nwmo
NUCLEAR WASTE MANAGEMENT ORGANIZATION
SOCIÉTÉ DE GESTION DES DÉCHETS NUCLÉAIRES

January 2004

NWMO BACKGROUND PAPERS
3. HEALTH AND SAFETY

3-4 CONSIDERATIONS IN DEVELOPING A SAFETY CASE FOR SPENT NUCLEAR FUEL MANAGEMENT FACILITIES AND ASSOCIATED INFRASTRUCTURE IN CANADA

Katherine Moshonas Cole, Patrick Reid & Ross Rock
Candesco Research Corporation

NWMO Background Papers

NWMO has commissioned a series of background papers which present concepts and contextual information about the state of our knowledge on important topics related to the management of radioactive waste. The intent of these background papers is to provide input to defining possible approaches for the long-term management of used nuclear fuel and to contribute to an informed dialogue with the public and other stakeholders. The papers currently available are posted on NWMO's web site. Additional papers may be commissioned.

The topics of the background papers can be classified under the following broad headings:

1. **Guiding Concepts** – describe key concepts which can help guide an informed dialogue with the public and other stakeholders on the topic of radioactive waste management. They include perspectives on risk, security, the precautionary approach, adaptive management, traditional knowledge and sustainable development.
2. **Social and Ethical Dimensions** - provide perspectives on the social and ethical dimensions of radioactive waste management. They include background papers prepared for roundtable discussions.
3. **Health and Safety** – provide information on the status of relevant research, technologies, standards and procedures to reduce radiation and security risk associated with radioactive waste management.
4. **Science and Environment** – provide information on the current status of relevant research on ecosystem processes and environmental management issues. They include descriptions of the current efforts, as well as the status of research into our understanding of the biosphere and geosphere.
5. **Economic Factors** - provide insight into the economic factors and financial requirements for the long-term management of used nuclear fuel.
6. **Technical Methods** - provide general descriptions of the three methods for the long-term management of used nuclear fuel as defined in the NFWA, as well as other possible methods and related system requirements.
7. **Institutions and Governance** - outline the current relevant legal, administrative and institutional requirements that may be applicable to the long-term management of spent nuclear fuel in Canada, including legislation, regulations, guidelines, protocols, directives, policies and procedures of various jurisdictions.

Disclaimer

Candesco Research Corporation

Considerations in Developing a Safety Case for Spent Nuclear Fuel Management Facilities and Associated Infrastructure in Canada

A Report Submitted to the Nuclear Waste Management Organization

Jan. 30, 2004

File NWMO_SC-R-00012-0

	Candesco Research Corporation	Rev Date: Jan. 30, 2004	Status: Issued
	Subject: Considerations in Developing a Safety Case for Spent Nuclear Fuel Management Facilities and Associated Infrastructure in Canada		File: NWMO_SC-R-00012-0

Issue 0D0	**Reason for Issue:** Initial outline draft for feedback from NWMO				
	Author: P. Reid R. Rock D. Lau	Verifier:	Reviewer:	Approver:	Date: Nov. 26, 2003
Issue 0D2	**Reason for Issue:** First draft incorporating all sections for review by NWMO				
	Author: K. M. Cole, P. Reid, R. Rock	Verifier:	Reviewer: G. Archinoff	Approver: P. Reid	Date: Dec. 19, 2003
Issue 0D3	**Reason for Issue:** Second draft, incorporating comments from NWMO, for NWMO expert review				
	Author: K.M. Cole, P. Reid, R. Rock	Verifier:	Reviewer: G. Archinoff	Approver: P. Reid	Date: Dec. 30, 2003
Issue	**Reason for Issue:**				
	Author:	Verifier:	Reviewer:	Approver:	Date:
Document Classification: Technical Document			Security Classification: PROTECTED-Commercial		

Table of Contents

Executive Summary

The long-term management of spent nuclear fuel must satisfy the concerns of the public, and meet the needs of regulatory, technical and government authorities. These authorities are committed to a number of safety objectives such as public safety, environmental protection, worker safety, material safety and security. The process for providing the confidence that these safety objectives will be met has evolved over many years of experience in risk industries into the requirement for a complete Safety Case.

The first objective of this paper is to provide an understanding of what is the nature of a Safety Case. That is, what are the key components that are necessary to build and communicate a convincing argument that a proposal has sound engineering, is environmentally safe, and will meet all regulatory requirements. The second objective is to describe what is involved in a Safety Case for options now being considered for the long-term management of nuclear fuel waste. The information in this document has been compiled from Canadian and international sources, and is consistent with the requirements of the Canadian nuclear regulator, The Canadian Nuclear Safety Commission (CNSC).

The Safety Case is the integration of arguments and evidence that describe, quantify and substantiate the safety, and the level of confidence in the safety, of a facility or activity. Concurrent with the advancement of Safety Case concepts has been the evolution of requirements in Canadian regulations for licensing facilities and associated activities. The licensing requirements are consistent with the Safety Case. In essence, if all the requirements for licensing are met, the information required for a complete Safety Case would also then be available. However, a Safety Case would also need to be well structured to assist in the communication of the conclusions on safety and the development of confidence in these conclusions.

The Safety Case must include the following:

(1) A **framework** within which the information – arguments or analyses and facts or evidence – must be presented. The key categories describing the framework for the Safety Case are:

- Organization and Scope
- Quality Assurance
- Safety Philosophy, Principles and Criteria

(2) A **complete set of facts** about the undertaking that provide the base of information for further analyses and assessments. This should include a description of the facilities and the activities proposed; a description of the procedures and processes for decision making; and the criteria and limits that will be imposed for the operation or performance of activities. The key categories describing the base of information for the Safety Case are:

- Documented Design
- Description of Activities and Facility Operation Program
- Public Safety and Protection of the Environment

- Occupational Safety
- Security and Safeguards

(3) The **analyses, assessments and arguments** that demonstrate satisfactory resolution of the safety issues raised. The set of information provided, specifically including the documented design and description of operation, is used to analyze the proposed facilities and activities and to evaluate the potential hazards. The ability of the design to address any issues raised is then evaluated by applying specifications for safety, determined through regulations, international recommendations, or best practices. Naturally, radiological hazards are emphasized in performing analyses for nuclear facilities, however all hazards must be addressed in the Safety Case. The analyses and assessments must be performed within the framework described and shown to be consistent with the collection of facts as documented. The key categories describing the analyses and assessments for the Safety Case are:

- Safety Analysis
- Accident Management
- External Hazards

The challenge in developing the safety case for the long-term management of spent nuclear fuel is to address all the phases of activity before and after long-term storage and before and after final disposal. This would include the overall approach to the long-term management solution being addressed, which includes the activities to handle the spent fuel, to contain and package it as required, transportation of spent fuel, handling the receipt of the spent fuel and its interim storage or final disposal.

The extended period of time for which an assessment would need to be valid makes the challenge even greater, as the time frames that have been considered in most developed Safety Cases include actual experience and verified performance of components and materials and predictable environmental conditions.

In reviewing the eleven key categories mentioned above and the lists of required information for each, it becomes clear that there is much work to do to establish a comprehensive Safety Case that is both technically sound and acceptable to two key stakeholders, the regulator and the public. The following recommendations are made to the NWMO in the context of furthering its work in these two critical areas.

1. To continue efforts to determine areas of greatest public concern with respect to spent nuclear fuel management and to make this information available for the development of the Safety Case.

2. To begin discussions with the CNSC to develop a working understanding of expectations with respect to regulations and standards, as well as methodologies needed for developing the Safety Case.

3. To further define the elements of the Safety Case applicable to the specific options and to assess the difficulty of meeting the requirements.

4. To interact with organizations in other jurisdictions that are involved in spent fuel management, specifically to better understand good industry practices, develop benchmark approaches with respect to safety and public acceptance, and learn lessons regarding technical acceptance criteria, obtaining regulatory approval and achieving public acceptance.

Glossary

AECB	Atomic Energy Control Board: former name of the CNSC
ALARA	As Low As Reasonably Achievable: an approach to radiation protection that emphasizes dose reduction when already below acceptable dose limits
CANDU	CANadian Deuterium natural Uranium: a Canadian power reactor design
CEAA	Canadian Environmental Assessment Act
CNSC	Canadian Nuclear Safety Commission: The Canadian nuclear regulator
EA	Environmental Assessment
IAEA	International Atomic Energy Agency
NPD	Nuclear Power Demonstration: an early CANDU reactor
NRX	Nuclear Reactor eXperimental: an early Canadian research reactor
NSCA	Nuclear Safety and Control Act
NWMO	Nuclear Waste Management Organization
QA	Quality Assurance

1 What is a Safety Case?

The Safety Case

The “Safety Case” is the documented disposition of all safety issues for a facility.

The term *safety case*, as applied to the context of spent nuclear fuel management in Canada, can be broadly defined as the documented disposition of all safety issues related to a particular management approach. “The Safety Case is the integration of arguments and evidence that describe, quantify and substantiate the safety and the level of confidence in the safety”[1]. The safety issues themselves cover a wide spectrum from the general, high level to extremely intricate, expert-level details. The substantiation of safety and confidence thereof can be achieved through the identification, elimination, mitigation and containment of risks associated with a proposed facility or activity. In general terms, the risk of an accident or failure is the combination of likelihood and consequence. Therefore an extremely unlikely accident with a significant consequence yields an overall risk level comparable to a very likely failure with minor consequence. In the safety case process, however, scenarios with low risk but significant consequence are often given a higher degree of scrutiny. This is because consequence is often perceived as the more important element risk, by both the regulators and the public. The probability of a major catastrophe that causes significant fatalities may be virtually zero; however the fact that such a large consequence accident cannot be proven impossible requires a thorough demonstration of safety, despite the low risk.

