2 Risk Analysis and the Ethics of Technological Risk

2.1 The Unfolding of the Fukushima Daiichi Nuclear Accident

On March 11, 2011, the Great East Japan earthquake with a magnitude of 9.0, occurring 130 km offshore, caused a major tsunami, approximately thirteen meters high, that hit the coast of Japan.[1] One of the affected areas was the Fukushima Daiichi nuclear power plant, which hosts six reactors, three of which were operational at the time of the earthquake. In line with their design, the operational reactors automatically "scrammed," that is, the control rods were instantly inserted into the reactor core to reduce the nuclear fission and the heat production.[2] However, as a result of the earthquake the plant was disconnected from its power lines; the connection with the electricity grid was needed for cooling down the reactor core. When all external power was completely lost, the emergency diesel generators kicked in to cool the reactor cores: this was another built-in design measure to improve safety. The real problem started to unfold when forty-five minutes after the earthquake the ensuing tsunami reached the coast: a series of waves inundated the plant causing serious damage, as a result of which eleven of the twelve emergency generators stopped working.

When reactors are designed, the complete loss of external power from electricity grids and from the internal power of the diesel generators – a situation referred to as "station blackout" – is anticipated. In a blackout, batteries come into action that can continue the cooling of the reactor. However, the problem was that the batteries were also flooded in reactors

[1] The course of events has been adapted from the World Nuclear Association's website (www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-accident.aspx) and from a report published by the Carnegie Endowment for International Peace; see Acton and Hibbs, *Why Fukushima Was Preventable.*

[2] Ibid., 4.

1 and 2, while reactor 3 had a functioning battery that continued working for about thirty hours.

More importantly, the problems in the Fukushima Daiichi accident were not only attributable to a lack of electricity. Soon after the tsunami had inundated the plant, the seawater pumps that were supposed to remove the extracted heat from the reactors were destroyed by the tsunami.[3] In boiling water reactors of the type operational in Fukushima Daiichi, water in a primary loop circulates around the reactor core, which produces enormous amounts of heat; that water then starts boiling and becomes the driving force of generators that produce electricity. The hot water is then cooled down through a secondary loop that takes away the heat from the primary loop. Cooled water then reenters the reactor core. The secondary loop is often connected to "fresh" sources of cool water, which explains why nuclear reactors are often built close to seas or rivers. So, even if electricity had been on supply, no fresh water from the sea could have circulated in the secondary loop. When the heated water could no longer be removed, the cooling water in the primary loop inside the reactor started to evaporate, turning into steam. That in turn oxidized the zirconium cladding that surrounded the extremely hot nuclear fuels. As a result, massive amounts of hydrogen were produced. The accumulation of hydrogen – in addition to the high pressure caused by the steam – led to an explosion in reactors 1 and 3. Since reactors 3 and 4 were connected with each other through their vent system, hydrogen also accumulated in reactor 4, leading to an explosion one day later. While reactor 4 was not operational at the time of the accident, it did host a large number of fuel rods in the spent fuel pools. Spent fuel rods are often kept in such a location to cool down before being shipped off. As was the case in the reactor cores, because of a lack of cooling, the water in the pools soon evaporated and after the explosion, the pool was unshielded and exposed to the open air. All the explosions led to the large-scale emission of radiation into the atmosphere. Ironically, the biggest concern surrounding the nuclear accident in Fukushima Daiichi did not relate to the reactors but rather to the spent fuel rods in the nonoperational reactor 4. In a report, the Japanese government revealed that for a time it had even considered evacuating Tokyo,[4] when it was not clear whether the pool could be managed and properly contained. Evacuating Tokyo, a city of 35 million people, could have

[3] Ibid., 5. [4] Quoted from Downer, "The Unknowable Ceiling of Safety."

easily led to many casualties and injuries, much distress, and major financial losses.[5]

It was indeed the convergence of several failures – "the perfect storm" – and the cascading effects that gave rise to one of the largest nuclear accidents in the history of nuclear power production. As a result, 300,000 people in the direct area were evacuated, many of whom have since returned to their homes.

2.1.1 The Aftermath of the Disaster

In November, 2017, six and half years after the accident, I visited the Fukushima prefecture, together with colleagues from the International Commission on Radiation Protection (ICRP). Upon our arrival in Fukushima City, the very first reminder of the accident was the air-monitoring stations on every major street corner that constantly monitored radiation levels, sometimes in real time and sometimes in the old-fashioned way with levels chalked up on small boards that were updated several times a day. Depending on the direction and the strength of the wind, there were days when radiation could shoot up to higher levels, but generally the boards were there to put across the "reassuring" message that the radiation levels in Fukushima City were far lower than the legally acceptable levels, at least at the time when I visited the city.[6]

The impact of the accident was most visible when I left the city. There were still many black bags literally behind many of the houses. This was a reminder of the first days after exposure but also of the first days after people were allowed to return to their homes, when the government had instructed the population on how to clean up radiation residue on the roofs and everything else that had been exposed to large amounts of radiation.

[5] Ibid.

[6] The radiation levels I registered in the days I spent there were around 0.135 microsieverts per hour (μSv/h). Please note that radiation exposure is always linked to time. In other words, the period of exposure – in addition to the radiation intensity – very much matters for the health impacts. It is, however, much more common to communicate legal exposure limits per year (rather than per hour). For instance, in different national legislation it is indicated that levels of radiation of 2 to 3 millisievert per year (mSv/y) are acceptable. The level of radiation registered by me in November, 2017 corresponds to 1.2 mSv/y, which is a considerable amount of radiation but still below the threshold line.

Those bags were then supposed to be collected by the government. While many had already been collected, there were still a number waiting to be removed from people's backyards. In addition to the collection of bags from private addresses, another, perhaps much larger, cleaning operation involved removing contaminated soil from public areas, where a layer of road, sidewalk, school playground, or any other public area literally had to be removed. Indeed, depending on the group of people potentially exposed to radiation, different thicknesses of layers had to be removed: in school playgrounds, for instance, larger portions were removed because children are generally more sensitive than adults to the health impacts of radiation. Contaminated soil was then bagged and shipped off to improvised waste treatment facilities in the hills, valleys, and any other places where, in this densely populated region, space was available for the creation of such facilities. In their first "destinations," the bags were inspected (and opened to remove any high-emitting sources), then rebagged in much thicker blue bags (to guard against leakage into the soil) before then being transported to their "second destination" – another similarly improvised facility. This major – and still ongoing – cleaning operation has resulted in 15–22 million cubic meters of "contaminated soil from decontamination work [being] piled up or buried at about 150,000 locations in [the] Fukushima Prefecture, including plots near houses and schoolyards."[7] The Japanese government is still looking for a "final destination" for all the contaminated soil. While the original plan was to dispose of the soil as waste, that plan was quickly revised when the magnitude of the problem became more apparent. The government considered reusing the soil for road construction, and also on agricultural land for crops that are not consumed by humans. The latter led to quite some controversy in Japan but also elsewhere, in conjunction with the possible dispersal of radiation. All agriculture is for human consumption at some level; also feed for animals will finally reach human bodies and the impact of radiation may be even be worse, through the process of *biomagnification*, or the worsening of toxic effects through the cascading of biological

[7] Ishizuka, "Official Storage of Contaminated Soil Begins in Fukushima." Different sources give different figures. The larger number of 22 million is reported by the Japanese Citizens' Nuclear Information Center; see www.cnic.jp/english/?p=4225the (consulted March 5, 2019).

impacts.[8] Meanwhile, the famous blue bags are a defining feature in the scenery of the Fukushima prefecture. The last stop during our visit was at one of the improvised facilities on top of a hill overlooking the beautiful Date City in the valley below, with the view of countless blue bags in the foreground.

