**INSTITUTE FOR RESOURCE AND SECURITY STUDIES**
**27 Ellsworth Avenue, Cambridge, Massachusetts 02139, USA**
**Phone: 617-491-5177 Fax: 617-491-6904**
**Email: info@irss-usa.org**

# SCOPE OF THE EIS FOR NEW NUCLEAR POWER PLANTS AT THE BRUCE SITE IN ONTARIO: Assessment of Accidents and Malfunctions

by
Gordon R. Thompson

June 2008

Prepared under the sponsorship of
Greenpeace Canada

**Abstract**

Bruce Power is considering the construction of new nuclear power plants. Pursuit of that option would require the preparation of an environmental impact statement (EIS). The Canadian Environmental Assessment Agency (CEAA) has published draft guidelines for the required EIS. CEAA's draft guidelines call for, among other matters, an assessment of the potential for accidents and malfunctions related to the proposed new plants. CEAA defines "accidents and malfunctions" as a category of events that includes accidents of a traditional type (events attributable to human error, natural phenomena, etc.) together with intentional, malevolent acts. This report reviews the treatment of accidents and malfunctions in CEAA's draft guidelines, and offers recommendations for a more thorough assessment of the potential for such events. To provide background for those recommendations, the report discusses relevant issues including criteria for the design of nuclear power plants, the safety & security characteristics of plant designs under consideration for use in Ontario, Canada's nuclear regulatory regime, and the adverse societal impacts of secrecy.

## About the Institute for Resource and Security Studies

The Institute for Resource and Security Studies (IRSS) is an independent, nonprofit, Massachusetts corporation, founded in 1984. Its objective is to promote sustainable use of natural resources and global human security. In pursuit of that mission, IRSS conducts technical and policy analysis, public education, and field programs. IRSS projects always reflect a concern for practical solutions to resource and security problems.

## About the Author

Gordon R. Thompson is the executive director of IRSS and a research professor at Clark University, Worcester, Massachusetts. He studied and practiced engineering in Australia, and received a doctorate in applied mathematics from Oxford University in 1973, for analyses of plasma undergoing thermonuclear fusion. Dr. Thompson has been based in the USA since 1979. His professional interests encompass a range of technical and policy issues related to sustainability and global human security. He has conducted numerous studies on the environmental and security impacts of nuclear facilities, and on options for reducing those impacts. For example, Dr. Thompson prepared a report in 2000 for the Standing Committee on Energy, Environment and Natural Resources of the Canadian Senate, discussing the accident risk posed by the Pickering 'A' nuclear generating station.

## Acknowledgements

This report was prepared by IRSS under the sponsorship of Greenpeace Canada. Shawn-Patrick Stensil assisted the author by obtaining information that was used during preparation of the report. The author, Gordon R. Thompson, is solely responsible for the content of the report.

**Contents**

**List of Tables**
(Tables appear at the end of the report.)

## 1. Introduction

Nuclear power plants have operated at the Bruce site in Ontario since 1966, producing electricity for the region.[1] In 2001, Bruce Power took over the operation of the plants comprising the Bruce A and Bruce B stations. Currently, Bruce Power is considering the construction of new nuclear power plants at the site.[2] Pursuit of that option would require the preparation of an environmental impact statement (EIS) by Bruce Power. In April 2008, the Canadian Environmental Assessment Agency (CEAA) published draft guidelines for the required EIS.[3] The draft guidelines are open for public comment until 18 June 2008.

CEAA's draft guidelines call for, among other matters, an assessment of the potential for accidents and malfunctions related to the proposed new nuclear power plants at the Bruce site.[4] This report reviews that aspect of CEAA's draft guidelines, and offers recommendations for a more thorough assessment of the potential for accidents and malfunctions. Our recommendations respond directly to CEAA's solicitation of public comments on its draft guidelines. In addition, the findings and recommendations in this report could be useful in other contexts where potential accidents and malfunctions related to nuclear power plants are being considered.

CEAA defines "accidents and malfunctions" as a category of events that includes accidents of a traditional type (events attributable to human error, natural phenomena, etc.) together with intentional, malevolent acts. Consideration of malevolent acts in an EIS for a commercial nuclear facility is a comparatively new development in the field of environmental assessment. CEAA deserves commendation for taking this step. There is, however, a need for improvement in CEAA's draft guidelines for considering malevolent acts, as discussed later in this report.

### *Role of an EIS*

Some people view the preparation of an EIS as a formality to be observed after the design of a project is completed. That is a misunderstanding. Instead, an EIS is intended to be part of a process to ensure that major projects serve broad interests of present and future generations. In setting out the guiding principles of an EIS in the draft guidelines, CEAA

---

[1] The Douglas Point nuclear power plant, which employed a prototype CANDU reactor and had a capacity of 220 MWe, operated at the Bruce site between 1966 and 1984. The Bruce A station and the Bruce B station are each comprised of four nuclear power plants, employing CANDU reactors. The four Bruce A plants first entered service between 1977 and 1979, and the four Bruce B plants first entered service between 1984 and 1987. See: Bruce Power, 2007, Section 3.
[2] Bruce Power, 2007.
[3] CEAA, 2008.
[4] Throughout this report, the term "nuclear power plant" means a fission reactor and its associated equipment, including equipment to produce electricity. Future (Generation IV or later) nuclear power plants might also produce hydrogen, potable water and/or process heat.

begins with the statement:[5] "Environmental assessment is a planning tool used to avoid or mitigate the possible adverse effects of development on the environment." Subsequently, CEAA specifies the factors that should be considered in an EIS. Those factors include not only environmental effects, but also the purpose of the project, the need for the project, alternatives to the project, and alternative means of carrying out the project.[6] Such factors are important to the EIS's role as a planning tool.

### *Sustainability as a guiding perspective*

This report focuses on only one aspect of the EIS – assessment of the potential for accidents and malfunctions. That potential must, however, be considered in its full context. To provide that context, we view accidents and malfunctions from the perspective of sustainability. CEAA's draft guidelines acknowledge the importance of sustainability, which they address through the concept of sustainable development, defined as follows:[7] "Sustainable development seeks to meet the needs of present generations without compromising the ability of future generations to meet their own needs." That definition was first articulated by the World Commission on Environment and Development (WCED) in 1987.

Sustainability of engineered systems, such as nuclear power plants, is a large subject.[8] Indeed, developing, refining and applying the principles of sustainability are likely to be major preoccupations of humanity throughout the 21st century. This report does not claim to provide a comprehensive discussion of the principles of sustainability. That task would require a much larger effort. Moreover, the principles of sustainability are evolving. There is no generally accepted, overall framework of sustainability principles, and no prospect of such a framework emerging soon. Yet, there is consensus among governments and international agencies that any new, large, long-lived engineered system should be designed according to sustainability principles. A new nuclear power plant would certainly be a large and long-lived system. Bruce Power envisions that its new nuclear power plants would enter service during the period 2015 to 2018, and then operate for 60 years.[9] Therefore, planning for such plants must reflect the sustainability needs and standards of the second and third quarters of the 21st century, to the extent that these can be predicted now.

### *Nuclear power and Ontario's electricity future*

Planning by the Ontario government for the province's electricity future employs a timeframe considerably shorter than the anticipated lifetime of nuclear power plants. At the government's direction, the Ontario Power Authority (OPA) has prepared an

---

[5] CEAA, 2008, Section 2.1.
[6] CEAA, 2008, Section 4.2.
[7] CEAA, 2008, Section 2.4.
[8] The term "engineered system" is used here to describe a system that is deliberately created or assembled by humans to serve specified functions.
[9] Bruce Power, 2007, Figure 4.

Integrated Power System Plan (IPSP) for the 20-year period beginning in 2007. OPA has applied to the Ontario Energy Board (OEB) for approval of the IPSP, and OEB has initiated a public proceeding to consider the application. The Ontario government has directed OPA to plan for nuclear capacity to meet base-load electricity requirements, while limiting Ontario's total in-service nuclear capacity to 14 GWe during the IPSP period.[10]

Part of Bruce Power's contribution to electricity planning is to consider the construction of new nuclear power plants at the Bruce Site. Bruce Power has envisioned the construction of up to four new plants, to provide approximately 4 GWe of additional generating capacity. These four plants would be constructed as two twin-unit modules.[11] More recently, in March 2008, the Ontario government invited a selected set of nuclear power plant vendors to submit proposals for construction of one twin-unit module. The module would have a total capacity of 2 to 3.5 GWe. It would be built at a currently unspecified site in Ontario, generally understood to be either the Bruce site or the Darlington site. The contract would include an option for construction of one or two additional units at a later date.[12] In late May 2008, Ontario's Energy Minister said that he expected to announce the location of the first two-unit module – either at Bruce or at Darlington – during June 2008.[13]

Construction of new nuclear power plants in Ontario must be viewed in the context of worldwide trends in the use of nuclear power. Worldwide trends will largely determine the types of plant that are available, the economics of the nuclear fuel cycle, standards for safety and security of nuclear facilities, public acceptability of nuclear power, and other factors. At present, trends related to nuclear power are unclear, and there are widely varying views about the merits and prospects of this energy source.

### *Scenarios for future use of nuclear power worldwide*

Nuclear power is in a transitional phase. Annual, worldwide capacity additions peaked in 1985 and have been modest since 1990.[14] If construction of nuclear power plants does not resume, total capacity will decline as plants are retired. Observers view this situation in widely differing ways. Some call for a nuclear power "renaissance" in which nuclear generating capacity rises substantially. Others prefer or expect a scenario in which nuclear capacity declines, leading to eventual disappearance of the industry.

The most ambitious visions of the nuclear renaissance are exemplified by a "technology roadmap" issued under the auspices of the US Department of Energy in 2002.[15] The roadmap proposed the development and use of a range of "Generation IV" nuclear fission

---

[10] Duncan, 2006.
[11] Bruce Power, 2007, Section 2.3.
[12] Infrastructure Ontario, 2008.
[13] CBC News, 2008c.
[14] IAEA, 2006a.
[15] NERAC/GIF, 2002.

reactors that would push against engineering limits in a variety of respects. Some reactor types would produce hydrogen as well as electricity, thereby providing fuel for use in vehicles and other applications. Reactors would be deployed in such large numbers that uranium reserves would become depleted during the latter part of the 21st century. To prepare for that eventuality, large-scale reprocessing would begin during the next few decades, and breeder reactors would be deployed beginning in about 2030.

A less extreme but still highly ambitious vision of the nuclear renaissance is contained in a study published under the auspices of Massachusetts Institute of Technology in 2003.[16] The authors saw no need for reprocessing or breeder reactors during at least the next 50 years. They offered an illustrative scenario for expansion of nuclear capacity using "Generation III" reactors whose designs would involve a comparatively small evolutionary step from the designs of present reactors. In the scenario, annual worldwide production of nuclear-generated electricity would rise by a factor of 4 to 6 between 2000 and 2050.

Many observers doubt the merits of nuclear power, and seek or expect a decline in its use.[17] Some argue that nuclear power can and should be phased out, even during an effort to dramatically reduce greenhouse gas emissions from electricity generation.[18] Others argue that scenarios for expansion of nuclear capacity are fanciful, and that the commercial nuclear industry is in terminal decline.[19]

*Types of new nuclear power plant envisioned for Ontario*

In January 2007, Bruce Power identified six types of nuclear power plant that it was considering. This group consisted of two CANDU plants (the ACR-1000, and the Enhanced CANDU-6), two pressurized-water-reactor (PWR) plants (the AREVA US EPR, and the Westinghouse AP1000, and two boiling-water-reactor (BWR) plants (the ESBWR, and the SWR-1000).[20] In its March 2008 solicitation of proposals for construction of new plants, the Ontario government narrowed this list, eliminating the Enhanced CANDU-6 and the SWR-1000.[21] Subsequently, the vendor of the ESBWR withdrew from the competition. Thus, the field of contending designs in Ontario now consists of:

(i) the US EPR, a PWR plant offered by AREVA;
(ii) the AP1000, a PWR plant offered by Westinghouse; and
(iii) the ACR-1000, a CANDU plant offered by Atomic Energy of Canada Ltd (AECL).

[16] Ansolabehere et al, 2003.
[17] Romm, 2008.
[18] Makhijani, 2007; Greenpeace International, 2007.
[19] Schneider and Froggatt, 2007.
[20] Bruce Power, 2007, Section 4.4.
[21] Infrastructure Ontario, 2008.

Each of these plant types is said to be in the Generation III category, as mentioned above.[22] According to Bruce Power, Generation III nuclear power plants are "safer, more efficient and easier to build" than the Generation II plants that comprise the majority of the world's fleet of nuclear power plants.[23] The comparative safety of Generation II plants and the plant types being considered for Ontario is discussed later in this report.

The three plant types now being considered for construction in Ontario have significantly differing characteristics from the perspective of safety and security. In other words, these plant types differ in their potentials for accidents and malfunctions. Bruce Power proposes to ignore those differences when preparing an EIS, offering instead the following approach:[24]

> "Bruce Power has not decided on a specific reactor design at this time. Accordingly, the EA [environmental assessment] will be "technology neutral" and will conduct an assessment of the likely effects of the Project by using typical bounding conditions to encompass all reactor designs. Accordingly, Bruce Power does not need to provide a detailed design of the reactor and the associated facilities but will identify sufficient bounding parameters and characteristics of the reactor and associated facilities so that an assessment can be made."

The merit of that approach is discussed later in this report.

### *Secrecy and its impacts*

The nuclear industry, and the bodies that regulate its safety and security, are prone to secretive behavior. Such behavior reflects a variety of motives. The nuclear industry has a legitimate need to protect trade secrets, but has also been known to hide embarrassing information that should be disclosed. Regulators have often chosen to not assess, or not disclose, the upper end of the range of risk associated with nuclear facilities, reflecting a paternalistic view of the public's ability to use such information. In recent years, as the potential for intentional, malevolent actions has become a salient issue, industry and regulators have become more secretive. This report discusses trends in secrecy, the relationship between secrecy and the criteria used for design of nuclear facilities, and the adverse impacts of secrecy.

### *Scope of this report*

To provide a proper context for addressing accidents and malfunctions, this report introduces two large subjects – the principles of sustainability, and the application of those principles to nuclear power in the 21st century. A thorough examination of both subjects, and their inter-connections, would involve two major tasks. First, a

---

[22] Some plant designs are said to be in a Generation III+ category. That designation has no technical meaning, because it presumes a generally-accepted classification scheme that does not exist.
[23] Bruce Power, Section 4.4.
[24] Bruce Power, 2007, Section 4.4.

comprehensive framework of sustainability principles, indicators and criteria would be developed, to the point where it could be used to assess the sustainability of any proposed engineered system. Second, that framework would be used to assess a proposed program of nuclear power, examining the entire nuclear fuel cycle from uranium mining through to plant decommissioning and disposal of radioactive waste.

Those tasks are not undertaken here. As an indication of the scale of effort that those tasks could require, consider a research project that is being conducted in the UK. In September 2007, a team of researchers based at the University of Manchester began a three-year project funded by a grant of 2.1 million UK pounds from the Engineering and Physical Sciences Research Council, with the objective of performing an integrated assessment of the sustainability of nuclear power.[25] The project involves tasks similar to the two described above, although the sustainability framework to be developed at Manchester will be less comprehensive because it will apply to energy options rather than engineered systems in general. If the project is well run, it will produce interesting results. It will not, however, provide the final word on the complex subjects that it addresses. Research and debate on these subjects will continue for many years.

Thorough assessment of the potential for accidents and malfunctions, for a particular design of nuclear power plant at a particular site, would be a major task. Such an assessment would require the participation of a team of experts possessing diverse knowledge and capabilities, and with access to detailed information about plant design. Many person-years of professional effort could be required, especially if the design had not been previously assessed or if new issues arose. The task would involve the use of sophisticated computer models. Development of such models, and the conduct of experiments to support and validate the models, requires significant expenditures.

This report does not attempt to provide a thorough assessment of the potential for accidents and malfunctions at plants of the types being considered for use in Ontario. Instead, this report reviews the treatment of that potential in CEAA's draft guidelines, and offers recommendations for a more thorough assessment. Some illustrative information about accidents and malfunctions is provided here to support our recommendations.

### *Key questions about accidents and malfunctions*

This report necessarily addresses a number of complex issues. To clarify those issues, it is useful to frame some key questions about accidents and malfunctions at new nuclear power plants in Ontario. These questions would apply equally to the proposed construction of new plants at either the Bruce or the Darlington site. The questions are:

(i) what criteria would be used to assess the safety and security of new plants?;
(ii) are these criteria adequate for the 21st century?;

[25] EPSRC, 2007.

(iii) what are the safety & security characteristics of the plant types under consideration?;
(iv) is Canada's nuclear regulatory regime adequate?; and
(v) what are the trends in secrecy about nuclear risks, and how do those trends relate to plant design?

*Structure of this report*

The remainder of this report has eight sections. Section 2 discusses sustainability and nuclear power. Then, Section 3 discusses the potential for accidents and malfunctions at nuclear power plants, and proposes a classification of these events that corrects deficiencies in CEAA's draft guidelines. Section 4 reviews international and Canadian criteria for the safety and security of new nuclear power plants, and proposes a more demanding set of criteria. That discussion informs a brief review, in Section 5, of the safety and security characteristics of the types of nuclear power plant that are being considered for use in Ontario. Section 6 addresses the adequacy of Canadian regulation of the safety and security of nuclear power plants. Secrecy and its impacts are discussed in Section 7. Conclusions and recommendations appear in Section 8, and a bibliography is provided in Section 9. All documents cited in this report are listed in the bibliography. Tables, numbered according to the relevant section of the report, appear at the end of the report.