The safety case is a key aspect of the process to obtain regulatory and public acceptance to site, construct and operate a waste management facility. Other important aspects include public communication processes, and the discharge of many legal and financial obligations. Furthermore, the safety case itself is not focused exclusively on technical or engineering issues; however these comprise the bulk of the effort expended in the safety case process. As will be discussed in later sections, many aspects of the safety case involve public consultation, which may lead to the disposition of issues that are not technical in nature, but nevertheless must be addressed in order to achieve public confidence in the safety of a facility.

Understanding and knowledge of the development of the underlying safety issues, their probability, consequences and risks will establish the context of the safety case. In other words, it will provide a background for what the safety case is, how it is addressed, and why it has evolved into its current form.

1.1 Emergence of Engineers as Responsible for Public Safety and Regulation of the Profession

In a broad sense, the Industrial Revolution represented a change from the use of small, simple machines built by craftsmen to the widespread mass production of large, complex machinery that could perform labours and harness power far in excess of any manual workforce. In the very early decades of this period, the engineer, as designer of the machines, was largely indistinguishable from a skilled craftsman; the development and improvement of the machines was largely done through trial and error, albeit with the application of scientific methods of control and measurement. Such machinery tended to be “human” in scale. Materials used did not permit very high torques, speeds or pressures, therefore failure of such components were primarily dangerous only to those in close proximity.

With improvements in manufacturing accuracy (for example, true cylinders with tight fitting pistons in steam engines), engineers were able to design and construct larger, more powerful engines. In the mid-nineteenth century, engineers merged the scientific methods of previous generations with the emerging scientific knowledge of thermodynamics to optimize designs and to develop entirely new concepts of power production and its practical application[2]. The successes of engineers in production of power and machinery on large scales led directly to widespread use of these technologies by the public. The caveat of this widespread use, however, is that failure of the technology can lead to consequences far more severe than when machines were simple, slow and relatively underpowered.

A practical example of this relationship between the increased use of technology by the public and their resulting exposure to failures of this technology is the development of European railways in the eighteenth and early nineteenth centuries. Between 1850 and 1914, the railroad system in Europe increased from 35,000 to one million kilometres of track[3]. In 1880, the French railway system carried 18 million passengers and by 1913 this increased over 30-fold to 547 million passengers. By 1914, the railways of Britain, France and Germany carried 6 billion passengers annually. Trains were larger, more powerful, and carried more people at ever faster speeds. This meant fault tolerances in design, materials and operation had to be improved; whereas the derailment of a small locomotive at 20 km/h in 1850 would be unlikely to injure more than a few people, an accident involving a 300-person passenger train traveling at 100 km/h in 1900 would be far more catastrophic. Similarly, the steam boilers used on increasingly powerful locomotives (as well as stationary machinery) were operating at higher temperatures and pressures. Accidents did happen, sometimes with significant loss of life (for example, in 1917 in Modane, France, an overloaded train carrying 1,000 French soldiers could not brake while travelling down a steep decline, leading to a derailment and over 800 deaths in the subsequent fire.)

In step with the expansion of the railway, governments responded by passing regulations that would protect the public through establishment of laws governing the designs produced by engineers (such as acts governing boiler and pressure vessels), and regulations governing the operations of facilities and equipment, as well as the engineers themselves. With their long history as craftsmen, engineers had originally organized themselves into guilds and related groups; the establishment of a regulatory environment subsequently led to the emergence of an engineering profession. Through the codification of laws and statutes, engineers assumed legal responsibility for the performance of their designs, as measured against the established regulations. Accidents often led to inquiries, both public and within the industry itself, to determine what failures led to the accident, and how improvements could be made to design and operation to minimize the likelihood of future failures. Whereas consequences of serious failure increased with the widespread use of larger machines, risk to the public was managed by the reduction in the probability of such failures (although public perception still tends to emphasize consequence over likelihood.) Due to the specialized nature of the technology, engineers were often the authors of their own regulations. This progression of events occurred in several industries, including transportation, power, construction, and manufacturing.

Beyond the laws, statutes and codes governing various aspects of engineered systems, responsibility of professional engineers to public safety is codified in provincial laws in Canada. In Ontario, for example, the Professional Engineers Act and associated Regulations apply. Section 77(2) of Ontario Regulation 941 reads, "A practitioner shall... regard the practitioner's duty to public welfare as paramount." Thus the engineer, in the role of the designer, must not forget the impact of the designs on the public well being. At one level, this applies to protecting the public from harm, and early nuclear safety regulations took this approach. More recently, however, consideration of public welfare has expanded to include protection of the environment.

1.2 Early Development of Nuclear Safety in Canada

The development of nuclear safety in Canada follows a similar trajectory to that of railways in Europe. In the 1940's, early nuclear research efforts were "bench scale" in size, where safety concerns were largely limited to protecting the experimenters from inadvertent exposure during tests. In the late 1940's, development of the first large scale Canadian experimental reactor, the NRX, did not identify reactor safety as a distinct topic although safe and controlled operation was a key design requirement [4]. Shielding was designed to protect the operators, and consideration was given to the atmospheric dispersion of radioactive releases. The site, Chalk River, Ontario, was chosen partially because of its isolation from populated areas. In addition, the original NRX design provided two different methods of controlling the reactor.

Despite the efforts of the designers, on December 12th, 1952 the NRX was seriously damaged in an accident. An experiment was underway, and the reactor was being operated outside of its normal mode. An operator error led to a sequence of events that eventually damaged the reactor core and released gaseous fission products into the atmosphere.

This accident prompted several reviews, eventually leading to fundamental changes to the approach taken in reactor safety design in Canada. This included separation of shutdown from control systems and multiple channel logic on instrumentation systems. These were not only desirable design features, they became regulatory requirements.

As with the development of railway technology in the previous century, experience with nuclear power technology led to increasingly powerful designs. A significant difference between a research reactor such as the NRX and the newly emerging power reactor designs was the higher temperatures and pressures present in the latter. Whereas the failure of a coolant pipe in the NRX may have led to localized fuel damage, a similar failure in a large power reactor could have far more significant consequences, and so additional mitigating features were added to the design.

In 1957, a key paper by Siddall [4] explored the objective of reactor safety. Sidall proposed that the basic approach for judging the safety of an activity should be the number of deaths per unit time due to that activity. His observation was that society implicitly accepts the risk of many activities; the detrimental consequences of carrying out a task such as driving a car or using electricity were sufficiently unlikely that they did not overtly concern the public. Other factors may also contribute to public acceptance of a particular risk, such as the sense of being in direct control and familiarity with the technology.

Around the same time, the Nuclear Power Demonstration (NPD) facility was being designed, the first reactor to employ several design concepts unique to CANDU. In preparing the first formal safety report for the NPD (called a “hazard” report at that time), the authors employed Siddall’s concept of public risk and proposed an objective of less than one death per 100 years of operation. The Reactor Safety Advisory Committee of the Atomic Energy Control Board essentially accepted this recommendation.

Around 1960, G.C. Lawrence proposed a reference upper limit for the likelihood of a “major accident” as once per 100,000 years, based on the premise that such an accident would lead to 1,000 fatalities, thus meeting the risk requirement of one death per 100 years of operation [4]. It is virtually impossible to design any particular system such that it will not fail more than once every 100,000 years. It is similarly difficult to demonstrate the safety of a facility over a similarly long period of time. Therefore in order to demonstrate such a high level of reliability for the facility as a whole, designers had to separate systems and design facilities such that failure of several protective layers would be required to have a significant accident. Whereas any one system may exhibit failure of once per year or once per decade, simultaneous failure of several would be demonstrated to be extremely unlikely. These concepts of separation and individual system reliability were eventually codified into the design requirements published by the AECB and later the Canadian Nuclear Safety Commission (CNSC).

The early development of nuclear technology in Canada was primarily focussed on development of nuclear power plants, and similarly so too was the regulatory environment. From the perspective of the safety case, the early work of Siddall, Lawrence and the NPD designers established the relationship between public safety and design requirements. The safety case had to demonstrate that under a variety of normal operation and accident conditions, the risk to the public presented by the facility was within acceptable limits. These limits, in turn, were set at levels that were expected to present little risk to the public as well as to be reasonable, allowing practical design. These same principles are applicable to the safety case associated with a long-term waste management facility.

This relationship between public safety and design, however, is not static, as both the technology and the public perception of risk have evolved significantly since the early 1960’s, as discussed in the following section.

1.3 Evolution of the Safety Case with Increasing Technical Knowledge and Experience

The requirements for the complete presentation of a safety case have evolved over the decades due to activity, scrutiny and regulation in a range of technological activities, and specifically in industries with known risks, such as the nuclear power industry. The evolution of the Safety Case in Canada has also been a product of the Canadian approach to nuclear safety regulation where the emphasis is on demonstrating the acceptability of a design meeting performance requirements rather than design criteria, as is the case in more prescriptive regulatory environments (e.g. the United States).

By establishing performance targets for systems, Canadian designers are given the flexibility to propose solutions of their own choosing. As long as the performance requirements and general design requirements of separation and independence of safety systems were demonstrably met, the design was considered acceptable. The design process for new, larger facilities, as well as emergence of new knowledge about the operation and behaviour of existing facilities, led to the broadening of the scope and depth of the performance requirements that had to be met. As the technology matured, so too did the regulations overseeing the technology.

Similarities and Differences Between Canadian and US Regulators

Canadian Nuclear Safety Commission

- Independent agency of the Government of Canada; up to seven members appointed by Order in Council.
- Reviews and audits nuclear activities and facilities for adherence to regulations but does not direct licensees how to design or manage their facilities. Emphasis is given to the concept of a safe operating envelope.