2.2 Assessing Technological Risk

Introducing new technology to society often brings great benefits, but it can also create new and significant risks. Understandably, much of the focus in engineering has been on addressing these risks with respect to different technologies and industries (e.g., the chemical industry) to assess, understand, and manage such risks. For instance, in the chemical industry, risk assessment methods have been proposed for describing and quantifying "the risks associated with hazardous substances, processes, actions, or events."[9] One of the most systematic approaches to assessing risk is the probabilistic risk assessment or probabilistic safety assessment. This is a method that is often used for assessing the risk of major accidents, such as a nuclear meltdown. A probabilistic risk assessment usually involves identifying an undesired outcome (typically a major accident) that we wish to prevent from happening. It aims to identify different sequences of events that could lead to such an outcome, and to assign probabilities to each event. A probabilistic risk assessment calculates the probability of the undesired effect, and risk-reduction efforts will then be devoted to reducing the probabilities of each individual event so that the probability of an ultimate accident will be reduced.[10]

[8] Yap, "Blowback over Japanese Plan to Reuse Tainted Soil from Fukushima."

[9] Covello and Merkhofer, *Risk Assessment Methods*, 3.

[10] Doorn and Hansson, "Should Probabilistic Design Replace Safety Factors?" Proske has conducted a comparison of computed and observed probabilities of failure and core damage frequencies following the Fukushima event which has again questioned the safety of nuclear power plants. Statisticians and parts of the public claim that there is a significant difference in the core damage frequencies based on probabilistic safety analysis and on historical data of accidents including the Fukushima event. See Proske, "Comparison of Computed and Observed Probabilities of Failure and Core Damage Frequencies."

Probabilistic risk assessment has proven to be rather influential in policy-making because it neatly conceptualizes risk and presents it to policy-makers in terms of probability of occurrence. These probabilities enable policy-makers then to agree on the minimum risks with which a new technology (or project) must comply.

One of the first questions that various reports reviewing the accident aimed to answer was whether the Fukushima disaster was the result of improper science and engineering practice, particularly in terms of risk assessment. Various reports responded to this question affirmatively, arguing that the Fukushima Daiichi accident was (at least partially) the result of "bad science," but also the result of bad governance by the policy-makers and the company that operated the reactor (i.e., TEPCO).[11] Indeed, the Fukushima Daiichi accident shows many instances of inappropriate assessment, but it remains above all else "a sobering warning against overconfidence in hazard prediction."[12] In this chapter, I will focus on several limitations of risk assessment. Naturally this is not intended to dismiss risk assessment but rather to make engineers more aware of what assessments involve.

2.2.1 The Science–Policy Interface: What Does "Probabilities" Mean?

At the heart of this (and other accidents), there is a more fundamental problem surrounding the science–policy interface, and more specifically policy-makers' expectations from science: expectations that are partially created by the scientists and engineers involved in making the assessments in question. Indeed, policy-making on technological risk very much depends on scientific findings, and specifically on risk and reliability assessments. The classic distinction made in risk discussions is between the scientific endeavors of risk assessments and the policy endeavors for risk management. It would be beyond the scope of this chapter systematically to review this distinction and other relevant literature on risk governance. Instead,

[11] More specifically regulators, who "regulate" risk, or determine the rules that a vendor needs to comply with, and then go on to monitor compliance with those rules. In this chapter, I shall not discuss those governance issues in detail. For more information, see Nuclear Accident Independent Investigation Committee, *The National Diet of Japan*.

[12] Acton and Hibbs, *Why Fukushima Was Preventable*, 11.

I will focus on one specific aspect of how the outcome of risk assessments is presented and used in policy-making on risky technologies. Risk assessments, especially probabilistic risk assessments, often conclude with the probability of an accident, which is then followed by a minimum criterion for making policy with respect to a specific technology. The probability of a nuclear meltdown is, for instance, often used when a minimum standard that a new nuclear reactor needs to comply with is presented. The seemingly exact numbers, figures, and engineering calculations can, however, sometimes appear to reflect a level of reliability and confidence that is not there.[13] This becomes particularly problematic when the public and policy-makers are encouraged to accept such calculations as *objective truths*,[14] especially when the implicit conclusion is that the indicated probability is "*so low as to be negligible.*"[15] Let me illustrate this by discussing the probabilities of fatal nuclear meltdown in nuclear reactors, specifically by examining what exactly the assigned probabilities mean.

A very important development in the systematic assessment of risks based on probabilities goes back to the 1970s, and was actually based on an improved understanding of how to reduce the risk of nuclear meltdowns. A couple of years before the Three Mile Island accident of 1979, the US Atomic Energy Commission initiated a new study to assess the safety of nuclear reactors by mapping all the events that could possibly lead to such an accident and then assigning probabilities to each single event. The study soon came to be known as the Rasmussen Report,[16] after the Massachusetts Institute of Technology professor Norman Rasmussen, who led the investigations; the proposed method was termed probabilistic risk assessment.[17] The Rasmussen Report found the core damage frequency of the then standard (so-called Generation II) reactors to be approximately 5×10^{-5}. While the historical data with regard to reactors operating between 1969 and 1979 suggested a more pessimistic probability of meltdown (namely 10^{-3}), thinking in terms of probability of core meltdown soon became acceptable for

[13] For a more detailed discussion of nuclear safety and probabilistic risk assessment, see Taebi and Kloosterman, "Design for Values in Nuclear Technology."

[14] Downer, "Disowning Fukushima."

[15] Downer, "The Unknowable Ceiling of Safety," 36; emphasis in original.

[16] Nuclear Regulatory Commission, *Reactor Safety Study*.

[17] Keller and Modarres, "A Historical Overview of Probabilistic Risk Assessment Development and Its Use in the Nuclear Power Industry."

nuclear energy policy in subsequent years:[18] a core meltdown of 10^{-4} was commonly accepted to be the minimum level of safety that different national legislations required new nuclear reactors to guarantee.[19]

Let us now have a closer look at this kind of probability actually means. In the first place, these probabilities indicate core damage frequency per *reactor per year*, that is, years of reactor operation, so an occurrence frequency of 10^{-4} corresponds to one accident in every 10,000 reactor years. On the basis of the number of reactors in operation in the 1980s (i.e., almost 500), this therefore meant that an accident could occur once in every twenty years.[20] However, in the 1980s, a supposed "nuclear renaissance" was anticipated that would entail a growth of as many as 5,000 reactors worldwide. Ten times more reactors would amount to ten times more reactor years. As a result, accidents could become ten times more likely. A core meltdown accident probability would then increase to once every two years,[21] which was deemed unacceptable in terms of both public confidence in nuclear energy and the political acceptability of nuclear energy.[22] Safer nuclear reactors were therefore needed.

2.3 How Did the Fukushima Disaster Fall through the "Cracks" of Risk Assessment?

In the previous section we discussed the actual meaning of probabilities in terms of risk assessments, arguing that risk assessments are potentially effective tools for public policy but only if we properly understand and use them. In the remainder of this section we will discuss why the Fukushima disaster was not anticipated, arguing that several issues that gave rise to the

[18] Minarick and Kukielka, *Precursors to Potential Severe Core Damage Accidents, 1969–1979*.

