MRS Advances © 2019 Materials Research Society
DOI: 10.1557/adv.2018.681

Probabilistic Performance Assessment vs. the Safety Case Approach

François Diaz-Maurin[1,2] and Rodney C. Ewing[1,3]

[1]Center for International Security and Cooperation, Stanford University, Stanford, CA 94305, USA
[2]Amphos 21 Consulting SL, C/ Venezuela 103, 08019 Barcelona, Spain
[3]Department of Geological Sciences, Stanford University, Stanford, CA 94305, USA

ABSTRACT

The "safety case" approach has been developed to address the issue of evaluating the performance of a geologic repository in the face of the large uncertainty that results for evaluations that extend over hundreds of thousands of years. This paper reviews the concept of the safety case as it has been defined by the international community. We contrast the safety case approach with that presently used in the U.S. repository program. Especially, we focus on the role of uncertainty quantification. There are inconsistencies between the initial proposal to dealing with uncertainties in a safety case and current U.S. practice. The paper seeks to better define the safety case concept so that it can be usefully applied to the regulatory framework of the U.S. repository program.

INTRODUCTION

Uncertainty quantification is one of the key issues in the safety analysis of geological repositories for radioactive waste disposal. In repository design, epistemic uncertainties arise when projecting coupled geophysical and geochemical processes over large temporal and spatial scales. These uncertainties limit the ability to predict the long-term behavior of the repository because of the unavoidable lack of knowledge about future geological conditions. In the U.S., probabilistic performance assessments (PPAs) have been used as the standard method in repository licensing [1]. Yet, the value of PPAs has been challenged [2]. PPAs include making probabilistic estimates of anticipated dose to the public or release to the environment hundreds of thousands of years into the future. These estimates are not compelling for regulatory decision-making because they cannot convincingly demonstrate whether a repository provides for a sufficient level of safety. Thus, one must expect public skepticism of statements that a repository is "safe enough."

Downloaded from https://www.cambridge.org/core. Stanford Libraries, on 08 May 2019 at 16:13:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1557/adv.2018.681

Downloaded from https://www.cambridge.org/core. Stanford Libraries, on 08 May 2019 at 16:13:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1557/adv.2018.681

PROBABILISTIC PERFORMANCE ASSESSMENT

Probabilistic risk analysis (PRA) was developed for the safety assessment of engineered systems. PRA was applied to the safety analysis of nuclear power plants for the first time in 1975 in a report for the U.S. Nuclear Regulatory Commission (NRC) known as the "Rasmussen Study" [3]. During a workshop organized in 1976 by the ERDA (Energy Research and Development Administration, a precursor to the DOE), nuclear engineers and mathematicians from the NRC, who were familiar with the recently developed PRA methodology for reactors, advocated for the extension of PRA to the safety assessment of nuclear waste repositories [2]. However, earth scientists and geotechnical engineers who were familiar with the uncertainties of geologic investigations, including those from ERDA, expressed concern over the use of mathematical models for assessing the risks of geological disposal [4]. Instead, they suggested the use of a qualitative assessment to evaluate the level of safety of proposed geological repositories based on a "systematic identification of those natural and anthropogenic 'features, events, and processes' (FEPs) that could cause or contribute significantly to failure of the repository to meet design or regulatory standards" [2].

In the decade 1978–1988, the Sandia National Laboratories, contracted by the NRC, developed a performance assessment (PA) methodology for licensing of geological repositories for the disposal of commercial high-level waste and spent fuel [5]. The development of a PA methodology was contentious because different scientific communities had very different views on how to model geological disposal systems, treat uncertainties, and assess safety levels. By the end of the 1980s, a probabilistic approach to PA developed by the engineering community would eventually become accepted by the U.S. regulatory agencies—the Environmental Protection Agency (EPA) and the NRC—for determining the long-term performance and evaluating the acceptability of geologic waste disposal systems [2]. The methodology included many of the features still present in modern PAs: identification of natural and anthropogenic FEPs, probabilistic models of FEPs, transport models of radionuclides by dissolution and transport by groundwater, environmental pathways and health effects models, as well as sensitivity analysis techniques [6].