## 2. Sustainability and Nuclear Power

### 2.1 Imperatives and Principles of Sustainability

During recent decades, citizens and governments have increasingly recognized the need to organize human affairs within the context of a finite Earth. One manifestation of that need is human-induced, adverse change in the climate.[26] Other signs of stressed ecosystems are also evident. The Millennium Ecosystem Assessment determined that 15 out of the 24 ecosystem services that it examined "are being degraded or used unsustainably, including fresh water, capture fisheries, air and water purification, and the regulation of regional and local climate, natural hazards, and pests".[27] By abusing ecosystems in this manner, we deplete renewable resources that are essential to human life. Non-renewable resources are also being depleted. For example, a growing body of analysis predicts a peak in world oil production within the next few decades.[28]

In our well-populated, competitive world, limits to the availability of resources and ecosystem services have implications for peace and security. For example, analysts are considering the potential for climate change to promote, through its adverse impacts, social disorder and violence.[29] It is increasingly evident that nations must cooperate to

[26] IPCC, 2007.
[27] MEA, 2005, page 1.
[28] GAO, 2007.
[29] Campbell et al, 2007.

protect and share the Earth's resources. International agreements such as the Framework Convention on Climate Change reflect that imperative. National policies on a range of issues – including energy, agriculture, forestry, transport, minerals, and urban planning – must be consistent with global needs.

Policy choices made now will determine the opportunities available to future generations. The future implications of current policy choices have been examined by analysts convened by the Stockholm Environment Institute (SEI).[30] These analysts identified six possible worldwide scenarios for human civilization over the coming century and beyond. In some scenarios, the world faces chronic, unresolved problems and conflicts. In others, the world descends into barbarism. The most attractive scenario, with the greatest opportunities for future generations, is one that the SEI analysts described as a New Sustainability Paradigm.

The concept of sustainability was brought to wide public attention by the World Commission on Environment and Development in 1987. WCED discussed the concept in terms of sustainable development, to emphasize that sustainability is compatible with improvement in the conditions of life for poorer societies. Since 1987, the concept of sustainability has been widely endorsed by governments and other entities. Yet, there has been comparatively little progress in making the concept operational at the level of specific policies and plans. In an effort to address that problem, the Organization for Economic Cooperation and Development (OECD) initiated a three-year project in 1998, seeking to identify sustainability principles and indicators that can be used in policy making. One product of the effort was a report by the OECD Nuclear Energy Agency (NEA), published in 2000, that discussed commercial nuclear power in the context of sustainable development.[31]

### *The NEA view of sustainability*

In discussing the concept of sustainability, the NEA report took as its starting point the WCED definition of sustainable development as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs". The NEA report elaborated on that definition by suggesting that sustainability involves the passing on to future generations of a stock of capital assets, which could be human-made, natural, or human and social. Human-made assets include buildings, machinery, and infrastructure. Natural assets include the environment, and the renewable and non-renewable resources that it can supply. Human and social assets include education, health, scientific and technical knowledge, cultures, institutions, and social networks.

According to the NEA, "strong sustainability" involves the preservation of an asset in its present form. That approach is relevant, for example, to ecosystems that are essential and

[30] Raskin et al, 2002.
[31] NEA, 2000.

irreplaceable. Earth's atmosphere fits that category. An alternative approach is "weak sustainability", whereby the loss of one asset (e.g., an area of forested land) is offset by creation of another asset (e.g., development of a city on the formerly forested land). The weak-sustainability approach requires tradeoffs, which create the potential for conflicts within and between generations. The strong-sustainability approach is conceptually simpler, but is rarely encountered in its pure form. For example, human-induced emissions of $CO_2$ to the atmosphere cannot be eliminated instantly, but must be reduced over time. With the best of intentions, we cannot pass on to coming generations an atmosphere containing $CO_2$ at the present concentration.

The NEA report contained a general discussion of nuclear power from the perspective of sustainability. That discussion addressed many of the relevant issues, including emissions of $CO_2$ and other greenhouse gases. The NEA report did not, however, provide an analytic framework that could be used to assess the sustainability of a proposed program of nuclear power, or to compare the sustainability of that program and the sustainability of other strategies to meet energy needs.

The NEA report discussed the potential for a nuclear power plant to experience a large, unplanned release of radioactive material to the environment. Such a release would substantially degrade human-made, natural, human, and social assets in the affected locations. For example, contaminated land and buildings would be abandoned, and exposed populations would experience higher rates of cancers. Thus, the release could have significant, adverse effects on sustainability.

According to the NEA, the probability of a large, unplanned release is low. Thus, a conceptual and analytic framework is needed to assess the sustainability implications of potential events with large, adverse consequences and low probability. That issue is not unique to nuclear power. For example, capture and sequestration of $CO_2$ is an energy option that could allow use of fossil fuels without adverse effects on Earth's climate. If a proposed project involves $CO_2$ sequestration on a large scale, an assessment of the sustainability of the project should examine the probability and consequences of a large, unexpected release of sequestered $CO_2$ to the atmosphere.

Analysts in the nuclear industry and its regulatory bodies address the potential for high-consequence, low-probability events by defining an indicator called "risk". They define that indicator as the arithmetic product of a numerical indicator of consequences and a numerical indicator of probability.[32] They typically argue that equal levels of risk should be equally acceptable to citizens. That argument has been made so often that it has become dogma. Yet, the argument is not a scientific statement. It is, instead, a statement representing a particular set of values and interests.

[32] In this report, the term "risk" is used in a more general sense, to encompass a range of qualitative and quantitative information about the potential for an adverse outcome.

The NEA report recognized that citizens may be more concerned about the potential for a high-consequence, low-probability event than about the potential for a low-consequence event with the same nominal level of risk. That concern can reflect a legitimate set of values and interests, skepticism about estimates of low probability, doubt that the complexity of consequences can be represented by simple indicators, and recognition that new phenomena can come into play when thresholds of consequence are exceeded.[33] The NEA report recommended that concerns of this type be heard, respected, and addressed by governments. Acceptance of that recommendation would require the abandonment of previous dogma about the acceptability of risk. Public-engagement processes and research could then be used to develop a new paradigm of risk and its acceptability.

### 2.2 Prudence, Uncertainty and the Precautionary Principle

A prudent citizen or public official will always give careful consideration to potential adverse outcomes of a proposed action. If the proposed action is the construction and operation of a nuclear power plant, two potential adverse outcomes will be particularly salient. One potential outcome, as mentioned above, would be a large, unplanned release of radioactive material from the plant to the environment. The second potential outcome would be the diversion of fissile or radioactive material from the plant by a national government or a sub-national group, for use in a nuclear or radiological weapon. The organizations that construct, operate and regulate nuclear power plants will implement measures intended to prevent these outcomes. Nevertheless, a prudent observer will consider the possibility that the preventive measures will fail. In view of the severe, adverse impacts that would be associated with these outcomes, it would be imprudent to ignore the possibility of their occurrence.

*Assessing the potential for an unplanned release*

The potential for a large, unplanned release of radioactive material is typically regarded by the nuclear industry and its regulators as a "safety" issue. An analytic art, known as probabilistic risk assessment (PRA), has been developed to estimate the probabilities and consequences of potential releases. The first PRA for a nuclear power plant was known as the Reactor Safety Study, and was published by the US Nuclear Regulatory Commission (NRC) in 1975.[34] A PRA for a nuclear power plant considers a range of scenarios (event sequences) that involve damage to the reactor core. The initiating events are categorized as "internal" events (human error, equipment failure, etc.) or "external" events (earthquakes, fires, strong winds, etc.). The core-damage scenarios that arise from these events are termed "accidents". PRAs typically do not consider initiating events that involve intentional, malevolent acts, although PRA techniques can be adapted to estimate

[33] There is evidence that the consequences of the 1986 Chernobyl reactor accident exceeded thresholds that brought new social and political phenomena into play. Many observers conclude that the accident undermined the legitimacy of the USSR government, contributing significantly to the breakup of the USSR. See, for example: Parsons, 2006.
[34] NRC, 1975.

the outcomes of such acts. The NRC adapted PRA techniques in developing its 1994 rule requiring protection of a nuclear power plant against attack using a vehicle bomb.[35]

A modern nuclear power plant has safety features – reactor shut-down systems, core cooling systems, etc. – with independent, redundant and diverse components. A core-damage accident at such a plant would typically involve a combination of independent failures that coincide, thereby overcoming the plant's safety features.[36] By contrast, during an intentional attack on a nuclear power plant, the plant's safety features would be challenged by a common factor – the attackers' intellectual and practical capabilities. Attackers with the motivation and resources to mount a significant attack would be likely to plan the attack with the specific intention of overcoming the plant's safety features and causing a large radioactive release.

Attacks on buildings in New York and Washington in September 2001 demonstrated that an attack on a civilian facility by a skilled, highly-motivated and well-resourced sub-national group is a credible event. Many observers agree that a nuclear power plant is a potential target of a future attack of this kind. Faced with this threat, risk analysts, regulatory bodies and plant designers must modify their approach. The traditional safety paradigm is insufficient. To understand the threat, risk analysts must think like skilled attackers. Regulatory bodies must capture those insights in appropriate rules and guidance documents. Resistance to attack must become an explicit objective in the design of a nuclear power plant.

A large, unplanned release of radioactive material from a nuclear power plant would be a comparatively rare event. Any estimate of the probability of such an event will be highly uncertain.[37] Many PRAs for nuclear power plants have been performed, and the results are useful for various purposes. However, PRA estimates of the probabilities of accidental releases should not be regarded as definitive, scientific findings. Those estimates rely on numerous assumptions and judgments. There is no certainty that all of the relevant factors are captured by a PRA. The findings cannot be validated by direct statistical evidence.[38]

At present, there is no statistical basis for a quantitative estimate of the probability of a large release caused by an intentional, malevolent act. It does not follow, as some have suggested, that malevolent acts should be ignored in risk analysis for nuclear power plants. In a policy or planning context, risk analysts could use judgment to assign minimum probabilities to postulated acts. That judgment could be combined with technical assessments of the vulnerability of plants to the postulated acts. Those

---

[35] NRC, 1994.
[36] In some core-damage accidents, a common cause – such as a powerful earthquake – would simultaneously overcome a number of safety features.
[37] Hirsch et al, 1989.
[38] There have been two core-damage accidents involving unplanned releases of radioactive material from commercial nuclear power plants. Those accidents occurred at Three Mile Island in 1979 (involving a small release) and Chernobyl in 1986 (involving a large release).

assessments would rely, in part, on PRA techniques. For nuclear power plants now operating in the USA, it is reasonable to assume that the probability of a large, radioactive release arising from a deliberate attack during the next few decades is at least 1 per 10,000 plant-years.[39]

*Assessing the potential for a diversion of material*

A second potential adverse outcome of operating a nuclear power plant, as mentioned above, is a diversion of fissile or radioactive material from the plant, for use in a nuclear or radiological weapon. That possibility is typically regarded by the nuclear industry and its regulators as a "safeguards" issue. Canada and many other countries have safeguards agreements with the International Atomic Energy Agency (IAEA). The purposes of these agreements include the prevention of diversion of fresh or spent fuel from nuclear power plants. If such diversion is successfully prevented, the fissile and radioactive material in the fuel will remain protected.

In the context of plant design, it is important to note that spent fuel could be diverted from some types of nuclear power plant with comparatively little technical effort. At such plants, prevention of diversion must rely primarily on administrative measures. CANDU plants, which employ on-line refueling, are in this category.[40]

A national government might, at some future date, break its safeguards agreement with the IAEA and extract fissile or radioactive material from the fresh or spent fuel of nuclear power plants under its control. Alternatively, a sub-national group might gain control of a quantity of fresh or spent fuel, and then extract fissile or radioactive material from that fuel. Either step could be the precursor to threatened or actual use of a nuclear or radiological weapon, which would be a severe, adverse outcome of the operation of nuclear power plants. There is no statistical basis for a quantitative estimate of the probability of that outcome. Nevertheless, a qualitative estimate of that probability is an inevitable component of an assessment of the sustainability of nuclear power. To ignore the issue would be to assume that the probability is zero.

*The precautionary principle*

The preceding discussion addresses two potential adverse outcomes of constructing a nuclear power plant – an unplanned release of radioactive material, and a diversion of fissile or radioactive material. The probability of either outcome is highly uncertain. Yet, either outcome would be significant from the perspective of the sustainability of nuclear power. In a policy or planning context, citizens and policy makers must grapple with this conjunction of uncertainty and significance. The precautionary principle offers guidance in such situations. This principle has been much discussed, and is incorporated in laws and regulations in Canada and elsewhere. It is mentioned in CEAA's draft

[39] Thompson, 2007.
[40] Fischer and Szasz, 1985.

guidelines as one of the principles that should guide an EIS.[41] To date, however, the precautionary principle lacks an internationally-agreed definition and framework for implementation.

In the Canadian Environmental Assessment Act of 1992, the concept of precaution appears twice in the Purposes section.[42] First, at 4 (1) (a), the Act states that one of its purposes is "to ensure that projects are considered in a careful and precautionary manner before federal authorities take action with them, in order to ensure that such projects do not cause significant adverse environmental effects". Then, at 4 (2), the Act states that federal government entities shall, in administering the Act, "exercise their powers in a manner that protects the environment and human health and applies the precautionary principle".

The Act further states, at 4 (1) (b), that one of its purposes is "to encourage responsible authorities to take actions that promote sustainable development and thereby achieve or maintain a healthy environment and a healthy economy". Thus, the Act seeks to promote principles of sustainability and of precaution. That general commitment has been applied to specific cases by panels convened under the Act.[43]

In April 2007, the Canadian government issued the Cabinet Directive on Streamlining Regulation.[44] That directive sets forth six objectives for regulation by the federal government. The third of those objectives states that the government will:

> "Make decisions based on evidence and the best available knowledge and science in Canada and worldwide, while recognizing that the application of precaution may be necessary when there is an absence of full scientific certainty and a risk of serious or irreversible harm".

One application of that objective would be to anthropogenic climate change. In that instance, the harm would be serious and irreversible if no action were taken to reduce emissions of greenhouse gases. Yet, there might not be full scientific certainty about the extent to which emissions should be reduced. The above-stated objective would call for early action, without waiting for full scientific certainty.

In the context of this report, serious and irreversible harm could arise from the taking of an action. The action would be the construction and operation of a nuclear power plant, if the design of the plant created a significant potential for an unplanned release of radioactive material, or for diversion of fissile or radioactive material. In this instance, the above-stated objective would favor the blocking of the plant's construction, even though the potential for harm could not be characterized with full scientific certainty as to consequences and probability.

---

[41] CEAA, 2008, Section 2.5.
[42] Justice Department, 2007.
[43] Gibson, 2000.
[44] Government of Canada, 2007.

## 2.3 Efforts to Address Sustainability Issues in Designs for New Nuclear Power Plants

During the past four decades, there have been various efforts to address sustainability issues while developing designs for new nuclear power plants. Some of those efforts are summarized here. Persons involved in those efforts have adopted the language of sustainability only in the past decade. A conceptual progression over time is evident, but that progression has not yet arrived at designs that reflect a comprehensive framework of sustainability principles. Moreover, the design concepts discussed here are almost entirely theoretical. The present fleet of nuclear power plants, and the Generation III plants that are currently being offered, do not employ these concepts to any significant extent.

### *Underground siting*

In the 1970s, there were several studies on constructing nuclear power plants underground. Those studies are exemplified by a report published in 1972 under the auspices of the California Institute of Technology (Caltech).[45] The report identified a number of advantages of underground siting. Those advantages included highly-effective confinement of radioactive material in the event of a core-damage accident, isolation from falling objects such as aircraft, and protection against malevolent acts. Based on experience with underground testing of nuclear weapons, the report concluded that an appropriately designed plant would provide essentially complete containment of the radioactive material liberated from a reactor core during a core-damage event.

The Caltech report described a preliminary design study for underground construction of a light-water-reactor power plant with a capacity of 1,000 MWe. The minimum depth of the underground cavities containing the plant components would be 150 to 200 feet. The estimated cost penalty for underground siting would be less than 10 percent of the total plant cost.

In an appendix, the Caltech report described four underground nuclear reactors that had been constructed and operated in Europe. Three of those reactors supplied steam to turbo-generators, above or below ground. The largest of those reactors and its above-ground turbo-generator made up the Chooz plant in France, which had a capacity of 270 MWe. In describing the European reactors, the report noted:[46]

> "The motivation for undergrounding the plant appears to be insurance of containment of accidentally released radioactivity and also physical protection from damage due to hostile military action."

---

[45] Watson et al, 1972.
[46] Watson et al, 1972, Appendix I.

