Review of an Existing Safety Case

John Goodenough, Charles Weinstock,
Carol Woody, Robert Ellison, William Nichols

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Objective and Overview

Objective for Today

- Explore how structured assurance arguments are used in practice

Overview

- Publicly Available Safety/Assurance Cases
- Review of a particular case (prose vs graphical)
- Observations
- What next?

Publicly Available Cases Found So Far

Cases provided from various sources:

- Critical System Labs:
  - Portions of safety arguments for an ATC display system
  - Portions of safety arguments for the Large Hadron Collider
  - Papers discussing safety cases for railways, CubeSats, and a nuclear reactor
  - The UK MOD Manual of Air System Safety Cases
- AdvoCATE (NASA): A paper about a safety case for an unmanned aircraft system
- Mallory Graydon (NASA): A safety case for geological disposal of nuclear waste in Switzerland *(this will be the focus of our discussion today)*

We were hoping to get a real case for an Air Force system that is being developed by Dependable Systems Corp, but it is still awaiting public distribution authorization

We reached out to other sources but they were not forthcoming with examples

NAGRA Opalinus Clay Nuclear Waste Disposal Case

"Perhaps the most comprehensive publicly available safety case I am aware of"

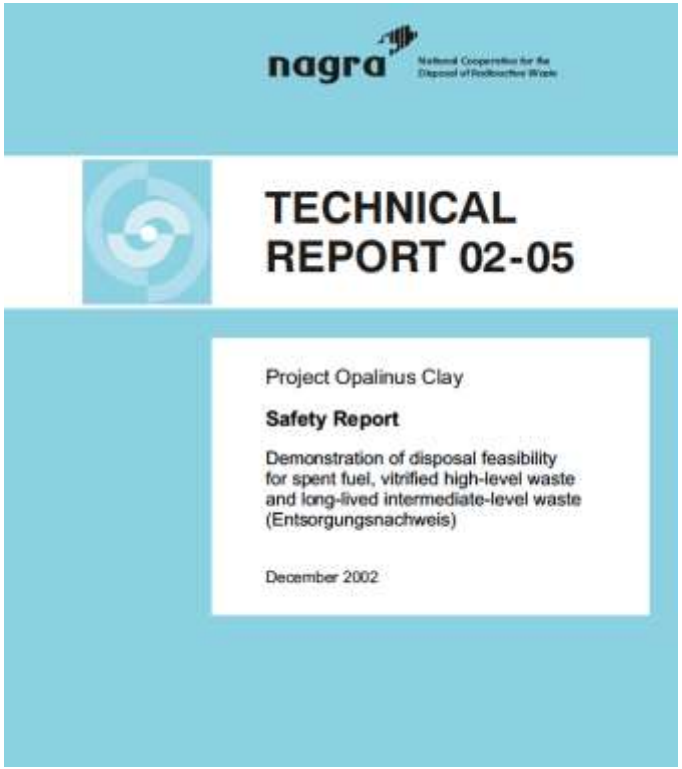
It's in prose – not a formal safety case notation, but at its core a safety case is just a well thought out explanation to a defined interested audience of the answers to three questions:

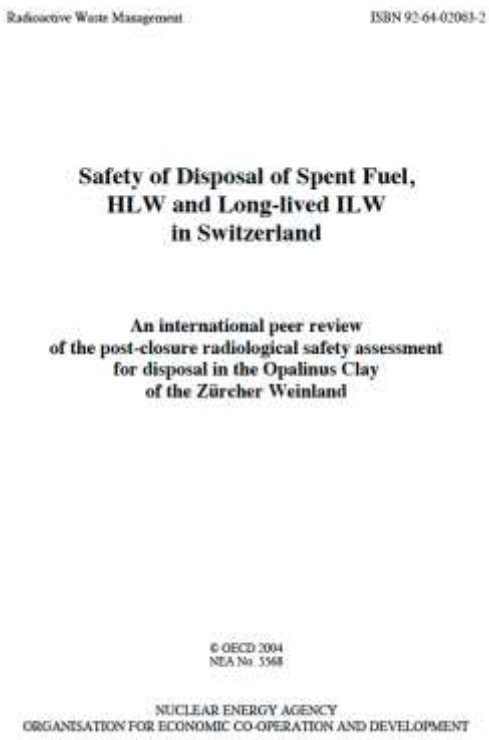
1. How can it hurt people?
2. What's being done to prevent that?
3. How will the developers know that they are done?

The OC case is for a single very expensive installation meant to be safe beyond the civilization that built it and covers everything from the geology of the site to construction techniques.

It is meant to invite critical enquiry from anyone who might have thought of something that the site's engineers didn't.