By 1985, "performance assessment" had become the term of choice to describe all risk-based, probabilistic analyses that were applied to nuclear waste disposal systems [2]. In 1991, OECD's Nuclear Energy Agency (NEA) defined PA as "an analysis to predict the performance of a system or subsystem, followed by a comparison of the results of such analysis with appropriate standards and criteria" [7]. In the 1990s, a distinction between PA and PRA needed to be maintained because PA did not necessarily imply a probabilistic evaluation of uncertainties [8]. In the United States, however, PA and PRA, as practiced, were synonymous because performance criteria were risk based and uncertainties were systematically evaluated using probabilistic methods [9]. Already in the mid-1980s, the U.S. regulatory framework specifically required the use of the PPA approach (*e.g.*, EPA's 40 CFR 191.12 [10]). Today, the NEA also recommends the quantitative evaluation of uncertainties in PAs of disposal systems [11] and the IAEA sees many benefits in adopting a probabilistic approach to the evaluation of these uncertainties [12].

Downloaded from https://www.cambridge.org/core. Stanford Libraries, on 08 May 2019 at 16:13:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1557/adv.2018.681

SAFETY CASE APPROACH

In contrast to the PPA, the safety case approach is broader and more inclusive. According to the IAEA, a safety case is “the collection of scientific, technical, administrative and managerial arguments and evidence in support of the safety of a disposal facility, covering the suitability of the site and the design, construction and operation of the facility, the assessment of radiation risks and assurance of the adequacy and quality of all of the safety related work associated with the disposal facility” [12]. According to the NEA, a typical safety case has to include several key components [11]:

1. A *safety strategy*—a high-level integrated approach used to achieve the objective of safe disposal. It includes several sub-strategies for the management activities, the repository siting and decision-making process, the performance assessments, and the development of a safety case. The safety strategy forms the basis for the communication with stakeholder groups. Thus, their feedback can improve the strategy during the development and operational phases of a geological repository.
2. An *assessment basis*—the technical and scientific content on which the safety assessment is based. It includes key components, such as: *(i) System concept*, both for the repository site and design, which typically includes a site-descriptive model, the location and layout of the repository, and a description of the engineered barriers. The system concept should also include a description of the expected safety functions of both engineered and natural barriers; *(ii) Scientific and technical information and understanding* in the form of a unified and consistent description of the various FEPs (and their interactions) that may affect the behavior and long-term performance of the geological repository; and (iii) *Methods of analysis, computer codes, models and databases*, which support the numerical modeling of the disposal system, its evolution and the quantification of its performance.

The safety strategy and the assessment basis form the starting points of each stage in the development of a safety case. Together, these elements form the evidence supporting analyses and arguments about the suitability of the repository site and design. A safety case is generally prepared at an early stage in the development of a geological disposal facility as a guide for development, siting, and design efforts [13]. The safety case is then iteratively updated and revised as new data are gathered about the site. At all times in the process, the level of confidence in the suitability of the site must be sufficient to gain political and public support so that the design and operation of the geological disposal facility can progress.

A safety case will conclude with a statement of confidence made by the implementer [11]. The statement of confidence is a compelling argument that states that the analyses and arguments developed and the evidence gathered provide enough confidence to achieve the safety goals and therefore supports the decision to proceed to the next stage of planning or implementation. However, when evidence, arguments and analyses do not give sufficient confidence for supporting a positive decision, then the assessment basis can be improved, the design revised, or the site abandoned [11]. The safety case approach, as proposed by the NEA, has been implemented by the Swedish nuclear waste disposal program [14].

Downloaded from https://www.cambridge.org/core. Stanford Libraries, on 08 May 2019 at 16:13:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1557/adv.2018.681

THE SAFETY CASE IN THE U.S. PROGRAM

In a report prepared for the U.S. Department of Energy, Sandia National Laboratories and Argonne National Laboratory defined the safety case approach for generic deep geologic disposal systems in the United States [15]. But the introduction of the safety case concept in the U.S. repository program reveals important departures from the initial definition proposed by the OECD's NEA. For instance, the safety case concept, as currently practiced in the U.S., no longer includes key components of the safety case such as the assessment basis and the iterative process of update and revision of the evidence, analyses and arguments. Instead, the safety case is reduced to a process of site selection, site characterization, and repository design serving the basis for evaluating the pre-closure and post-closure safety [16]. However, the safety case approach is much more than the extension to pre-closure safety of the PPA approach which, by U.S. regulations, is limited to evaluating post-closure safety. According to the NEA, a safety case approach is a process in which safety criteria are decided first and then evidence come to provide confidence—or not—that a repository site and design can meet those criteria. Therefore, the introduction of the safety case approach in the U.S. program, so far, has not remained true to the original concept proposed by the international community.

