Policy Studies Review, Vol. 1, No. 4, May, 1982

ACCOUNTABILITY AND CREDIBILITY IN THE MANAGEMENT OF COMPLEX HAZARDOUS TECHNOLOGY

Robert Anthony

For the public to accept a complex hazardous technology such as nuclear energy, the organizations sharing the responsibility for its management must be both credible and accountable. The need to prevent occasional human errors from having serious consequences nearly always leads to the adoption of multiple barriers against failure. Unfortunately, the different actions taken to enhance credibility, accountability, or multiple barrier against failure conflict with one another. The purposes of this paper are to show how these conflicts arise and to present three policy options based on information exchange that could reduce the level of conflict.

Throughout the paper, the general points are illustrated primarily by reference to a leak of liquid, high-level nuclear wastes from a storage tank at Hanford, Washington. Because weekly measurements performed by technicians were not systematically compared by day supervisors, 115,000 gallons of waste was able to escape into the soil beneath one tank over a period of six weeks before being detected (Metlay, 1978). Backup, dry-well monitoring also failed to detect the leak. Should those who established and reviewed the monitoring procedures be held accountable for this failure along with the day supervisors? The original designers performed extensive soil tests which convinced them that even if there were moderate leaks, toxic material would not reach the water table or migrate in the arid climate until it could be recovered and disposed of permanently (Hilberry, 1978). Should an event such as this affect confidence in the entire decision-making process guiding nuclear waste management at Hanford?

THE NEED FOR MULTIPLE BARRIERS AGAINST FAILURE IN COMPLEX SYSTEMS

As increasingly complex technical or social systems evolve, they become more failure-prone unless their constituent parts are exceptionally reliable, or there are backups to compensate for part failures. For very complex systems with moderately reliable parts and high demands for dependability, the backup strategy is much preferred. The principal theories of how dependable systems can be composed from less dependable parts—reliability theory, stability theory, and information theory—all employ this strategy, which I term "multiple barriers against failure" (von Neumann, 1956; May, 1971; Shannon, 1948). The strategy includes providing logically independent options, simple redundancy, feedback, and remedial actions.

Even though these theories were first developed for physical systems, biological and social systems also use the multiple barrier strategy. The social system of interest here—the decision-making process that guides

hazard management—will be represented in terms of information exchange and the roles of its participants; the corresponding multiple barriers include administrative and regulatory review, adversarial forums, and Congressional oversight.

The necessary physical steps for storing liquid wastes are shown in Figure 1. Material flows and physical properties dictate the relationships among the steps and the multiple barriers within each step. In this greatly simplified picture, each step is assumed to be independent of the last; in other words, the two steps of final disposal—of liquids and of tanks—will be independent both from storage and from one another. Thus, all the steps must succeed if the storage program is to succeed. On the other hand, chemical deterioration of the tanks and the potential for leaks generate the need for redundant or remedial alternatives if dependable storage at each step is to be ensured. Each of these alternatives is a barrier to unacceptable release of radioactivity; thus, only one alternative must succeed in each step for the system to work.

Figure 2 shows a simplified diagram of the corresponding institutional assurances of success in nuclear waste management. This structure is similar to that for the technical assurances, except that it involves two equally essential sequences of decision-making, one for hardware and the other for the operating staff. At every step of the decision-making process, each level provides a barrier as a backup for the others.