[19] The Nuclear Regulatory Commission often distinguishes the probability of core-melts from the probability of core-melts with significant releases (i.e., a major accident, like Fukushima). The frequency of 10^{-4} refers to the former and not to the latter, and it is a standard from the 1970s. Modern reactors are expected to perform at a probability that is substantially lower. Nuclear Regulatory Commission, *Safety Goals for the Operations of Nuclear Power Plants*. I wish to thank John Downer for pointing this out to me.

[20] Each year, 500 reactor years would pass, which means that based on the probability of 10^{-4}, the expected number of accidents would be 5×10^{-2} (i.e., 500×10^{-4}), or simply once in every twenty years.

[21] Calculation: $5{,}000 \times 10^{-4} = 5 \times 10^{-1}$ or simply once in every two years.

[22] Weinberg and Spiewak, "Inherently Safe Reactors and a Second Nuclear Era."

accident could have been anticipated and hence, the accident could have been prevented. Let us discuss several limitations of risk assessment, or what risk assessment cannot anticipate.

Interestingly, the Onagawa power plant, which was actually closer to the epicenter of the earthquake and experienced tsunami waves as high as the Fukushima Daiichi plant, was not affected.[23] This gives rise to the question as to why the Fukushima Daiichi plant was affected. Different reports have concluded that the Fukushima Daiichi accident was the result of problematic assumptions made in the risk assessments. There were at least four important aspects of risk assessment that were problematic, insufficient, or faulty.

First, when designing the Fukushima Daiichi power plant in 1960s, TEPCO estimated the maximum height of a tsunami to be about 6.1 m, less than half the height of the waves that reached the plant. This was based on historic seismic evidence in the region.[24] The question is, which earthquakes over what period would have to be taken into account? The design of the Fukushima Daiichi plant seems to have taken too short a historical period into account. The elevation of the reactor was determined on the basis of the Shioya-Oki earthquake in 1938, which had a maximum magnitude of 7.8 on the Richter scale.[25] TEPCO made two sets of calculations in 2008 based on datasets from different sources, each of which suggested that tsunami heights could top 8.4 m – possibly even rising above 10 m. Even if the height of the barrier had been raised to 8.4 m (as suggested), safety measures for 10 m would have been insufficient, since the tsunami waves on the day of accident reached an altitude of approximately 13 m. The reason why the Onagawa plant – closer to the epicenter of the March, 2011 earthquake – was not affected was that a "wider" time frame on the basis of historic events, including an earthquake in 869 with a magnitude of 8.3 on the Richter scale, resulted in expected wave heights of 13.6 m, which proved to be the appropriate estimation.[26] This pinpoints an important issue with regard to new scientific insights and how those are reflected in actual safety policies; the Fukushima Daiichi plant was designed in the 1960s, when seismology was a much less mature science. While TEPCO was already catching up on the new

[23] Synolakis and Kânoğlu, "The Fukushima Accident Was Preventable," 6.
[24] Acton and Hibbs, *Why Fukushima Was Preventable*, 12.
[25] Abe, "Tectonic Implications of the Large Shioya-Oki Earthquakes of 1938."
[26] Synolakis and Kânoğlu, "The Fukushima Accident Was Preventable," 6.

insights in order to make its plant safer, its improvements did not go fast enough and, even with the proposed adjustment, they would not have been sufficient to prevent the accident.

Second, it has been argued that the tsunami risk was inappropriately understood and included in the risk assessment.[27] Tsunami risk, even though very familiar in Japan, was added to the nuclear power plant guidelines of Japan's Nuclear Safety Commission only in 2006.[28] It has been observed by tsunami experts that there was insufficient understanding of an important tsunami risk phenomenon:[29] that is, while individual waves 10 km from the coast were maximally 6 m high, it was the convergence of earlier waves coming back from the land and the incoming waves that culminated in the *new* waves, all of which gave rise to tsunami heights as high as 13 m.[30]

Third, the total loss of off-site power (i.e. grid) and on-site power (i.e. diesel generators and batteries) was not considered as a possibility.[31] This loss of on-site electricity occurred because the power from the electricity grid was disconnected as a result of the tsunami and the diesel generators were situated at an insufficiently high elevation, which resulted in their being inundated, unlike what had been predicted in the risk assessment. Indeed, such station blackouts were anticipated in the assessments; that is, batteries were added to the design of the plants as an extra layer of safety. The problem was that the batteries were also partially inundated, and they could last for only a short time. What would happen if the batteries also did not work (or stopped working) was not anticipated in the risk assessments.

Fourth, and in conjunction with the latter, crucial components were flooded during the tsunami. As mentioned in the previous paragraph, the batteries were placed beneath the inundation level, which was why the electricity in the plant was completely lost, and other crucial components for safety – such as the seawater pumps – were not protected either, so that they were severely damaged after the tsunami arrived on the coast. More generally, one might argue that the focus of risk assessment for nuclear

[27] IAEA, *The Fukushima Daiichi Accident Report by the Director General*.
[28] Acton and Hibbs, *Why Fukushima Was Preventable*.
[29] Synolakis and Kânoğlu, "The Fukushima Accident Was Preventable."
[30] Acton and Hibbs, *Why Fukushima Was Preventable*, 10.
[31] Synolakis and Kânoğlu, "The Fukushima Accident Was Preventable."

power plants is often mainly – or sometimes solely – upon the core damage. As mentioned earlier in the description of this case, the biggest reason for concern in the Fukushima Daiichi disaster was not the reactor cores of the operational (and nonoperational) reactors: the reason why the Japanese government even considered evacuating Tokyo was the presence of the spent fuel rods pool in nonoperational reactor 4.

In conclusion, there were indeed several aspects of risk assessments that had been clearly carried out inappropriately, which is why several reports concluded that the Fukushima Daiichi accident could have been prevented, but let us have a closer look to see what we could and should expect from risk assessments and, more importantly, whether we can anticipate and address all possible risks.

2.4 What Risk Assessments Cannot Anticipate: "Normal Accidents"

Since risk and reliability assessments are becoming increasingly influential in how we actually perceive and deal with risk, it is important that we also critically review these assessment methods. If the science were done properly, could we assume that we could, in principle, anticipate and include all risk in our (probabilistic) assessment? How we deal with uncertainties remains a major problem. I will review several important limitations of reliability assessments, and more specifically probabilistic assessments, arguing that – in principle – there are things that risk assessments *cannot* address. From the outset, it should be stated that I am merely trying to make engineers sensitive to what can and cannot be anticipated with such assessments, all of which could potentially help engineers to gain a richer notion of what risks entail and how we can deal with them. The next section, on the societal issues of risk assessments, serves the same purpose. A fuller understanding of risk in engineering could also improve how assessment is presented and used in policy-making, all of which could be more conducive to better use of risk assessment in public policy. What, then, are the risks that we cannot anticipate?