Since the 1970s, underground siting of nuclear power plants has been considered by various groups. For example, in 2002 a workshop was held under the auspices of the University of Illinois to discuss a proposed US-wide "supergrid". That grid would transmit electricity – via superconducting DC cables – and liquid hydrogen, which would provide cooling to the DC cables and be distributed as fuel. Much of the energy fed to the grid would be supplied by nuclear power plants, which could be constructed underground. Motives for placing those plants underground would include "reduced vulnerability to attack by nature, man or weather" and "real and perceived reduced public exposure to real or hypothetical accidents".[47]

*The PIUS reactor*

In the 1980s the reactor vendor ASEA-Atom developed a preliminary design for an "intrinsically safe" commercial reactor known as the Process Inherent Ultimate Safety (PIUS) reactor. An ASEA-Atom official described the company's motives for developing the reactor as follows:[48]

> "The basic designs of today's light water reactors evolved during the 1950s when there was much less emphasis on safety. Those basic designs held certain risks, and the control of those risks led to an increasing proliferation of add-on systems and equipment ending up in the present complex plant designs, the safety of which is nevertheless being questioned. Rather than to continue into this 'blind alley', it is now time to design a truly 'forgiving' light water reactor in which ultimate safety is embodied in the primary heat extraction process itself rather than achieved by add-on systems that have to be activated in emergencies. With such a design, system safety would be completely independent of operator actions and immune to malicious human intervention."

The central goal of the PIUS design was to preserve fuel integrity "under all conceivable conditions". That goal translated to a design specification of "complete protection against core melting or overheating in case of:

- any credible equipment failures;
- natural events, such as earthquakes and tornadoes;
- reasonably credible operator mistakes; and
- combinations of the above;

and against:

- inside sabotage by plant personnel, completely knowledgeable of reactor design (this can be considered an envelope covering all possible mistakes);
- terrorist attacks in collaboration with insiders;

[47] Overbye et al, 2002.
[48] Hannerz, 1983, pp 1-2.

- military attack (e.g., by aircraft with 'off-the-shelf' non-nuclear weapons); and
- abandonment of the plant by the operating personnel".[49]

To meet those requirements, ASEA-Atom designed a light-water reactor – the PIUS reactor – with novel features. The reactor pressure vessel would contain sufficient water to cool the core for at least one week after reactor shut-down. Most of that water would contain dissolved boron, so that its entry into the core would inherently shut down the reactor. The borated water would not enter the core during normal operation, but would enter through inherent mechanisms during off-normal conditions. The reactor pressure vessel would be made of pre-stressed concrete with a thickness of 25 feet. That vessel could withstand an attack using 1,000-pound bombs. About two-thirds of the vessel would be below ground.

ASEA-Atom estimated that the construction cost of a four-unit PIUS station with a total capacity of 2,000 MWe would be about the same as the cost of a station equipped with two 1,000 MWe "conventional" light-water reactors. The PIUS station could be constructed more rapidly, which would offset its slightly lower thermal efficiency. Thus, the total generating cost would be about the same for the two stations. ASEA-Atom estimated (in 1983) that the first commercial PIUS plant could enter service in the early 1990s, if a market existed.[50] To date, no PIUS plant has been ordered.

### *PRIME reactors*

In 1991, a study conducted at Oak Ridge National Laboratory examined various types of commercial nuclear reactor that were under development at the time.[51] Some types of reactor represented a comparatively small evolutionary step from existing reactors. Their safety systems tended to be simpler, and to rely more on passive mechanisms, than the safety systems of existing reactors. Other types of reactor were said to have PRIME characteristics. That acronym applied to designs with the features:

- Passive safety systems;
- Resilient safety systems;
- Inherent safety characteristics (no need for safety systems);
- Malevolence resistance; and
- Extended safety (remaining in a safe state for an extended period after an accident or attack).

The Oak Ridge study identified several types of reactor as being in the PRIME category. Those reactors, which were in various stages of development, were: the PIUS reactor; the ISER reactor being developed in Japan; the Advanced CANDU Project; modular, high-temperature, gas-cooled reactors being developed in the USA and Germany; and a molten-salt reactor being developed jointly by the USSR and the USA. The Oak Ridge

[49] Hannerz, 1983, page 3.
[50] Hannerz, 1983, pp 73-76.
[51] Forsberg and Reich, 1991.

study did not set forth a framework of indicators and criteria that could be used to assess the comparative merits of those reactors, or to determine if a reactor belonged in the PRIME category.

*Generation IV reactors and fuel cycles*

During the past decade, proponents of a nuclear power renaissance have begun to use the language of sustainability, especially in connection with proposed Generation IV reactors and fuel cycles. Those proponents argue that use of fast-spectrum reactors and closed fuel cycles could extend the life of uranium reserves, allow the use of thorium as a fuel, and reduce the amount of radioactive waste that would be sent for disposal. The reactors could have passive-safety features and be refueled at long intervals by removing and replacing a "cassette" of fuel, thus avoiding onsite access to fuel. Fission heat could be used to produce electricity, hydrogen, process heat, and/or potable water.[52]

As stated in Section 1, above, the proposed Generation IV reactors would push against engineering limits in a variety of respects. Linking those reactors to a closed fuel cycle would add another level of technical difficulty. Costs are almost impossible to predict. The overall strategy assumes major technological advance across several fronts, an implementation plan that unfolds over a century or longer, strong centralized control by national governments and supra-national entities, and public acceptability of those actions. The feasibility of that strategy, and its contribution to sustainability, are highly questionable. Nevertheless, the European Commission's Directorate-General for Research offers that strategy as a long-term, sustainable future for nuclear power. Generation IV systems would be developed over the next several decades. During that period, Generation III reactors would be constructed as an interim source of electricity. The Directorate-General concedes that the Generation III reactors would not meet sustainability criteria.[53]

### 2.4 A Broader View of Sustainability

Since WCED introduced the concept of sustainable development in 1987, research and practical experience have led to a deeper understanding of the imperatives and principles of sustainability. It is now recognized that sustainability involves a range of considerations, including the flexibility and resilience of engineered, natural, and social systems.[54] The precautionary principle has become part of the sustainability paradigm.

Engineers who seek to implement the sustainability paradigm in practical situations typically view the pursuit of sustainability as a multi-objective optimization problem.[55] To address such a problem, analysts must identify system boundaries, seek an understanding of the dynamic behaviors and interactions of the relevant systems,

[52] See, for example: Wade, 2000.
[53] European Commission, 2007.
[54] Homer-Dixon, 2007.
[55] Sahely et al, 2005.

articulate a framework of indicators and criteria, and apply a process of optimization. Nuclear power has not yet been subjected to such an analysis. A group at the University of Manchester, as discussed in Section 1, above, recently began that task. According to their funding agency, "it is far from clear how sustainable the nuclear option is overall, compared to other generating options".[56]

## 3. Accidents, Malfunctions, Malevolent Acts and the Potential for Disaster

### 3.1 CEAA Classification of Accidents and Malfunctions

CEAA's draft guidelines provide a brief introduction to accidents and malfunctions in Section 8.6, and a more detailed discussion in Section 12. Section 8.6 states that information on accidents and malfunctions should be provided in a separate section of the EIS. Our discussion here focuses on Section 12, which identifies three categories of accidents and malfunctions, as follows:[57]

> "• *Nuclear accidents*, directly involving the nuclear reactor such as serious damage to the reactor core;
> • *Conventional accidents*, consisting of all other accidents and malfunctions resulting in chemical or radiological releases. Radiological releases are those that are not directly involved the reactor core and may include nuclear accidents such as out of reactor criticality events associated with nuclear fuel.
> • *Malevolent acts*, consisting of those physical initiating events or forces (e.g., fires, explosions, punctures, aircraft crashes) that could result from potential sabotage or terrorist scenarios."

In discussing *nuclear accidents*, CEAA's draft guidelines state that the proponent must demonstrate that a proposed nuclear power plant meets the safety goals articulated by the Canadian Nuclear Safety Commission (CNSC) in its October 2007 draft document, *Design of New Nuclear Power Plants, RD-337*.[58] Those goals are set forth in Table 3-1 of this report, and are discussed further in Section 4.2, below. As mentioned in the notes to Table 3-1, the CNSC Staff is currently proposing a weakening of the safety goals. CEAA's draft guidelines state that a credible demonstration by the proponent that the CNSC safety goals are met must involve provision of a "high-level safety analysis" that includes a "system level probabilistic safety assessment".

In discussing *conventional accidents*, CEAA's draft guidelines specifically mention criticality events outside the reactor core, but also allow for a range of events leading to chemical or radiological releases.

In discussing *malevolent acts*, CEAA's draft guidelines state that the proponent must compare the environmental effects resulting from malevolent acts with the effects of

---

[56] EPSRC, 2007.
[57] CEAA, 2008, Section 12. The quoted passage is clearly in need of copy-editing.
[58] CNSC, 2007a.

nuclear accidents and conventional accidents. The draft guidelines do not provide any guidance about characterizing malevolent acts by probability, severity, credibility or other indicators. As the guidelines now stand, it appears that the proponent is free to choose any set of malevolent acts for the purpose of preparing an EIS.

### 3.2 The Potential for Accidents at Nuclear Power Plants

For the purposes of this report, an accident at a nuclear power plant is defined as an unplanned release of hazardous material to the environment, when the release is not attributable to an intentional, malevolent act. The release could be to the atmosphere, and/or to ground or surface water. The released material would be hazardous to living entities because of its radiological and/or chemical properties.

Atmospheric releases deserve special attention because a plume of hazardous material could travel downwind for tens or hundreds of km, affecting large areas. Releases of radioactive material also deserve special attention, because operating nuclear power plants contain very large amounts of such material. Thus, atmospheric, radioactive releases are particularly significant from the perspective of environmental assessment.[59] Within that category of releases, two types of release are dominant in terms of the potential scale of environmental impacts. One type of release is from a reactor core, and the other is from stored spent fuel. The potential scale of a release from spent fuel is not universally understood, and is not recognized in CEAA's draft guidelines.

*The role of PRA*

There is a large body of technical literature addressing the potential for, and consequences of, an atmospheric release of radioactive material following accidental damage to a reactor core. This literature typically falls under the rubric of probabilistic risk assessment, as mentioned in Section 2.2, above. In the PRA field, the events that initiate an accidental release are categorized as "internal" events (human error, equipment failure, etc.) or "external" events (earthquakes, fires, strong winds, etc.). PRAs typically do not consider initiating events that involve intentional, malevolent acts, although PRA techniques can be adapted to estimate the outcomes of such acts.

PRAs for nuclear power plants are conducted at Levels 1, 2 and 3, in increasing order of completeness, as discussed below. A thorough, full-scope PRA would be conducted at Level 3, and would consider internal and external initiating events. The findings of such a PRA would be expressed in terms of the magnitudes and probabilities of a set of adverse environmental impacts, and the uncertainty and variability of those indicators. The adverse impacts would include:

---

[59] Radioactive material released to the atmosphere from a nuclear power plant would travel downwind in a plume of gases and small particles. The particles would settle on the ground and other surfaces at downwind locations, and would then be re-distributed by rain, wind, etc. Humans could be irradiated through various pathways including inhalation, external exposure, and ingestion of contaminated food and water.

(i) "early" human fatalities or morbidities (illnesses) that arise during the first several weeks after the release;
(ii) "latent" fatalities or morbidities (e.g., cancers) that arise years after the release;
(iii) short- or long-term abandonment of land, buildings, etc.;
(iv) short- or long-term interruption of agriculture, water supplies, etc.; and
(v) social and economic impacts of the above-listed consequences.

The magnitudes and probabilities of such adverse impacts would be estimated in three steps. First, a Level 1 PRA analysis would be performed. In that analysis, a set of event sequences (accident scenarios) leading to damage to the reactor core would be identified, and the probability (frequency) of each member of the set would be estimated. The sum of those probabilities across the set would be the total estimated core-damage probability. Second, a Level 2 PRA analysis would be performed. In that analysis, the potential for release of radioactive material to the atmosphere would be examined across the set of core-damage sequences. The findings would be expressed in terms of a group of release categories characterized by magnitude, probability, timing, isotopic composition, and other characteristics.

Third, a Level 3 PRA analysis would be performed, to yield the findings described above. In that analysis, the atmospheric dispersion, deposition and subsequent movement of the released radioactive material would be modeled for each of the release groups determined by the Level 2 analysis. The dispersion modeling would account for meteorological variation over the course of a year. Then, the adverse environmental impacts of the released material would be estimated, accounting for the material's distribution in the biosphere.

If done thoroughly, this 3-step estimation process accounts for uncertainty and variability at each stage of the process. A thorough, full-scope, Level 3 PRA is expensive and time-consuming. It yields estimated impacts expressed as statistical distributions of magnitude and probability, not as single numbers. Even after such a thorough effort, there are substantial, irreducible uncertainties in the findings.[60]

*The radioactive inventory available for release*

The core of a nuclear reactor consists of a set of fuel assemblies, together with cooling channels, support structures, etc. After a period of use, fuel assemblies become "spent", and are removed from the reactor and placed in storage. Active or spent fuel assemblies contain a variety of radioactive isotopes.[61] One isotope, namely cesium-137, is

[60] Hirsch et al, 1989.
[61] In an operating reactor, an active fuel assembly contains radioactive isotopes with half-lives ranging from seconds to millennia. After the reactor is shut down or a fuel assembly becomes spent (i.e., it is discharged from the reactor), the assembly's inventory of each isotope declines at a rate determined by the isotope's half-life. Thus, an atmospheric release from an operating reactor would contain short- and longer-lived

especially useful as an indicator of the potential for radiological harm. Cesium-137 is a radioactive isotope with a half-life of 30 years. This isotope accounts for most of the offsite radiation exposure that is attributable to the 1986 Chernobyl reactor accident, and for about half of the radiation exposure that is attributable to fallout from the testing of nuclear weapons in the atmosphere.[62] Cesium is a volatile element that would be liberally released during accidents or attack scenarios that involve overheating of nuclear fuel.

To illustrate the inventories of cesium-137 associated with a nuclear power plant, consider the Indian Point 2 (IP2) and Indian Point 3 (IP3) plants now operating in New York state. These are Westinghouse PWR plants. Each plant has a generating capacity of 1,080 MWe. Spent fuel discharged from each reactor is stored under water in a pool adjacent to, but outside, the reactor's containment. Each pool now contains an amount of spent fuel that is approaching the pool's storage capacity. Accordingly, an independent spent fuel storage installation (ISFSI) is being built on the site, to provide additional storage capacity. At the ISFSI, spent fuel will be stored dry, inside helium-filled storage modules that stand on a concrete pad in the open air.

The reactor cores of the IP2 and IP3 plants each contain about 420,000 TBq of cesium-137. When fully used, a condition that will be attained within the next several years, the spent-fuel pools at these plants will each contain about 2,500,000 TBq of cesium-137. One of the storage modules at the ISFSI will hold about 48,000 TBq of cesium-137. For comparison with these quantities, note that the 1986 Chernobyl reactor accident released to the atmosphere about 90,000 TBq of cesium-137. Also, atmospheric testing of nuclear weapons, mostly in the 1950s and 1960s, released about 740,000 TBq of cesium-137.[63] Detonation of a 10-kilotonne-yield fission weapon would release about 70 TBq of cesium-137.[64] Clearly, the release of a substantial fraction of the cesium-137 inventory at the IP2 or IP3 plant would create comparatively large radiological consequences.

*Probabilities of core-damage accidents and radioactive releases*

As mentioned above, a PRA conducted at Level 1 estimates the probability of damage to the core of a reactor. Significant damage to the core is a necessary precursor to a large release of radioactive material from the reactor to the environment. PRAs vary widely in their estimates of the probability of core damage. This variation can reflect genuine differences between nuclear power plants, or differences in analytic approaches and assumptions. To illustrate, the US Nuclear Regulatory Commission (NRC) conducted a

---

isotopes, while a release from a spent-fuel-storage facility would contain only longer-lived isotopes. That difference has implications for the environmental impacts of a release, and for the emergency response that would be appropriate.

[62] DOE, 1987.

[63] The fallout from atmospheric testing of nuclear weapons was widely distributed across the planet, mostly in the Northern hemisphere. By contrast, an atmospheric release from a nuclear power plant would typically create a concentrated plume that would travel downwind at a comparatively low altitude.

[64] Thompson, 2007, Table 2-2.

major study that examined the accident potentials of five nuclear power plants, each of a differing design. The median estimates of core-damage probability varied across a range of more than two orders of magnitude, considering only internal initiating events.[65] In that instance, the variation reflected genuine differences between plants.

Another aspect of a PRA is the estimation of the conditional probability of a specified release of radioactive material, given the occurrence of core damage.[66] The above-mentioned NRC study found wide variation of this conditional probability across the five plants that were examined.[67] Other PRAs show similar variation.

Despite years of experience with PRA, there is continuing uncertainty and controversy about PRA findings. That situation is not surprising, given the complexity of PRA analysis and the lack of direct empirical data to validate much of that analysis. In illustration, consider the findings of PRAs recently conducted for the IP2 and IP3 plants by their owner, Entergy.

Entergy estimates the probability of core damage, accounting for internal and external events and uncertainty, at 1.4 per 10,000 reactor-years for the IP2 plant and 0.9 per 10,000 reactor-years for the IP3 plant. Entergy further estimates that the conditional probability of an Early High release of radioactive material is 4 percent for the IP2 plant and 8 percent for the IP3 plant.[68] The difference between these numbers is interesting, because the plants are almost identical. It is also interesting to note that neither plant could meet the CNSC safety goals set forth in Table 3-1, according to Entergy's findings.[69]

This author has examined the implications for Entergy's PRA findings of a recent NRC-sponsored study on the vulnerability of steam generator tubes during a certain type of core-damage scenario.[70] All other aspects of the two PRAs were held constant. This single change raised the conditional probability of an Early High release to 52 percent for the IP2 plant and 54 percent for the IP3 plant.[71] The author's analysis has been submitted to NRC in the context of a proceeding about license extensions for the IP2 and IP3 plants.