US Nuclear Regulatory Commission

- Independent agency of the United States Government; up to five members appointed by the President and confirmed by the Senate.
- Reviews and audits nuclear activities and facilities, but emphasizes the development of detailed technical specifications that are applicable to more than one facility.

In the early 1970's, large scale nuclear plants were being built, and even larger facilities were in the late stages of design. New performance requirements emerged, such as single and dual failure dose limits. Mid-way through the design of Bruce A, engineers determined a practical containment facility would be inadequate to meet the dual-failure dose limits in the event of a loss of reactor regulation accident. Thus the concept of a second, independent shutdown system was introduced and subsequently codified as a design requirement for all power reactors thereafter.

As with the 1952 NRX accident, accidents in the 1970's and 1980's at nuclear energy facilities around the world led to the review of the design of reactors used in Canada, and to a greater awareness of the importance of the skills of the people who operate them. In 1979, a partial melting of the core occurred in Unit 2 at Three Mile Island. Deficient control room instrumentation, unfavourable response of materials used in the core, and inadequate emergency response training were determined to be root causes of the accident. These findings led to design changes within the Canadian plants to address these issues, including higher regulatory scrutiny of training programs.

In April 1986, the destruction of Chernobyl Unit 4 reinforced the vital importance of the separation of safety and control systems, the use of containment, and the operation of the facility within its safety limits. Much of what went wrong in the Chernobyl accident was already addressed in Canadian regulations (for example, Canadian power reactors require containment structures, whereas Chernobyl did not have one); however, similarities in the core designs led to the development of new accident scenarios to consider in the demonstration of safety.

Smaller failures can also lead to changes in regulatory requirements. A minor accident involving the failure of a pressure tube within Pickering Unit 2 in 1983 led to new regulations associated with the inspection and maintenance of the fuel channels, as well as a better understanding of the safety issues associated with facility ageing

In the specific case of nuclear technology, many of the most serious failures addressed in the safety analysis aspects of a safety case have never occurred. This presents a challenge for those whose duty it is to discharge or disposition those safety issues associated with those accidents or adverse conditions for which there is no direct data or first-hand experience. Computer simulation tools, therefore, have been used extensively to ascertain both the safety limits and the safety margins of a particular design under extreme conditions. Many aspects of the safety case, therefore, rely upon computer simulations of the expected behaviour or response of the facility, not direct measurements.

In the late 1980's and throughout the 1990's, the computer simulation tools used for safety analysis came under scrutiny by the Regulator. Although the simulation results themselves demonstrated the safety of the design, the accuracy of the tools used to derive the results was questioned. A large verification and validation effort was undertaken, which led to the concepts of code qualification and strict configuration control. A key aspect of code qualification is validation, the process by which scale tests and experiments can be used to provide confidence in the results of full-scale, facility-wide simulations. Future safety cases will have to address the qualification of the tools and their controls used in the design and for simulating accident conditions.

Over the past 15 years, there has been a tremendous growth in the development of the concepts of quality systems and quality management in industrial applications. The value of a safety culture and the role of good quality systems and effective management controls have been demonstrated to reduce occurrence of small failures, which were shown to be potential precursors to larger incidents. It is therefore concluded by safety managers that the likelihood of major failures is similarly reduced. Whereas previously it was sufficient to demonstrate that a facility was safe to operate based on its design, it is now necessary to demonstrate that it is also well managed and operated within a well-founded safety culture. This shifts the focus of regulation from a one-off assessment to an ongoing one. These examples demonstrate that the Safety Case is not static, but rather is a reflection of an entire body of knowledge built up with experience. Research and development, both in response to new designs as well as in the investigation of accident root causes, has led to broader understanding of the science and technology of nuclear energy projects, and subsequently refined the Safety Case needed to demonstrate the adequacy of a facility.

1.4 Evolution of the Safety Case with Public Perception and Concerns

In the past, the fundamental technical aspect of a Safety Case presented to the CNSC was demonstration of public safety by means of analysis showing that doses released in normal operation, as well as from accidents, were below targets established by the Regulations. These targets, in turn, were based on the philosophy that risks should be kept within levels acceptable to the public. Whereas the early risks were loosely based on analytical review of potentially harmful activities that were already accepted by the public and therefore implicitly considered "reasonable risks", more recently greater public scrutiny of the nuclear licensing process has changed the scope of the safety case by broadening the range of risks to be addressed.

A key evolution in the mandate of the Canadian Nuclear Safety Commission is the inclusion of protection of the environment within the laws governing nuclear regulation in Canada. Section 3 (a) of the Nuclear Safety and Control Act (NSCA) 1997 [5], states,

> *[The purpose of this Act is to provide for] the limitation, to a reasonable level and in a manner that is consistent with Canada's international obligations, of the risks to national security, the health and safety of persons and the environment that are associated with the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information.*

Another important aspect of the current regulatory environment is public participation. The CNSC is not simply a protector of the public welfare, but rather establishes a framework in which the public can actively participate in the licensing process. In Section 9 (b) of the Act, an objective of the Commission is to inform the public of the activities of both the Commission itself and those it licenses, and the effects of these activities on both the environment and public safety. Furthermore, the Act identifies the role of public hearings in the licensing process, as well as the special case of public hearings to investigate the possibility of environmental contamination due to nuclear activities [Section 46(1)].

Besides the Nuclear Safety and Control Act, the other key act associated with the safety case is the Canadian Environmental Assessment Act (1992) [6]. The CEAA assists the CNSC in discharging its duties with respect to environmental protection. In recent years, most projects involving significant changes to, or refurbishment of, nuclear facilities have undergone environmental assessments. As with the NSCA, the CEAA identifies public participation as an objective of the Act, however this does not necessarily lead to public hearings. In October 2003 the CEAA was revised to align the environmental assessment process with the requirements of the Nuclear Safety and Control Act, and to ensure that an assessment is performed before the CNSC licenses a nuclear-related project.

The safety case, therefore, is subject to open consultation with the public via a hearing process, both within the NSCA and the CEAA. The public nature of the hearing process, however, has revealed issues where the demonstration of adequate environmental and public protection has met technical requirements, but not public perception of protection. A very recent example of this is given below.

In mid-December 2002, the CNSC held public hearings on the Environmental Assessment Screening Report for the return to service of units 3 and 4 of the Bruce Nuclear Generation Station A. Forty-eight requests for public intervention were accepted by the Commission. In one submission, the assumption that the restart of the station was not likely to adversely affect the lake whitefish population was challenged. In the Screening Report, the approach taken was to assess the impact on those parts of the ecosystem most likely to be adversely affected by the project. These parts were called Valued Ecosystem Components, or VECs. This type of approach is common in such assessments, as it simplifies the problem of assessing environmental impact in a way that ensures that the predicted effects are bounding (i.e. that no other part of the ecosystem will be more adversely affected than the parts assessed in the study). VECs were initially selected by the Report’s technical specialists based on a methodology and criteria approved by the CNSC staff. In this process, round whitefish rather than lake whitefish were chosen due to the observation that the former are more common close to Bruce A. The intervenor, however, cited on-going collaborative research with Ontario Power Generation and Bruce Power on the impacts of nuclear generating stations on various whitefish population as a source of additional information about the ecology of this species that was not fully addressed in the Screening Report. Further, the intervenor expressed concern with the selection of round whitefish over lake whitefish as the VEC for the assessment based on the aforementioned process while “ignoring other criteria, notably socioeconomic importance.” The Commission replied,

> “The intent was not to say that lake whitefish is not a valuable national resource for Lake Ontario commercial fishermen, as well as for aboriginal fisheries. The intent was simply to choose a species that, because of its biological characteristics, would be more exposed to the thermal impacts and impingement/entrainment of the Bruce station.”

The intervenor, however, called into question the scientific validity of the approach taken by the Environmental Assessment Screening process that led to this conclusion. Rather than engage in a long debate regarding the validity of the approach, Bruce Power committed to amend the Report to address the specific impacts on lake whitefish, in addition to round whitefish.

This public hearing process revealed a difference between the application of a technical process and the public perception of what the process *should* have addressed. The safety case was prepared using the common methodology of selecting the most likely impacted species, whereas the intervenor was concerned that a species more important to their social and economic status was not addressed, even though the original approach did address the intervenor’s concern in a manner that was bounding.

Although this example is obtained from the hearings for the restart of a nuclear power plant, the public perception is not expected to be fundamentally different for other nuclear technologies, including waste management.

The importance of public consultation to the success of a safety case is summarized very succinctly in the Report of the Nuclear Fuel Waste Management and Disposal Concept Environmental Assessment Panel, 1998 (The Seaborn Panel, as noted in Section 3.3.5 below) [7]. The panel concluded that “without public trust and confidence, any initiative to manage nuclear fuel wastes in the long term will face difficulties.” Indeed, this comment was made in support of that Panel’s own conclusion that the disposal concept it assessed was technically but not socially acceptable.

It is difficult to determine far in advance of a public hearing process exactly where the differences between the prepared safety case and the public’s concerns will arise. Because the NSCA and CEAA allow for public intervention, simply meeting technical requirements may not always be sufficient to demonstrate an acceptable safety case in the public arena. Strategies for addressing this will have to be incorporated into the planning of the safety case.

2 Elements of a Safety Case for a Long-Term Waste Management Approach in Canada

In summary, the Safety Case is comprised of a set of requirements that, when assembled, demonstrate an acceptable level of safety of an undertaking (undertaking is used here to mean the collective facilities, operations and activities that are being proposed for any particular long-term nuclear waste management option). In developing the Safety Case for the waste management options, the undertaking would include facilities and activities required in the processing, transportation, storage, and or disposal of the nuclear fuel waste. It will include the design, construction and operation of processing, management, long-term storage or disposal, depending on the option being reviewed. The safety case will also consider design and operation of systems and components required for the transportation, as well as the transportation itself.