First of all, assessment methods are often based on the premise of perfect human performance.[32] It is because of this assumption – that the operator will always function flawlessly – that after accidents government reports often conclude that "calculations would have been sound if people had only

obeyed the rules."[33] The official Fukushima report also concluded that the accident had to be viewed as a "man-made" disaster.[34] Nongovernmental reports on Fukushima reiterated the same conclusion; for instance, the Carnegie Report concluded that "the Fukushima accident does not reveal a previously unknown fatal flaw associated with nuclear power," and rather "it underscores the importance of *periodically reevaluating plant safety* in the light of dynamic external threats and of *evolving best practices*."[35] This is in a way true, because the types of risks manifested during the unfolding of the chain of accidents were known: i.e., proper periodic reevaluating of tsunami risks, and following international best practice as well as best practice from other plants elsewhere in Japan (such as in the Onagawa plant), could have prevented the chain of accidents. Yet, while we can try to estimate lower bounds and upper bounds of the occurrence probabilities,[36] the fundamental issue remains, which is that some risks cannot be fully anticipated; ironically, we learn from the mistakes of each accident to make our engineering systems less prone to similar risks. An important lesson learned from the Fukushima accident was that the diesel generators and batteries should have been placed at a higher altitude even if the tsunami risk assessments assessed otherwise. This might sound like common sense, but it was not standard practice in many nuclear power plants throughout the world, including even those situated close to rivers and coastlines. This was perhaps due to an overconfidence in the risk assessments regarding the potential wave lengths of tsunamis. More generally speaking, we need always to deal with the "paradox of safety," meaning that "safety is often measured in its absence more than in its presence"; the term "accident" essentially means that "as long as hazards ... and human fallibility continue to co-exist, unhappy chance can combine them in various ways to bring about a bad event."[37] We can therefore conclude that several impacts cannot be systematically included in risk and safety assessments.

[32] Recent improvement to risk assessment methods have introduced a human error probability in order to incorporate human error in quantitative risk assessments. See for instance Steijn et al., "An Integration of Human Factors into Quantitative Risk Analysis Using Bayesian Belief Networks towards Developing a 'QRA+.'"

[33] Downer, "Disowning Fukushima," 296.

[34] Nuclear Accident Independent Investigation Committee, *The National Diet of Japan*.

[35] Acton and Hibbs, *Why Fukushima Was Preventable*, 2; emphasis added by me.

[36] Cooke, *Experts in Uncertainty*.

[37] Reason, "Safety Paradoxes and Safety Culture."

Second, and in conjunction with the latter issue, some risks simply cannot be anticipated. In highly complex socio-technical systems with many interconnected components (as in the case of nuclear power plants), there are incidents that are very difficult to predict and, therefore, to prevent from happening. The sociologist Charles Perrow calls these "Normal Accidents."[38] In other words, he means that complex systems are *messy*, and that even functionally unrelated elements can influence each other in ways thatare very difficult (if not impossible) to anticipate.[39] The explosion in reactor 4 in the Fukushima Daiichi plant vividly illustrates a Perrovian Normal Accident. It involved an unanticipated coincidence that – because reactors 3 and 4 were connected – led to an explosion.[40] The result was something potentially much worse than the meltdowns in the reactor cores of reactors 1 and 3. Perrow's Normal Accidents are an acknowledgment of the limitations of assessment, a point that has been observed by other scholars, albeit differently expressed. "The bitter reality is that severe nuclear accidents will occur in the future, no matter how advanced nuclear technologies become; we just do not know when, where, and how they will occur."[41]

Perrow's Normal Accidents are, in principle, instances of unanticipated risks. We could also conceive of risks that could essentially be anticipated, yet that we choose not to include in our calculations because we consider them to be statistically negligible or because we argue that our engineering system can withstand such risks. This is the third limitation of risk assessments; John Downer calls it the framing factor that pertains to "outside-the-frame" limitations and gives the example of a "fuel-laden airliner being hijacked by extremists and then flown into a nuclear plant."[42] While this kind of risk has been recognized by the builders of modern reactors, no attempt is made to calculate its probability (and to include that in the probabilistic risk assessment). Instead, the engineers argue that the hardened containment building around the reactor can withstand such an impact. Even if we assume that this statement is true, we could argue that

[38] Perrow, *Normal Accidents*.

[39] This is based on John Downer's reading of Perrow; see Downer, "The Unknowable Ceiling of Safety," 44.

[40] It seems that while reactors 3 and 4 were connected for the purpose of air circulation efficiency, it was not included in the risk assessments.

[41] Ahn et al., *Reflections on the Fukushima Daiichi Nuclear Accident*, viii.

[42] Downer, "The Unknowable Ceiling of Safety," 40.

the explosion and ensuing fire of such an attack could seriously disrupt the reactor's surrounding safety systems by disconnecting the grid cables, diesel generators, and batteries, and maybe even the cooling pumps that take water to the reactor. Generally speaking, one could say that security issues associated with a reactor – be it a cyber-attack or someone intentionally trying to make the reactor malfunction and cause a meltdown – are the type of risks that are not typically included in most probabilistic assessments.[43]

2.5 The Ethics of Risk: Social Acceptance versus Ethical Acceptability

An important criticism of risk assessment methods has often been that they ignore societal and ethical aspects of risk. This criticism has led to two important developments in the literature. First, a powerful strand of social science scholarship is devoted to developing the concept of the "social acceptance" of technological risk, arguing that when introducing technological risks, people need to accept – or at least tolerate – those same risks.[44] During the last three decades, social acceptance studies have gained more relevance for major technologies, most notably in relation to large-energy projects such as sizable wind parks and nuclear energy technologies.[45] This is due to the controversies and public opposition emerging from the introduction or implementation of such technologies.

In discussions about risky technologies, a distinction is often made between the actual acceptance of technology and the ethical questions concerning which levels of risk *should* be acceptable to the public.[46] The second development in the literature on risk assessment methods has come from

[43] This argument is about the usual approaches to with risk assessment. However, important efforts to quantify security risks with methods and techniques from Game Theory and decompositioning techniques (such as attack trees) and combining or combining safety and security risks need to be acknowledged. See Chockalingam et al., "Integrated Safety and Security Risk Assessment Methods."

[44] Flynn, "Risk and the Public Acceptance of New Technologies."

[45] Chung, "Nuclear Power and Public Acceptance"; Albrechts, "Strategic (Spatial) Planning Reexamined"; Wüstenhagen, Wolsink, and Bürer, "Social Acceptance of Renewable Energy Innovation."

[46] Grunwald, "Technology Policy between Long-Term Planning Requirements and Short-Ranged Acceptance Problems"; Hansson, "Ethical Criteria of Risk Acceptance"; Asveld and Roeser, *The Ethics of Technological Risk*.

the fields of ethics and philosophy. There is a growing body of literature in applied ethics that takes up the issue of the ethical acceptability of risky technologies.[47] It has been argued that when focusing on social acceptance alone, we might easily overlook important ethical issues; so there is a noticeable gap between social acceptance and ethical acceptability.[48] Fittingly, many philosophy researchers are now considering methods for assessing the *ethics of technological risk* and consequently the *ethical acceptability* of risky technology. These assessments often involve conceptual philosophical considerations.