---

[65] NRC, 1990, Figure 8.1.
[66] Combining core-damage probabilities and conditional probabilities of specified releases yields a group of potential release categories characterized by magnitude, probability, and other indicators. Development of those release categories completes the Level 2 step of a PRA.
[67] NRC, 1990, Section 9.
[68] Thompson, 2007, Tables 4-1, 5-3 and 5-4.
[69] According to Entergy, the probability of an Early High release is 6 per 1 million reactor-years for the IP2 plant, and 7 per 1 million reactor-years for the IP3 plant. The CNSC draft safety goals in Table 3-1 state that the probability of a Large Release must be less than 1 per 1 million reactor-years, and should be less than 0.1 per 1 million reactor-years.
[70] The relevant core-damage scenario is one in which, during a significant period of the scenario, the primary and secondary sides of the steam generator are dry, and the primary side is at high pressure.
[71] Thompson, 2007, Tables 5-3 and 5-4.

*Credibility of Bruce Power's approach*

As mentioned in Section 1, above, Bruce Power's proposed approach to assessing the potential for accidents and malfunctions, in the context of the EIS, is to ignore differences between plant designs. The preceding paragraphs show, however, that PRA findings vary significantly among plant designs.[72] Also, Bruce Power proposes to submit some kind of bounding analysis that is "technology neutral". Such an analysis could not approach the quality and credibility of a thorough PRA. Moreover, the findings of even the most thorough PRAs are uncertain and controversial.[73] Thus, Bruce Power's proposed approach could not yield a credible assessment of the potential for accidents and malfunctions.

*Accidents affecting stored spent fuel*

At nuclear power plants in the USA and elsewhere, large amounts of spent fuel are stored under water in pools adjacent to reactors. Those pools currently employ high-density racks, to maximize the amount of spent fuel that can be stored in each pool. This practice has been adopted because it is the cheapest mode of storage of spent fuel. Unfortunately, the high-density configuration would suppress convective cooling of fuel assemblies if water were lost from a pool.

Several reputable studies have agreed that loss of water from a pool would, across a range of water-loss scenarios, lead to spontaneous ignition of the zirconium alloy cladding of the most recently discharged fuel assemblies. The resulting fire would spread to adjacent fuel assemblies and propagate across the pool. Extinguishing the fire, once it had been initiated, would be difficult or impossible. Spraying water on the fire would feed an exothermic reaction between steam and zirconium. The fire would release a large amount of radioactive material to the atmosphere, including tens of percent of the pool's inventory of cesium-137. Large areas of land downwind of the plant would be rendered unusable for decades. Loss of water could arise in various ways as a result of an accident or an intentional, malevolent act.[74]

Measures are available for dramatically reducing the risk of a fire in a spent-fuel pool. Notably, pools could be re-equipped with low-density racks, as was intended when the plants were constructed. Table 3-2 summarizes the characteristics of this option and other options for risk reduction.

---

[72] An interesting difference among the three plant designs that are being considered for use in Ontario is that the fuel in the EPR and the AP1000 would be driven to a burnup about three times higher than in the ACR-1000. The core inventory of cesium-137, per GWt of capacity, would vary in rough proportion to the maximum burnup.
[73] Hirsch et al, 1989.
[74] Alvarez et al, 2003; National Research Council, 2006; Thompson, 2007.

This author is not aware of any study on the potential for an accidental release of radioactive material from spent fuel stored at a nuclear power plant employing a CANDU reactor. Absent such a study, the potential remains unknown.

*Releases from other parts of a nuclear power plant*

The preceding discussion in Section 3.2 has addressed the potential for accidental, atmospheric release of radioactive material from a reactor core or from stored spent fuel. Other parts of a nuclear power plant contain radioactive or hazardous chemical material. The potential for release of some of that material should be examined in an EIS. The environmental impacts of such releases would, however, be much smaller than the impacts that could arise from a release from a reactor core or spent fuel.

*Scale of environmental impacts*

The IP2 and IP3 plants are typical members of the world's fleet of nuclear power plants. As discussed above, the core of each of the IP2 and IP3 plants contains about 420,000 TBq of cesium-137. Numerous studies show that an accident could release tens of percent of the core's inventory of cesium-137. Also, each of the spent-fuel pools at these plants has a cesium-137 inventory approaching 2,500,000 TBq. Studies show that accidental loss of water could lead to a fire that releases tens of percent of a pool's inventory of cesium-137. Thus, an environmental assessment for these plants must consider the potential for an atmospheric release containing hundreds of thousands of TBq of cesium-137.[75]

CNSC's draft safety goals for new nuclear power plants, as set forth in Table 3-1, address the probability of a Large Release. According to CNSC, the probability of such a release must not exceed 1 per 1 million reactor-years (plant-years), and should not exceed 0.1 per 1 million reactor-years. A Large Release is defined by CNSC as a release exceeding 100 TBq of cesium-137.

CNSC's Large Release is a tiny fraction of the release that is known to be credible for nuclear power plants now operating. The Large Release is also a tiny fraction of the release (90,000 TBq of cesium-137) that occurred at Chernobyl in 1986. Thus, CNSC's draft safety goals do not provide useful guidance for the preparation of an EIS.

Estimating the magnitudes of potential releases of radioactive material is a necessary step toward assessing the environmental impacts of those releases. Computer models are

[75] Existing CANDU plants in Ontario have the potential to release large amounts of radioactive material to the atmosphere. For example, a study involving this author modeled the impacts of a release from the Darlington station that included 70,000 TBq of cesium-137. The estimated lifetime population dose, as a weighted average across the most common weather conditions, would be 2.7 million person-Sv. For comparison, the 1986 Chernobyl accident led to an estimated lifetime population dose of 0.6 to 1.2 million person-Sv, about half of which will be accrued within the former USSR. See: IRSS, 1992, Volume 2, Annex III.

available for assessing the impacts of potential releases. An EIS should provide findings from such models across the full range of releases.

Estimation of economic and social impacts involves the prediction of human behavior and the assigning of monetary values to human preferences. The findings are typically sensitive to the assumptions that are made. For example, a study sponsored by Defence Research and Development Canada estimated the economic impact of an open-air explosion of a radiological dispersal device (dirty bomb) at the CN Tower in Toronto.[76] The assumed release consisted of 37 TBq of cesium-137. The estimated economic impact varied considerably, according to the cleanup standard that was assumed in the analysis. That standard was expressed in terms of the radiation dose rate that would remain after completion of the cleanup. For a cleanup standard of 500 mrem per year, the estimated economic impact would be $28 billion, whereas for a cleanup standard of 15 mrem per year the impact would be $250 billion. The magnitudes of these impacts are interesting, considering that the assumed release (37 TBq of cesium-137) is a tiny fraction of the release that could occur from a nuclear power plant (hundreds of thousands of TBq of cesium-137).

An EIS for a nuclear facility should fully inform the public about the risks posed by that facility. In assessing economic and social impacts, the EIS should not make arbitrary assumptions about parameters, such as cleanup standards, that significantly influence the findings. Instead, the EIS should show how the findings vary across a range of assumptions.

*Cumulative impacts across the site*

At the Bruce site, new nuclear power plants would be added to a site where plants are already operating. An EIS should consider the cumulative impacts of all the hazardous facilities on the site, including nuclear power plants and facilities for storing spent fuel and other radioactive wastes. In the context of accidents and malfunctions, it would be especially important to consider the cumulative outcomes of events – such as an earthquake – that could affect more than one facility.

### 3.3 The Potential for Malevolent Acts at Nuclear Power Plants

As discussed in Section 2.3, above, during the past four decades there have been studies about designing nuclear power plants to resist intentional, malevolent acts. ASEA-Atom devoted considerable effort to developing the PIUS design, whose specifications included an ability to resist malevolent acts. Yet, commercial nuclear power plants now operating around the world are not specifically designed to resist malevolent acts. They have some capability to resist such acts as a byproduct of other design objectives (e.g., riding out a specified earthquake). Also, plants are currently protected by guard forces, gates, etc., to

[76] Cousins and Reichmuth, 2007.

differing extents in different countries. Nevertheless, the present plants are vulnerable to a variety of credible attacks, as discussed below.

The vulnerability of the present fleet of nuclear power plants does not reflect a lack of design options. Nuclear engineers have always been able to design plants that are much more robust. In illustration, nuclear reactors used for naval propulsion are designed to ride out battle shock. The commercial nuclear industry and its regulators have chosen to not include resistance to attack as one of their design objectives.

CNSC's draft criteria for the design of new nuclear power plants, expressed in the document RD-337, include resistance to attack as a design objective. The approach that CNSC has taken to this issue is discussed further in Section 4.2, below. As noted above, CEAA's draft guidelines for the Bruce Power EIS require the consideration of accidents and malfunctions that include malevolent acts. CNSC and CEAA deserve commendation for addressing the potential for malevolent acts. In both instances, however, there is need for improvement in the agency's approach.

*Potential modes and instruments of attack on nuclear power plants*

A consultant to CNSC has examined potential modes and instruments of attack on a nuclear power plant, and has recommended an approach to incorporating these threats in the design criteria for new plants. The consultant's recommendations are discussed further in Section 4.2, below. Among the instruments of attack considered by the consultant were a large commercial aircraft, an explosive-laden smaller aircraft, and an explosive-laden land vehicle.

Table 3-3 describes some potential modes and instruments of attack on a nuclear power plant, and also describes the defenses that are now provided at US plants. There is no defense against a range of credible attacks. Among the instruments of attack mentioned in Table 3-3 is a large commercial aircraft. In September 2001, aircraft of this type caused major damage to the World Trade Center and the Pentagon. However, such an aircraft would not be optimal as an instrument of attack on a nuclear power plant. Large commercial aircraft are comparatively soft objects containing a few hard structures such as turbine shafts. They can be difficult to guide precisely at low speed and altitude. A well-informed group of attackers would probably prefer to use a smaller, general-aviation aircraft laden with explosive material, perhaps in a tandem configuration in which the first stage is a shaped charge. Table 3-4 provides some information about shaped charges and their capabilities.

*Probability of a successful attack*

There is no statistical basis for a quantitative estimate of the probability that a nuclear power plant will be attacked. However, if a given attack scenario is postulated, one can apply PRA techniques to estimate the conditional probabilities of various outcomes. As

mentioned in Section 2.2, above, NRC took that approach in developing its vehicle-bomb rule of 1994.

This author is not aware of any systematic application of PRA techniques to assess the vulnerability of a nuclear power plant to a range of postulated attacks. If such analysis were performed, parts of the analysis would not be appropriate for publication. This author has conducted a preliminary examination of the vulnerability of the IP2 and IP3 plants to attack. That examination showed that a group of sophisticated, determined attackers would have a range of opportunities to cause a large, atmospheric release of radioactive material from a reactor core and/or a spent-fuel pool.[77] In other words, the conditional probability of such a release would be high.

That finding can be combined with a qualitative assessment of the probability that an attack will be mounted. For some policy purposes, it may be useful to assign a numerical value, based on informed judgment, to the probability of an attack or an attack-induced release. In that context, this author has argued that it is reasonable to assume that the probability of a large, radioactive release arising from a deliberate attack on a US nuclear power plant during the next few decades is at least 1 per 10,000 plant-years.[78] The same number could reasonably be used for a Canadian plant.

*Magnitude of an attack-induced release*

A hostile group might attack a nuclear power plant with the objective of rendering the plant inoperable, rather than causing a large release. Alternatively, the attackers would specifically aim to cause a large release. In either case, the group would need to be sophisticated and determined in order for the attack to have a substantial conditional probability of success. If such a group sought to cause a large release, its members would plan accordingly. For example, it is likely that the group would arrange for a direct breach of the reactor containment. Thus, it would be prudent to assume that the magnitude of an attack-induced release would be at or above the upper end of the range of release magnitudes that would be expected for accidental releases.

*Diversion of fissile or radioactive material*

As mentioned in Section 2.2, above, one potential adverse outcome of operating a nuclear power plant is a diversion of fissile or radioactive material from the plant, for use in a nuclear or radiological weapon. Such a diversion would fit within the category of intentional, malevolent acts. The potential for such a diversion should be assessed in an EIS, as part of the examination of accidents and malfunctions.

[77] Thompson, 2007, Section 7.5.
[78] Thompson, 2007.

### 3.4 A Proposed Classification of Accidents and Malfunctions

CEAA's draft guidelines have classified accidents or malfunctions as described in Section 3.1, above. There are various deficiencies in that approach. For example, the draft guidelines do not recognize the potential for a large release of radioactive material from stored spent fuel. Also, the draft guidelines do not recognize the potential for diversion of fissile or radioactive material.

A proposed classification is set forth in Table 3-5. That classification rectifies the deficiencies mentioned above. Also, it identifies the major modes of impact of accidents and malfunctions, and shows how those modes are linked to the events that initiate accidents and malfunctions.

As mentioned in Section 3.1, above, CEAA's draft guidelines do not provide any guidance about characterizing malevolent acts by probability, severity, credibility or other indicators. It appears that the proponent is free to choose any set of malevolent acts for the purpose of preparing an EIS. That situation is not compatible with the purposes of an EIS. CEAA should provide specific guidance about the selection of malevolent acts for consideration.

Section 4.2, below, describes the status of CNSC's specification of the malevolent acts to be considered in designing a new nuclear power plant. CNSC has not yet specified the acts to be considered, although a consultant to CNSC has offered some suggestions. In the absence of a specification by CNSC, CEAA could draw guidance from the consultant's suggestions, and from the safety criteria that we propose in Section 4.3, below.

## 4. Criteria for Safety and Security of New Nuclear Power Plants

### 4.1 International Criteria

The International Atomic Energy Agency is responsible for, among other matters, the development of criteria for the safety and security of nuclear power plants. The IAEA's criteria are discussed here, focusing on criteria for design and siting of new plants.

In 2000, IAEA published document NS-R-1 in its Safety Standards Series. The document was titled *Safety of Nuclear Power Plants: Design*.[79] NS-R-1 reflected the consensus of IAEA Member States at the time. It was intended for application primarily to land-based, stationary nuclear power plants with water-cooled reactors. It established "design requirements for structures, systems and components important to safety". It addressed events that are "very unlikely", such as severe accidents that result in large

[79] IAEA, 2000.

releases of radioactive material, but it did not address "extremely unlikely" events such as the impact of a meteorite.[80]

NS-R-1 did not discuss intentional, malevolent acts. That omission presumably reflects the consensus of Member States in 2000. The IAEA has considered malevolent acts in documents published more recently, as discussed below.

*"Design-basis" and "beyond-design-basis" accidents*

NS-R-1 articulated a set of safety objectives for new nuclear power plants. Those objectives are summarized in Table 4-1. A general objective was supported by specific objectives relating to radiation protection and technical safety. The technical safety objectives embraced a concept that is currently employed in the reactor-safety field worldwide. The concept is that certain potential accidents are taken into account in designing a nuclear power plant, while others are not. Accidents in the first category are known as "design-basis" accidents, and would not involve core damage if the plant functioned as designed. Accidents in the second category are known as "severe" accidents or "beyond-design-basis" accidents. Those terms are used interchangeably in NS-R-1. Accidents in the second category would involve core damage.

The practice of dividing potential reactor accidents into two categories has been so widely adopted that many persons now working in the nuclear industry and its regulators may be unaware of the practice's origins. Those origins date from the first two decades of the commercial nuclear power industry (roughly, 1953-1975), when the foundations of the industry were laid. The basic designs of the present fleet of nuclear power plants were established at that time.

Until 1975, the nuclear industry and its regulators, with some limited exceptions, equated design-basis accidents with credible accidents. It was assumed that accidents of greater severity, involving significant damage to a reactor core, were non-credible.[81] That assumption became untenable when the Reactor Safety Study was published in 1975.[82] The Three Mile Island accident of 1979 and the Chernobyl accident of 1986 demonstrated empirically that core-damage accidents are indeed credible. At that point, the industry could have gone back to the drawing board, and developed new, safer types of reactor. Indeed, ASEA-Atom took that step, developing and attempting to market the PIUS design in the early 1980s. The nuclear industry as a whole took a different path, and regulators participated in that decision. The formerly "non-credible" accidents became "beyond-design-basis" accidents. PRAs were performed to estimate the "risk" of a beyond-design-basis accident, and that risk was deemed "acceptable" if its estimated value was below some threshold. NS-R-1 reflected that paradigm.

---

[80] IAEA, 2000, pp 1-2.
[81] Okrent, 1981.
[82] NRC, 1975.

PRAs have yielded useful, practical knowledge. They have identified deficiencies in the design, operation and maintenance of nuclear power plants. Some of those deficiencies have been corrected, thereby reducing the probability of a radioactive release. PRA findings have guided the development of capabilities for offsite emergency response. Nevertheless, it should not be forgotten that the need for PRAs derives from fundamental weaknesses in design. The present fleet of commercial reactors, and the proposed Generation III reactors, are unable to ride out a variety of credible events outside their design basis. If subjected to such an event, one of these reactors would experience core damage and, potentially, a release of radioactive material to the environment.

NS-R-1 did not specify any quantitative target for the risk of a beyond-design-basis accident. Instead, it specified qualitative targets. For example, as shown in Table 4-1, NS-R-1 called for a plant to be designed such that "the likelihood of accidents with serious radiological consequences is extremely low". NS-R-1 did not provide further guidance about implementing that objective.