The list of requirements, as presented here, has been developed by grouping of detailed requirements of the Nuclear Safety and Control Act [5] and relevant Regulations [7]-[14] into general categories that would be typically used in the development of a Safety Case (see Figure 1). All of these are requirements that a proponent of a facility required for the long-term management of nuclear waste will likely be expected to demonstrate to the regulator and to the public. It is anticipated that any of the options will require the licensing of a Class 1B facility under the NSCA. Class 1B facilities include the following two categories: 1) a plant for the processing, reprocessing or separation of an isotope of uranium, thorium or plutonium, and 2) a facility for the disposal of a nuclear substance generated at another nuclear facility. Furthermore, in presenting these requirements here, consideration has also been given to international recommendations [15]

In this section, required information has been grouped into eleven categories. In order for the Safety Case to be effective, the information assembled must be complete and consistent. Some categories contain elements that are used as a basis for other categories or elements. Some categories include elements that provide a framework that is necessary for the development of others. Still other categories contain requirements for analyses that would then indicate modifications in others or are interdependent in some other way. It is the combination of all the elements in all the categories that forms the basis for providing assurance that no undue risk will be imposed on the workers, the public or the environment as a result of the undertaking proposed. None of these elements are sufficient on their own, but all are necessary for providing this assurance.

It should be noted that there are no rules or standards currently for presenting or for grouping these requirements. The categories presented here reflect experience in developing Safety Cases for nuclear power plant licensing in Canada, internationally establishing a Safety Case for a fusion research reactor, as well as the use of expert judgement in recognizing that the Safety Case for long-term waste management will need to deal with a different set of challenges. For example, the long-term storage, emphasis will be required in assurance that the management or governance structures can ensure that the systems and safety culture will be maintained in the long-term. In the case of a disposal facility, emphasis will be needed in the assurance that the engineered and natural systems can function reliably into the long-term future in the absence of a governance system and safety culture.

The Safety Case elements must cover a broad scope of information that must include:

- the technical and programmatic aspects that provide prevention of and protection against accidents or long term degradation of systems or conditions that are not planned and that demonstrate the mitigation measures in the case these were to occur;

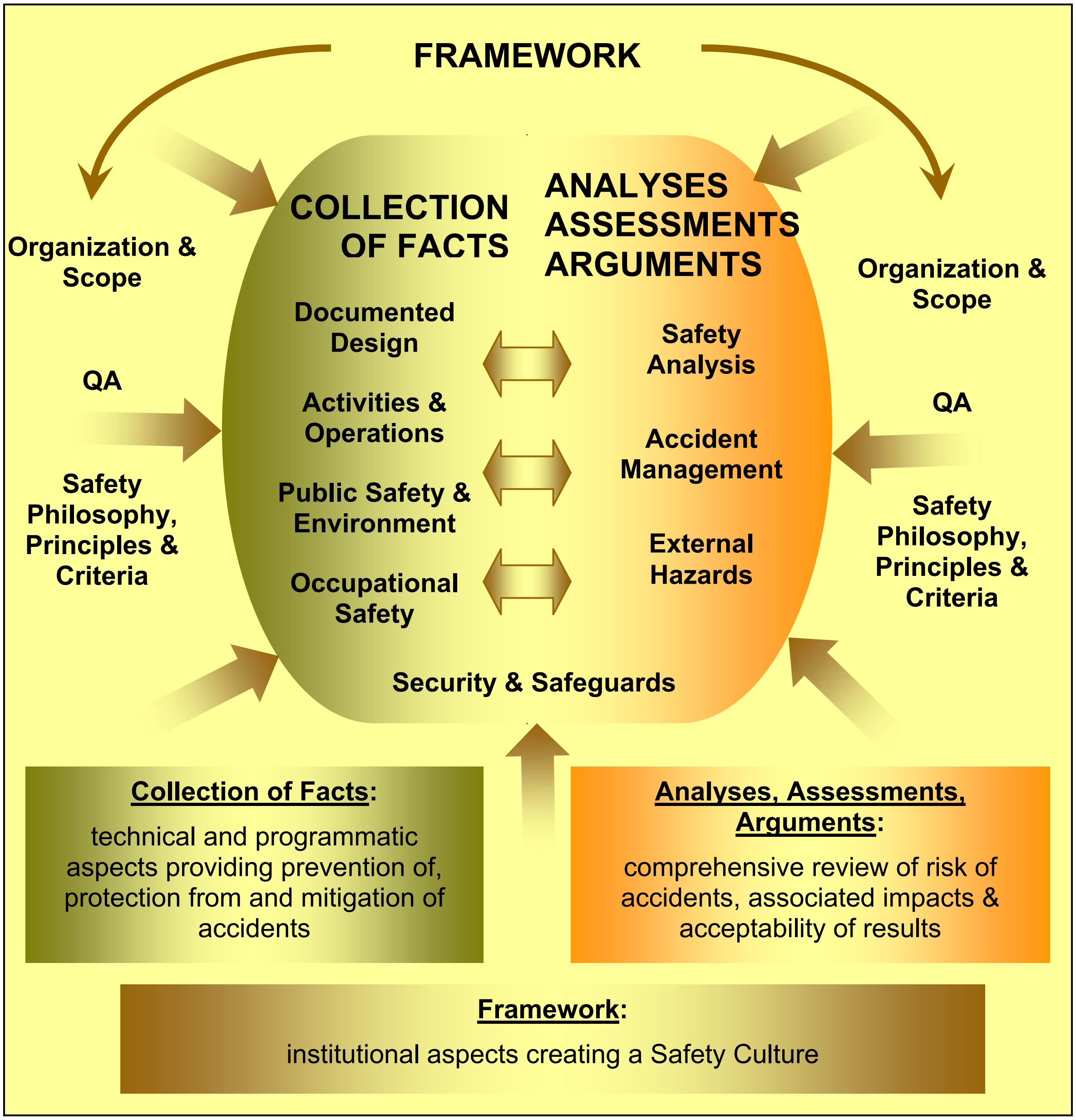

Figure 1 - Key Categories for a Safety Case

- a comprehensive assessment of the risk of accidents or long term degradation of systems or conditions, the associated impacts and the acceptability of results; and,

- institutional aspects that create a safety culture aimed at preventing the precursors to accidents or long term degradation of systems or conditions.

This latter includes aspects such as quality assurance, organizational structure, clear assignment of responsibilities, etc. These are factors that have been proven to contribute to a healthy safety culture in a work environment where the precursors to accidents are avoided or acceptably limited. If these factors are not adequately addressed, they have been shown to become contributors to a loss of instituted safety culture leading to a work environment prone to errors and, possibly, accidents.

Each of the eleven sub-sections below gives a general description of each Safety Case category and provides a list of logically grouped elements. These are preliminary lists, provided to give the reader a sense of the scope and extent that would be required for each category of information.

It is recognized that the selection of titles for these categories and the list of elements for each could in theory be arranged differently. Nonetheless, all of the elements would need to be included in any Safety Case. For example, here we include the definition of the organization separately from quality assurance although some may argue that the organizational structure should be part of QA. This may be debated; however, what is not debatable is that the description of the organization and the associated allocation of responsibilities and authorities are necessary for a complete Safety Case and therefore must be provided.

The Safety Case is an important tool for creating acceptance. The quality, the verifiability and the consistency of the information will greatly affect the effectiveness of the Safety Case in developing acceptance for any particular nuclear waste management option being considered. Finally, consideration will need to be given to how the information is communicated to each stakeholder group.

This document provides an outline of the necessary information for a Safety Case in the context of the long-term spent fuel management options. It is important to understand that the development of a Safety Case is an iterative process whereby the Safety Case that is developed and successively improved as information is gathered, the site(s) established and designs detailed. In the licensing of a Class I facility, the first step is acquiring a site licence, followed by a construction, and then an operations licence. In this approach, each successive licence requires further analysis and greater confidence in the Safety Case presented.

2.1 Organization and Scope

The first category defines the framework within which the facilities and the activities exist. The elements listed below bound the proposed undertaking by defining its purpose and scope and by identifying the legal processes under which the activities and facilities are approved. As part of the framework for developing the Safety Case, it is required to define the organization and the associated responsibilities and authorities. This provides a clear understanding about the corporate entity that has responsibility, and within which any facilities are constructed and the undertaking is conducted.

Figure 1: Key Categories for a Safety Case

Furthermore, the description of the organization recognizes that individuals in specific positions will be responsible for ensuring that the information provided in the elements will be undertaken as described. This is a fundamental building block in creating the necessary safety culture.

The development of a safety culture that encourages taking responsibility and prioritizing safety has been identified as a basic requirement for limiting accidents, system failures or the degradation of conditions by avoiding their precursors. This element has been included here as it is rooted in the setting of clear roles and responsibilities of all groups that will be interacting, as well as being part of the "framework" within which the Safety Case is developed. Throughout this section, elements that contribute to the development of the safety culture are highlighted.

The following is an indicative list of elements for this category. All of these would be necessary for defining the framework for the Safety Case for any of the options:

- Purpose and scope of facilities;
- Purpose and scope of activities to be carried out;
- Description of licensing process;
- Description of environmental assessment process;
- Identification of the corporate entity responsible for the activities, facilities, and operations of the facility;
- Description of the organizational structure, identifying allocation of responsibilities and authorities;
- Safety Culture:
  - Responsibility of the individuals and the operating organization;
  - Regulatory control and independent verification.