Many authors have emphasized the interrelatedness of the two concepts of social acceptance and ethical acceptability.[49] Lack of social acceptance can sometimes be attributed to the fact that important ethical issues that the new technologies engender are overlooked in the decision-making phase. For instance, public opposition to siting issues may stem from an unfair distribution of risk and benefit between a local community (which will be exposed to additional risks) and a larger region or even nation (which will enjoy the benefits). It has, for instance, been empirically shown that in the case of sustainable energy technologies, the acceptance of individual members of a community is affected by those members' social norms, as well as by their feelings about distributive and procedural justice. In the case of major wind energy projects, it has also been argued that what matters is "not only mere acceptance, but [also] the ethical question of acceptability."[50] I will focus on two approaches to assessing the ethical acceptability of technologies. In conjunction with each approach, I will also discuss why focusing solely on social acceptance may turn out to be utterly inadequate when the ethical issues associated with risk are addressed.

[47] See, e.g., Hansson, "Ethical Criteria of Risk Acceptance"; Asveld and Roeser, *The Ethics of Technological Risk*; Hansson, "An Agenda for the Ethics of Risk."

[48] Van de Poel, "A Coherentist View on the Relation between Social Acceptance and Moral Acceptability of Technology"; Taebi, "Bridging the Gap between Social Acceptance and Ethical Acceptability."

[49] Cowell, Bristow, and Munday, "Acceptance, Acceptability and Environmental Justice"; Van de Poel, "A Coherentist View on the Relation between Social Acceptance and Moral Acceptability of Technology."

[50] Oosterlaken, "Applying Value Sensitive Design (VSD) to Wind Turbines and Wind Parks."

First I will focus on individual-based approaches to ethically consenting to risk. While the need to ensure social acceptance does itself stem from the deeper ethical belief that when an individual is exposed to certain risks, they should be able to be informed about and consent to those risks, it is also relevant to know to what extent the individual has been informed about the risk and has the freedom to consent to it. Second, I will discuss approaches to ethical acceptability that focus on the consequences for ethical evaluation of an action, aiming to reduce the negative and increase the positive consequences of risks and some associated distributional concerns.

2.5.1 Individual-Based Approaches: Informed Consent

At the beginning of this chapter, I described my first encounter with the nuclear accident in Fukushima City in the form of air-monitoring stations on major street corners. Similar stations are also found along the roads in the region. The basic idea behind these stations was, indeed, to inform the population about the radiation risks they were being exposed to. The more fundamental ethical thinking is the belief that whenever risk is being imposed on an individual, that individual has the moral right to be informed about and to consent to the risk. The right to be informed was formalized in environmental law through the Aarhus Convention, which grants a number of rights to the public. It mentions (1) "access to environmental information" and (2) "public participation in environmental decision-making."[51] Consenting to such risk is an additional criterion originating from the *informed consent* principle.

The principle of informed consent has its roots in biomedical ethics, where it is used with regard to medical procedures (e.g., surgery) and clinical practices (e.g., testing a new drug). Its deeper fundamental roots go back to respecting an individual's autonomy, in the *deontological* – or duty-based – school of thinking in ethics. As was asserted by Immanuel Kant, the dignity of the individual needs to be inherently respected.[52] In Kantian thinking,

[51] While this convention primarily refers to "the state of the environment," it also includes "the state of human health and safety where this can be affected by the state of the environment." This quotation is from the website of the United Nations Economic Commission for Europe; see http://ec.europa.eu/environment/aarhus/.

[52] Respect for autonomy could also be defended from the perspective of John Stuart Mill, whose ideas about utilitarianism will be discussed later in this chapter and in the next

therefore, respect for autonomy "flows from the recognition that all persons have unconditional worth, each having the capacity to determine his or her own moral destiny."[53] So when an individual rational agent who can decide for themselves is exposed to some risk, they have every right to be fully informed about the consequences of such risk and to consent to it.[54] Informed consent is built on the two crucial assumptions of (1) being fully informed and (2) consenting to the risk. Let us review these assumptions.

The first assumption is that when people accept (or consent to) a proposed risk, they will have been correctly and fully informed beforehand. The literature on environmental justice provides many examples of why this is a problematic assumption.[55] For instance, in a case study of a uranium enrichment facility in Louisiana, local communities were asked to "nominate potential sites for a proposed chemical facility."[56] While the communities did apparently nominate – and hence consent to – host sites, there were several inherent ethical problems with this situation. One was that the company never informed the local communities about the exact nature of these "chemical plants"; enrichment facilities are indeed chemical plants, but they are very specific types with radiological risks. In addition, the company never presented any quantitative or qualitative risk assessments. Thus "it [was] impossible to know, reliably, the actual risks associated with the plant" when accepting those risks. As a matter of fact, after the nuclear accident, many people in the Fukushima prefecture started measuring levels of radiation for themselves, essentially questioning the officially communicated levels (and exclusion zones). This gave rise to a proliferation of all kinds of devices and citizen-science approaches to measuring and communicating radiation levels in the region.[57] The second assumption upon which informed consent is built is that those who are exposed to potential risk

chapter. Mill's account is very much that individual freedoms need to be respected as long as they do not interfere with or hamper another individual's freedom. The interested reader might like to consult the discussion of autonomy in biomedical ethics: See Beauchamp and Childress, *Principles of Biomedical Ethics*, chap. 4.

[53] Ibid., 103.

[54] Scheffler, "The Role of Consent in the Legitimation of Risky Activity."

[55] Wigley and Shrader-Frechette, "Environmental Justice," 72.

[56] This is a quotation from the draft Environmental Impact Statement of the NRC. It is quoted here from Wigley and Shrader-Frechette, "Environmental Justice," 71.

[57] Taebi, "Justice and Good Governance in Nuclear Disasters."

must consent to that risk. These assumptions also lead to the question of whose consent we should actually take into account and, in conjunction with that, whether we can give each individual a veto vote.

From the early days of engineering ethics, there have been different proposals for applying informed consent to technological risks because there, too, autonomous individuals are being exposed to risks, to which they should in principle be able to consent.[58] This principle is straightforwardly applicable in biomedical ethics, where usually the interest of just one individual patient is at stake, but extending it to include collective technological risk can be rather problematic. As Sven Ove Hansson correctly argues, informed consent is "associated with individual veto power, but it does not appear realistic to give veto power to all individuals who are affected for instance by an engineering project."[59] In the same vein, while we must respect the rights of each individual who is exposed to risk, modern societies would not be able to operate if all imposition of risk were prohibited.[60]

We can further safely assume that the "affected groups from which informed consent is sought cannot be identified with sufficient precision," and hence, the question of whose consent is being sought seems to be highly relevant.[61] This is also reflected in the Louisiana enrichment facility case study concerning the site-application process, where the opinions of host communities located very close to the proposed facilities were not considered. Instead, communities further away from the facilities were consulted.[62] There are also ample other examples of local communities objecting to a proposed local facility against is broader (often national) public endorsement of the same technology; wind energy provides many rich examples.[63] The reason why communities often have more difficulty with proposed facilities at a local level touches on the more fundamental question of the distribution of the burdens and benefits of new technology, or – to put it more bluntly – the winners and losers that new technology creates. This is

[58] Martin and Schinzinger, *Ethics in Engineering*.
[59] Hansson, "Informed Consent out of Context."
[60] Hansson, "An Agenda for the Ethics of Risk," 21.
[61] Hansson, "Informed Consent out of Context," 149.
[62] Wigley and Shrader-Frechette, "Environmental Justice."
[63] Devine-Wright, *Renewable Energy and the Public*; Pesch et al., "Energy Justice and Controversies."

the focus of the next subsection, on the consequence-based approach to ethical acceptability.