*Recommendations and requirements regarding design features*

NS-R-1 set forth general recommendations and specific requirements regarding the design features of nuclear power plants, from a safety perspective. The general recommendations are exemplified by Table 4-2, which shows a recommended hierarchy of preference in selecting a plant design feature. There was some merit in the hierarchy. It called for choosing an inherently safe design as the first preference, or a passively safe design as the second preference. That recommendation would move a plant design toward the PRIME category discussed in Section 2.3, above. However, the hierarchy in Table 4-2 was deficient in important respects. It ranked continuously-operating, active safety systems on the same level as passive safety features, which is a serious deficiency. It stated that a preference should be exercised if "that can reasonably be achieved", but provided no criterion for determining what is reasonable.

Two examples illustrate the specific design requirements that were set forth in NS-R-1. First, NS-R-1 stated that "Structures, systems and components important to safety shall generally not be shared between two or more reactors in nuclear power plants".[83] That requirement appears to rule out the plant designs used for the present CANDU stations in Ontario. At those stations, up to eight reactors share safety systems, including containment and core-cooling systems. The second example is the statement in NS-R-1 that "The means for shutting down the reactor shall consist of at least two different systems to provide diversity".[84]

The overall pattern of design recommendations and requirements in NS-R-1 was to set forth vague, elastic recommendations about plant performance, but precise, rigid requirements regarding particular aspects of plant design, such as the number of reactor

[83] IAEA, 2000, page 24.
[84] IAEA, 2000, page 30.

shut-down systems. That approach is exactly opposite to the approach that would be taken if a regulator were seeking to maximize creativity in plant design. To maximize creativity and safety, a regulator would set forth precise, highly-demanding performance requirements, but would say comparatively little about design details.

*Storage of spent fuel*

NS-R-1 set forth requirements for the storage of spent (i.e., irradiated) fuel.[85] Those requirements addressed several specific design issues, such as the prevention of criticality. There was, however, no recognition of the potential for a large release of radioactive material as a result of an accident or a malevolent act affecting a facility for storage of spent fuel.

As discussed in Section 3.2, above, there is a substantial potential for a large release of radioactive material from spent fuel stored at nuclear power plants in the USA and elsewhere. That potential arises from the practice of storing spent fuel in pools equipped with high-density racks. NS-R-1 was silent on that issue. IAEA's failure to address the risk of a spent-fuel-pool fire, and the measures available to reduce that risk, is a grave deficiency in NS-R-1.

*Consideration of malevolent acts*

NS-R-1, which was published in 2000, did not discuss malevolent acts. IAEA documents published more recently have discussed such acts. For example, in 2006, IAEA published a study on advanced nuclear power plant design options to cope with external events.[86] That study involved the participation of plant designers from a number of Member States. Design options considered in the study had, to varying extents, attributes in the PRIME category discussed in Section 2.3, above. Those attributes include the ability to resist malevolent acts. The study did not yield specific design requirements for new nuclear power plants.

*Sustainability*

NS-R-1 did not discuss sustainability. In 2006, IAEA published a document on nuclear power and sustainable development.[87] That document did not provide a framework that could be used to assess the sustainability of a proposed program of nuclear power. It did not provide any guidance on the design of a nuclear power plant according to sustainability principles.

[85] IAEA, 2000, page 45.
[86] IAEA, 2006b.
[87] IAEA, 2006a.

*Summary of NS-R-1*

The design guidance in NS-R-1 reflected a paradigm in which potential accidents are in two categories – those within, and those beyond, the design basis. Accidents in the latter category are addressed probabilistically. That paradigm derives from fundamental weaknesses in the design of present nuclear power plants. NS-R-1 set forth vague, elastic recommendations about the safety performance of a plant. It did not address malevolent acts or potential releases from stored spent fuel. Its guidance was not compatible with principles of sustainability.

*IAEA siting document NS-R-3*

In 2003, IAEA published document NS-R-3 in its Safety Standards Series. The document was titled *Site Evaluation for Nuclear Installations*.[88] Its stated purpose was to "establish requirements for criteria" regarding the siting of all types of fixed nuclear installation except underground or offshore installations.

NS-R-3 stated that the main objective of site evaluation, in terms of nuclear safety, is "to protect the public and the environment from the radiological consequences of radioactive releases due to accidents".[89] At a later point, NS-R-3 discussed the implications for radiological risk of the site's features, the distribution of the surrounding population, and the characteristics of the nuclear installation. NS-R-3 stated that the combined effect of those factors should be such that:[90]

> "The radiological risk to the population associated with accident conditions, including those that could lead to emergency measures being taken, is acceptably low."

In that statement, and elsewhere, NS-R-3 explicitly adopted the nuclear industry's traditional definition of risk as the arithmetic product of a numerical indicator of consequences and a numerical indicator of probability. [91]

The above-quoted statement about radiological risk was the closest that NS-R-3 came to articulating criteria for assessing the merit of a site. The main function of NS-R-3 was to identify issues that should be addressed in site evaluation.

---

[88] IAEA, 2003.
[89] IAEA, 2003, page 4.
[90] IAEA, 2003, page 9.
[91] In this report, the term "risk" is used in a more general sense, to encompass a range of qualitative and quantitative information about the potential for an adverse outcome.

### 4.2 Canadian Criteria

In Section 3.1, above, there is mention of the Canadian Nuclear Safety Commission's October 2007 draft document RD-337, titled *Design of New Nuclear Power Plants*.[92] CEAA's draft guidelines state that the proponent must demonstrate that a proposed nuclear power plant meets the safety goals set forth in RD-337. The stated purpose of RD-337 was to "set out the expectations" of CNSC regarding the design of new plants. Thus, RD-337 can be regarded as a guidance document. One could reasonably expect RD-337 to be generally consistent with NS-R-1 and with design standards in leading industrialized countries. CNSC has encouraged that expectation by stating that its regulatory framework is aligned with "international standards and best practices", and that new nuclear power plants built in Canada "will meet the highest standards".[93]

Standards set forth in IAEA documents have been described as "lowest common denominator" standards that can be met in many Member States.[94] Thus, in comparing NS-R-1 and RD-337, one would expect the latter to have additional requirements and be generally more demanding. That is true in some respects, but not in all, as discussed below.

RD-337 shared with NS-R-1 the same basic paradigm, in which potential accidents are in two categories – those within, and those beyond, the design basis. Accidents in the former category are addressed deterministically, while those in the latter category are addressed probabilistically. That paradigm is linked with the nuclear industry's traditional definition of risk, and with the dogma that equal levels of risk are equally acceptable. The deficiencies of the two-tier accident paradigm are discussed in Section 4.1, above, and the deficiencies of the traditional approach to risk are discussed in Sections 2.1 and 2.2, above. Those deficiencies apply to RD-337, just as they apply to NS-R-1.

In late May 2008, the CNSC Staff published a document containing a revised version of RD-337, which the Staff submitted to the CNSC Commissioners for approval at the Commission meeting of 10 June 2008.[95] The revised version of RD-337 contains changes from the October 2007 draft. These changes include a significant weakening of the quantitative safety goals, as explained in the notes to Table 3-1. The following discussion generally refers to the October 2007 draft, which is referenced in CEAA's draft guidelines.

---

[92] CNSC, 2007a.
[93] CNSC, 2006, page 3.
[94] Harvie, 2004, page 3.
[95] Dallaire et al, 2008.

*Consideration of malevolent acts*

NS-R-1 did not consider malevolent acts. By contrast, RD-337 did consider such acts, stating:[96]

> "The design shall include provisions that promote security and robustness in response to malevolent acts, in accordance with applicable regulations and modern standards and codes."

Having articulated that goal, RD-337 proceeded to introduce the concept of design-basis threats (DBTs) and beyond-design-basis threats (BDBTs), which are analogous to the two categories of accident mentioned above. DBTs were described as "credible malevolent acts", while BDBTs were described as "severe" DBTs. That terminology is reminiscent of pre-1975 practice regarding accidents, when design-basis accidents were equated with credible accidents.

RD-337 did not characterize either category of threat. (This situation continues in the May 2008 revision of RD-337.) A consultant to CNSC has examined the issue of designing nuclear power plants to resist malevolent acts, and has offered recommendations intended to "facilitate the development of regulatory requirements".[97] The consultant postulated one type of DBT that is similar to aspects of the DBT employed in the USA by NRC, and a second type of DBT that could include "a common large commercial aircraft at speeds which can reasonably be achieved at low altitudes or an executive jet or a personal aircraft with a load of explosives taking off from an unregulated airfield". The consultant also provided examples of potential BDBTs, including "a large malevolent, explosive laden, vehicle or a LPG tanker gaining access past the physical protection barriers by stealth, deceit or force".[98]

The consultant recommended that CNSC be the "prime developer" of the DBTs and BDBTs. Implementation of that recommendation would exclude citizens from participating in the determination of DBTs and BDBTs. Such exclusion would be antithetical to the principles of sustainability, and would be unnecessary. Citizens could be engaged in dialogue on this issue without broad dissemination of detailed technical information (e.g., computer models describing the response of a structure to blast) that might assist malicious persons in Canada or elsewhere.

*Quantitative safety goals*

NS-R-1 did not set forth quantitative safety goals. By contrast, RD-337 set forth the quantitative safety goals shown in Table 3-1. In that table one will observe, for example, that the upper limit on the probability of core damage would be 1 per 100,000 plant-

[96] CNSC, 2007a, page 36.
[97] Asmis and Khosla, 2007.
[98] Asmis and Khosla, 2007, pp 66-67.

years, while the upper limit on the probability of a large release of radioactive material would be 1 per 1 million plant-years. As explained in the notes to Table 3-1, the May 2008 revision of RD-337 significantly weakens the safety goals in two respects. First, the quantitative goals in the "should be less than" category are abandoned. Second, the quantitative goals in the "shall not exceed" category are retained, but with different language. The revised RD-337 states that the sum of frequencies of all event sequences that can lead to a specified outcome "is less than" a numerical value.

Core damage or a large release would be instances of a beyond-design-basis accident. RD-337 did not explain how the probability of a BDBT would relate to the quantitative safety goals. As discussed previously in this report, there is at present no statistical basis for a quantitative estimate of the probability of a postulated malevolent act. Nevertheless, in a policy or planning context, judgment can be used to assign minimum probabilities to postulated acts.

Consideration of the potential for BDBTs could prevent CNSC from determining compliance with the quantitative safety goals in RD-337. If that potential were arbitrarily set aside, determining compliance could still be difficult or impossible. The determination would rely on PRAs, but PRA findings are highly uncertain.[99] Those findings cannot be directly validated by experience. For example, Table 3-1 shows a target probability of 1 per 1 million plant-years for core damage.[100] Yet, worldwide operating experience of commercial nuclear power plants through 2007 is about 12,900 plant-years, and Canadian experience is about 560 plant-years.[101] Two core-damage events have occurred worldwide while that experience was accruing.

Practical experience in Canada casts doubt on PRA findings for CANDU plants.[102] For example, on one occasion designers of the Pickering A station estimated the probability of a particular event sequence at 1 per 10 billion plant-years. An almost identical event occurred a few weeks later.[103] Also, Canada lacks a fully developed PRA culture. PRAs performed in Canada for CANDU reactors find extremely low probabilities for large releases. Based on those findings, the PRAs do not estimate the radiological impacts of large releases. Yet, the low probabilities are not credible.[104] The practice of ignoring large releases deprives citizens and policy makers of needed information. For example, in a recent analysis of the radiological risk of continued operation of the Pickering 'B' station, the largest release considered included 71 TBq of Cesium-137.[105] That is a comparatively small release, and is categorized as such in Table 3-1.

---

[99] Hirsch et al, 1989.
[100] The CNSC Commissioners may follow the recommendation of the CNSC Staff to abandon the target values (the "should be less than" values) in Table 3.1. In that event, the safety goals would lack any provision for uncertainty or variability in PRA findings. Such a position by CNSC would undoubtedly be controversial and could lead to litigation.
[101] Extrapolated from Table 1 of: IAEA, 2006a.
[102] Beare, 2005.
[103] Beare, 2005, page 33.
[104] Thompson, 2000; IRSS, 1992.
[105] SENES, 2007, Table B.5.3-1.

*Recommendations and requirements regarding design features*

Like NS-R-1, RD-337 set forth general recommendations and specific requirements regarding the design features of nuclear power plants, from a safety perspective. NS-R-1, as shown in Table 4-2, set forth a recommended hierarchy of preference in selecting plant design features. By contrast, RD-337 described a similar set of design features, but did not place them in a hierarchy of preference. Instead, RD-337 stated that features should be adopted where "that can be reasonably achieved".[106] That approach was a significant retreat from the safety standard established by NS-R-1.

*Storage of spent fuel*

Like NS-R-1, RD-337 set forth requirements for the storage of spent (i.e., irradiated) fuel.[107] Those requirements addressed several specific design issues, such as the prevention of criticality. Like NS-R-1, RD-337 failed to recognize the potential for a large release of radioactive material as a result of an accident or an act of malice affecting a facility for storage of spent fuel.

*Summary of RD-337*

RD-337 was generally consistent with NS-R-1 and reflected the same paradigm. A notable difference between the two documents was that RD-337 considered malevolent acts, while NS-R-1 did not. RD-337 introduced the concept of design-basis threats and beyond-design-basis threats, but did not characterize either category of threat. Also, RD-337 set forth quantitative safety goals, while NS-R-1 did not. However, CNSC's ability to determine compliance with the quantitative safety goals is questionable. RD-337 retreated from the safety standard established by NS-R-1 regarding preferences in selecting plant design features. RD-337 did not address potential releases from stored spent fuel.

*CNSC siting document RD-346*

In October 2007, CNSC published draft document RD-346, titled *Site Evaluation for New Nuclear Power Plants*.[108] Its stated purpose was to "set out the expectations" of CNSC regarding site evaluation for new plants. Thus, RD-346 can be regarded as a guidance document.

In late May 2008, the CNSC Staff published a document containing a revised version of RD-346, which the Staff submitted to the CNSC Commissioners for approval at the

[106] CNSC, 2007a, page 13.
[107] CNSC, 2007a, pp 61-62.
[108] CNSC, 2007b.

Commission meeting of 10 June 2008.[109] The following discussion generally refers to the October 2007 draft.

The guidance provided in RD-346 consisted primarily of an identification of issues that should be addressed in site evaluation. RD-346 offered some criteria regarding non-radiological impacts of a nuclear power plant on the local environment.[110] However, RD-346 offered no criteria for assessing the merit of a site from a safety perspective.

RD-346 stated that site evaluation should take into account "all phases of the NPP life cycle, from site preparation to abandonment".[111] That provision appropriately recognized that site features significant for safety, such as the population distribution in the surrounding region, could change over time. At a CNSC public meeting discussing RD-346 prior to its release, a participant suggested that the same provision should apply to existing nuclear power plants. The CNSC official chairing the meeting acknowledged that suggestion.[112] To date, CNSC has not acted on the suggestion. One could broaden the suggestion, to argue that existing plants should not be allowed to operate for an extended period if they cannot comply with the design and siting standards used for new plants.

### 4.3 A Proposed Set of Criteria

As an alternative to the guidance set forth in the CNSC and IAEA documents reviewed above, criteria for the design and siting of nuclear power plants are proposed here. The proposed criteria focus on the potential for an unplanned release of radioactive material – i.e., on safety.

The criteria proposed here would provide a benchmark for consideration of accidents and malfunctions in the EIS for the proposed Bruce nuclear power plants. As mentioned in Section 1, above, CEAA requires that the factors to be considered in an EIS include not only environmental effects, but also the purpose of the project, the need for the project, alternatives to the project, and alternative means of carrying out the project. Bruce Power proposes to build nuclear power plants whose design reflects the risk paradigm described in Sections 4.1 and 4.2, above. Our proposed criteria reflect an alternative paradigm, which should be presented in the EIS.

Table 4-3 describes the proposed criteria. They are purely deterministic. All the events that they are intended to accommodate are within the plant's design basis. Thus, they offer a clear alternative to the paradigm employed by IAEA and CNSC, in which design-basis accidents are addressed deterministically and beyond-design-basis accidents are

---

[109] Dallaire et al, 2008.
[110] CNSC, 2007b, Table 5.1.
[111] CNSC, 2007b, page 1.
[112] Comment by Shawn-Patrick Stensil and response by Chairperson, CNSC public meeting, Ottawa, 13 September 2007, transcript pp 156-158.

addressed probabilistically. The proposed criteria reject that two-tier paradigm, and also reject the nuclear industry's traditional concept of risk and its acceptability.

The criteria set forth in Table 4-3 are not definitive. At various points, they state that a parameter would be "specified", but they leave that specification open or suggest a tentative value for consideration. The intention is that the final parameters would be determined by public processes, as discussed below.

Table 4-3 provides design-basis criteria for a plant's safety performance under two conditions – reactor operation, and reactor refueling. The criteria for reactor operation are similar to those articulated by ASEA-Atom for the PIUS reactor. The criteria for reactor refueling reflect an expectation that the plant's containment would be somewhat compromised during refueling. The maximum release specified under the refueling criteria could be linked to the frequency of refueling for a particular plant design.

Both of these sets of criteria are performance-based. They would encourage creativity in plant design, providing an opportunity to move beyond the present designs, whose basic features were established in the 1950s and 1960s. Compliance with the criteria for reactor operation could be demonstrated, to a substantial extent, by testing of the actual plant prior to its entry into service. For example, the plant's ability to ride out a loss of power and normal heat sinks, and abandonment by operators, could be tested directly. Other aspects of compliance would be established through conservative modeling and analysis.