Similarly, the IAEA's definition of a safety case also reveals departures from NEA's initial definition [12]. Although any concepts and methods can understandably evolve, some key aspects of the safety case, as originally proposed by the NEA, have either been removed or made less consistent within IAEA's framework. For instance, and similarly to the U.S. definition, the notion that the safety strategy can be revised based on evidence gathered is still present, but it no longer makes explicit what exactly should be revised. In particular, unlike NEA's latest definition [11], the IAEA does not mention whether the site itself could be reconsidered in the situation where there is not sufficient confidence that the site is suitable to achieve the safety goals. These different definitions illustrate how the concept of safety case is fundamentally subject to many interpretations. To effectively implement this approach, the concept of the safety case therefore needs further clarification in the context of the U.S. geologic disposal program.

COMPARISON OF THE TWO FRAMEWORKS

The crux of the safety case approach is an iterative process of updating and revising the argument about safety as new data are gathered about the site. A typical PPA in the U.S. repository program also includes iterations. Once the system-level analysis is constructed and the overall performance metrics have been estimated, iterations are made about the characteristics of the proposed disposal system, that is the waste form, repository design, and site [1]. In the PPA framework, iterations are made until the estimated performance meets the programmatic and regulatory needs, that is *regulatory compliance*. But these iterations only concern the technical aspects of a PPA. They do not imply the possible revision of the safety strategy. In a PPA, iterations are reduced to the optimization of the repository design [17]. The optimization of the disposal system has implications for how uncertainties will be treated. In PPAs, the successive iterations serve the purpose of reducing as much as possible the uncertainties based on new data about the site and the repository design. In this approach, epistemic uncertainties are thought to be reducible. In practice, however, a significant amount of epistemic uncertainty will remain in any mature PPA [1]. For instance, at the proposed Yucca Mountain repository in Nevada, new data about the site provided direct evidence that the groundwater could travel downwards some 300 meters from the surface to the repository horizon in about 50 years—thus, much faster than previously thought [18]. Therefore, the key assumption that the unsaturated zone at Yucca Mountain would remain dry at least during current climate conditions was falsified. Based on this new evidence, the repository design was revised by the addition of titanium drip shields to delay the access of water to the waste package and avoid the possibility of localized corrosion during the thermal period [19]. But the Yucca Mountain site was never reconsidered even though the key assumption that the site is "dry" was falsified by new data.

In a safety case approach, a site can be reconsidered based on new evidence. But this requires that the assumptions be made explicit, *a priori*. This is a key aspect of the safety case approach, as proposed by the NEA, where the applicant must make explicit in advance what the safety strategy is and then this strategy is constantly refined as the site is studied [11–13]. A PPA works backwards; it attempts to "demonstrate that the design and operation of the facility are compliant with the relevant safety requirements" [12].

DISCUSSION AND CONCLUSIONS

The value of a safety case approach resides in the way it uses quantitative information in the decision-making process. For instance, the quantification of epistemic uncertainties serves only as a guide to additional research or to a qualitative argument (*i.e.*, a "safety case") about the possible long-term behavior of the repository. To ensure that the safety case approach meets this objective, some have recommended that the uncertainty quantification of sub-surface systems start by defining clearly and unambiguously all hypotheses (*e.g.*, uncertainties on all parameters), *a priori* [20]. In the context of geological disposal systems, this corresponds to making explicit the safety strategy and its associated assumptions early in the development of a safety case. This would allow the safety strategy to be updated and revised based on new evidence obtained about the site.

Given the use of probabilistic approaches to uncertainty quantification in geological disposal systems, applicants should rely on rigorous principles of how to reason about evidence and hypotheses. This proposal is not new. Already in the 1990s, some called for PPAs to be entirely "evidence-based" through the strict application of the Bayes' theorem [21]. The safety case approach provides the opportunity to respond to this call by being explicit about what the assumptions are and whether new evidence confirm or contradict these assumptions. Because the safety case approach allows the safety strategy to be updated and revised as comments from stakeholders are received it is an essential component in building trust in the evaluation of the safety of a specific repository. This suggests that the use of the safety case approach could be an important step forward in resetting America's nuclear waste strategy and policy [22].

Downloaded from https://www.cambridge.org/core. Stanford Libraries, on 08 May 2019 at 16:13:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1557/adv.2018.681

Downloaded from https://www.cambridge.org/core. Stanford Libraries, on 08 May 2019 at 16:13:25, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1557/adv.2018.681

ACKNOWLEDGMENTS

The project leading to this publication has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No 739850, as well as from the MacArthur Foundation under the Nuclear Security Fellowship program of the Center for International Security and Cooperation (CISAC) at Stanford University. The authors thank Peter Swift for his perceptive arguments against some of the basic tenets of this paper.