2.5.2 Collective, Consequence-Based Approaches

Another leading approach to assessing acceptability of risk involves looking at the consequences of risky technology. Indeed, risky technology is often presented to society from the perspective of its benefits (e.g., well-being). By looking at the benefits and comparing them with the risks, we can – in principle – determine whether the new technology is justified. The fundamental thinking behind this goes back to *consequentialism* as proposed by Jeremy Bentham, which argues that for an action to be morally right, it should produce net positive consequences. The idea behind this school of thought in ethics is that we should tally the good and the bad consequences in order to be able to compare the categories and arrive at a conclusion about the rightness of an action or, in this case, a proposed technology. Consequentialism is a highly influential approach not only in public policy but also at the interface of engineering and policy. It has also been extensively criticized in the literature. I will discuss the approach, its applicability to engineering assessments, and the relevant criticism in Chapter 3. Let me just touch upon one criticism here that is very relevant in the context of risk, which is that consequentialism cannot deal with the distributional issues of risk.

Consequentialism is essentially an approach in which we aggregate the good and bad consequences and in which no serious distinction is made between those to whom those consequences accrue. Distributional issues, however, underlie new technologies, both spatially and temporally. When risky facilities are sited, several fundamental ethical issues need to be addressed in the realm of the spatial, including questions about how environmental burdens and benefits should be distributed. In addition, there are also more practical questions with ethical relevance, such as the matter of how to establish an acceptable distance between potential major accidents with risky technology and residents who would be exposed.[64]

The distributional issue becomes more complex when we have to deal with international (spatial) and intergenerational (temporal) risks. Some

[64] Watson and Bulkeley, "Just Waste?"; Basta, "Siting Technological Risks."

technological projects engender international risks. For instance, some of the technological solutions propoed for dealing with climate change, such as *geoengineering* (i.e., intentional climate change designed to reverse undesired change), raise serious international procedural and distributive justice questions as well as those regarding international governance and responsibility.[65] The multinational character of such proposals makes it virtually impossible to address their desirability only in social acceptance studies. They are perhaps most ethically complex in relation to temporal distribution, alternatively known as *intergenerational* issues. For instance, at what pace should we consume nonrenewable resources, and what level of change in the climatic system will be acceptable to future generations? These questions become especially intricate when new technology that could help us to safeguard future interests compromises the interests of people alive today. Such a situation gives rise to moral questions that are not easy to address in public acceptance studies. For example: Do we have a moral obligation to provide benefits for or to prevent losses for future generations if that comes at a cost to ourselves?

2.6 How to Deal with Uncertainties in Technological Risks

In assessing technological risks, we will inevitably run into the problem of social control of technology, also known as the Collingridge dilemma: that is, the further we are in the development of new technology, the more we will know about the technology (and the associated risks) and the less we can control it. Let me first offer some explanation regarding definitions, because until now, I have used "risk" as a rather generic term. Ibo van de Poel and Zoë Robaey have presented a helpful taxonomy that is particularly relevant to discussions about the risks of new technology and the associated uncertainties. They distinguish between risk, scenario uncertainty, ignorance, and indeterminacy.[66] In discussions of technological risk, we speak of risks when we are familiar with the nature of the consequences and can meaningfully

[65] See, e.g., Pidgeon et al., "Deliberating Stratospheric Aerosols for Climate Geoengineering and the SPICE Project."

[66] Van de Poel and Robaey have a category called "normative ambiguity" that I have not included here; see Van de Poel and Robaey, "Safe-by-Design." Instead, I will present the idea of normative uncertainties in risk discussions: see Taebi, Kwakkel, and Kermisch, "Governing Climate Risks in the Face of Normative Uncertainties."

assign a probability to those consequences;[67] "scenario uncertainty" is a situation when "we do not know all the scenarios (or failure mechanisms) that may lead to an undesirable outcome"; "ignorance" is a situation in which "we not only lack knowledge of all failure mechanisms but furthermore do not know about certain undesirable consequences that might occur"; and indeterminacy is when users or operators "may employ a technology differently than foreseen or expected by the designers."[68] I will add a fifth category: normative uncertainties as situations in which there is uncertainty from a normative (ethical) point of view as to which course of action with respect to risk should be preferred.[69]

Many principles in engineering safety – which aims to increase safety – have been devised to reduce the uncertainties associated with risks, including situations of ignorance and indeterminacy.[70] I will first focus on how engineering has endeavored to respond to this quest, before moving on to discuss approaches that are informed and driven by ethics.[71]

2.6.1 Redundancies, Barriers, and Safety Factors

In engineering, common approaches to acknowledging uncertainties include, among others, building and including redundancies, safety barriers, and safety factors.[72] Redundancies are additional components added to an engineering system to protect the system from failing in one component: For instance, the diesel generators inside a nuclear reactor are often multiplied with redundancy in mind. Safety barriers are often physical systems designed to protect against a certain type of risk; the sea wall in the Fukushima Daiichi reactor is a typical example of such a physical barrier

[67] See for other definitions of risk Hansson, "Risk and Safety in Technology."

[68] Van de Poel and Robaey, "Safe-by-Design," 298–99.

[69] Taebi, Kwakkel, and Kermisch, "Governing Climate Risks in the Face of Normative Uncertainties."

[70] Möller and Hansson, "Principles of Engineering Safety"; Doorn and Hansson, "Should Probabilistic Design Replace Safety Factors?"

[71] There are also mathematical ways of dealing with uncertainties, for instance by "integrating out" uncertainties; see Van Gelder, "On the Risk-Informed Regulation in the Safety against External Hazards."

[72] It is not my intention to systematically review safety engineering approaches. For an overview see Doorn and Hansson, "Should Probabilistic Design Replace Safety Factors?"

that was supposed to protect against tsunami risks.[73] With their roots in antiquity, safety factors are perhaps the oldest of these ways of reducing uncertainty in engineering. They have mostly been used in construction engineering and mechanical engineering, in order to design engineering artifacts and constructions that are able to resist loads higher than those they should withstand during their intended use.[74] A bridge, for instance, could be designed to withstand loads three times the maximum weight it needs to withstand; the safety factor would then be 3. This safety factor is a direct way of acknowledging the unanticipated hazards that could take place. While the rationale of adding extra strength to construction has very old roots, it was only in the nineteenth century that numerical values were added to quantify the extent of the extra strength to be added to a system.[75] Basically, the less we know, the larger the safety factor should be. Likewise, the larger the potential major consequences of an undesired effect (e.g., a hydropower dam collapsing), the greater the safety factor should be.

More nuanced thinking in safety engineering has guided us toward expressing risks in terms of probabilities of occurrence. Probabilistic risk assessment has been presented by some as an alternative to safety factors. Probabilistic approaches, the probabilistic risk assessment being a prominent type, are intended to address risk in terms of the probabilities of the different scenarios that could lead to an undesired effect, the aim being to reduce each probability so that the total probability of occurrence of an accident will be reduced. They also focus on reducing the probabilities of a possible undesired impact after a risk has materialized.

In general, probabilistic assessments have been contrasted with deterministic approaches to risk, such as safety factors, in that they present a more nuanced view of the notion of risk. Some disagree, however, maintaining that probabilistic assessment is not necessarily superior to deterministic approaches because a risk to which no meaningful probability can be assigned needs to be addressed by the use of a safety factor.[76] The inability to assign meaningful probabilities to certain events has indeed been a serious problem in probabilistic risk assessment, as has also been discussed above.