Table 4-3 provides deterministic siting criteria, expressed in terms of maximum radiological impacts from design-basis events. Those criteria would translate into permissible distributions of population and land use in regions surrounding a plant. Compliance would be established through conservative modeling and analysis.

*Public processes for deciding on final criteria*

The criteria set forth in Table 4-3 provide a point of departure for public processes that could yield final criteria for the design and siting of new nuclear power plants. That transition could occur in two steps. First, the general structure of the criteria would be debated, and modified as appropriate. Second, final specifications would be established for the various parameters that appear in Table 4-3, or the analogous parameters that would appear in a modified structure.

Suitable public processes would engage local and provincial governments, and a broad range of other groups of stakeholders, in dialogue about citizens' preferences regarding the safety and sustainability of nuclear power. That dialogue should be informed by technical analyses that respond to stakeholder questions. All aspects of the dialogue should occur openly, even when the dialogue addresses the potential for malevolent acts. An essential feature of any sustainable energy system is that it should be robust against malevolent acts by virtue of its inherent properties, and should not require protection

through secrecy. Indeed, secrecy and related measures, such as surveillance of the population, are antithetical to sustainability.

## 5. Safety and Security Characteristics of Plant Designs under Consideration in Ontario

### 5.1 Scope of this Discussion

In Sections 5.2 through 5.4, below, this report provides a brief review of the safety and security characteristics of the three types of nuclear power plant that are being considered for construction in Ontario. A thorough assessment of these plants' potentials for accidents and malfunctions would be a much bigger task, as discussed in Section 1, above.

One source of information about the characteristics of the three types of plant is a March 2008 report that summarizes a review conducted by IAEA for the UK Health and Safety Executive.[113] That review evaluated the designs of these three plant types (and the ESBWR, which is no longer a contender in Ontario) against IAEA safety standards.

### 5.2 The AREVA US EPR

The above-mentioned IAEA review is one source of information about the EPR. Another source of information is a report that AREVA submitted to NRC in 2005, providing a technical description of the EPR.[114] A study for Greenpeace International briefly examined the EPR as part of a broad review, published in 2005, of the hazards of nuclear power.[115]

The EPR is a PWR plant that represents a comparatively small evolutionary step from predecessor PWRs including the French N4 and the German KONVOI. It has a net generating capacity of 1,600 MWe, which is substantially above the capacities of the AP1000 and the ACR-1000. It uses both active and passive safety systems. By comparison with the predecessor PWRs, some safety systems have been added, and some have been deleted. For example, systems to depressurize the primary circuit under accident conditions have been added to the EPR, and the high-pressure safety injection system has been deleted. As another example, the EPR has four accumulators in its emergency core cooling system, whereas the KONVOI plants have eight accumulators. The volume of the EPR containment has been reduced, in part reflecting new calculations that show lower production of hydrogen during an accident.

A new feature of the EPR is a "core catcher" (core retention system) below the reactor pressure vessel. This feature is intended to accommodate accident situations in which the core would melt, fall to the base of the vessel, and then melt through the vessel's lower

[113] IAEA, 2008.
[114] AREVA, 2005.
[115] Hirsch et al, 2005.

head. The core catcher is designed to spread the molten material across a horizontal surface, allowing the material to cool and solidify. The IAEA reviewers noted the experimental work and analysis underlying the design, but were not convinced that the core catcher would work in all core-melt situations. They called for further review of the need for a containment-venting capability, to protect the containment from over-pressurizing in the event that the core catcher did not function properly.

AREVA has described safety objectives for the EPR design, expressed probabilistically.[116] One objective is to achieve a mean probability of core damage of less than 1 per 100,000 reactor-years, accounting for internal and external events (excluding earthquake and sabotage) and all operational modes. Another objective is to achieve a mean probability of a Large Release of less than 1 per 1 million reactor-years. It is interesting to compare these design objectives with CNSC's draft safety goals, as shown in Table 3-1. The EPR objectives would satisfy CNSC's upper limits of probability but would not satisfy the target levels, which are an order of magnitude lower. In that context, it is noteworthy that NRC has warned that estimated core-damage probabilities lower than 1 per 100,000 reactor-years "should be viewed with caution because of the remaining uncertainties in PRA (e.g., events not considered)".[117] These observations may shed light on the CNSC Staff recommendation to abandon the target levels of the draft safety goals.

The IAEA review noted that AREVA has completed a PRA at Level 1 (estimation of the probability of core damage). The findings of that study could be compared with the core-damage objective. AREVA has not completed a PRA at Level 2 (estimation of the probabilities and other characteristics of potential releases to the atmosphere). Thus, the Large-Release objective cannot yet be compared with PRA findings. Note that a thorough PRA would be conducted not only at Levels 1 and 2, but also at Level 3 (estimation of the probabilities and other characteristics of potential environmental impacts).

The containment of the EPR is a vertical, reinforced-concrete cylinder with a domed top. The wall of the cylinder is 1.3 m thick, and the dome is 1.0 m thick. Surrounding the containment is a shield building with a similar configuration. The shield building's wall and dome are each 1.8 m thick. In combination, these two structures would provide more protection against external attack than is typical for Generation II nuclear power plants. For example, at the IP2 and IP3 plants, the containment wall is 1.4 m thick, the dome is 1.1 m thick, and there is no shield building. Nevertheless, the EPR shield building and containment could be breached by instruments available to sub-national groups. In illustration, Table 3-4 shows that a shaped charge could penetrate such structures.

The EPR's spent-fuel pool is adjacent to, but outside, the containment. That arrangement is typical for Generation II PWRs. However, the base of the EPR pool is above grade,

---

[116] AREVA, 2005, page 1-2.
[117] NRC, 1990, page 8-2.

whereas at most US PWRs the base of the pool is below grade. Thus, draining of the pool might be more readily accomplished at the EPR. It appears that the EPR pool would be equipped with high-density racks, creating the potential for a spent-fuel fire in the event of water loss. Neither AREVA nor the IAEA reviewers seem to be aware of this hazard. In this context, a positive feature of the EPR is that the building housing the spent-fuel pool is comparatively robust.

*Summary*

From safety and security perspectives, the EPR is an incremental improvement by comparison with typical Generation II PWRs. Its ability to meet CNSC's draft safety goals is questionable. An accident or attack at an EPR could lead to a large, atmospheric release of radioactive material, as at Generation II plants. The EPR could not meet the safety criteria set forth in Table 4-3.

### 5.3 The Westinghouse AP1000

The above-mentioned IAEA review is one source of information about the AP1000. Another source is a Westinghouse document summarizing the characteristics of the AP1000.[118] A conference paper provides a third source.[119] Those sources provide sufficient detail for our purpose.

The AP1000 is a PWR plant that represents an evolutionary step from predecessor Westinghouse PWRs. It has a net generating capacity of 1,100 MWe. Its development was guided by two primary objectives. First, Westinghouse sought to make the AP1000 easier and cheaper to build, operate and maintain than the predecessor plants. Second, Westinghouse sought to significantly reduce the probability of core-damage accidents.

Pursuit of those objectives led to a design with a number of new features. These include a passive system for emergency core cooling, a passively-cooled containment system, a system to depressurize the primary circuit, and canned circulating pumps in the primary circuit. It should be noted that the nominally passive systems in the AP1000 are not passive to the extent that the central systems of a PIUS reactor would be. Operation of the AP1000 systems would require the opening and closing of valves.

The AP1000 does not have a core catcher, as does the EPR. Instead, the AP1000 is designed so that the reactor cavity could be flooded, thereby cooling the outside surface of the reactor pressure vessel. The objective would be to retain molten core material inside the vessel. The IAEA reviewers have called for assessment of the consequences if molten core material were not retained.

[118] Westinghouse, 2007.
[119] Cummins et al, 2003.

Westinghouse has performed a PRA at Levels 1, 2 and 3. The Level 3 analysis would, of course, have to be completed on a site-specific basis. According to Westinghouse experts writing in 2003, the estimated probability of reactor core damage, accounting for internal and external events, and accidents during shutdown, is 0.4 per 1 million reactor-years, and the probability of a Large Release is 0.4 per 10 million reactor-years.[120] Those PRA findings, if credible, would satisfy CNSC's draft safety goals, as shown in Table 3-1. As mentioned earlier in this report, there is reason to question the credibility of such low-probability findings.

The containment of the AP1000 consists of a vertical, steel cylinder with a wall thickness of 4.4 cm. That structure is surrounded by a cylindrical shield building made of reinforced concrete, with a wall thickness of 0.9 m. Those structures, in combination, would be considerably more vulnerable to attack than the analogous structures at the EPR. It is clear that Westinghouse did not consider protection from external assault to be a high-priority design objective.

As at the EPR, the AP1000 spent-fuel pool is adjacent to, but outside, the containment. It appears that the AP1000 pool would be equipped with high-density racks, thus creating the potential for a spent-fuel fire in the event of water loss. Neither Westinghouse nor the IAEA reviewers seem to be aware of this hazard.

*Summary*

From the perspective of reactor accidents, the AP1000 is an improvement by comparison with typical Generation II PWRs. It may be able to meet CNSC's draft safety goals, to the extent that low-probability PRA findings are credible. However, the AP1000 has a comparatively high vulnerability to attack, and in that respect is not an improvement on Generation II PWRs. An accident or attack at an AP1000 could lead to a large, atmospheric release of radioactive material, as at Generation II plants. The AP1000 could not meet the safety criteria set forth in Table 4-3.

### 5.4 The AECL ACR-1000

The above-mentioned IAEA review is one source of information about the ACR-1000. Another source is an AECL document summarizing the characteristics of the ACR-1000.[121]

The ACR-1000 is a CANDU plant that represents a comparatively small evolutionary step from predecessor CANDUs built outside Ontario, but a larger step from the CANDUs now deployed in Ontario. The Ontario CANDUs – at the Pickering, Bruce and Darlington sites – are unusual by comparison with other CANDUs and Generation II nuclear power plants worldwide, because safety systems are shared by 8 units (at

[120] Cummins et al, 2003, pp 7-8.
[121] AECL, 2007.

Pickering) or 4 units (at Bruce A, Bruce B, and Darlington). By contrast, most nuclear power plants in the world are primarily stand-alone units from a safety-systems perspective, although there can be cross-connections among safety systems and sharing of particular plant features such as control rooms.

The ACR-1000 is designed as a stand-alone plant, although it could be built in a two-unit block. It has a net generating capacity of 1,100 MWe. It incorporates a number of design changes compared with predecessor CANDUs. A large part of the purpose of these changes is to reduce the costs of construction and operation. For example, the ACR-1000 contains 250 Mg of heavy water, whereas each Darlington unit contains 590 Mg. The major explanation for that difference is that the ACR-1000 is cooled by light water instead of heavy water. The ACR-1000 employs low-enriched fuel instead of natural-uranium fuel. The ACR-1000 fuel would be driven to a burnup of 20 MWt-days per kgU, compared to 8 MWt-days per kgU at Darlington.

Use of low-enriched fuel and light-water cooling in the ACR-1000 offer the prospect of the reactor having a negative void coefficient of reactivity in the event of loss of coolant from the primary circuit. AECL claims that the ACR-1000 reactor has that property. If that claim is correct, AECL has finally cured a fundamental design deficiency that has raised a safety concern about all predecessor CANDUs. Those reactors have a positive void coefficient. As a result, occurrence of a loss-of-coolant accident, coincident with a failure of the reactor shutdown systems, could lead to a rapid rise in power that causes violent disruption of the reactor core within a few seconds.[122]

AECL's ability to achieve its design objectives for the ACR-1000, including a negative void coefficient, is thrown into question by the scrapping of the two MAPLE reactors at AECL's Chalk River laboratories in May 2008.[123] These are 10 MWt, pool-type reactors employing low-enriched fuel, and were intended to produce medical isotopes. They were designed and built by AECL. Their construction was completed in 2000, and they have been undergoing commissioning since then. AECL has now concluded that the reactors are unfit to operate, and that their deficiencies cannot be rectified within any reasonable budget and timeframe. It appears that the deficiencies include sticking of control rods and shutoff rods, and a positive power coefficient of reactivity that could produce power excursions.[124]

AECL claims that the probability of core damage at the ACR-1000, accounting for internal events only, is 0.3 per 1 million reactor-years during operation, and 0.1 per 1 million reactor-years during shutdown. That claim is not based on PRA findings. According to the IAEA reviewers, AECL plans to prepare a PRA at Level 1 and a partial analysis of issues that would be addressed in a PRA at Level 2. AECL has no plan to prepare a PRA at Level 3, reflecting the lack of a fully developed PRA culture in Canada. In the absence of PRA findings at Level 2, it is reasonable to assume that an accident at

[122] Thompson, 2000, page 7.
[123] CBC News, 2008a.
[124] MacKenzie, 2008.

an ACR-1000 could release to the atmosphere an amount of radioactive material comparable to the amount that could be released from an existing CANDU plant in Ontario. Studies indicate that the latter release could be substantial.[125]

The containment of the ACR-1000 consists of a vertical cylinder with a domed top, made of pre-stressed concrete and equipped with a steel liner. The wall thickness of the cylinder is 1.8 m. The vulnerability of this structure to external assault would be intermediate between the vulnerability of the EPR containment/shield structures and the vulnerability of the AP1000 containment/shield structures.

The spent-fuel pool of the ACR-1000 is adjacent to, but outside, the containment. The risk posed by this arrangement is unknown, because there has been no study of the potential for a large release of radioactive material from a spent-fuel pool at a CANDU plant.

*Summary*

From safety and security perspectives, the ACR-1000 appears to be an incremental improvement by comparison with predecessor CANDU plants. The extent of any safety improvement is difficult to assess because PRA findings for the ACR-1000 are not available. Moreover, it appears that AECL does not intend to prepare a comprehensive PRA at Level 2. Available information indicates that an accident or attack could lead to a large, atmospheric release of radioactive material from the reactor core. The potential for a release from stored spent fuel is unknown. The ACR-1000 could not meet the safety criteria set forth in Table 4-3.

## 6. Adequacy of Canadian Regulation of Safety and Security of Nuclear Power Plants

The potential for accidents and malfunctions at nuclear power plants is determined, in part, by the adequacy of regulation of the plants' safety and security. CNSC provides that regulation in Canada. In the present context, at least three major questions arise regarding the adequacy of CNSC's regulation. First, are CNSC's criteria for the design and siting of new plants adequate? Second, given CNSC's present reliance on a probabilistic paradigm of safety, is the PRA culture in Canada adequate to support that paradigm? Third, does CNSC have the necessary independence and authority to perform its functions?

*Design and siting criteria*

As shown in Section 4, above, CNSC's design and siting criteria reflect a paradigm in which potential accidents and malfunctions at a nuclear power plant are categorized as "design-basis" events that would not lead to a substantial radioactive release if the plant functioned as designed, and "beyond-design-basis" events that could lead to such a

[125] Thompson, 2000; IRSS, 1992.

release. Events in the latter category are addressed probabilistically, using the concept of risk. Although purportedly scientific, the risk concept as currently applied is actually a form of dogma. The probabilistic paradigm reflects fundamental weaknesses in design. Generation II nuclear power plants, and the proposed Generation III plants, are unable to ride out a variety of credible events outside their design basis. An alternative paradigm is available, as illustrated by the proposed safety criteria set forth in Table 4-3.

*Canada's PRA culture*

As discussed in Section 4.2, above, Canada lacks a fully developed PRA culture. PRAs performed in Canada for CANDU reactors find extremely low probabilities for large releases. Based on those findings, the PRAs do not estimate the environmental impacts of large releases. Yet, the low probabilities are not credible.[126] The practice of ignoring large releases deprives citizens and policy makers of needed information. Moreover, Canada's isolation from best practice in the PRA field leaves CNSC unprepared to implement the probabilistic safety paradigm that it has articulated for new plants, including the safety goals set forth in Table 3-1.

*CNSC's independence and authority*

A credible regulator must be able to demonstrate, on a sustained basis, its independence from political pressure, and its ability to exert authority.[127] CNSC's independence and authority have been brought into question by events in recent months related to operation of the NRU reactor at Chalk River.[128] That reactor produces a substantial fraction of the radioisotopes used for medical tests and procedures worldwide. Its continued operation is particularly important in light of AECL's failure to make the MAPLE reactors operational. In November 2007, CNSC ordered the NRU reactor to be closed, pending the upgrading of safety systems. CNSC had been dissatisfied with AECL's progress in making the upgrade. In December 2007, the Canadian parliament voted to override CNSC's order, and the NRU reactor was re-started. Continuing tension between the CNSC President and the Canadian government led to the President's dismissal in January 2008. This author lacks the information needed to assess the technical and legal merits of the positions taken by parties to this dispute. Nevertheless, the episode undermines the credibility of CNSC as an independent regulator with real authority.