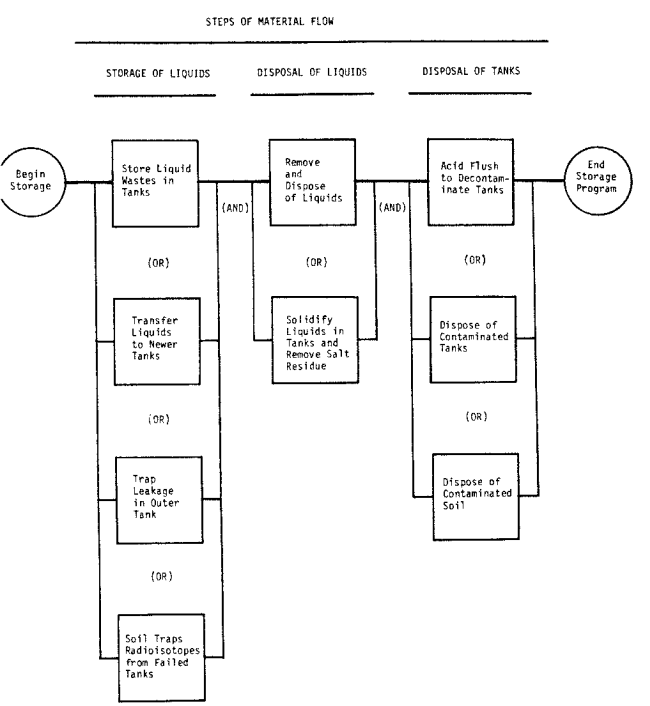
The distinction between the models for institutional and technical assurances lies in the criteria for success. If the decision-making process is to be deemed successful, it must assure all significant parties that their interests are both recognized and treated appropriately. This distinction is comparable to that between *being* safe and *knowing* that one is safe. Therefore, each decision-making step must have full public confidence based upon multiple institutional assurances which permit the discovery and redress of potential failures in the hazard management process. For example, the leak in tank 106T at Hanford represents a failure to have technicians compare their measurements; a failure of supervisors to realize they were excessively distracted by the press of other duties; a failure of the regulatory review mechanism to diagnose previous smaller leaks as the result of operator conditions; and a failure of policy-makers to recognize the lack of an essential consolidation of administrative activities.

INTRINSIC POLICY PROBLEMS AND OPTIONS FOR ADDRESSING THEM

Multiple barriers against failure is only one of three attributes necessary for managing complex hazardous technologies. The other two are accountability, which is the basis for the rewards and sanctions needed to pursue an organizational purpose (Thompson, 1967), and credibility, which is necessary in order to obtain acceptance of, and responsiveness to, delegated decisions (Whittaker, 1967; Laroche, 1977). From a broad and informed perspective, these two additional requirements support one