REFERENCES

1. P.N. Swift, in *Geological Repository Systems for Safe Disposal of Spent Nuclear Fuels and Radioactive Waste (Second Edition)* edited byM.J. Apted and J. Ahn (Woodhead Publishing, 2017), pp. 451–473.
2. R.C. Ewing, M.S. Tierney, L.F. Konikow, and R.P. Rechard, Risk Anal **19**, 933 (1999).
3. U.S. NRC, *An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants* (U.S. Nuclear Regulatory Commission, Washington DC, USA, 1975).
4. J.D. Bredehoeft, A. England, D. Stewart, N. Trask, and I. Winograd, *Geologic Disposal of High-Level Radioactive Wastes: Earth-Science Perspectives* (U.S. Department of the Interior, U.S. Geological Survey, Alexandria, VA, USA, 1978).
5. J.E. Campbell, R.T. Dillon, M.S. Tierney, H.T. Davis, P.E. McGrath, F.J. Pearson, H.R. Shaw, J.C. Helton, and F.A. Donath, *Risk Methodology for Geologic Disposal of Radioactive Waste: Interim Report* (Sandia National Laboratories, Albuquerque, NM, USA, 1978).
6. R.N. Cranwell, R.V. Guzowski, J.E. Campbell, and N.R. Ortiz, *Risk Methodology for Geologic Disposal of Radioactive Waste: Scenario Selection Procedure* (Sandia National Laboratories, Albuquerque, NM, USA, 1990).
7. OECD Nuclear Energy Agency, *Disposal of High-Level Radioactive Wastes: Radiation Protection and Safety Criteria, Proceedings of an NEA Workshop, Paris, 5-7 November 1990* (Nuclear Energy Agency, Organisation for Economic Co-operation and Development, Paris, France, 1991).
8. OECD Nuclear Energy Agency, *Disposal of Radioactive Waste: Review of Safety Assessment Methods, A Report of the Performance Assessment Advisory Group of the Radioactive Waste Management Committee* (Nuclear Energy Agency, Organisation for Economic Co-operation and Development, Paris, France, 1991).
9. R.P. Rechard, Risk Anal **19**, 763 (1999).
10. U.S. Environmental Protection Agency, *Title 40 Code of Federal Regulations Part 191, Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes; Final Rule* (1985), pp. 38066–38089.
11. OECD Nuclear Energy Agency, *The Nature and Purpose of the Post-Closure Safety Cases for Geological Repositories* (OECD NEA, Paris, 2013), p. 53.
12. IAEA, *The Safety Case and Safety Assessment for the Disposal of Radioactive Waste* (International Atomic Energy Agency, Vienna, Austria, 2012), p. 120.
13. OECD Nuclear Energy Agency, *Post-Closure Safety Case For Geological Repositories: Nature and Purpose* (Nuclear Energy Agency, Organisation for Economic Co-operation and Development, Paris, France, 2004), p. 54.
14. A. Hedin and J. Andersson, *SKB's Safety Case for a Final Repository License Application* (OECD Nuclear Energy Agency, Paris, France, 2014), p. 8.
15. G. Freeze, M. Voegele, P. Vaughn, J. Prouty, W.M. Nutt, E. Hardin, and S.D. Sevougian, *Generic Deep Geologic Disposal Safety Case, Rev 1* (Sandia National Laboratories and Argonne National Laboratory for U.S. Department of Energy, Used Fuel Disposition Campaign, 2013), p. 356.
16. R.J. MacKinnon, S.D. Sevougian, C.D. Leigh, and F.D. Hansen, *Towards a Defensible Safety Case for Deep Geologic Disposal of DOE HLW and DOE SNF in Bedded Salt* (Sandia National Laboratories, Albuquerque, NM, USA and Livermore, CA, USA, 2012), p. 62.
17. W. Weiss, Ann ICRP **41**, 294 (2012).
18. D. Metlay, in *Prediction: Science, Decision Making, and the Future of Nature* (Island Press, Covelo, CA, 2000), pp. 199–228.
19. R.P. Rechard and M.D. Voegele, Reliab Eng Syst Safe **122**, 53 (2014).
20. C. Scheidt, L. Li, and J. Caers, editors, *Quantifying Uncertainty in Subsurface Systems* (Wiley & the American Geophysical Union, New York, N.Y., 2018).
21. B.J. Garrick and S. Kaplan, Risk Anal **19**, 903 (1999).
22. Reset Steering Committee, *Reset of America's Nuclear Waste Management Strategy and Policy* (Stanford University, Stanford, CA, 2018).