In October 2007, CNSC issued a draft version of its guidance document RD-337. In May 2008, the CNSC Staff published a revised version of RD-337, which may be approved by

---

[126] For example, a focused review of the Darlington Probabilistic Safety Evaluation (DPSE) identified core-damage sequences that DPSE had not examined. One such sequence involved a failure of service water supply, and would have been familiar to analysts conducting PRAs for PWRs. Consideration of just this one neglected sequence increased the estimated probability of core damage in the most dangerous core-damage category (FDC0) by a factor of 4. The reviewers predicted that a full-scope review of DPSE would reveal other significant deficiencies. See: IRSS, 1992, Volume 2.
[127] CNSC, 2007c.
[128] CBC News, 2008b.

the CNSC Commissioners at their meeting on 10 June 2008.[129] Changes in the revised version include a significant weakening of the quantitative safety goals for a new nuclear power plant, as explained in the notes to Table 3-1. The time interval over which this weakening occurred includes a period of political interference in the regulatory functions of CNSC, as described in the preceding paragraph. The conjunction of these events will feed suspicion that CNSC's independence has been compromised.

**7. Secrecy and its Impacts**

The nuclear power industry and its regulators, in Canada and elsewhere, are prone to secretive behavior. For some limited purposes, such as protection of trade secrets or the privacy of personnel, secrecy is widely accepted and is comparatively harmless. In the context of accidents and malfunctions, however, secrecy has significant, negative impacts. Those impacts should be addressed in an EIS.

Nuclear power plants can experience accidents and malfunctions that lead to severe impacts on the environment. Assessing the potential for such impacts requires thorough technical analysis, supported by detailed information about plant design. Some people argue that analysis of this type should be performed in private settings by experts who announce their findings to citizens and policy makers. That approach might be preferred by many experts. Experience shows, however, that the approach leads to an entrenched culture of secrecy. Such a culture is not compatible with a clear-headed, science-based understanding of risks. Entrenched secrecy perpetuates dogma, stifles dissent, creates opportunities for corruption, and can create a false sense of security. In illustration, the culture of secrecy in the former USSR was a major factor contributing to the occurrence of the 1986 Chernobyl reactor accident.[130]

Some countries have a tradition of governmental secrecy. Other countries, including Canada and the USA, have recognized the benefits of an open society. In the latter group of countries, a considerable amount of information about nuclear power plants and their risks has been publicly available until recent years. Much of this information has been accessible through the regulatory agencies. Since the attacks on New York and Washington in September 2001 that situation has changed, as discussed below.

Prior to September 2001, there were differences between the USA and Canada regarding the availability of information about accidents and malfunctions at nuclear power plants. A notable difference related to the creation of information, rather than its dissemination. In the USA, numerous PRAs were conducted at Level 3, and there was considerable scientific and public debate about the risks of large releases of radioactive material. In Canada, by contrast, the PRA culture was less developed.[131] As a result, Canada has seen less scientific and public debate about the risks of large releases.

---

[129] Dallaire et al, 2008.
[130] Thompson, 1998.
[131] The Canadian nuclear industry and its regulators were also comparatively reluctant to share PRA-related information with independent analysts and the public. For example, the conduct of an independent review

Since September 2001, NRC has become notably more secretive. NRC has justified this position by pointing to the risk of attack on nuclear power plants and other nuclear facilities. Yet, NRC has not required its licensees to strengthen the existing plants. Nor has NRC required that robustness against attack be a major design objective for new plants. One could suspect that a major motive for NRC's secrecy is protection of the status quo. NRC opposes requests by state and local governments and citizen groups that malevolent acts be considered in EISs.[132]

CNSC has departed from US practice by including resistance to malevolent acts in its proposed design criteria for new nuclear power plants. Similarly, CEAA has departed from US practice by requiring consideration of malevolent acts in an EIS. Both agencies deserve commendation for their new approach. It remains to be seen, however, if these agencies can accommodate the consideration of malevolent acts without resorting to excessive secrecy. Such secrecy would create adverse impacts on Canadian society. CNSC has already adopted a secretive approach regarding the risks posed by existing nuclear power plants.[133]

CNSC could greatly reduce the need for secrecy by requiring that new nuclear power plants be highly robust against attack. If a plant is robust against credible attacks, secrecy about its design and operation serves no purpose. The proposed safety criteria set forth in Table 4-3 would provide a high degree of robustness. To date, CNSC has not specified the DBTs and BDBTs that must be considered in the design of a new nuclear power plant.

CEAA could help Canadian citizens and policy makers to understand the impacts of secrecy, by comparing the risks posed by Generation III plants with the risks posed by alternative plants with a high degree of robustness. The proposed safety criteria set forth in Table 4-3 would provide a benchmark to assist that comparison.

---

of the Darlington Probabilistic Safety Evaluation was hindered by Ontario Hydro, which delayed its provision of a full set of DPSE documents for more than 6 months. When those documents were eventually provided, they revealed significant deficiencies in DPSE. See: IRSS, 1992, Volume 2, Annex I, pp a-c.

[132] Since 2002, NRC has been involved in litigation with a group of intervenors, led by San Luis Obispo Mothers for Peace, who request that an EIS be prepared for a proposed ISFSI at the Diablo Canyon site, to address the environmental impacts of malevolent acts. The intervenors have been supported by a ruling from the 9th Circuit of the US Court of Appeals. NRC refuses to implement that ruling at sites beyond the reach of the 9th Circuit, and the intervenors allege that NRC has not properly implemented the ruling in the Diablo Canyon instance.

[133] In illustration, Greenpeace Canada has requested a copy of the PRA for the Pickering B units. CNSC has refused to order Ontario Power Generation (OPG) to provide this PRA. In so doing, CNSC has accepted OPG's argument that the PRA should be available only to OPG personnel on a "need to know" basis. See: CNSC, 2008. This approach, although it may be well-intentioned, will inevitably create an entrenched culture of secrecy that will suppress a clear-headed understanding of risks. A more sophisticated approach could allow independent review of the PRA without disclosing information that would assist malevolent actors.

## 8. Conclusions and Recommendations

Major conclusions of this report are as follows:

C1. Any new, large, long-lived engineered system should be designed according to sustainability principles, including the precautionary principle. That requirement would apply to any new nuclear power plant.

C2. The environmental impacts of potential accidents and malfunctions at a new nuclear power plant should be assessed against a framework of sustainability principles.

C3. Potential accidents and malfunctions include a large, unplanned release of radioactive material from the plant to the environment, and the diversion of fissile or radioactive material from the plant for use in a nuclear or radiological weapon. CEAA is to be commended for including malevolent acts in the category of accidents and malfunctions.

C4. Analysts in the nuclear industry and its regulators have developed PRA techniques to estimate the consequences and probabilities of unplanned releases of radioactive material from nuclear power plants. Those analysts employ a concept called "risk", which they define as the arithmetic product of a numerical indicator of consequences and a numerical indicator of probability. They typically argue that equal levels of risk should be equally acceptable to citizens. That argument is not a scientific statement. It is, instead, dogma representing a particular set of values and interests.

C5. Citizens may be more concerned about the potential for a high-consequence, low-probability event than about the potential for a low-consequence event with the same nominal level of risk. That concern can reflect a legitimate set of values and interests, skepticism about estimates of low probability, doubt that the complexity of consequences can be represented by simple indicators, and recognition that new phenomena can come into play when thresholds of consequence are exceeded.

C6. The nuclear power industry and its regulators have embraced a paradigm in which potential accidents and malfunctions are categorized as "design-basis" events that would not lead to a substantial radioactive release if the plant functioned as designed, and "beyond-design-basis" events that could lead to such a release. Events in the latter category are addressed probabilistically, using the concept of risk. The probabilistic paradigm reflects fundamental weaknesses in design. Generation II nuclear power plants, and the proposed Generation III plants, are unable to ride out a variety of credible events outside their design basis.

C7. Nuclear power plants could be designed to ride out a range of credible events outside the design basis of Generation II and Generation III plants. Adoption of such new designs would allow the present, probabilistic paradigm to be replaced by a set of deterministic safety criteria.

C8. The plant designs under consideration by Bruce Power vary significantly in their safety and security characteristics, and in the extent to which they have been subjected to PRA analysis.

C9. Bruce Power proposes to provide a "technology neutral" assessment of the potential for accidents and malfunctions. That assessment would not be credible.

C10. Quantitative safety goals for new nuclear power plants, as currently proposed by CNSC Staff, are significantly weaker than safety goals previously articulated by CNSC. That change, and other developments, raise questions about the independence of CNSC.

C11. The nuclear power industry and its regulators are prone to secretive behavior. Secrecy creates significant adverse impacts. Secretive behavior by industry and regulators is in part attributable to the adoption of plants that are unable to ride out a variety of credible events outside their design basis. Adoption of plant designs that are more robust could eliminate the need for secrecy.

**********

Based on the preceding conclusions and the body of this report, recommendations are offered here in the context of CEAA's draft guidelines. The recommendations are:

R1. CEAA should revise its classification of accidents and malfunctions. The classification set forth in Table 3-5 provides an appropriate model.

R2. CEAA should reject Bruce Power's proposal to provide a "technology neutral" assessment of the potential for accidents and malfunctions.

R3. CEAA should require Bruce Power to provide a Level 3 PRA for each of the plant designs under consideration. The PRA should consider internal and external initiating events, and all operational states of the plant. The PRA should consider a full range of potential releases from the reactor core and from stored spent fuel. The EIS should summarize the findings of these PRAs, and should include the PRAs themselves as appendices.

R4. CEAA should require Bruce Power to provide, for each of the plant designs under consideration, an assessment of the environmental impacts of radioactive releases arising from a range of credible malevolent acts that affect the reactor core or stored spent fuel. The EIS should summarize the findings of these assessments, and should include the assessments themselves as appendices. CEAA should select the range of credible malevolent acts to be considered. In so doing, CEAA should employ the DBTs and BDBTs determined by CNSC if these are available. Absent a CNSC determination, CEAA could draw guidance from suggestions by a CNSC consultant, and from the set of malevolent acts encompassed by the safety criteria proposed in Section 4-3 of this report.

R5. The EIS should use the safety criteria proposed in Section 4-3 as a benchmark for assessing environmental impacts of potential accidents and malfunctions. The criteria proposed in Section 4-3 would provide a performance envelope for a "benchmark plant". Environmental impacts would be assessed for the plant designs under consideration and for the benchmark plant, across the same set of initiating events, including malevolent acts.

R6. The EIS should assess the mode and degree of secrecy that would accompany the adoption of each of the plant designs under consideration, or the adoption of the benchmark plant described in recommendation R5. The EIS should also assess the environmental impacts (social and economic impacts, etc.) of the anticipated secrecy.

R7. The EIS should assess, for each of the plant designs under consideration, the potential for diversion of fissile or radioactive material for illicit use, and the environmental impacts of such diversion.

## 9. Bibliography

(AECL, 2007)
Atomic Energy of Canada Ltd., *ACR-1000 Technical Summary* (Mississauga, Ontario: AECL, August 2007).

(Alvarez et al, 2003)
Robert Alvarez and seven other authors, "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States", *Science and Global Security,* Volume 11, 2003, pp 1-51.

(Ansolabehere et al, 2003)
Stephen Ansolabehere and nine other authors, *The Future of Nuclear Power: An Interdisciplinary MIT Study* (Cambridge, Massachusetts: Massachusetts Institute of Technology, 2003).

(AREVA, 2005)
AREVA, *EPR Design Description* (Lynchburg, Virginia: Framatome ANP, Inc., August 2005).

(Asmis and Khosla, 2007)
G. J. Kurt Asmis and Jagjit Khosla, Report to the CNSC, *Guidance on Meeting Regulatory Expectations for the Engineering Safety Aspects of Protection from Malevolent Events, RSP-0218* (Ottawa: Asmis Consulting, 19 March 2007).

(Beare, 2005)
John W. Beare, *Review of ACR-LBD-001, Licensing Basis Document for New Nuclear Power Plants in Canada, Draft dated 2004 December* (Ottawa: CNSC, file No. 34-R240-2, 31 March 2005).

(Bruce Power, 2007)
Bruce Power, *Bruce Power New Build Project Environmental Assessment: Project Description, Version 3* (Tiverton, Ontario: Bruce Power, January 2007).

(Campbell et al, 2007)
Kurt M. Campbell et al, *The Age of Consequences: The Foreign Policy and National Security Implications of Global Climate Change* (Washington, DC: Center for Strategic and International Studies, Center for a New American Security, November 2007).

(CBC News, 2008a)
CBC News, "Development halted on 2 new medical isotope reactors", 16 May 2008, accessed at <http://www.cbc.ca/technology/story/2008/05/16/aecl-maple.html> on 21 May 2008.

(CBC News, 2008b)
CBC News, "Nuclear safety watchdog head fired for 'lack of leadership': minister", 16 January 2008, accessed at <http://www.cbc.ca/canada/story/2008/01/16/keen-firing.html> on 21 May 2008.

(CBC News, 2008c)
CBC News, "Nuclear location decision expected next month", 26 May 2008, accessed at <http://www.cbc.ca/money/story/2008/05/26/nuclear-site.html> on 3 June 2008.

(CEAA, 2008)
Canadian Environmental Assessment Agency, *Guidelines for the Preparation of the Environmental Impact Statement for Bruce Power's New Nuclear Power Plant Project, Draft* (Ottawa: CEAA, April 2008).

(CNSC, 2008)
Canadian Nuclear Safety Commission, "Written submissions regarding the request by Greenpeace Canada on the release of the Pickering B Probabilistic Risk Assessment Document, CMD 08-H4.29", 11 April 2008.

(CNSC, 2007a)
Canadian Nuclear Safety Commission, *Design of New Nuclear Power Plants, RD-337, Draft* (Ottawa: CNSC, October 2007).

(CNSC, 2007b)
Canadian Nuclear Safety Commission, *Site Evaluation for New Nuclear Power Plants, RD-346, Draft* (Ottawa: CNSC, October 2007).

(CNSC, 2007c)
Canadian Nuclear Safety Commission, *Regulatory Independence: Law, Practice and Perception – A Report to the Canadian Nuclear Safety Commission* (Ottawa: CNSC, August 2007).

(CNSC, 2006)
Canadian Nuclear Safety Commission, *Licensing Process for New Nuclear Power Plants in Canada, INFO-0756* (Ottawa: CNSC, February 2006).

(Cousins and Reichmuth, 2007)
Tom Cousins and Barbara Reichmuth, "Preliminary Analysis of the Economic Impact of Selected RDD Events in Canada", presentation at the CRTI Summer Symposium 2007, Gatineau, Quebec, 11-14 June 2007. CRTI is the CBRNE Research and Technology Initiative, a program of Defence Research and Development Canada. The conference proceedings (available from CRTI) list the presentation as CRTI 05-0043RD, titled "Economic Impact of Radiological Terrorist Events".

(Cummins et al, 2003)
W. E. Cummins and two other authors (all from Westinghouse Electric Company), "Westinghouse AP1000 Advanced Passive Plant", Proceedings of ICAPP '03, Cordoba, Spain, 4-7 May 2003, Paper 3235.

(Dallaire et al, 2008)
Mark Dallaire and two other authors, Information and Recommendations from Canadian Nuclear Safety Commission (CNSC) Staff regarding Regulatory Documents RD-346 and RD-337, a document submitted to the CNSC Commissioners for approval at the Commission meeting of 10 June 2008. The document was published on 27 May 2008.

(DOE, 1987)
US Department of Energy, *Health and Environmental Consequences of the Chernobyl Nuclear Power Plant Accident, DOE/ER-0332* (Washington, DC: DOE, June 1987).

(Duncan, 2006)
Dwight Duncan, Ontario Minister of Energy, letter to Jan Carr, CEO of Ontario Power Authority, Re: Integrated Power System Plan, 13 June 2006.

(EPSRC, 2007)
Engineering and Physical Sciences Research Council, Details of Grant EP/F001444/1, "Sustainability Assessment of Nuclear Power: An Integrated Approach", accessed on 6 December 2007 at <http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/F001444/1>.

(European Commission, 2007)
Directorate-General for Research, European Commission, *The Sustainable Nuclear Energy Technology Platform: A vision report, EUR 22842* (Brussels: European Communities, 2007).

(Fischer and Szasz, 1985)
David Fischer and Paul Szasz, *Safeguarding the Atom: A Critical Appraisal* (London: Taylor and Francis, 1985).

(Forsberg and Reich, 1991)
Charles W. Forsberg and William J. Reich, *Worldwide Advanced Nuclear Power Reactors with Passive and Inherent Safety: What, Why, How, and Who* (Oak Ridge, Tennessee: Oak Ridge National Laboratory, September 1991).

(GAO, 2007)
US Government Accountability Office, *Crude Oil: Uncertainty about Future Oil Supply Makes It Important to Develop a Strategy for Addressing a Peak and Decline in Oil Production, GAO-07-283* (Washington, DC: GAO, February 2007).

(Gibson, 2000)
Robert B. Gibson, "Favouring the Higher Test: Contribution to Sustainability as the Central Criterion for Reviews and Decisions under the Canadian Environmental Assessment Act", *Journal of Environmental Law and Practice*, Volume 10, 2000, pp 39-56.

(Government of Canada, 2007)
Government of Canada, "Cabinet Directive on Streamlining Regulation", came into effect 1 April 2007, accessed at <http://www.regulation.gc.ca> on 17 December 2007.

(Greenpeace International, 2007)
Greenpeace International, *Nuclear Power is Not the Answer to Climate Change* (Amsterdam: Greenpeace International, 2007).

(Hannerz, 1983)
K. Hannerz, *Towards Intrinsically Safe Light Water Reactors* (Oak Ridge, Tennessee: Institute for Energy Analysis, February 1983).

(Harvie, 2004)
J. D. Harvie, *Review of Licensing Approach Proposed for the Advanced CANDU Reactor* (Ottawa: CNSC, consultant report RSP-0184C, September 2004).