Two Documents: The Case and a Peer Review

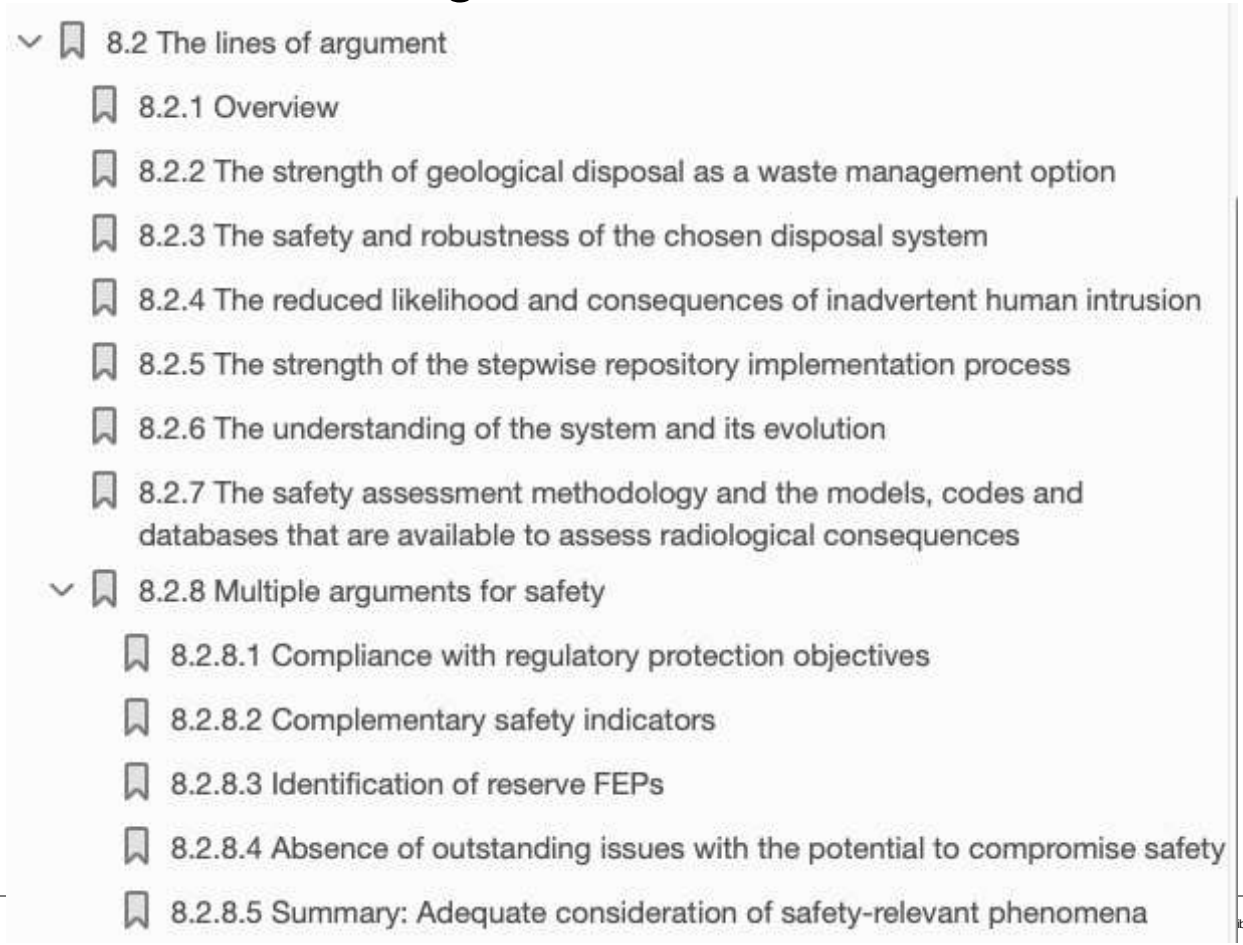




Safety Case Table of Contents

Chapter 8: The Safety Case and Results

Section 8.2: The Lines of Argument



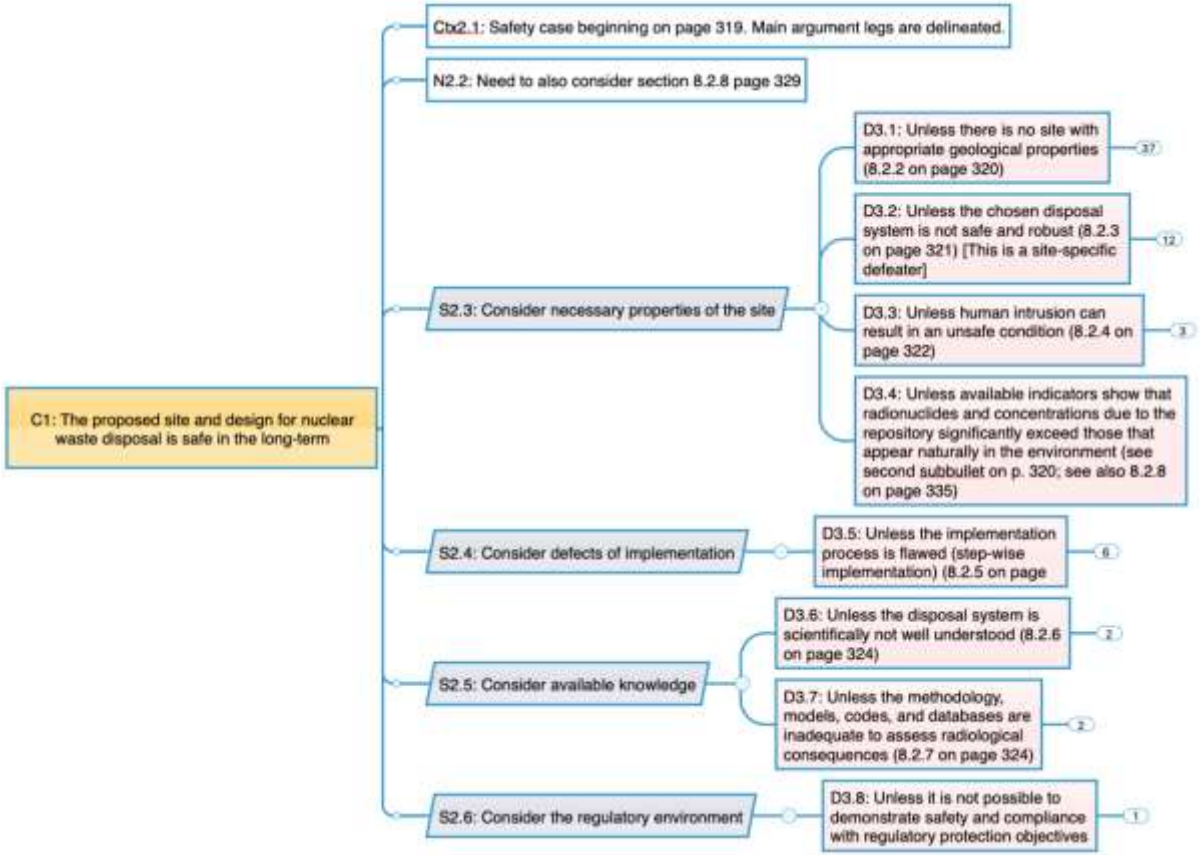
Section 8.2.2: The Strength of Geological Disposal

8.2.2 The strength of geological disposal as a waste management option

Radioactive waste needs to be managed in a way that ensures the safety of humans and the protection of the environment, as well as providing security from malicious intervention, now and in the future. According to current understanding, geological disposal is the only waste management option that offers long-term passive safety. Placing the waste in a deep rock formation favours security in that it reduces the possibility of irresponsible interference. Furthermore, the feasibility of safe geological disposal is supported by:

- **The existence of suitable rock formations** – In Switzerland and elsewhere, deep rock formations exist in which events and processes that might convey radionuclides to the surface environment are either absent, or extremely rare or slow.
- **Safety assessments conducted world-wide** – The findings of integrated safety assessments conducted world-wide for a wide range of sites and designs support the possibility of safe geological disposal.