[73] IAEA, *Safety Related Terms for Advanced Nuclear Plants*.

[74] Hammer, *Product Safety Management and Engineering*.

[75] Doorn and Hansson, "Should Probabilistic Design Replace Safety Factors?"

[76] Möller and Hansson, "Principles of Engineering Safety."

Sometimes, a probabilistic risk assessment is used in conjunction with a deterministic approach such as using a safety factor.

2.6.2 Changing the Design Philosophy: Safe-by-Design

Systematic risk assessments such as probabilistic risk assessments have contributed to making technologies safer by helping to reduce the probability of an accident.[77] Among other things, they have triggered a change in the design philosophy of nuclear reactors – from being active to passive and ultimately to becoming inherently safe reactors. Active safety regimes are those that depend on human intervention (along with other external sources such as electricity grids). Existing nuclear power reactors (of the Generation II type) partially deploy this safety philosophy. When some of the "potential causes of failure of active systems, such as lack of human action or power failure" have been removed, we call the systems *passively* safe.[78] Generation II reactors have been adjusted – to some degree – to include this design philosophy. For instance, when the earthquake was detected in the Fukushima plant, the operational reactors scrammed as designed so that the control rods were automatically inserted into the reactor core to slow down the chain reaction and heat production and prevent damage to the reactor core. The surrounding safety features of these reactors also assumed a certain degree of passivity in that – in principle – they did not rely on external sources such as electricity grids. Reactors are supposed to remain safe with diesel generators and batteries when all external power is disconnected. When reliance on more external factors has been reduced, higher levels of passivity can be achieved, for instance, by removing reliance on all power sources (externally or internally produced) for cooling. Generation III and III+ reactors incorporate this safety philosophy into their design, for instance by including large sources of water at a higher altitude that can flow into the reactor and cool down the reactor core if the external power and the ability to cool down the reactor are shut down. Passively safe reactors already

[77] One might argue that it is only the structural or procedural measures that make technologies safer; the probabilistic risk assessment helps to quantify the risk levels and may recommend which measures to take from a decision tree analysis. This paragraph draws on Taebi and Kloosterman, "Design for Values in Nuclear Technology."

[78] IAEA, *Safety Related Terms for Advanced Nuclear Plants*, 10.

reduce the probability of an accident substantially (by a factor of about a hundred times).[79]

A policy of inherent safety elevates safety to a different level by removing certain hazards altogether. Simply put, if you do not want your system to be exposed to fire hazard, you should build it from a material that cannot even catch fire; you will then make it inherently resistant to fire hazard.[80] Likewise, if we want to build reactors that are resistant to meltdown risks, we should build their cores from materials than cannot melt at the temperatures produced in the reactor.[81]

Safety improvement in reactor design can follow two different paths. First, an existing design can be improved incrementally. Incremental improvement does not mean small improvements; the above-mentioned example of reducing the likelihood of a meltdown could be achieved by introducing one incremental safety improvement, for instance reducing some of the complexities of the system such as the number of pipes, valves, cables, or any other physical components that could fail. It could also be realized by simply rearranging the safety systems; e.g., bringing safety pumps closer to the reactor vessel would already represent a substantial reduction in complexity and, hence, a safety improvement.[82] Moreover, passively safe features could be achieved by placing sources of water at a higher altitude, which could provide the "safety-related ultimate heat sink for the plant" for the existing design of conventional nuclear power plants.[83]

Safety improvement can also be achieved by introducing *revolutionary* changes to design, that is designing from scratch with safety as the leading criterion. The notion of Design for Values, as presented later in this book, is very much in line with the idea discussed here, but it is not only about the value of safety; other key values of engineering such as sustainability, security, and affordability can play a crucial role in design too.[84]

On a related subject, a fairly recent approach to engineering design is what is termed the Safe-by-Design approach, which has been developed to

[79] See Taebi and Kloosterman, "Design for Values in Nuclear Technology," 809.

[80] Nolan, *Handbook of Fire and Explosion Protection Engineering Principles*.

[81] For more information regarding the three safety regimes in relation to new reactors, see Taebi and Kloosterman, "Design for Values in Nuclear Technology."

[82] Ibid., 820. [83] Schulz, "Westinghouse AP1000 Advanced Passive Plant," 1552.

[84] This is a reference to the so-called Pebble-Bed reactors, which are inherently safe and cannot melt down; see Goldberg and Rosner, *Nuclear Reactors*.

address safety issues at the research and development and design stage. It was introduced particularly in response to the unanticipated risks presented by emerging technologies such as synthetic biology or nanotechnology. Safe-by-Design aims to mitigate risks as much as possible during the design process rather than "downstream during manufacturing or customer use."[85] This is a fascinating approach that frontloads thinking about safety at an early stage of development.

In the beginning of this subsection, I distinguished between risk, scenario uncertainty, ignorance, and indeterminacy. I have adopted this taxonomy from the work done by Van de Poel and Robaey on the Safe-by-Design approach, particularly focusing on how Safe-by-Design deals with more complex uncertainties. Risk can be eliminated "by taking away the (root) causes," which can result in inherent safety approaches as discussed above; Safe-by-Design can further set out to "either reduce the likelihood of undesirable scenarios (or failure mechanisms) or to reduce the consequences of undesirable scenarios, for example by providing containment."[86] The strategies for reducing risk are not always successful in dealing with scenario uncertainty because they can consider only known scenarios, which is why unknown scenarios must be dealt with differently. This may mean deploying safety factors (as discussed above), but safety factors are not directly applicable – as Van de Poel and Robaey argue – to synthetic biology, nanotechnology, and other emerging technologies.[87]

Situations of ignorance – which, simply put, are situations in which we don't know and we don't know that we don't know – are perhaps even more difficult to deal with in Safe-by-Design approaches, because we do not even know the nature of what could go wrong and how to design for (or against) it. The response to ignorance is often sought in precautions involving thinking about risk (such as the Precautionary Principle, as will be discussed below) and in adaptive approaches to risk governance, which do not rely on anticipation of risk but, instead, enable us to deal with potential risk if and when it materializes.[88]

[85] Morose, "The 5 Principles of 'Design for Safer Nanotechnology.'"

[86] Van de Poel and Robaey, "Safe-by-Design," 299. [87] Ibid.

[88] Klinke and Renn, "Adaptive and Integrative Governance on Risk and Uncertainty"; International Risk Governance Council, "Risk Governance Guidelines for Unconventional Gas Development."

Indeterminacy is also very difficult to design for because it relates to human factors in risk when technology is entering into use . This issue has been discussed earlier in this chapter with respect to the social aspects of risk that need to be acknowledged. Van de Poel and Robaey distinguish between two types of indeterminacy: the knowable and the unknowable. The first type are ones that we may be able to forecast and design for.[89] The best example is perhaps designing a passively safe reactor which, in principle, does not depend on an operator who must actively pay attention and intervene if the core starts to get too hot or the pressure rises. This approach was – as discussed above – a response to the Chernobyl disaster, which was partially the result of inattentive operators. The second type of indeterminacy is, however, much more difficult to design for because – as with ignorance – we don't know what we don't know about certain human mistakes during operations. That remains a fundamental challenge in discussions on risk assessment and management.

