SAND2007-5251C

The Safety Case

KHNP Training Program
Module 6: Assembly of a Safety Case

August 14, 2007

Rick Beauheim
Sandia National Laboratories
Carlsbad Programs Group

SAND 2007-XXXP

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Outline

1. Safety Assessments
2. Safety Case
3. Safety Strategy
4. Assessment Basis
5. Synthesis
6. Case Studies

[Primary source: NEA. 2004. Post-closure Safety Case for Geological Repositories]

Safety Assessments

- Safety assessments are one component of, and support, a safety case
- Safety assessment is the process of systematically analyzing the hazards associated with the facility and the ability of the site and the design of the facility to provide for the safety functions and to meet technical requirements*
- Safety assessment includes quantification of the overall level of performance, analysis of the associated uncertainties, and comparison with the relevant design requirements and safety standards*

* IAEA Safety Standard No. WS-R-4

Safety Case

- A safety case is the synthesis of evidence, analyses, and arguments that quantify and substantiate a claim that the repository will be safe after closure*
- Safety cases become more comprehensive and rigorous as a program progresses
- The safety case provides a basis for informed discussion at all levels of technical sophistication

*NEA (2004)

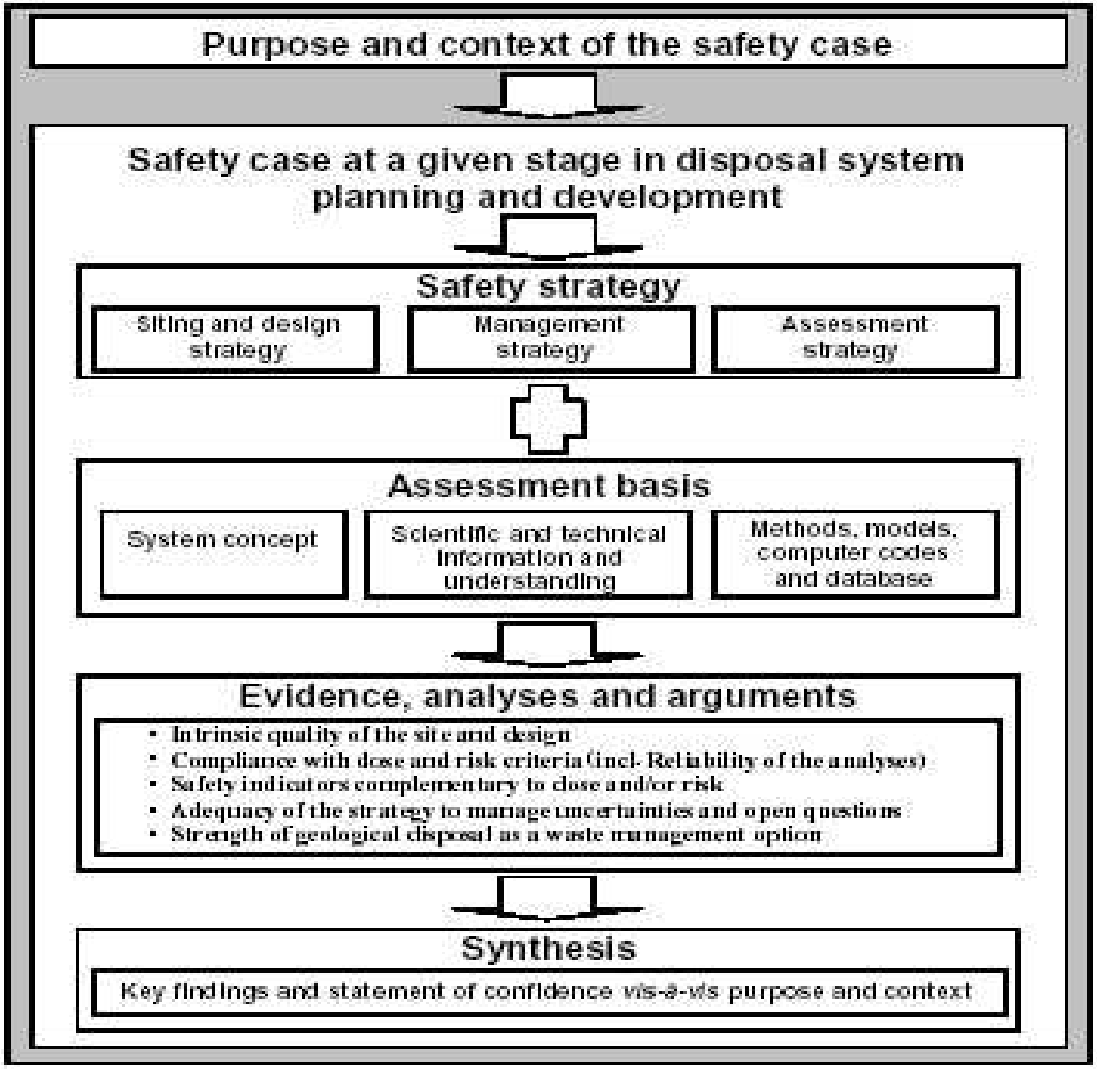
Role of a Safety Case

- A safety case, in the form of a structured set of documents, is typically required at major decision points in repository planning, implementation, and operation
- The safety case must be adequate to support the decision being made and, consequently, becomes more complex as the project advances
- The effort involved in preparing a safety case and presenting it to scientific, technical, regulatory, and public review ensures that safety is explicitly and, importantly, visibly considered at each stage of a project

Elements for Documenting the Safety Case

- The purpose and context of the safety case should be stated clearly—always relate to the decision under consideration
- The safety strategy should be described
- The assessment basis must be described
  - System concept
  - Scientific and technical knowledge base
  - Methods of analysis
- A synthesis must be made to draw together key evidence, analyses, and arguments that quantify and substantiate a claim of safety

Relationship of Safety Case Elements



Presentation of a Safety Case

- Purpose and context of the safety case must be clear
  - The stage in the project currently reached
  - How the required attributes of the geological setting of the repository will be tested or confirmed