2.2 Quality Assurance

The second category, quality assurance (QA), defines the processes that provide assurance that facilities are designed, constructed, commissioned and operated in the manner documented and approved, and that activities are planned and performed in the manner documented and approved. The requirements in this element, along with those in the first element (Organization and Scope) provide the foundation upon which the remaining elements are developed and implemented.

A well-documented and fully implemented QA program is essential in developing the safety culture. QA programs ensure that people have the necessary qualifications and experience for their work and that facilities are designed to assist, not hinder performance. Among other things, the QA program ensures that responsibilities are communicated and embraced. This group of elements identifies the processes and programs implemented to ensure that the designs and activities are as documented, and that the analyses are performed and verified in conformance with known and accepted methods. QA affects all activities and will affect the implementation of all elements that contribute to the Safety Case.

The following is an indicative list of QA requirements necessary for defining the Safety Case. It should be noted that QA is used for assuring quality in all aspects of a project, such as efficiency, timeliness, etc., not only those that are safety related. In developing the Safety Case, only those aspects of QA that are relevant to safety are of interest.

- Overall QA program
- Quality Assurance Manual
- Design QA program
- Procurement, construction and commissioning QA programs
- Operations QA program
- Human Factors Engineering Program Plan
- Interface among responsible groups
- Audits and Assessments

2.3 Safety Philosophy, Principles and Criteria

The third category contains the basis for assessing the adequacy of safety in the proposed undertaking. It is important to define these elements in order to ensure that from the beginning a consistent philosophy underlies the design and operation of the facility and that this philosophy is reflected in the various analyses and assessments that are performed in preparing the Safety Case. The underlying philosophy should inform the basic principles applied to development of the facility as a whole as well as the other elements of the safety case. The safety philosophy and principles will in turn inform the criteria that are used to evaluate the results of the various analyses and assessments.

Regardless of the spent fuel management option selected, the safety approach should emphasize the prevention of accidents and the degradation of conditions over consequence mitigation. Development of a safety culture and transparent decision-making are also important factors providing a basis for the safety approach.

In this category, the elements include describing the safety objectives, the adopted safety approach (including safety principles and criteria) and the success criteria for performing a safety analysis. These fundamental bases are then used in the development of the elements in other categories such as design, environmental assessment, occupational safety, etc.

- Overall safety objectives
- Safety approach
- Safety principles
- General design criteria and any specific design requirements related to safety or environment
  - Defence-in-depth
  - Underlying technical principles
- Safety analysis requirements and rules
- Requirements for code classification and registration of containers and packaging.

2.4 Documented Design

The fourth category of elements deals with the documentation of the design of the facilities. This element, along with the activities and operations described in the next category, must be described sufficiently to provide reliable information for further assessment and analysis.

The design must show consistency with the safety philosophy and with the results of the analysis as described in the category below on safety analysis. As this information is a substantial input to the safety analysis and will require modification as per the results to address any concerns that are raised, design description and the safety analysis are iterated until a consistent Safety Case is achieved. As well, the design is interdependent with elements in other categories and must be consistent with them.

Systems that are expected to support operations (e.g. power, cooling, ventilation, communications, etc.) would be described here along with their designed capacity and reliability. For example, electric power could be required for the operation of safety systems during both normal and off-normal conditions related to the handling of the spent fuel.

The following is an indicative list of elements to provide a sense of the type of information that will be required in adequately documenting the design:

- Description of facilities
- Hazard information
  - Name, quantity, and form of nuclear substances to be handled
  - Name, quantity and form of non-radioactive hazardous substances to be on site
- Description of engineered safety features
- Systems supporting safety (electricity, cooling, communications, etc.)

2.5 Description of Activities and Facility Operational Program

This category of elements describes foundational programs and procedures essential to developing a safety culture, including the description of safety activities to be performed and defining the acceptable conditions under which the facilities may operate. These elements describe the programs, procedures, and criteria within which the activities of the next two categories of public safety, protection of the environment and occupational safety, are performed. Some of the criteria presented here will also be used as data for the safety analysis, and some of the information in this category may be iterated as a result of the safety analysis.

The organizational structure and responsibilities could be grouped with these elements instead of separately describing them in the first category of organization and scope. Regardless of where that information is located, the organization and responsibilities must be shown to be consistent with the overall process and activities.

The following is an indicative list of elements for this category:

- Qualification and training program
- How safety related operations are planned, approved, and controlled.
- Maintenance, testing and inspection programs
- Limiting conditions for safe operation
  - Action levels
  - Surveillance requirements
- Administrative controls
- Minimum staffing and equipment availability requirements

- Review and auditing of operations program
- Feedback of operating experience
- Emergency planning and preparedness including operational emergency response (first aid, fire)

2.6 Public Safety and Protection of the Environment

The sixth category provides principles and information on the programs that will be in place to ensure that the safety of the public and of the environment is maintained throughout the operation of the facilities, and on the the performance of the activities that are proposed for the undertaking. Here are described the programs for the minimization, control and monitoring of releases so as to protect the public and the environment. The information in this category is used as input to the safety analysis and may also be modified as per the results of the safety analysis. As with other design elements, the development of this information is iterative.

Specifically, this category includes information on normal operational releases of radioactive material and the measures to control and monitor these releases. All aspects of the design that are specific to controlling and monitoring releases to the environment are included. Ultimately, this information is intended to demonstrate that the impact of normal conditions on the environment and the public is acceptable and that the risk as a result of possible off-normal conditions is acceptable.

The following is an indicative list of elements for ensuring public safety and environmental protection:

- Name, form, characteristics and quantity of any hazardous substances
- Description of management of solid, liquid and gaseous wastes (radioactive and non-radioactive)
- Environmental protection policies
- Environmental protection measures and procedures
- Effects on the environment and the health and safety of persons, and measures to prevent or mitigate those effects
- Location of points of release, maximum volumes and concentrations, volume and flow rate of releases of nuclear substances and hazardous substances into the environment, including their physical, chemical and radiological characteristics in respect to various populations of interest
- Description of effluent and environmental monitoring program
- Measures to control releases of nuclear substances and hazardous substances
- Monitoring program and equipment

2.7 Occupational Safety

The seventh category provides principles, criteria and information on programs designed to ensure the safety of the workers during operation of the facilities and performance of activities. The interdependence of this group of elements with the safety analysis is similar to that of the sixth category (Public Safety and Protection of the Environment). The programs, procedures and equipment described here must demonstrate that a safe environment will exist for workers during normal conditions and sufficient measures are taken to prevent workers from being exposed to the hazards of off-normal circumstances. The establishment of a worker health and safety policy along with the programs and procedures that uphold the policy are not only required by the regulator, but are important in the development of a safety culture.

The following is an indicative list for this element to provide a sense of the type of information that will be required. Note that the occupational safety element must address not only radiological hazards, but overall worker health and safety and industrial hygiene issues, as well as specific conventional hazards such as fire.

- Worker health and safety policy, program, procedures and awareness
- Description of Radiation Protection Program in design
  - Facilities, equipment and instrumentation
  - Sources of radiation in the facility
  - Aspects of facility design that address radiological safety and hazardous material safety
  - Access control and zoning
  - Ventilation for radiological safety
  - Radiation monitoring systems
- Description of Radiation Protection Program in operation
  - Work permits and work control
  - ALARA
  - Staff training program for Radiation Protection
  - Handling and movement of radioactive materials
  - Worker dose assessment for normal operations (including maintenance)
  - Audit and review
- Protection against industrial hazards
- Fire protection

2.8 Safety Analysis

The eighth category includes a group of elements to provide assurance that the impact of a facility or activity is known and acceptable and specifically that the impact of off-normal conditions is known, bound, and of acceptable risk. The core of this is the safety analysis, a commonly used term to mean an examination of possible accidents, system failure and/or degradation of conditions, and further identifying the risk and impact of these and the mitigation of these impacts. The safety analysis is carried out in reference to the documented design and the facility operational program, by means of a process that meets the quality assurance program defined for the facility and in a manner consistent with the safety philosophy, principles and criteria under the organization defined for the waste management facility.

The requirements associated with this element include a defined analysis technique, a safety analysis plan, appropriate feedback between the safety analysis and the design of the facility and its operational program, and the analysis itself. The following is an indicative list of the required elements anticipated to meet the need for safety analysis:

- Acceptance criteria
- Framework of safety analysis and methods used in analysis
- Identification and Categorization of initiating events

  - Internal hazards
  - External hazards
- Safety analysis assumptions, methods and computer programs (codes)
- Validation and verification of methods and codes
- Accident analysis results:
  - Operating Limits and Conditions
  - Design Criteria/Codes and Standards
  - Demonstration that acceptance criteria are met

2.9 Accident Management

The ninth category of information, accident management, describes the programs and methods that are to be used to minimize the impact of accidents. The two fundamental elements for accident management are the minimization of the possible impact by reducing the possible release of radioactive releases and secondly the contingency planning and response in the case of an accidental release.

For the Safety Case, the practical methods proposed to address each of these two elements must be outlined. The accident scenarios are described in the safety analysis and the methods to protect workers and the public are described in the occupational safety and environment and public protection elements. Here, the specific measures taken in the design of the facility to minimize releases, and the programs that are in place for responding to accidents will be described.

Typical details that would be required are listed below:

- Accident release minimization
  - Ventilation design
  - Source minimization
- Emergency planning and response
  - First response training
  - Public information planning

2.10 External Hazards

The tenth group of elements addresses the possibility of external events, natural or man-made, that could impact the facility or the activities. This is an extension of the safety analysis, which deals with impacts on the undertaking from external sources. This would include, for example, the effect on the facility of extreme weather, or the effect on a transport truck carrying nuclear fuel waste of a collision with another truck.