Figure 1

Technical Assurances of Safe Storage for High-level Radioactive Liquid Wastes

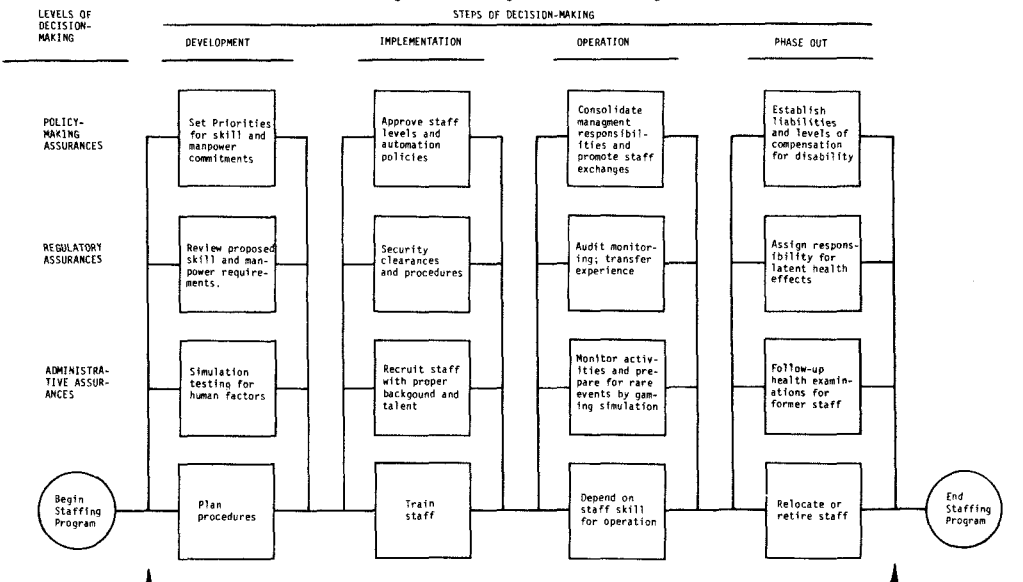


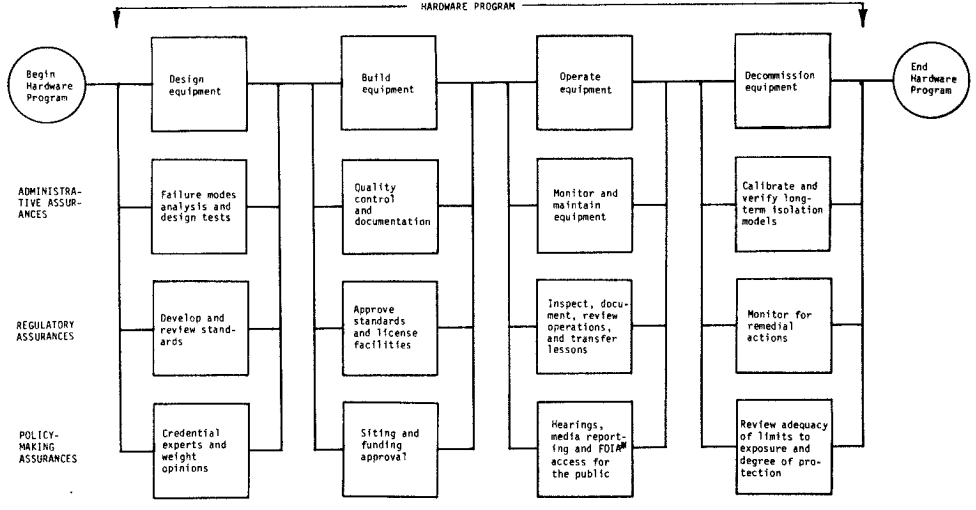
KEY: "(AND)" represents the logical relationship between steps; each step must individually succeed.

"(OR)" represents the logical relationship between multiple barriers to release at each step; at least one barrier must succeed.

Figure 2

Some Institutional Assurances of Success in the Decision-Making Process Guiding Nuclear Waste Management





* FOIA refers to the Freedom of Information Act rights of access to administrative and regulatory reports.

another; it is difficult to imagine credibility without accountability or vice versa.

For example, emphasis on managers' accountability for failures draws attention to those failures and erodes credibility. Conversely, if one participant uses technical expertise to enhance his credibility, he cannot share accountability with someone else in the event of a serious system failure. Nevertheless, clear accountability is one important component of credibility while refinement of expert understanding of hazards and processes lays the basis for improved accountability. The tension between the conflicting and the mutually reinforcing relationship of these two attributes puts a premium on the breadth of perspective and knowledgeability of decisionmakers.

Three policy options that could reduce the conflicts inherent in multiple barrier strategies will be considered here. These options foster broad perspectives and informed judgment in the decision-making process.

- An extensive, systematic, and ongoing program of staff exchanges among administrators, regulators, and outside policy-makers.

- An independent information clearinghouse to serve administrators, regulators, and policy-makers—including the media and the public.

- Analytical studies to anticipate and scope the information burden and decision-making issues associated with managing the hazard.

These options will be discussed as possible solutions to three distinct conflicts between the need for multiple barriers and the other requirements of hazard management—accountability and credibility.

Conflicts Between Multiple Barrier Strategies and Accountability

Since several of the multiple barriers must fail in order for the system to fail, accountability cannot be traced to a single source. This feature of systems using the multiple barrier strategy is illustrated by the contrast between the upper and lower diagrams in Figure 3a. The upper diagram shows that without multiple barriers, or "redundancy," the failure of the entire system can be caused by the failure of single part, such as "a." In sharp contrast, when there are multiple barriers, all of those at any one step must fail for the system to fail; for example, those parts designated "c" in the lower diagram. Establishing accountability is rendered even more difficult by the possibility that eight or more parts labeled "b" could fail, yet the system could function. Which system performed better: the one with three parts "c" failing, causing system failure; or another with eight failed parts "b" that by good fortune appears to continue to function?

For example, at Hanford, shift supervisors, administrators, monitors, and designers shared responsibility for the spill. Each may have performed as well as could be humanly expected; the spill may have resulted from an

unfortunate combination of engineering compromises and preoccupation with even more serious matters. Furthermore, the remedial actions taken, such as computerizing the instrumentation, taking more readings, consolidating management responsibilities, and enforcing internal audits, may represent an appropriate response to the various contributions of each decisionmaking and technical barrier. Finally, if soil absorption, the last barrier, proves to be high, the judgments which originally shaped the facility and its procedures, would be vindicated.

Policy options to reduce the ambiguities in accountability inherent in multiple barriers depend on the development of a method for reviewing the decisions that contributed to any serious system malfunction. Staff exchange programs help reviewers and managers understand the relationships involved and provide first-hand bases for judging the hard-to-assess quality of human error (Sheridan, 1980). An information clearinghouse could trace job-mobile personnel, identifying those responsible for the decisions that contributed to eventual failures. It could also establish and maintain a comprehensive listing of currently recognized nuclear energy issues (Mayo, 1980), so that the basis for accountability would be generally accepted *before* serious malfunctions occurred. An analysis of the information burden on decision-makers could anticipate the confusion arising from the simultaneous failures of many barriers; this strain on timely decision-making is symbolized by the more than 100 alarms that went off at the Three Mile Island reactor during the first few minutes of the accident (American Physical Society, 1980).