(Hirsch et al, 2005)
Helmut Hirsch and three other authors, *Nuclear Reactor Hazards: Ongoing Dangers of Operating Nuclear Technology in the 21st Century* (Amsterdam: Greenpeace International, April 2005).

(Hirsch et al, 1989)
H. Hirsch and three other authors, *IAEA Safety Targets and Probabilistic Risk Assessment* (Hannover, Germany: Gesellschaft fur Okologische Forschung und Beratung, August 1989).

(Homer-Dixon, 2007)
Thomas Homer-Dixon, *The Upside of Down: Catastrophe, Creativity, and the Renewal of Civilization* (Toronto: Vintage Canada, 2007).

(IAEA, 2008)
International Atomic Energy Agency, "IAEA Generic Review for UK HSE of New Reactor Designs against IAEA Safety Standards", prepared for UK Health and Safety Executive, 3 March 2008, revised 14 March 2008, accessed at <http://www.hse.gov.uk/newreactors/technicalreports.htm> on 20 May 2008.

(IAEA, 2006a)
International Atomic Energy Agency, *Nuclear Power and Sustainable Development* (Vienna: IAEA, April 2006).

(IAEA, 2006b)
International Atomic Energy Agency, *Advanced nuclear plant design options to cope with external events, IAEA-TECDOC-1487* (Vienna: IAEA, February 2006).

(IAEA, 2003)
International Atomic Energy Agency, *Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3* (Vienna: IAEA, November 2003).

(IAEA, 2000)
International Atomic Energy Agency, *Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1* (Vienna: IAEA, September 2000).

(Infrastructure Ontario, 2008)
Infrastructure Ontario, Request for Proposals, Nuclear Procurement Project, RFP No. OIPC 08-00-1027, 7 March 2008.

(IPCC, 2007)
Intergovernmental Panel on Climate Change, *Fourth Assessment Report, Climate Change 2007: Synthesis Report* (Geneva: IPCC, 2007).

(IRSS, 1992)
Institute for Resource and Security Studies, *Risk Implications of Potential New Nuclear Plants in Ontario* (Toronto: Coalition of Environmental Groups for a Sustainable Energy Future, November 1992).

(Justice Department, 2007)
Canada Department of Justice, "Canadian Environmental Assessment Act (1992, c. 37)", current to 1 December 2007, accessed at <http://laws.justice.gc.ca> on 5 January 2008.

(MacKenzie, 2008)
Rennie MacKenzie, "AECL abandons plans to develop Maple isotope production reactors", *Nucleonics Week*, Volume 49, Number 21, 22 May 2008.

(Makhijani, 2007)
Arjun Makhijani, *Carbon-Free and Nuclear-Free: A Roadmap for US Energy Policy* (Muskegon, Michigan: RDR Books, 2007).

(MEA, 2005)
Millennium Ecosystem Assessment, *Ecosystems and Human Well-Being: Synthesis* (Washington, DC: Island Press, 2005).

(National Research Council, 2006)
National Research Council Committee on the Safety and Security of Commercial Spent Nuclear Fuel Storage (a committee of the Council's Board on Radioactive Waste Management), *Safety and Security of Commercial Spent Nuclear Fuel Storage: Public Report* (Washington, DC: National Academies Press, 2006).

(NEA, 2000)
Nuclear Energy Agency, *Nuclear Energy in a Sustainable Development Perspective* (Paris: OECD, 2000).

(NERAC/GIF, 2002)
Nuclear Energy Research Advisory Committee (US Department of Energy) and Generation IV International Forum, *A Technology Roadmap for Generation IV Nuclear Energy Systems, GIF-002-00* (Washington, DC: DOE, December 2002).

(NRC, 1994)
US Nuclear Regulatory Commission, "10 CFR Part 73, RIN 3150-AE81, Protection Against Malevolent Use of Vehicles at Nuclear Power Plants", *Federal Register,* Volume 59, Number 146, 1 August 1994, pp 38889-38900.

(NRC, 1990)
US Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, NUREG-1150* (Washington, DC: Nuclear Regulatory Commission, December 1990).

(NRC, 1975)
US Nuclear Regulatory Commission, *Reactor Safety Study, WASH-1400 (NUREG-75/014)* (Washington, DC: Nuclear Regulatory Commission, October 1975).

(Okrent, 1981)
David Okrent, *Nuclear Reactor Safety: On the History of the Regulatory Process* (Madison, Wisconsin: University of Wisconsin Press, 1981).

(Overbye et al, 2002)
Thomas J. Overbye and three other authors, *National Energy Supergrid Workshop Report* (Urbana-Champaign, Illinois: University of Illinois, November 2002).

(Parsons, 2006)
Robert Parsons, "Chornobyl 20 Years After: A Nuclear Nightmare Becomes a Political Disaster", Radio Free Europe / Radio Liberty, 20 April 2006, accessed at <http://www.rferl.org> on 10 January 2008.

(Raskin et al, 2002)
Paul Raskin et al, *Great Transition: The Promise and Lure of the Times Ahead* (Boston, Massachusetts: Stockholm Environment Institute, 2002).

(Romm, 2008)
Joe Romm, *The Self-Limiting Future of Nuclear Power* (Washington, DC: Center for American Progress Action Fund, June 2008).

(Sahely et al, 2005)
Halia R. Sahely and two other authors, "Developing sustainability criteria for urban infrastructure systems", *Canadian Journal of Civil Engineering*, Volume 32, 2005, pp 72-85.

(Schneider and Froggatt, 2007)
Mycle Schneider and Antony Froggatt, *The World Nuclear Industry Status Report 2007* (Brussels: Greens-EFA Group in the European Parliament, November 2007).

(SENES, 2007)
SENES Consultants Limited, *Credible Malfunction and Accident Scenarios Technical Support Document (Final), Refurbishment and Continued Operation of Pickering B Nuclear Generating Station Environmental Assessment* (Richmond Hill, Ontario: SENES Consultants, December 2007).

(Thompson, 2007)
Gordon R. Thompson, *Risk-Related Impacts from Continued Operation of the Indian Point Nuclear Power Plants* (Cambridge, Massachusetts: Institute for Resource and Security Studies, 28 November 2007).

(Thompson, 2000)
Gordon Thompson, *A Review of the Accident Risk Posed by the Pickering 'A' Nuclear Generating Station* (Cambridge, Massachusetts: Institute for Resource and Security Studies, August 2000).

(Thompson, 1998)
Gordon Thompson, "Science, democracy and safety: why public accountability matters", in: F. Barker (editor), *Management of Radioactive Wastes: Issues for local authorities* (London: Thomas Telford Ltd., 1998).

(Wade, 2000)
David C. Wade, "21st Century Energy Sustainability – Nuclear's Role", paper submitted to the IAEA meeting, Contribution of Advanced Reactors for Sustainable Development, Vienna, 12-16 June 2000; Argonne National Laboratory Document ANL/RA/CP-102184.

(Watson et al, 1972)
M. B. Watson and four other authors, *Underground Nuclear Power Plant Siting* (Pasadena, California: Environmental Quality Laboratory, California Institute of Technology, September 1972).

(Westinghouse, 2007)
Westinghouse Electric Company, "Ready to Meet Tomorrow's Power Generation Requirements Today, AP1000", 2007, accessible at <http://www.ap1000.westinghousenuclear.com/>.

**Table 3-1**
**Safety Goals for a New Nuclear Power Plant, as Specified in CNSC Draft Regulatory Document RD-337**

| Type of Outcome | Safety Goals | |
|---|---|---|
| | Sum of frequencies of all event sequences that can lead to this outcome …….. | |
| | Should be less than | Shall not exceed |
| Small Release to the Environment (more than 1,000 TBq of Iodine-131) | 1 per 1 million plant-years | 1 per 100,000 plant-years |
| Large Release to the Environment (more than 100 TBq of Cesium-137) | 1 per 10 million plant-years | 1 per 1 million plant-years |
| Core Damage (significant core degradation) | 1 per 1 million plant-years | 1 per 100,000 plant-years |

**Notes:**
(a) The table as shown describes the safety goals set forth at: Canadian Nuclear Safety Commission, *Design of New Nuclear Power Plants, RD-337, Draft*, Ottawa: CNSC, October 2007, page 5.
(b) On 27 May 2008, the CNSC Staff published a document containing a revised version of RD-337, which the Staff submitted to the CNSC Commissioners for approval at the Commission meeting of 10 June 2008. At page 5 of the revised RD-337, revised safety goals are set forth, exhibiting the following changes from the table above. First, the numerical goals in the "should be less than" category are abandoned. Second, the numerical goals in the "shall not exceed" category are retained, but with different language. The revised RD-337 states that the sum of frequencies of all event sequences that can lead to a specified outcome "is less than" a numerical value. Each of these changes represents a significant weakening of the safety goals.

**Table 3-2**
**Selected Options to Reduce the Risk of a Spent-Fuel-Pool Fire at a Nuclear Power Plant that Employs High-Density Pool Storage**

| Option | Passive or Active? | Does Option Address Fire Scenarios Arising From: | | Comments |
|---|---|---|---|---|
| | | Malevolent Acts? | Other Events? | |
| Re-equip pool with low-density, open-frame racks | Passive | Yes | Yes | • Would substantially reduce pool inventory of radioactive material<br>• Would prevent auto-ignition of fuel in almost all cases |
| Install emergency water sprays above pool | Active | Yes | Yes | • Spray system must be highly robust<br>• Spraying water on overheated fuel could feed Zr-steam reaction |
| Mix hotter (younger) and colder (older) fuel in pool | Passive | Yes | Yes | • Could delay or prevent auto-ignition in some cases<br>• Would be ineffective if debris or residual water block air flow<br>• Could promote fire propagation to older fuel |
| Minimize movement of spent-fuel cask over pool | Active | No (Most cases) | Yes | • Could conflict with adoption of low-density, open-frame racks |
| Deploy air-defense system (e.g., Sentinel and Phalanx) at plant | Active | Yes | No | • Implementation would require presence of military personnel at plant |
| Develop enhanced onsite capability for damage control | Active | Yes | Yes | • Would require new equipment, staff and training<br>• Personnel must function in extreme environments |

**Table 3-3**
**Some Potential Modes and Instruments of Attack on a Nuclear Power Plant**

| Attack Mode/Instrument | Characteristics | Present Defenses at US Plants |
|---|---|---|
| Commando-style attack | • Could involve heavy weapons and sophisticated tactics<br>• Successful attack would require substantial planning and resources | Alarms, fences and lightly-armed guards, with offsite backup |
| Land-vehicle bomb | • Readily obtainable<br>• Highly destructive if detonated at target | Vehicle barriers at entry points to Protected Area |
| Small guided missile (anti-tank, etc.) | • Readily obtainable<br>• Highly destructive at point of impact | None if missile launched from offsite |
| Commercial aircraft | • More difficult to obtain than pre-9/11<br>• Can destroy larger, softer targets | None |
| Explosive-laden smaller aircraft | • Readily obtainable<br>• Can destroy smaller, harder targets | None |
| 10-kilotonne nuclear weapon | • Difficult to obtain<br>• Assured destruction if detonated at target | None |

**Source:**
Gordon R. Thompson, *Risk-Related Impacts from Continued Operation of the Indian Point Nuclear Power Plants*, Cambridge, Massachusetts: Institute for Resource and Security Studies, 28 November 2007, Table 7-4. Further citations are provided in that table and its supporting narrative.

**Table 3-4**
**The Shaped Charge as a Potential Instrument of Attack**

| Category of Information | Selected Information in Category |
|---|---|
| General information | • Shaped charges have many civilian and military applications, and have been used for decades<br>• Applications include human-carried demolition charges or warheads for anti-tank missiles<br>• Construction and use does not require assistance from a government or access to classified information |
| Use in World War II | • The German MISTEL, designed to be carried in the nose of an un-manned bomber aircraft, is the largest known shaped charge<br>• Japan used a smaller version of this device, the SAKURA bomb, for kamikaze attacks against US warships |
| A large, contemporary device | • Developed by a US government laboratory for mounting in the nose of a cruise missile<br>• Described in detail in an unclassified, published report (citation is voluntarily withheld here)<br>• Purpose is to penetrate large thicknesses of rock or concrete as the first stage of a "tandem" warhead<br>• Configuration is a cylinder with a diameter of 71 cm and a length of 72 cm<br>• When tested in November 2002, created a hole of 25 cm diameter in tuff rock to a depth of 5.9 m<br>• Device has a mass of 410 kg; would be within the payload capacity of many general-aviation aircraft |
| A potential delivery vehicle | • A Beechcraft King Air 90 general-aviation aircraft will carry a payload of up to 990 kg at a speed of up to 460 km/hr<br>• A used King Air 90 can be purchased in the US for $0.4-1.0 million |

**Source:**
Gordon R. Thompson, *Risk-Related Impacts from Continued Operation of the Indian Point Nuclear Power Plants*, Cambridge, Massachusetts: Institute for Resource and Security Studies, 28 November 2007, Table 7-6. Further citations are provided in that table and its supporting narrative.

**Table 3-5**
**Proposed Classification of Potential Accidents and Malfunctions at a New Nuclear Power Plant**

| Mode of Impact of Accident or Malfunction | Type of Accident or Malfunction | | |
|---|---|---|---|
| | **Accidents Initiated by Internal Events** | **Accidents Initiated by External Events** | **Releases and Diversions Initiated by Intentional, Malevolent Acts** |
| Unplanned release of radioactive material from the reactor core | X | X | X |
| Unplanned release of radioactive material from stored spent fuel | X | X | X |
| Unplanned release of radioactive or hazardous chemical material from another part of the plant | X | X | X |
| Diversion of fissile or radioactive material for illicit use | Not applicable | Not applicable | X |

**Note:**
The symbol X indicates that the potential for accidents and malfunctions in the designated category should be assessed in an EIS.

**Table 4-1**
**Safety Objectives for New Nuclear Power Plants, as Specified in IAEA Safety Standards Series Document NS-R-1**

| Objective | Characteristics of Objective |
|---|---|
| General Nuclear Safety Objective | • Protect individuals, society and the environment from harm by establishing and maintaining effective defenses against radiological hazards |
| Radiation Protection Objective | • Ensure that, in all operational states, radiation exposure within the plant, or due to any planned release of radioactive material from the plant, is kept below prescribed limits and as low as reasonably achievable<br>• Ensure mitigation of the radiological consequences of any accident |
| Technical Safety Objective | • Take all reasonably practicable measures to prevent accidents and to mitigate their consequences should they occur<br>• Ensure, with a high level of confidence, that the radiological consequences of any accident taken into account in designing the plant would be minor and below prescribed limits<br>• Ensure that the likelihood of accidents with serious radiological consequences is extremely low |

**Source:**
International Atomic Energy Agency, *Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1*, Vienna: IAEA, 2000, pp 3-4.

**Table 4-2**
**Hierarchy of Nuclear Power Plant Design Characteristics Relevant to Safety, as Specified in IAEA Safety Standards Series Document NS-R-1**

| **Preference in Selecting a Plant Design Feature** | **Design Characteristics Relevant to Safety**<br>**The expected plant response to any postulated initiating event shall be those of the following that can reasonably be achieved ……** |
|---|---|
| First Preference | No significant safety-related effect, or a change toward a safe condition by virtue of inherent characteristics of the plant |
| Second Preference | The plant is rendered safe by passive safety features, or by the action of safety systems that are continuously operating |
| Third Preference | The plant is rendered safe by the action of safety systems that are brought into service in response to the initiating event |
| Fourth Preference | The plant is rendered safe by specified procedural actions |

**Source:**
International Atomic Energy Agency, *Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1*, Vienna: IAEA, 2000, page 11.

**Table 4-3**
**Proposed Safety Criteria for Design and Siting of a New Nuclear Power Plant**

| Application of Criteria | Criteria |
|---|---|
| Safety performance of the plant during reactor operation (design-basis criteria) | No significant damage of the reactor core or adjacent stored spent fuel in the event of:<br>• Loss of all electrical power (AC & DC), compressed air, other power sources, and normal heat sinks for an extended period (e.g., 1 week);<br>• Abandonment of the plant by operating personnel for an extended period (e.g., 1 week);<br>• Takeover of the plant by hostile, knowledgeable persons who are equipped with specified explosive devices, for a specified period (e.g., 8 hours);<br>• Military attack by specified means (e.g., 1,000-pound air-dropped bombs);<br>• An extreme, specified earthquake;<br>• Conceivable erroneous operator actions that could be accomplished in a specified period (e.g., 8 hours); or<br>• Any combination of the above. |
| Safety performance of the plant during reactor refueling (design-basis criteria) | A specified maximum release of radioactive material to the accessible environment in the event of:<br>• Loss of reactor coolant at a specified time after reactor shut-down, with replacement of the coolant by fluid (e.g., air, steam, or unborated water) creating the chemical and nuclear reactivity that would maximize the release of radioactive material, at a time when the plant's containment is most compromised; and<br>• Any combination of the events specified above, in the context of reactor operation. |
| Site specification (radiological-impact criteria) | In the event of the maximum release of radioactive material specified above, in the context of reactor refueling, radiological impacts would not exceed specified values regarding:<br>• Individual dose;<br>• Population dose; and<br>• Land areas in various usage categories that would be contaminated above specified levels. |

**Note:**
The criteria in the first two rows of this table would apply to spent fuel stored adjacent to the reactor core. Separate criteria would apply to an independent facility for storing spent fuel, whether onsite or offsite.