The requirements are essentially categorized in two, as indicated below. A full list under each would only be possible after assessments of the external hazards for the particular site and the particular options are performed.

- Human initiated hazards;

- Natural hazards.

2.11 Security and Safeguards

The final category addresses the obligations of the organization controlling the nuclear fuel waste regarding the security of the public and the safeguards agreements in international treaties. This would include a description of the programs and the implementation of measures to keep the public away from the hazardous substances and also to keep safeguarded materials from illegal uses.

Details regarding security and safeguards are often classified. It would not be expected that the details of this information would form part of the publicly available documents, although it will be necessary for the regulator to be satisfied with the information.

The following is an indication of the type of information that the regulator would require.

- Measures to control access to site, including screening of employees;
- Description of security equipment, systems and procedures;
- Description of on-site and off-site communications equipment, systems and procedures;
- Description of structure and organization of nuclear security guard service, including duties, responsibilities and training of nuclear security guards;
- Plan and procedures to assess and respond to breaches of security;
- Identification of any prescribed substances, equipment or information to be present on the site;
- Measures to prevent illegal use, possession or removal of nuclear substances, prescribed equipment or prescribed information;
- Measures to facilitate Canada’s compliance with any applicable safeguards agreement.

3 Differences in Developing a Safety Case for the Current Three Options

This section discusses the elements of a Safety Case provided in Section 2. Briefly, the typical content for each element and the challenges in developing this content for the Safety Case of each of the three options considered for long-term spent fuel management are described. This is not an assessment of the options, rather it provides some expert judgement on the types of issues that will be dealt with in the various scenarios that are currently being considered.

Safety Case Elements	Brief Review of Possible Content and Challenges
Organization and Scope	
1-1 Purpose and scope of facilities; 1-2 Purpose and scope of activities to be carried out;	Here the purpose and scope of the undertaking is defined. The information provided must identify what exactly is being considered, from the point of view of facilities and activities, to what extent and how these will be used and for what purpose. All the options under consideration may have the same overall purpose, but the scope will vary depending on the management approach selected. Extended longer-term management at current sites may not include transportation but may include more extensive monitoring over the long-term and should include milestones in the future for re-assessment. The activities for processing the spent fuel and for its transferral and transportation should be identified as part of the scope where appropriate.

1-3 Description of licensing process; 1-4 Description of environmental assessment process;	The licensing activities will differ depending on the management approach even though, assuming that the options are all within Canada, they are all subject to the same acts and regulations for licensing and EA. Depending on the scope, some regulations may not be applicable in certain options (e.g. transportation for the at-site option). A greater challenge will be licensing facilities or activities that have not been licensed before within Canada. In these cases, a review of the acts and regulations will reveal if changes will need to be made, or if the new facilities or activities can be licensed under the current framework, and if so, a clarification of the process to be adopted. The approach would need to be laid out, be consistent with the regulator's expectations and provide no less confidence in the outcome than proven regulations and processes.
1-5 Identification of the corporate entity responsible for the activities, facilities and operations of the facilities; 1-6 Description of the organizational structure identifying allocation of responsibilities and authorities;	For each option, this will include a definition of the organization and the hierarchy to clearly present the responsibilities and authorities during the processing and handling of the spent fuel, the organization and the responsibility for the spent fuel during transfers, transportation and disposal, where required. Confidence will be engendered by defining an organization that addresses the lessons that have been learned throughout the decades of experience with organizations that are effective and promote high quality work with a priority on safety. The greater challenge will be in establishing confidence in the selection of the overall management approach and the corporate or governmental entity with the legal responsibility for the spent fuel and its safe disposition. Another consideration will be the overall organization that will need to be in existence for a long period of time, possibly through regulatory and political transitions.

1-7 Safety Culture: ▪ Responsibility of the individuals and the operating organization; ▪ Regulatory control and independent verification;	The greatest differences and challenges will be in confidently establishing responsibility for circumstances and events that may need to be addressed a long way into the future. Other difficulties could arise from adverse events that occur as a result of procedural non-compliance resulting in spent fuel not being disposed of in a timely manner, or for events post-disposal that were not foreseen. A separate issue to be resolved is the need for establishing the responsibility in the case of extended interim storage for future decisions.
Quality Assurance	
2-1 Overall QA program 2-2 Quality Assurance Manual 2-3 Design QA program 2-4 Procurement, construction and commissioning QA programs 2-5 Operations QA program 2-6 Human Factors Engineering Program Plan	Regardless of which option is under consideration, QA will begin with design and will continue through construction and commissioning and into operations. QA programs will be required that describe how each of these phases will be handled. In particular, the programs will also define how change control is managed to maintain both (a) a design that is fully assessed and analyzed, and (b) procedures that are re-assessed in light of changes to them. Other than recognizing that the options will have differing facilities and activities to consider, the development of QA programs will be similar for all options.
2-7 Interface among responsible groups	Consistent with the organizational structure and the hierarchy described in the first element, this requires that the interface, between those responsible for either physical or legal transfer of the material, be clearly defined.
2-8 Audits and Assessments	This describes the program that will be implemented to provide for internal and external assessment of the activities and the facilities. A program of assessments to be conducted by the internal organization will be expected as will be necessary external audits from the regulator, or perhaps other organizations.

Safety Philosophy, Principles and Criteria	
3-1 Overall safety objectives	The overall safety objectives of the facility will be only slightly affected by which management option is selected. The relative emphasis between different objectives may, however, be affected. For example, above-ground storage might require a larger number of workers in closer proximity to the stored fuel. This would result in a greater emphasis on overall objectives related to radiological protection of the workers than would be the case for an option in which workers spent very little time in close proximity to the fuel (i.e., in the deep geological disposal option). Such an option would likely result in a greater emphasis on objectives related to the reliability of engineered and natural systems into the long term future in the absence of a governance system and safety culture. Above ground facilities would also have different requirements for security and protection against external events, both human and natural.
3-2 Safety approach	Selection of the safety approach could be affected by the management option selected. Deep geological disposal may be better suited to an approach that depends heavily on passive safety features and consequence assessment focussed on examination of a small number of worst-case accident scenarios whose consequences would bound any other potential events. On the other hand, on-site above-ground storage may be better suited to an approach that emphasizes protection afforded by more active accident mitigation systems coupled with a probabilistic risk assessment.

3-3 Safety principles 3-4 General design criteria and any specific design requirements related to safety or environment ▪ Defence-in-depth ▪ Underlying technical principles	The safety principles to be applied to the selected management option should be guided by best practices and should be consistent with the overall safety philosophy of the organization. If a particular management option presents safety challenges that are unique to it, the safety principles would need to reflect that uniqueness. For example, centralized storage and deep geological disposal both require transportation of spent fuel and so safety principles applicable to transportation are needed. On the other hand, on-site storage would require a more complex organization; the safety principles of the organization would need to account for that. The design criteria and design requirements that are related to safety and the environment will also be different for different options. Since deep geological disposal involves less active operational upkeep, it is likely that the design criteria and design requirements will be more extensive and more difficult to define. On the other hand, the design criteria and requirements for centralized storage would likely be easier to define, given the possibility of operational intervention being used to meet overall safety goals. Finally, on-site storage of fuel would have some of the advantages of centralized storage, plus no requirements to have design criteria and requirements related to transportation of spent fuel. However, the multiplicity of locations (and hence of design considerations related to locale) would tend to increase the amount of work required to prove that the design criteria and requirements are met throughout.

3-5 Safety analysis requirements and rules	Setting safety analysis requirements and rules depends on both the management option selected and on the safety approach adopted. Hence, the safety analysis requirements and rules will be different for different options. Deep geological disposal involves a type of facility that has never been licensed before in Canada and so the safety analysis requirements and rules will have to be re-defined for that option. Doing this will be challenging if they are to be acceptable to the regulator and the public and still achievable, although preliminary work has been done as indicated by the submissions that have been made (for example to the Seaborn Panel [7]). On the other hand, the requirements and rules for interim on-site storage have already been defined and implemented in analyses. It would be expected that the rules and criteria for longer-term on-site management and centralized long-term management could be developed as an extension of these existing rules and criteria. Centralized long-term storage and deep geological disposal would require the additional task of setting requirements and rules for transportation of larger quantities of spent fuel than have been transported in the past in Canada. In any of the potential options, the span of time to be considered in any of the options will make defining these requirements and rules a challenge.

3-6 Requirements for code classification and registration for containers and packaging.	This element would encompass containers and packaging for storage, disposal and transportation, as appropriate. The challenge here is two-fold. First is the transportation of larger quantities of spent fuel than have been transported in the past in Canada. Second would be the development of containers for the long-term storage or disposal. With respect to transportation of these quantities of spent fuel, there will be the need to establish criteria for packaging and transportation that would be specific to the materials being transported. These could be based on criteria currently used for the transportation of high-level radioactive materials including smaller amounts of spent fuel. The criteria established for transportation of spent fuel by other countries and consistent with the IAEA standards should be reviewed in developing criteria.
Documented Design	
4-1 Description of facilities	This is a straightforward requirement to describe the facilities proposed. Here, facilities mean all structures and buildings, and the equipment found inside such structures or servicing them. All the facilities that are required for the particular option considered, where activities are performed, or where the spent fuel is handled, transported, stored or disposed are included. Any disposal facilities, or on-site or centralized long-term management facilities plus all supporting facilities will be included, such as for the handling and packaging of nuclear waste and other hazardous materials. All support equipment in these facilities, in particular those related to safety such as heating or cooling, ventilation, instrumentation including radiological condition monitoring, control and display, access control systems and all hot cell and remote handling systems will be described.

