Human Factors, System Safety, and Systems Engineering in the Transportation of U.S. High-Level Waste

Dennis L. Price and Sherwood C. Chu

U.S. Nuclear Waste Technical Review Board

Abstract

The U.S. Nuclear Waste Technical Review Board is an independent agency charged with evaluating the technical and scientific validity of the U.S. Department of Energy's program to manage the disposal of spent fuel and defense high-level waste. The Board has continued to emphasize the importance of using a true system approach in designing the waste management system. The Board has recommended the application of basic design disciplines such as human factors, system safety, and systems engineering. A top-level system study needs to be undertaken that focuses on minimizing handling. The analysis must be well done, in a timely manner, and without the inclusion in the analysis of arbitrary and artificial constraints.

Introduction to the NWTRB

The U.S. Nuclear Waste Technical Review Board is *not* part of the U.S. Department of Energy — the DOE. The Board is an independent agency — created in 1987 by the U.S. Congress to provide an unbiased technical evaluation of activities undertaken by the DOE as part of its program to manage the disposal of civilian spent fuel. Members of the Board are nominated by the National Academy of Sciences and appointed by the President. There currently are 10 members.

Among the areas the Board is looking at are site-characterization activities and activities relating to the packaging and transport of spent nuclear fuel. It has been decided that high-level radioactive waste from reprocessing at defense-related facilities also will be disposed of as part of the civilian program. So the Board plans to look more closely at the packaging and transport of defense high-level waste in the future as well.

The Board has offices and a small staff located near Washington, D.C., and with the assistance of that staff the Board produces reports, usually two per year. These reports go to the U.S. Congress and the Secretary of Energy. To facilitate the evaluation process, the Board is divided into panels according to technical issues.

The Board believes that the management of spent fuel and high-level waste should be viewed as a true system, and that view must include *all* processes, beginning with waste generation and extend-

ing through waste emplacement and beyond. Also, a true system approach means using *systems engineering* in the design and analysis of the whole system and its components, without imposing arbitrary or artificial constraints on the analysis.

Conclusions About the DOE's Transportation Effort

After looking at the DOE's program, the Board's Panel on Transportation & Systems discovered that the transportation effort of the DOE's Office of Civilian Radioactive Waste Management (OCRWM) was not being addressed from a true system approach. Furthermore, that effort did not include a system safety program *or* a human factors program. In its first report to Congress and the Secretary of Energy (NWTRB, March 1990), the Board recommended that the DOE initiate these programs.

The Human Factor

As members of the human race, we are painfully aware that our limitations often contribute to the failure of our plans. "The best laid plans of mice and men gang aft agley", said Robert Burns, an eighteenth-century Scottish poet. When we translate that into modern English, what it means is that we must be very sensitive to the interaction between humans and technology, and the "human factor."

Even in countries that have what we consider excellent transportation systems, accidents and fatality numbers are entirely too high. Why? Humans make mistakes. In the United States, these mistakes contribute heavily to the 40,000 to 50,000 transportation deaths annually. If we add to our already very busy transportation system the additional transports of spent fuel and high-level radioactive waste, it is reasonable to foresee increasing opportunities for the effects of the "human factor."

However, it is not only a matter of simply adding more transports to the busy systems we have today; today's transportation systems will be changing dramatically in the future. How will the Japanese transportation system look in the year 2020? How will the U.S. transportation system look in 2020? That is when, according to the current schedule, the transport of spent fuel and high-level waste in the United States will be peaking.

We already know that *new transportation technology* is developing. Take a look at the highway example. We can expect greatly increased traffic volume, but with comparatively little room to accommodate this ever increasing volume using traditional methods, such as broadening or building new roads. What's the answer? One answer might be smart roads and smart vehicles, which guide traffic on to less congested roads. Such technologies are not only on the drawing boards, but becoming reality. For example, scientists are now testing systems that will help detect nearby objects; identify driver impairments; enhance night vision; identify possible collisions; and move heavy traffic smoothly.

However, each innovative technology brings with it the opportunity for innovative human error. Let's look at the truck cab of a futuristic vehicle that has been designed to carry spent fuel and high-level waste. In addition to the instruments and controls normally found in a trailer truck cab, we might find displays and controls for:

1. a vehicle tracking system that tracks the location of the truck
2. an emergency communications system for notifying the nearest emergency facilities

3. a cask monitoring system that documents conditions within the cask
4. a special fire control system, and
5. an intelligent vehicle/highway system, which will help the driver position the vehicle in heavy traffic, avoid hidden objects, and drive efficiently.

