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

Author(s)
Davis, Michael

Citation
Journal of applied ethics and philosophy, 4: 1-10

Issue Date
2012-08

DOI
10.14943/jaep.4.1

Doc URL
http://hdl.handle.net/2115/50468

Type
bulletin (article)

File Information
jaep4-1_micael davis.pdf

Hokkaido University Collection of Scholarly and Academic Papers: HUSCAP
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.
The nuclear disaster that Japan suffered at Fukushima 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 workers, to have injured around 200,000 and 1,000,000 premature deaths worldwide, to have forced the permanent abandonment of a city of around 50,000 (Pripyat), and to have ruined perhaps a 100,000 square km of farmland. Over 200,000 people 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 ten thousand workers killed filters for the secondary cooling loop). At 4 am, the pumps feeding the polisher stopped. We still do not know the cause of the shutdown. When a bypass was not opened, condenser cooling water leaked down the primary feed-water pumps. 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 decay) to increase the temperature in the reactor vessel (Fukushima Dai-ichi). 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 and a Fukushima Dai-ii. 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 havoc for so long in Japan. It became a nuclear problem when 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 release 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 alarm, along with higher than normal temperatures on the discharge line and unusually high temperatures and pressures in the containment building, clearly indicated that there was a problem). 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 carry the coolant to the containment movement, but steam in the system (itself the product of rising temperature) prevented coolant flow through the core. As the coolant stopped circulating, it increasingly turned to steam. Just as the core was bathed in a sea 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 fuel pellets. The pellets then released more radioactivity into the reactor coolant, producing more hydrogen gas, leading to still further explosion in the containment building in the afternoon.

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 jumped from 30 degrees Fahrenheit to 50 degrees Fahrenheit, 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 escaped from the containment, and the plant’s emergency core cooling system was turned off at 7 am (almost three hours after the incident began) did contaminate 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 have been too quick to respond to the disaster, a typical engineering response. Its report ended with recommendations for changes in controls, quality assurance, maintenance, operator training, management, and extra.

The National Nuclear Regulatory Commission (NRC) may have been too quick to respond to the disaster, a typical engineering response. Its report ended with recommendations for changes in controls, quality assurance, maintenance, operator training, management, and extra.

The nuclear disaster that Japan suffered at Fukushima has been compared with other major nuclear disasters, especially the 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 workers, to have injured around 200,000 and 1,000,000 premature deaths worldwide, to have forced the permanent abandonment of a city of around 50,000 (Pripyat), and to have ruined perhaps a 100,000 square km of farmland. Over 200,000 people 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 ten thousand workers killed filters for the secondary cooling loop). At 4 am, the pumps feeding the polisher stopped. We still do not know the cause of the shutdown. When a bypass was not opened, condenser cooling water leaked down the primary feed-water pumps. 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 decay) to increase the temperature in the reactor vessel (Fukushima Dai-ichi).

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 and a Fukushima Dai-ii. 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 havoc for so long in Japan. It became a nuclear problem when 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 release 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 alarm, along with higher than normal temperatures on the discharge line and unusually high temperatures and pressures in the containment building, clearly indicated that there was a problem). 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 carry the coolant to the containment movement, but steam in the system (itself the product of rising temperature) prevented coolant flow through the core. As the coolant stopped circulating, it increasingly turned to steam. Just as the core was bathed in a sea 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 fuel pellets. The pellets then released more radioactivity into the reactor coolant, producing more hydrogen gas, leading to still further explosion in the containment building in the afternoon.

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 jumped from 30 degrees Fahrenheit to 50 degrees Fahrenheit, 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 escaped from the containment, and the plant’s emergency core cooling system was turned off at 7 am (almost three hours after the incident began) did contaminate 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 have been too quick to respond to the disaster, a typical engineering response. Its report ended with recommendations for changes in controls, quality assurance, maintenance, operator training, management, and extra.

The nuclear disaster that Japan suffered at Fukushima has been compared with other major nuclear disasters, especially the 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
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). 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 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 generators were still stopped. The control-rod columns and causing the 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 dampening of the reactor core by the atomic “negative coefficients” (an unusual feature of any Japan had experienced in 1400-years of recorded history (http://en.wikipedia.org/wiki/List_of_earthquake_0kes_in_Japan, accessed April 2015)).

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 maintenance experiment focused on refinements in the switching sequences of the electrical supplies for the reactor. The experiment was shut down with an automatic emergency shutdown. Because no danger to the reactor was anticipated, the engineers did not formally coordinate the experiment with the reactor’s chief designer or scientific manager. Indeed, the experiment did not even have the approval of the onsite representative of the Soviet nuclear power plant. Only the director of the plant approved it (and even his approval did not follow standard procedures).