4-2 Hazard information ▪ Name, quantity, and form of nuclear substances to be handled ▪ Name, quantity and form of non-radioactive hazardous substances to be on site	The hazards refer to the substances anticipated to be present at the facility or facilities. Particularly significant will be the spent fuel for which the facilities have been designed, and particularly the form, quantity and type at the various steps of the spent fuel management process for the various described facilities. All waste must be described in regards to radioactive hazard levels, as well as non-radioactive hazards. Differences will exist depending on pre-disposal or pre-storage processing that may be included in one or another option. Other hazardous substances used in the operation of the facilities or in any of the waste streams resulting from the handling and management of the spent fuel will need to be identified.
4-3 Description of engineered safety features.	This addresses the physical barriers and the systems for the confinement and control of the release of radioactive material and other hazardous substances, as well as the reliability of such systems. These systems will depend on the safety approach described below and will differ depending on the long-term spent fuel management option. For options of final disposal, confidence in the effectiveness of engineered systems declines with the length of time of service expected of them. The expectation regarding final disposal is that post-closure there will not be any need for further human intervention for any purpose, including safety and environmental protection, unless continued monitoring and retreivability are considered desirable by the public or the host community. It would be difficult to confidently assure the availability of staff and organizations for the length of time that the spent fuel continues to be a concern.

4-4 Systems supporting safety (electricity, cooling, communications, etc.).	The safety analysis and assessments of worker safety and environmental safety will identify systems that play a basic role in limiting accidents and the impact of off-normal conditions. These systems will play roles in identifying or mitigating accidents during the processing and handling of spent fuel in all options, in transportation for either of the centralized options, and for maintaining safe conditions in either centralized or on-site storage option. These systems would be described for all phases where they are required.
Activities and Facility Operational Program	
5-1 Qualification and training program	A document prescribing the knowledge and experience that would be deemed sufficient to properly and safely execute operations and maintenance activities during normal conditions. Although all options will have training programs and will need to identify the acceptable qualifications for the proposed activities and facility operations, the complexity increases with increased human interface and the need for a robust program to endure over a long time period. Although fairly straightforward as a requirement, developing an appropriate qualification and training program for each of the options may be a challenge.
5-2 How safety related operations are planned, approved, and controlled. 5-3 Maintenance, testing and inspection programs	Best industry standard processes for planning, controlling and approving work should be implemented for activities needed for all the options. The activities that will be subject to this are those performed to manage the spent fuel prior to disposal or storage, as well as the activities at the spent fuel storage or disposal facility, and the activities required to monitor and control the site post-disposal or storage. The activities to be performed by the groups responsible for the management of the spent fuel (including final disposal if appropriate) must be described sufficiently to assure consistency with the safety approach and the documented design.

5-4 Limiting conditions for safe operation ▪ Action levels ▪ Surveillance requirements ▪ Administrative controls	Determined through Safety Analysis. These requirements must be consistent with the safety analysis considerations and the description of facility and operational activities. The action levels that will be set as a function of the Safety Analysis will be as challenging to define as the performance of assessments and development of safety requirements for new facilities and operations. The facility surveillance and environmental monitoring requirements will be based on best practices and standards. The expectation is that in the case of final disposal, there would be minimal further human monitoring or interface. However, there may be a need to consider a continued monitoring to increase public confidence for a specific management approach.
5-5 Minimum staffing and equipment availability requirements	Establishing minimum staffing and equipment availability requirements is important to define the organization, provide input for occupational safety assessments, safety analysis and accident management. Having credible minimum staff and equipment availability levels is necessary to establish the validity of the safety case to both the regulator and the public.
5-6 Review and auditing of operations program 5-7 Feedback of operating experience.	It is important to provide feedback from audits and assessments and to share information among Canadian sites as well as monitoring information from experience world-wide and across various industries. The regulator's scrutiny of the safety case will include a comparison of facts and arguments with those of other comparable facilities and activities. Consistency between the Canadian approach to safety with proven technologies and solutions from internationally respected organizations will be an important asset toward increasing confidence in the experts preparing the safety case and in the regulator and the public reviewing it.

5-8 Emergency planning and preparedness including operational emergency response (first aid, fire)	Having appropriate emergency planning and preparedness in place is essential to support the safety conclusions of the public safety, environmental protection and occupational safety assessments. The content required for this element is largely a function of the possible accident conditions analysed in the various options. It is critical that the content of this element is consistent with the assumptions of the safety analysis and accident management. This is an element that needs to satisfy potential conditions while there are facilities that are operating or that have a reasonable possibility of changing and are therefore being monitored. There may be a need to address this issue for final deep geological disposal in order to satisfy public confidence that any analysis suggesting no impact on the environment or the public post-disposal is true. This element will be partially based on the predictions of the Safety Analysis and partially on meeting expectations of the public and perhaps of the regulator. One aspect of this that will be uniquely applicable to spent nuclear fuel management is the possibility of very long-term processes that may eventually result in unacceptable consequences.
Public Safety and Protection of the Environment	
6-1 Name, form, characteristics and quantity of any hazardous substances 6-2 Describe management of solid, liquid and gaseous wastes (radioactive and non-radioactive)	Identifying the hazards anticipated to be present, their form and characteristics is a standard activity in the preparation of a safety case that should not pose any significant challenges. “Wastes” in this context includes not only solid waste but also liquid and gaseous effluents from the facilities handling and packaging the spent fuel. There are many years of safe operating experience at Canadian nuclear facilities that would be a basis in establishing an acceptable approach to managing the waste streams, or maintaining the equipment used in these activities. A challenge will be to consider the environmental effects of releases of small magnitude but occurring over long time periods.

6-3 Environmental protection policies 6-4 Environmental protection measures and procedures	Environmental policies and procedures will need to take into account the long term of the facilities to be licensed. The process for environmental assessment routinely requires assessment of impact into the future, although modification may be required of methods for assessment of these facilities, as well as the application of environmental protection measures and procedures.
6-5 Effects on the environment and the health and safety of persons, and measures to prevent or mitigate those effects	Once the analysis has been performed and an understanding of the possible releases to the environment have been determined, an assessment of the effect of such releases on the environment and a dose assessment on the public would need to be performed. The methodology for public dose assessment is fairly well developed and the key remaining unknown would be the establishment of an understanding with the regulator on the specifics of the methodology to be applied. Of greater uncertainty, at this time, is determining the effects of radiological releases on non-human biota, which is still a growing area of study.
6-6 Location of points of release, maximum volumes and concentrations, volume and flow rate of releases of nuclear substances and hazardous substances into the environment, including their physical, chemical and radiological characteristics	This is a straightforward requirement and would be expected to conform to the design specifications of the facility, which may be iterated as a result of the safety analysis and the ensuing public dose assessment. No particular challenges for spent fuel facilities are foreseen.
6-7 Description of effluent and environmental monitoring program 6-8 Measures to control releases of nuclear substances and hazardous substances 6-9 Monitoring program and equipment	There are no particular challenges anticipated in meeting this requirement except in determining the length of time into the future that a monitoring program would be required post-disposal. Although the expectation is that after disposal, no further human intervention, including monitoring, should be required, it may be necessary to institute some environmental monitoring to address any lingering issues of public concern.

Occupational Safety	
7-1 Worker health and safety policy, program and procedures	There are no particular challenges anticipated in establishing health and safety policies, programs and procedures that will meet the regulatory requirements and industry standards. As part of the safety case, it would be necessary to document these for both radiological and industrial health and safety. The above-ground nuclear facilities would be expected to have similar policies to other nuclear facilities in Canada. The industrial safety standards of the mining industry should be reviewed in establishing appropriate health and safety policies for deep geological activities during operation and during construction. The third area of worker safety to consider will be transportation, if a centralized disposal or storage site is selected. This will be of greater significance if all the spent fuel is transported by trucks across small remote roads, and lesser if transported by barge.
7-2 Description of Radiation Protection Program in design ▪ Facilities, equipment and instrumentation ▪ Sources of radiation in the facility ▪ Aspects of facility design that address radiological safety and hazardous material safety ▪ Access control and zoning ▪ Ventilation for radiological safety ▪ Radiation monitoring systems	As for other new facilities, it will be necessary to establish a radiation protection program early on so as to take into account radiological occupational safety during design of the facilities. Identification of the sources of hazards and descriptions of the facilities and equipment relevant to radiation protection will be part of the safety case. As important, and relevant to assuring a healthy safety culture, is the application of sound radiological protection principles such as ALARA and concepts such as access control and radiation area zoning. Showing the impact of applying these concepts to the design, provide a foundation for developing the occupational safety elements of the safety case.

7-3 Description of Radiation Protection Program in operation ▪ Work permits and work control ▪ ALARA ▪ Staff training program for Radiation Protection ▪ handling and movement of radioactive materials ▪ Worker dose assessment for normal operations (including maintenance) ▪ Audit and review 7-4 Protection against industrial hazards 7-5 Fire protection	Similar to the health and safety policy and program described above, the Radiation Protection Program should be a straightforward issue to deal with, as would a program to protect against industrial hazards, including chemical hazards, falling, confined spaces, etc. The specific hazards and conditions present in the facilities that will be constructed will need to be identified. The practices in radiation protection and conventional occupational safety have been well developed over the many years of operating experience in nuclear facilities, in mining and in transportation. It is necessary to specify the measures that will be taken in all areas of concern.
Safety Analysis	
8-1 Acceptance criteria	Setting the acceptance criteria should be technically similar for the management and handling aspects for both deep geological disposal and the centralized and on-site storage options. However, the different perceptions of acceptable risk for options with different time frames will result in different safety criteria. The challenge will be in developing acceptance criteria for possible impact during phases of long duration with minimal human interface. Acceptance criteria currently exist for the current on-site storage of spent fuel. Whether these would be acceptable for longer term storage is an unknown. Acceptance criteria will also be required for transportation accidents and impact of such events. These criteria could be based on current criteria for the transportation of high-level waste, and those used by other countries. The larger volume of waste than has been transported in Canada in the past, distance and multiple trips will affect the criteria that would be deemed acceptable technically by the regulator, but also that would be accepted by the public.