Just think of the potential opportunities for human error.

Innovative technology means innovative human error. Do any of you remember those old-fashioned, wind-up alarm clocks? Do any of you still have one of those? I don't remember the last time I saw one of those things. Remember how they worked? Easy, you set the time, wound it up, and turned the alarm hand indicator to the desired wake-up time. You could go to sleep without a worry. At 7:00 a.m., the alarm sounded, just as expected. Then came the *digital* clock with all of its buttons and dials. Check the time. Set the alarm for 7:00; go to sleep; then you wake yourself up at 8:00 — in a panic. The alarm didn't go off. Why not? With a little detective work, you discover that you set the alarm for seven p.m., twelve hours late. This isn't a problem you had with the old clock. New technology breeds new errors.

Or, look at aviation. Few pilots today would say that our air navigation system would be improved by going back to the old system, hand calculation of time and distance and the visual recognition of way points. Too much opportunity for error, right? However, the latest technology in air navigation has created its own opportunities for navigational errors. One has the nickname "finger trouble." It consists of entering the wrong data in the on-board navigational computer through a keyboard error. Some believe this was the error that resulted in the unfortunate shoot-down of a Korean Airliner that strayed into restricted airspace over the former Soviet Union in the mid-1980s. Innovative technology breeds innovative such human error.

When a *new* vehicle control center is installed in a *new* trailer cab designed to haul a *new* cask design on a *new* highway system, what will be the *new* sources of human error, and most important, what will be the consequences of such human error?

Cascading errors, in which one error sets off a chain of errors resulting in a chain of accidents also is of concern. Yes, even good, conscientious people lose control of things now and then. Consider this letter from Mr. Smith to his boss.

> *Dear Mr. Jones:*
>
> *Yesterday morning I arrived at work early. I saw that during the night the top layers of brick and fresh mortar from the construction the day before had been toppled by a storm. I cantilevered a pulley from the top of the building, strung a rope through the pulley and attached it to a barrel on the ground. I placed some bricks in the barrel and raised it to the roof.*
>
> *After making repairs to the wall, I noticed bricks and debris on the roof left-over from previous work. I tidied up the roof, putting the materials in the barrel. Then I went down to the ground and unfastened the rope to lower the barrel.*
>
> *It was then that I discovered that the barrel's weight was greater than my own. The barrel proceeded down; I proceeded up. Halfway up, I met the barrel coming down, it struck me on the left side of the face breaking my left jaw. It continued down; I continued up, mashing my fingers in the pulley. Just then, the barrel struck the ground, breaking open, losing it's load.*

Now I was heavier than the barrel. The barrel started up; I started down. Halfway down, I met the barrel coming up, it struck me on the right side of the face, breaking the other side of my jaw. It continued up, I continued down, falling on the pile of bricks left by the barrel. The sharp bricks cut a part of my anatomy better left unmentioned.

It was then that I must have lost my presence-of-mind, for I let go of the rope. When the barrel hit, it seemed to impact my whole body. I am still a little dazed; therefore, please excuse my absence from work.

Sincerely,
George Smith

Mr. Smith is obviously very conscientious — nevertheless, he is very injured. Mistakes can cascade until even very conscientious humans lose control. This has happened already in nuclear power plants, at Three Mile Island and at Chernobyl, for example; but it must not happen during the transportation of spent fuel or high-level waste.

Experts recognize the problem. At the university where I teach, Virginia Tech, a research team conducted a survey of 637 persons from five groups, including safety professionals, government employees in nuclear-related jobs, employees of environmental organizations, and Native Americans. Respondents were asked to rate the personal risk involved in ten health and safety situations, such as, natural disaster, motor vehicle accidents, job accidents, accidents around the home, etc. Risk associated with the transportation of spent fuel and transportation accidents involving spent fuel was rated lowest of all. But when respondents were asked to look specifically at *that* risk, they said that human error would be the most likely cause of radiation release during both interstate highway and railway transport of spent fuel. Almost 52 percent of the respondents reported a "high" or "very high" likelihood for human error to cause a release of radiation on interstate highways, and almost 42 percent found this to be the case for railways. (Roop, Price, and Pacquet 1992)

Those involved in the transport of spent fuel or hazardous materials of any kind know that human error is a major cause of concern. The question is: What can we do about it? Well we design the system with these issues in mind.