- **Observations of natural systems** – Indirect support for safety also comes from observations of natural systems, including the longevity of uranium ore deposits in many different geological environments around the world. This includes the observed retention of most of the radioactive inventory of the Oklo natural reactor over a period of ~ 2 billion years. Furthermore, there is ample evidence of the importance of the natural processes of solubility control, sorption and diffusion in attenuating concentrations of species dissolved in porewater.
- **Characteristics of surface facilities versus geological disposal** – Radioactive waste can be stored for a time in surface facilities. The safety of these facilities is, however, dependent on continued societal stability, which is subject to uncertainties that are far greater than those associated with the evolution of conditions deep underground in geological formations that would be suitable to host a repository. As a long-term waste management option, deep

Section 8.2.2 Graphically (First Two Levels)



Switch to MindManager for discussion of the graphical argument

The Value of the Graphically Structured Approach

The prose argument appears to have been sufficient to convince a committee of SMEs that the Opalinus Clay case was sound, but there are two main benefits to using a graphical approach

1. The structured assurance case analysis can surface reasoning gaps that were otherwise overlooked
2. The graphical structure makes the case more accessible to:
   - Non-SMEs who are otherwise technically aware
   - Certifying authorities

N.B., the graphical structure can include links to more complete detailed prose, tables, or other relevant documents so nothing is lost while a lot is gained

What Next?