8-2 Framework of safety analysis and Methods used in analysis	Defining the framework and the methods that can demonstrate confidence for the analyses will pose a challenge for all three current options. In the case of deep geological disposal, there has been considerable research on relevant phenomena that are consistent with the long time frames characterizing spent fuel disposal, although the conditions may change over these long time frames. Safety analysis of dry storage has been successfully performed in the past, although the time frames considered are very different from those required for the on-site or centralized long-term management options of spent fuel. In any case, the challenge will be to develop a framework that can confidently demonstrate that the safety requirements considered by the regulator will be met, over the required timeframe.
8-3 Identification and Categorization of initiating events ▪ Internal hazards ▪ External hazards	This will require a systematic identification and categorization of initiating events for processes that will be new to the regulator. The demonstration of completeness may require both top-down and bottom-up assessments of possible conditions and initiating events. The possibility of utilizing processes that have been tried on other new facilities should assist in providing confidence in the final results. The breadth of current practices will assist in developing an approach, possibly a combination of processes that will confidently compile a complete set of initiating events.
8-4 Safety analysis assumptions, methods and computer programs (codes) 8-5 Validation and verification of methods and codes	Defining the assumptions, methods and codes, as well as verifying and validating the codes, will not likely pose a significantly different level of challenge for any of the three options. The main issues will be in utilizing computer programs and codes that will have sufficient acceptance for the long time frames for which it is not possible to have them fully validated. Much cross-referencing with best industry methods and approaches to this issue should provide the best resource for establishing regulatory confidence.

8-6 Accident analysis results: ▪ Operating Limits and Conditions ▪ Design Criteria/Codes and Standards ▪ Demonstration that acceptance criteria are met	Performing safety analysis of spent fuel management will be a unique challenge for any of the options as provided in the assessment for 8-1 to 8-5 above. The results of this analysis will provide information that will be then used to modify the design or the operating assumptions. Finally, the analysis must confidently demonstrate that the acceptance criteria that will have already been defined are met. This is a case where care must be taken that the criteria are established prior to the performance of the analysis. It is important that it is made clear that the design is based on the acceptance criteria, and not the reverse. If in the analysis the acceptance criteria are not met, the design would be modified and the analysis performed again to see if the criteria can be met. Iteration of the design in this manner generally provides more confidence in the safety level of the design.
Accident Management	
9-1 Accident release minimization	Accident release minimization is a very important part of the safety case. Many of the methods of accident release minimization will be specified in the design and operational criteria and will be used as input to the safety analysis. The approach to minimizing possible releases will affect the methods accepted for transportation, handling and storage of the spent fuel. A balance between the size of the possible source for release, the number and robustness of the physical barriers and the efficiency of operation will be required to provide the necessary confidence that accident releases are minimized. The design principle of ALARA will need to be addressed in regard to minimizing releases as will the principle of multiple barriers.

9-2 Emergency Planning and Response	This element may include activities to be undertaken during an accident that are necessary to be consistent with the safety analysis, assessment of external events, or security issues. However, it may go further than that as the emergency plan and response will not only consider the results of the assessments, but will be developed to provide confidence to stakeholders that measures are in place to effectively mitigate the impact of any possible accident scenario. At this time, there does not appear to be any reason that any of the spent fuel management options will pose a greater challenge in respect to defining this element than previous nuclear installations.
External Events	
10-1 Natural hazards	Defining the range of potential natural hazards that could affect the facility will be different between the different options. Natural hazards will need to be considered for transportation and for all handling activities, wherever these activities are required. Furthermore, for deep geological disposal, natural hazards will be considered after disposal. Consideration of the impact of geological changes over the very long time-frame may prove to be a challenge in estimating these changes. For on-site and centralized storage options, a number of weather-related natural hazards will likely have to be considered for the storage sites considered (one or several).

10-2 Man-made hazards	Defining potential hazards due to human activities, whether intentional or accidental, will also be different for the different options. It is anticipated that the deep geological disposal option will benefit from the fact that, once the spent fuel is placed in the repository, it is much less likely to be subject to human activities than either of the above-surface storage options. Hazards resulting from human intervention will need to be addressed for transportation of spent fuel to either of the centralized options.
Security and Safeguards	
11-1 Measures to control access to site 11-2 Description of security equipment, systems and procedures 11-3 Description of on-site and off-site communications equipment, systems and procedures 11-4 Description of structure and organization of nuclear security guard service, including duties, responsibilities and training of nuclear security guards 11-5 Plan and procedures to assess and respond to breaches of security	The measures described here are specifically for the security against criminal elements of the public and security to protect the public itself. A description of the programs and the implementation of measures will be required. It would not be expected that the details of this information would form part of the publicly available documents, although it will be necessary for the regulator to be satisfied with the information. Security provisions may be patterned after similar provisions at nuclear facilities. Special provisions will also have to be made to deal especially with transportation. Some security procedures may be required as part of the emergency planning and response and the safety analysis.

11-6 Identification of any prescribed substances, equipment or information to be present on the site 11-7 Measures to prevent illegal use, possession or removal of nuclear substances, prescribed equipment or prescribed information 11-8 Measures to facilitate Canada's compliance with any applicable safeguards agreement	Safeguard procedures should be similar at a spent fuel storage site to what is required at an operating nuclear power plant, although the larger amount of fuel may require different controls and inspections. Safeguards would have to be maintained during transportation for both deep geological disposal and for centralized storage. Particularly for centralized storage and on-site storage, considerations of how to maintain safeguards over the very long time frame while the spent fuel is still accessible may pose unique challenges, especially given that that the high initial levels of radioactivity will decay over time, removing a proliferation barrier. In all cases, consideration must be given to the safeguards agreements and binding international treaties. Confidence that the spent fuel is at a known location, especially if it has been disposed and is not intended to be retrieved is one such consideration that will need to be met.

4 Recommendations

This document has provided an outline of the necessary information for a Safety Case in the context of the long-term spent fuel management options. It has also provided a preliminary review of challenges and issues that can be expected in developing a Safety Case. In reviewing the eleven categories and the lists of required information for each, it becomes clear that much work is needed to establish a comprehensive Safety Case that is both technically sound and acceptable to two key stakeholders, the regulator and the public. The following recommendations are made in the context of furthering work in these two critical areas.

1. It is recommended that NWMO continue efforts to determine areas of greatest public concern with respect to spent nuclear fuel management and that this information be directly accounted for in the preparation of the Safety Case.

2. It is recommended that NWMO begin discussions with the CNSC to develop a better understanding of expectations with respect to regulations and standards, as well as methodologies needed for developing the Safety Case.

3. It is recommended that further effort be put into defining the elements of the Safety Case applicable to the specific options and into assessing the difficulty of meeting the requirements.

4. It is recommended that interaction with organizations in other jurisdictions that are involved in spent fuel management be promoted, specifically to better understand good industry practices and to develop benchmark approaches with respect to safety and public acceptance. Such feedback would provide valuable lessons learned about obtaining regulatory approval and public acceptance, as well as technical acceptance criteria.

5 References

[1] IAEA Safety Standard Series No. DS134, “Geological Disposal of Radioactive Waste”, 2003

[2] Mason, S., “A History of the Sciences”, Collier Books, New York, 1962,

[3] Weber, E., “A Modern History of Europe”, W.W. Norton & Co., New York, 1971.

[4] D.G. Hurst et al., “Canada Enters the Nuclear Age: A Technical History of Atomic Energy of Canada Limited as Seen from Its Research Laboratories”, Atomic Energy of Canada, 1997.

[5] Nuclear Safety and Control Act (1997, c. 9)

[6] Canadian Environmental Assessment Act (1992, c. 37)

[7] “Report of the Nuclear Fuel Waste Management and Disposal Concept Environmental Assessment Panel”, A report to the Ministers of the Environment and of Natural Resources, February 1998

[8] Canadian Nuclear Safety Commission, “General Nuclear Safety and Control Regulations”, Canada Gazette Part II, Vol. 134, No. 13, pp. 1127-1169

[9] Canadian Nuclear Safety Commission,”Class I Nuclear Facilities Regulations”, Canada Gazette Part II, Vol. 134, No. 13, pp. 1185-1193

[10] Canadian Nuclear Safety Commission, “Packaging and Transport of Nuclear Substances Regulations”, Canada Gazette Part II, Vol. 134, No. 13, pp. 1239-1253

[11] Canadian Nuclear Safety Commission, “Radiation Protection Regulations”, Canada Gazette Part II, Vol. 134, No. 13, pp. 1171-1183

[12] Canadian Nuclear Safety Commission, “Nuclear Substances and Radiation Devices Regulations”, Canada Gazette Part II, Vol. 134, No. 13, pp. 1217-1237

[13] Canadian Nuclear Safety Commission, “Nuclear Security Regulations”, Canada Gazette Part II, Vol. 134, No. 13, pp. 1255-1271

[14] Canadian Nuclear Safety Commission, “Nuclear Non-Proliferation Import and Export Control Regulations”, Canada Gazette Part II, Vol. 134, No. 13, pp. 1272-1315

[15] IAEA Safety Standard Series No. WS-G-2.6, “Predisposal Management of High Level Radioactive Waste”, International Atomic Energy Agency, Vienna, 2003