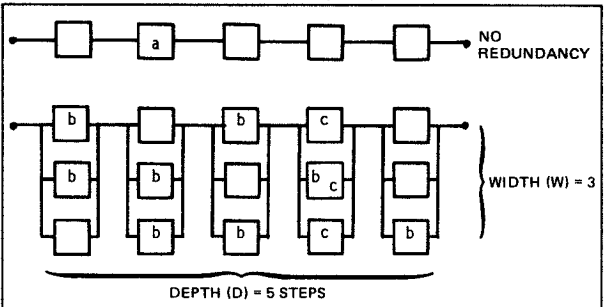
Multiple Barrier Strategies Threaten Credibility

Although multiple barrier strategies by nature presuppose occasional failures in individual hardware components or decision matters, obvious failures tend to discredit the decision-making process. A mathematical analysis of the tradeoff between increased reliability for all system parts and the addition of more parts as backups—for example, increasing the redundancy in the lower diagram of Figure 3a—shows that in most situations, adding more parts is much more effective. Consequently, economy-of-effort argues for more backup rather than greater individual part dependability. When the "parts" are decision-makers, their credibility is at stake whenever errors are made. Moreover, frequent individual errors simply reflect upon the credibility of the entire process, whether or not serious system failure is likely.

Even after the spill at Hanford, more of the same single-walled carbon tanks were ordered. While changes in both the tanks and monitoring procedures have reduced the frequency and size of spills, continued dependence on soil absorption is suspect because radioactive contaminants of uncertain origin have been reported in the nearby Columbia River (Hollocher, 1975). Thus, the decision not to adopt double-walled or stainless steel tank designs leave some question about the commitment of the facility managers to place safety considerations above economic ones.

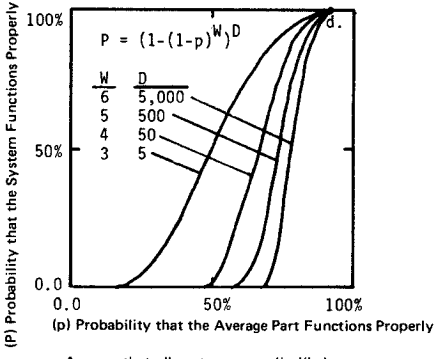
The multiple barrier strategy commits the manager to accepting continual small errors as well as the task of assessing their significance.

Figure 3a
The Ability of Redundancy to Compensate for
Part Failure in Complex Systems



a. If a single part fails, the system fails.
b. If these 8 parts fail, no step fails so the system functions.
c. If these 3 parts fail, the 4th step fails so the system fails.

Figure 3b
Redundancy Enables Very Complex Systems
To Be Much More Reliable Than Their Parts



Assume that all parts are equally likely to fail, then moderate changes in redundancy at each step enables very complex systems to remain much more reliable than their parts. For example, point (d.) corresponds to 99.5 percent system reliability at only 90 percent part reliability.

Three general kinds of assessments can be made: the error was insignificant but produced an overreaction; the error revealed a need for change and the adjustments were appropriate; or the error was symptomatic of pending disaster while the responses were cosmetic. Thus, the frequency of errors by itself is a poor indicator of risk.

Policy options to reduce the impact of continual partial failures on decisionmaker credibility must help reveal honest errors before they create more serious problems or worse embarrassment while protecting decision-makers from excessive criticism or the need to invest heavily in justifying every action. Staff exchange programs would provide an independent yet informed basis for interpreting the significance of decision-maker errors to those outside the process. An information clearinghouse could provide insiders with a more acceptable, confidential way to register concerns than the all-or-nothing whistle-blowing options of today; this might also reduce the penalties involved in using established official channels of reporting and reviewing difficulties. Analyses of alternative site selection procedures might show that a lottery among technically acceptable sites for final disposal of the Hanford wastes would eliminate the political stigma for elected officials accompanying selection by parliamentary process.