Human Factors and System Safety Programs

Both human factors and system safety engineers should be involved when designing systems to transport radioactive waste. Of course, *everyone* associated with this program should be very conscious of the overriding need for safety. However, the Board believes that there should be individuals working on the program whose *sole job* — sole responsibility — is safety.

A human factors program is one that provides a *life-cycle* application of what is known about human psychological, physiological, and physical limitations in the design and operation of systems, to optimize system safety and operability. In other words, such a program addresses design issues, like human error. The potential for human error to affect operational performance is a general concern that requires careful engineering design, accompanied by state-of-the-art allocation of system functions to operators and machines. A human factors program is staffed by professional human factors scientists and engineers.

In our first report we defined a system safety program as one that provides a *life-cycle* application of safety engineering and management techniques to the design of system hardware, software, and operations. We stated that such a program should be staffed by professional system safety engineers whose duties are dedicated to safety. Once you have looked at all the possible potentials for human error, you apply system safety engineering to reducing human error — you must *design the system to minimize error.* We don't live in a risk-free world, and taking some risks is reasonable, but which ones? Since no one can foresee and preclude all possible human errors, we must constantly strive toward two goals:

1. foresee the foreseeable
2. accept only reasonable risks

And one group of people whose techniques are designed to ensure proper foresight and risk acceptance are trained system safety engineers and professionals. One tool they use is the Management Oversight and Risk Tree — MORT (Johnson 1980), which is a planning tool based on the philosophy that an undesired event, like an accident, can happen for only two reasons:

1. through "oversight," or
2. through the occurrence of an "accepted risk."

Both reasons could be the result of prudent practice: that is,

1. the oversight — that which went unnoticed — could not have been reasonably foreseen
2. proper analysis revealed the risk was reasonable to accept.

Proper analysis is reasonable. Proper systems analysis identifies reasonably foreseeable hazards. The system safety engineer brings an expertise in analytical techniques that will help identify what is "reasonably noticeable." The legal and moral test that is part of our mandate is to foresee that which is reasonably foreseeable. We must reason. There are only two ways to reason:

1. inductively
2. deductively.

If state-of-the-art safety techniques for these two reasoning processes are applied properly, then the foresight gained is arguably "reasonable." A reasonable approach includes hazard identification. When proper and reasonable techniques are applied, the foreseeable is seen, and that which is not *reasonably* foreseeable may be "overseen." But such oversight can be defended as prudent.

This reasonable process also can be applied to *risk acceptance.* Risks that are identified through a reasonable process, but have not yet been analyzed and assessed, *cannot be accepted* as reasonable risks to take. The expected frequency and severity of the discovered potential hazard must be analyzed along with the spectrum of consequences that could occur. This must be done *before* one can decide if a risk is acceptable. Three steps are involved in determining what constitutes "acceptable risk."

1. Identify a risk
2. Analyze the risk
3. Decide whether or not the risk can be reduced and/or accepted

Any prudent program must also involve those experts skilled in probabilistic risk assessment and in the decision sciences.

Even though spent fuel has been shipped routinely for the past 40 years with an excellent safety performance record, the Board has continued to emphasize system safety and human factors recommendations in its reports (NWTRB, November 1990; May 1991). Why? I think it's pretty clear:

Once planned waste disposal shipments to a repository are underway — and maybe even before then if spent fuel goes first to an interim storage facility — the number of annual shipments of spent fuel and high-level radioactive waste will increase. The number of persons involved in — and who may be affected by — such shipments also will increase, as will the levels of public awareness and concern.

We also will be seeing the development and implementation of new equipment and systems at reactor sites, at the repository site, and perhaps at sites in between. These kinds of changes must be evaluated for *new* hazards.

And *old* hazards that have not been apparent because they did not cause incidents or accidents during the relatively infrequent shipments of the past may become apparent when the scale and diversity of operations increase.

The opportunity exists *now* for all parties involved in the design of our high-level waste management system to address these changes and their effects before — rather than after — they occur. Techniques need to be implemented that will more than just maintain the current level of safety. The Board believes that system safety and human factors engineering programs are among the management tools that will help fulfill that need.

Handling

Since transportation is only a part of a developing, complex spent fuel management system, the Board believes that the DOE needs to better understand and analyze the relationships and interactions among the various elements of the entire system. The Board recognizes that understanding all aspects of the management and disposal of high-level waste and spent fuel is not an easy task. Regardless of the complexities, however, system concerns must address *all* processes involved — beginning with waste generation and extending through storage, transport, emplacement, and beyond.