Finally, Safe-by-Design can be a helpful approach for addressing normative uncertainties, or situations in which there is more than one right answer to the ethical questions surrounding risk. Nuclear waste disposal provides an excellent example, because there are various different methods for dealing with it, for instance in a retrievable fashion that allows for future generations either to retrieve and further deactivate it (and hence respects their freedom of action) or to permanently dispose of it, which is the better option from the perspective of future safety. How to deal with nuclear waste is essentially an ethical question, but one with several (diverging and even contrasting) ethical implications. Yet we cannot state with certainty that one option is to be preferred from an ethical point of view. Safe-by-Design is presented in public policy to encourage frontloading these questions of safety, but also to help weigh safety against other important ethical considerations.

2.6.3 The Precautionary Principle

One important definition of the Precautionary Principle is laid down in the Rio Declaration on Environment and Development (1992): It requires that

[89] Van de Poel and Robaey call this "designing out indeterminacy"; see Van de Poel and Robaey, "Safe-by-Design," 301.

"lack of full scientific certainty shall not be used as a *reason* for postponing cost-effective measures to prevent environmental degradation."[90] What this means is that a lack of full scientific certainty that a hazard exists is not a valid reason against preventive action. Later approaches to the Precautionary Principle involved more prescriptive guidelines, such as the Wingspread Statement (1998), which prescribes that "precautionary measures should be taken" in certain situations.[91] The literature on the Precautionary Principle is full of examples of "late lessons from early warnings,"[92] including health problems associated with lead in petrol fuel combustion that were responded to long after the first problems were observed, and asbestos in construction material. The latter is a commonly cited example in discussions of the Precautionary Principle, since the first signs of its associated health problems date back to 1906; in the "1930s and 1940s cancer cases were reported in workers involved in the manufacture of asbestos," but it was only in 1989 that the first ban on asbestos was introduced. Various studies have concluded that thousands of lives could have been saved if the early warnings had been taken seriously.[93]

The Precautionary Principle is perhaps one of the most misinterpreted and misunderstood ethical principles. Because of the abundance of examples in the literature that seem to imply that the use of risky technologies or materials should have been stopped when the first signs of risk were visible, the Precautionary Principle is often understood in a binary mode and as a conservative, risk-averse restriction on innovation. As a result, in some parts of the world the principle has had difficulty in becoming embedded in serious thinking about risk. However, it can also be interpreted as a principle that can guide action and make us more sensitive to certain risks. Per Sandin's approach, for instance, is helpful in that it distinguishes between four common elements, which can be recast into the following if-clause: "*If* there is (1) a threat, which is (2) uncertain, *then* (3) some kind of action (4) is

[90] See www.un.org/documents/ga/conf151/aconf15126-1annex1.htm; italic added by me.

[91] See www.iatp.org/sites/default/files/Wingspread_Statement_on_the_Precautionary_Prin.htm.

[92] This is the title of a large report prepared by the European Environment Agency, including many historic examples of early warnings that were not taken seriously in time; see European Environment Agency, "Late Lessons from Early Warnings."

[93] Randall, *Risk and Precaution*, 4.

mandatory."[94] The first two clauses will then relate to risk assessments and indicate "*when* the precautionary principle can be applied," while the latter two clauses are about "*how* to apply the principle."[95]

2.6.4 Resilience Engineering

As an acknowledgment that perhaps some uncertainties cannot be reduced and that we should regard them as a given, it has been argued that we should build our systems so that they are resilient. Resilience, generally speaking, concerns the ability of a system to regain a stable position after a disturbance such as a major mishap.[96] It is therefore relevant to the capacity of a system, and as such it "reflects a significant shift away from traditional risk management strategies that focus on levels of risk."[97] The concept has become popular in the early 2000s, and it has been discussed a lot in disaster management and, for instance, in relation to how to return the infrastructure to predicate conditions.[98] The Organization for Economic Co-operation and Development (OECD) defines resilience as the idea that "people, institutions and states need the right tools, assets and skills to deal with an increasingly complex, interconnected and evolving risk landscape ... to increase overall well-being."[99]

Resilience has many different definitions and approaches. Neelke Doorn argues that these vary not only between disciplines but also within disciplines. As an example, she mentions the evolution of the concept in the influential reports of the Intergovernmental Panel on Climate Change (IPCC), where the definitions seem to change from absorption and adaptations to more sophisticated anticipation and reduction of risk as well as recovery of the system.[100]

[94] Sandin, "Dimensions of the Precautionary Principle."

[95] Hansson, "The Precautionary Principle," 264; emphasis in original.

[96] Hollnagel, "Resilience."

[97] Doorn, "Resilience Indicators," 711–12.

[98] Liao, "A Theory on Urban Resilience to Floods"; OECD, *Guidelines for Resilience Systems Analysis*; Doorn, "How Can Resilient Infrastructures Contribute to Social Justice?"

[99] OECD, *Guidelines for Resilience Systems Analysis*, 1.

[100] Doorn, "Resilience Indicators," 713.

2.6.5 Technology as a Social Experiment

The last approach to dealing with the inherent uncertainties of new technologies – including situations of ignorance – is to consider technology as a social experiment. Van de Poel argues that the current appraisals of technologies with large impacts on society (such as synthetic biology) cannot be scientifically proven either through "science-based or evidence-based approaches" or through "precautionary approaches," because these both fail to account for "important actual social consequences of new technologies and making us blind to surprises"; he further argues that we should consider technology a social experiment.[101] Following the principles of biomedical ethics (several of which have been mentioned in the previous sections of this chapter), Van de Poel presents a number of principles that can help to assess the ethical acceptability of responsible experimentation. A social experiment should be set up in a "flexible" fashion, and it should not "undermine resilience," while risks and hazards should remain contained "as far as is reasonably possible," and it should be "reasonable to expect social benefits from the experiment."[102]

2.7 Summary

Risk is a crucial aspect of any engineering practice. The introduction of new technology to society often brings great benefits, but it can also create new and significant risks. Serious efforts have been made to assess, map, understand, and manage these risks. For instance, in the chemical industry, risk assessment methods have been proposed for describing and quantifying the risks associated with hazardous substances, processes, actions, and events. Perhaps the most notable example is the probabilistic risk assessment approach, originally developed to systematically understand and reduce both the risk of meltdown in nuclear reactors and the risk of crashes in aviation. However, these and other risk analysis methods have limitations, some of which I have discussed by reviewing how the Fukushima Daiichi nuclear

[101] Van de Poel, "An Ethical Framework for Evaluating Experimental Technology"; Robaey and Simons, "Responsible Management of Social Experiments."

[102] Van de Poel, "Nuclear Energy as a Social Experiment," 289. See also Taebi, Roeser, and Van de Poel, "The Ethics of Nuclear Power"; Van de Poel, "Morally Experimenting with Nuclear Energy."

accident could fall through the cracks of risks assessments. Naturally, this is not intended to dismiss risk assessments, but rather to make engineers more aware of what assessments can and in particular cannot do, in connection with, for example, the concept of Normal Accidents as introduced by Charles Perrow. Risk assessment methods have been criticized for ignoring the social and ethical aspects of risk, so I have discussed the ethical issues associated with risk analysis, distinguishing between individual-based approaches to ethics of risks (e.g., informed consent) and collective and consequence-based approaches. I have finished by reviewing several methods for dealing with uncertainties in engineering design and applications, including redundancies, barriers, and safety factors, as well as discussing the Precautionary Principle and more modern approaches that take safety to the core of engineering design, specifically Safe-by-Design.