  - How the feasibility of the manufacture or construction of the engineered barrier system will be achieved
  - How the repository will be constructed, operated, and closed
  - How these procedures will be controlled, as well as programmatic and practical factors that constrain the project

Presentation of a Safety Case (2)

- The scope, level of detail, and style of presentation of a safety case will vary depending on the intended audience, the decision under consideration, and any regulatory requirements related to that decision
  - Technical specialists, regulators, and the wider scientific community will expect a detailed presentation and rigorous analyses
  - Political decision makers need to be confident that the concerns of their constituents are being considered and resolved
  - Public audiences may need a more qualitative, understandable safety case that may focus more on the near future (current population and next generation or two) than on the distant future
- No matter the audience or level of detail being presented, consistency and technical accuracy must always be maintained

General Considerations in Presentation of a Safety Case

- Transparency
- Traceability and historical perspective
- Openness with respect to uncertainties and confidence
- Peer review

Safety Strategy

- The safety strategy is the high-level integrated approach adopted for achieving safe disposal
- It has three principal components:
  - The overall management strategy of the activities required for repository planning, implementation and closure, siting and design, safety assessment, and waste characterization
  - The siting and design strategy
  - The assessment strategy

Safety Strategy—Precautionary Principal

- The safety strategy should err on the side of caution
- The siting and design strategy should aim at developing a reliable and robust system characterized by a lack of complex, poorly understood, or difficult to characterize features and phenomena, an ease of quality control, and an absence of, or insensitivity to, detrimental phenomena
- The assessment strategy should provide a range of arguments and analyses that are well-founded, supported by multiple lines of evidence, and adequate in their treatment of uncertainty

Safety Strategy—Need for Flexibility

- Flexibility should be built into the planning and implementation of a repository
- It is important because of the long time scales involved and the scarcity of data early in the process
- A stepwise approach should be adopted that allows for the information gained at each stage to inform decisions taken for subsequent stages
- Completion of each stage allows a time for scientific and regulatory review, as well as opportunities for political and public consultation and involvement