A very good way of approaching these issues is by looking carefully at the *one* activity that seems to bind together all these processes. That activity is *handling*. Think about all of the handling that could take place:

- *loading* and *storing* high-level waste or spent fuel after generation
- *removing* it from the storage facility
- *loading* it into transport casks
- *loading* and *unloading* it at points of origin and destination
- *storing* it again, and finally
- *emplacing* it. We also must keep open the option of
- *retrieving* it.

Incidents of both human error and equipment malfunction can be expected to rise with increased frequency of handling.

We must have an integrated *system view* of all handling from initial pool storage through repository emplacement, and even beyond. The Board's recommendations reflect this kind of *system*

view and clearly underscore the high priority of developing a radioactive waste management system that *minimizes* the handling of spent fuel throughout the life cycle. We need to do careful systems engineering and design to identify promising concepts that minimize handling.

Such promising concepts surely involve casks. The type of casks that are chosen, for example, will affect all of the players involved in the system and will help determine how the utilities store spent fuel on site, how it is transported, how interim storage facilities will be designed, the design of repository receiving and storage facilities, which emplacement concepts at the repository are chosen, and, finally, how the system will affect the managers, workers, and the public who are part of this system.

Currently, the DOE is emphasizing only single-purpose casks that would be used for transport. There are, however, several other concepts, such as dual-purpose casks and the *universal* cask. Those aren't the only options either. There are other viable options in addition to the single-, dual-, and universal-cask concepts. For example, one alternative configuration that would reduce handling might be to place the fuel assemblies in a canister, which is, in turn, transported on site to a dry-storage bunker. When it is time to ship, the canister can be inserted directly into a shipping cask without having to be returned to the pool for transfer. This concept might be compatible for the handling of high-level waste as well as of spent fuel.

Systems Engineering and Analysis

The Board believes that the advantages and disadvantages — including cost — of different types of casks as well as other components of the system should be evaluated by the DOE using a true system approach and *systems engineering and analysis*. There is opportunity here for creative thinking if we remain open to new solutions. Systems engineering, if done well, will allow us to do this kind of creative thinking and to evaluate how various components can affect other parts of the waste management system.

But doing good systems engineering is not enough — systems engineering must be timely — to ensure that major system acquisitions are made based on a sound understanding of the needs, functions, and interfaces of the various components of the system. And true systems engineering *can not* occur if arbitrary and artificial constraints are figured into the analysis.

Conclusions

To ensure the safety of any complex system, such as those being developed to transport radioactive wastes, three areas of technical expertise should be built into the design process. These areas include

1. human factors engineering
2. system safety engineering, and
3. systems engineering and analysis.

Human factors engineering will help us to minimize the potential for human error. System safety engineering will enable us to foresee the foreseeable risks and to choose only reasonable risks. Systems engineering and analysis will help ensure that all of the processes involved are understood and properly integrated. If, in fact, these three disciplines are applied correctly as the system to manage the disposal of radioactive waste is evolving, the efficiency and safety of that system should be greatly improved.

Bibliography

Johnson, W.G. 1980. *MORT Safety Assurance Systems.* Marcel Dekker. New York.

Nuclear Waste Technical Review Board. 1990. *First Report to the U.S. Congress and the U.S. Secretary of Energy.* 061-000-00747-4. March 1990. Washington,D.C.: U.S. Government Printing Office.

Nuclear Waste Technical Review Board. 1990. *Second Report to the U.S. Congress and the U.S. Secretary of Energy.* 061-000-00752-1. November 1990. Washington, D.C.: U.S. Government Printing Office.

Nuclear Waste Technical Review Board. 1991. *Third Report to the U.S. Congress and the U.S. Secretary of Energy.* 061-000-00762-8. May 1991. Washington, D.C.: U.S. Government Printing Office.

Nuclear Waste Technical Review Board. 1991. *Fourth Report to the U.S. Congress and the U.S. Secretary of Energy.* 016-036006-4. December 1991. Washington, D.C.: U.S. Government Printing Office.

Nuclear Waste Technical Review Board. 1991. *Fifth Report to the U.S. Congress and the U.S. Secretary of Energy.* 016-000-00785-7. June 1992. Washington, D.C.: U.S. Government Printing Office.

Roop, E., D.L. Price, and V.L. Pacquet. 1992. "Summary of the Transportation of Spent Fuel. Attitudes Summary," in proceedings of the Waste Management '92 Conference, Tucson, Arizona, March 1992.