Sustained Credibility Erodes Support for Multiple Barriers

Relatively trouble-free operation in hazard management, whether by good fortune or competent effort, sustains credibility, but it also erodes support for backup barriers. As shown in Figure 3b, relatively small investments in backup parts (simply represented as redundancy) can maintain high overall reliability for complex systems. For example, an increase from 5 steps to 5,000 steps in system complexity requires an increase of only 3 to 6 in redundancy at each step to hold system reliability "P" at better than 99.5 percent for part reliabilities "p" greater than 90 percent. However, the more complex system's reliability deteriorates very rapidly if part reliabilites are degraded below 90 percent.

In the Hanford case, one might ask why an embarrassing leak was needed to motivate the review of monitoring and management procedures? Is another embarrassment needed to initiate final disposal of stored wastes and recovery of the contaminated soil? Might the storage facility's budget and manpower be cut if the economy turned sour, nuclear materials production declined, or fear of terrorism tightened security and limited outside review?

Policy options needed to maintain support for multiple barriers despite a lack of crisis conditions rest upon establishing believable indicators of need. Staff exchanges with outside groups would help waste managers broaden their base of political support and legitimacy by testifying to the *potential* for failure. An information clearinghouse could sponsor surveys and studies of emergent issues, offering advance warnings of threats to reliability due to changing conditions in the economy, nuclear energy, community, or world stress. Analysis of the decision-making process could systematize the conflicting arguments concerning the risks of premature versus tardy disposal of the stored wastes.

SUMMARY

The requirements for dependable management of complex hazardous technologies include multiple barriers against serious failure, clear accountability for errors, and credibility for the decision-making process. Unfortunately, these requirements are in direct conflict. These conflicts can undermine the public's assurance that their health and safety concerns are being properly addressed. However, these conflicts can be reduced through an awareness that hazard management is based primarily on information exchange and evaluation rather than physical system construction and operation.

Existing policies emphasize either integrated design, development, and operation of hazardous technology or adversarial processes such as regulation, litigation, and parliamentary debate. While these are all necessary policy elements, by themselves they probably cannot reconcile the conflicts identified in this study. Three new policy options—an extensive and systematic staff exchange program among decisionmaking organizations; an independent clearinghouse that gathers and provides information for all parties but is outside the organization's line authority; and a concerted effort to analyze the anticipated information burden and scope of decision-making issues associated with hazard management—have potential for reducing the conflicts and thereby creating an environment for sensible public involvement in policies for controlling hazards.

REFERENCES

American Physical Society (1980) "Study Blames 'People Related Problems' for TMI Accident," *Physics Today*. State & Society, February.

Hilberry, Norman (1978) "Remarks on Managerial Errors and Public Participation," Nuclear Regulatory Commission, 1978, *Op. cit.*

Hollocher, Thomas C. (1975) "Storage and Disposal of High-Level Radioactive Wastes," *The Nuclear Fuel Cycle*. Cambridge, Mass.: Union of Concerned Scientists, the MIT Press.

Laroche, Micheal (1977) "A Model of Attitude Change in Groups Following Persuasive Communications: An Attempt at Formalizing Research Findings," *Behavioral Science* 22:246-257.

May, Robert M. (1971) *Stability and Complexity in Model Ecosystems*. Princeton, N.J.: Princeton University Press.

Mayo, Louis H., Henry H. Hitchcock, Robert W. Anthony, Lynne D. Filderman, Donald S. Kaufman, and Milton C. Marney (1980) *Public Concerns and Alternative Nuclear Power Systems*. Washington, D.C. Program of Policy Studies in Science and Technology of the George Washington University.

Metlay, Daniel S. (1978) "History and Interpretation of Radioactive Waste Management in the United States," Nuclear Regulatory Commission, 1978, *Op. cit.*

Shannon, C.E. (1948) "A Mathematical Theory of Communications," *The Bell Technical Journal* 27:379-426 and 623-656.

Sheridan, Thomas B. (1980) "Human Error in Nuclear Power Plants," *Technology Review*. February.

Thompson, James D. (1967) *Organizations in Action: Social Science Bases of Administrative Theory*. New York: McGraw-Hill.

U.S. Nuclear Regulatory Commission (1978) *Essays on Issues Relevant to the Regulation of Radioactive Waste Management*. Washington, D.C.: NUREG-0412.

von Neumann, John (1956) "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components," in C.E. Shannon and J. McCarthy (eds.), *Automata Studies*. Princeton, N.J.: Princeton University Press.

Whittaker, James O. (1967) "Resolution of the Communication Discrepancy Issue in Attitude Change," in C.W. & Muzafer Sherif (eds.), New York: Wiley.