The experiment began just after 1:23 am on April 26, 1986. The displaced control rods were then picked 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 main coolant pumps while the experiment mistakenly inserted the control rods too far, nearly shutting down the reactor. Control-room personnel soon decided to restore the power and extract without warning power output began to increase and stabilize at 170–200 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 dampening of the reactor core by the massive emergency core damage (an unusual feature of any Japan had experienced in 1400-years of recorded history (http://en.wikipedia.org/wiki/List_of_earthquake_0kes_in_Japan, accessed April 2015)). 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. As the 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 dampening of the reactor core by the huge area (as much as five-hundred km away) — and, eventually, less dangerous fallout over much of the world. The effort to halt the nuclear contamination and avert a much greater disaster soon involved over 500,000 workers and an estimated eighteen billion roubles, crippling the Soviet economy.

Because most of those directly involved in the Chernobyl disaster soon died of radiation poisoning, there are many uncertainties about the exact sequence of events. Nonetheless, we can be sure that the actual disaster would not have occurred had the experiment not been carried out. Chernobyl was as much an engineering disaster as Three Mile Island: both the immediate and underlying causes were ordinary engineering decisions, whether in operation or design.
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 local concentration was too low to trigger the devices. These systems seem to have failed when the electrical power did.

Reactor 1’s containment survived the explosion. There was no significant release 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 in 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 due to a lack of cooling as the tsunami flooded the reactor buildings to the highest level. The plants did not have leakproof containment vessels that can withstand the pressure of a tsunami. Even some less sophisticated containment vessels were considered too weak to resist a large tsunami; generator-building basements might not have leaked upward. Safety devices normally burn such hydrogen, but the local concentration was too low to trigger the devices. These systems seem to have failed when the electrical power did.

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 Hurricane Katrina was nowhere near New Orleans even to report to it. Everyone who could be evacuated had been. By August 31 (two days after Katrina struck), 80% of New Orleans, a city almost emptied of inhabitants, was under water, with water reaching close to the rooftop level of five buildings.

On March 26, 2007, a year and a half after Katrina passed through New Orleans, the Interagency Performance Evaluation Task Force (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.

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 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 increasingly detailed government studies suggested that 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 significant changes in control of many of the structures and the governmental agencies. For 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 and construction”), go for higher quality 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 more expensive, but even with the support of a simple earthen levee) was a mistake. It is replacing the canals’ I-walls with heavily-braced T-walls locked down by twenty-one meter H-piles angled out in two directions. The use of simple levees was also judged a mistake. The Corps is now “armorizing” all levees where they seem vulnerable to overtopping, that is, covering them with something water will not so easily flow through or quickly wash away. 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 as much or as little levee (or flood control system) as one’s budget permits. One party in a complex social decision in which the future is uncertain is developing minimum standards for evaluating alternative designs. 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 space is needed on necessity 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 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 operations. 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 buttons that moved dampening 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. That is why the operators 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 some systems to fail 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 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 human error.

How likely is a catastrophic failure at any moment? Not very. Perhaps only 10^-3 at any time. But over many years and many reactors even such small risks add up. One author recently calculated that there are: 

\[
\text{450 nuclear power plants in the world. There have been 4 meltdowns in history, one each at Chernobyl and Three Mile Island so far at Fukushima, as partial meltdowns count as meltdowns. That is a ~1.5% failure rate. (Lindsay, 2011)}
\]

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 occurrence of events — like drawing that the three days by six Sigma). 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 had more working backups for its cooling system. But 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 willing to say to an already-engaged engineer on his or her last day on duty to consider the option (more or less figuratively) to 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 an explicit precautionary principle (though it will involve, 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 incorrect. The 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 risks of 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 billion device-hours). So, no product of engineering is (strictly speaking) “failure proof” (all things considered).

Most, perhaps all, nuclear power plants now in operation were built in violation of the planning principle suggested above (at least when the calculation of probability takes into account that human beings will operate the plant). The analogy with gambling is interesting. Gambling is, in fact, much the same. For example, 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 Banjiao, China, in 1975, seems to have killed at least 100,000 people. Another one, at Banqiao, killed 544,000 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 a dam failure in 1889 (Wiki, “Johnston Flood”). In contrast, one of the most common industrial accidents 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 with the option of an alternative, like the wind, solar, or nuclear power, it is obvious that the decisions we will make – such as the choice of energy sources for electricity 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 say to an already-engaged engineer on his or her last day on duty to consider the option (more or less figuratively) to blow up in her face. Managers 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 an explicit precautionary principle (though it will involve, 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 incorrect. The 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 risks of 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
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, 2013 (“The engineer, public safety, and economic constraints”); a seminar for the Department of Philosophy and Ethics, The Technical University-Eindhoven, The Netherlands, May 13, 2013 (“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


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 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 pluralistic 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 the adoption of a new moral rule do 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 can simulate a moral decision on a new case, but merely take different norms and rules can be derived. 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.