, a good predictor of what will happen over, say, the next hundred years (rather than a chance coincidence of events— like winning the lottery three days in a row). No, 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 made the working backup for its cooling system 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 quoted saying, “let’s push the button without any— or even any rough— engineering advice.” We might have 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. Reasoning like this is standard 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 adopt the precautionary principle (even if the precautionary principle is (technically) not a precautionary principle (though it is practical). 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 the known 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 have been built in violation of the engineers’ planning principle suggested above (at least when the calculation of probability takes into account that human beings will operate the plant). The analogy with games of chance is perhaps direct, but not for the high probabilities expected at Fukushima. 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, the dam at Banqiao, China, in 1975, seems to have killed at least 120,000 people. But no one, I think, would have the decision (more or less figuratively) blow up in her face.

One of the reasons we need to evaluate risk by multiplying harm’s disvalue by the harm’s probability is that engineers design with the (usually) justified expectation that other engineers will be present to look at what they design. The works of engineering, even of nuclear engineering, are identical when commissioned, slowly differentiate with time and use, including continuing maintenance, but not necessarily in the expected way. This is a reminder that part of what makes engineering so reliable is that engineers design with the (usually) justified expectation that other engineers will be present to look at what they design. The works of engineering, even of civil engineering or mechanical engineering, do not last long without continuing maintenance or repair, and those decisions similar to those that had damaged the other four units.

This aspect of what happened at Fukushima is a reminder that part of what makes engineering so reliable is that engineers design with the (usually) justified expectation that other engineers will be present to look at what they design. The works of engineering, even of nuclear engineering, are identical when commissioned, slowly differentiate with time and use, including continuing maintenance, but not necessarily in the expected way. This is a reminder that part of what makes engineering so reliable is that engineers design with the (usually) justified expectation that other engineers will be present to look at what they design. The works of engineering, even of nuclear engineering, are identical when commissioned, slowly differentiate with time and use, including continuing maintenance, but not necessarily in the expected way.
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 it 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 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 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 comments of several reviewers for this journal.

References


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 often 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-criterion) 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.

Abstract

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-criterion) 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