Safety Strategy—
Robustness and the Multi-Barrier System

- A repository is said to be robust if multiple, complementary factors provide wide safety margins
- Geologic stability, absence of natural resources, and isolation (decoupling) from near-surface phenomena all contribute to safety
- Engineered barriers add to the geological barrier, making a multi-barrier system
- Engineered barriers can be designed to complement one another, and to be effective at different times in the future

Safety Strategy—
Characterizing and Managing Uncertainties

- Uncertainties should be identified during safety assessment
- Uncertainties can be managed by increased data collection, improved models, and/or design changes
- Modeling can use probabilistic techniques to account for uncertainties, or can use conservative values for uncertain parameters
- Uncertainties must be openly acknowledged and treated transparently

Assessment Basis—Components

- The assessment basis consists of the information and analysis tools used for safety assessment and includes:
  - The system concept
  - The relevant scientific and technical data
  - The assessment method, models, computer codes, and databases
- Quality and reliability of the components of the assessment basis are critical

Assessment Basis—Presentation and Support for System Components

- System components include the host rock and surrounding geological environment, the surface site, waste inventory, engineered barriers, and repository design
- The description of each component should include:
  - Its geometry and constituents
  - Its safety functions
  - Its expected evolution and performance
- Must show the system is realistic and feasible:
  - Describe site characterization procedures
  - Describe quality management procedures and waste acceptance criteria
  - Evaluate feasibility of constructing repository

Assessment Basis—Presentation and Support for Scientific and Technical Information

- Presentation of scientific and technical information should show that the information is consistent, well-founded, and adequate for safety assessment
- The research and site investigation programs should be shown to be comprehensive
- Important to include diverse sources of information providing multiple lines of argument
- Documentation should be traceable and transparent, providing clear records of how and where data are used and the QA system that was used

Assessment Basis—Presentation and Support for Assessment Method

- The approach should be logical, clear, and systematic
- The assessment should be conducted within an auditable framework
- The approach should be continually improved through an iterative process
- The approach should be peer-reviewed
- Implementors and safety assessors should be in close communication as data are acquired
- Sensitivity analyses should be performed to ensure that scenarios and calculations address uncertainties

Assessment Basis—Presentation and Support for Assessment Method (2)

- Suitable criteria must be established for FEPs screening
- FEPs should be compared to the international FEPs lists
- Evidence supporting the choice of scenarios, models, and data should come from multiple sources and be supported by multiple lines of argument
- Models should be traceable to well-established principles or relevant empirical relationships
- Computer codes should be developed and verified in a QA environment
- A clear strategy and methods for handling uncertainties should be apparent

Synthesis—
Evidence, Analyses, and Arguments

- General evidence for the strength of geological disposal as a waste management option
- Evidence for the intrinsic quality of the site and design
- Safety indicators complementary to dose and risk
- Arguments for the adequacy of the strategy to minimize uncertainties and open questions

Synthesis—
Emphasizing Different Aspects

- The emphasis placed on different lines of arguments and analyses can vary depending on:
  - The concerns and requirements of the intended audience
  - The time scale over which safety is being discussed
  - The stage of project development and level of confidence that has been established
  - The expected evolution of the system, and associated uncertainties, and their implications for performance

Synthesis and Statement of Confidence

- A synthesis should include a statement of confidence that the information available supports a decision to go forward
- The safety case is a basis for decision-making and must be convincing to the decision-makers, so the synthesis should be complete and convincing

Summary

- Preparation of a safety case should be a primary management objective
- The safety case pulls together all the work that has been done, and assembles it into a comprehensive and consistent story about how the repository will be constructed and operate in a safe manner
- The safety case needs to address the concerns of all types of audiences in forms intelligible to them
- A safety case should be peer-reviewed
- The high quality of the underlying work may be overlooked if the safety case and its synthesis are not themselves of high quality

Example—Dossier 2005 Argile

- Andra prepared three levels of synthesis for different types of readers:
  - The 240-page Synthesis for technical and regulatory reviewers
  - A 40-page summary in question and answer format for the interested public with some technical understanding
  - A 4-page brochure for the general public

Example—SAFIR 2 Report

- ONDRAF/NIRAS prepared one detailed (~270 pages) synthesis (Technical Overview of the SAFIR 2 Report) for technical and regulatory reviewers