Exhibit 9

STATE OF NEVADA
AGENCY FOR NUCLEAR PROJECTS/
NUCLEAR WASTE PROJECT OFFICE

NWPO-SE-007-88

THE EFFECTS OF HUMAN RELIABILITY IN THE TRANSPORTATION OF SPENT NUCLEAR FUEL

by

Seth Tuler
Roger E. Kasperson
Samuel Ratick

Center for Technology, Environment, and Development
Clark University

June, 1988

The Nevada Agency for Nuclear Projects/Nuclear Waste Project Office was created by the Nevada Legislature to oversee federal high-level nuclear waste activities in the state. Since 1985, it has dealt largely with the U.S. Department of Energy's siting of a high-level nuclear waste repository at Yucca Mountain in southern Nevada. As part of its oversight role, NWPO has contracted for studies designed to assess the socioeconomic implications of a repository and of repository-related activities.

This study was funded by DOE grant number DE-FG08-85-NV10461.

STATE OF NEVADA
AGENCY FOR NUCLEAR PROJECTS/
NUCLEAR WASTE PROJECT OFFICE

NWPO-SE-007-88

THE EFFECTS OF HUMAN RELIABILITY IN THE TRANSPORTATION OF SPENT NUCLEAR FUEL

by

Seth Tuler
Roger E. Kasperson
Samuel Ratick

Center for Technology, Environment, and Development
Clark University

June, 1988

The Nevada Agency for Nuclear Projects/Nuclear Waste Project Office was created by the Nevada Legislature to oversee federal high-level nuclear waste activities in the state. Since 1985, it has dealt largely with the U.S. Department of Energy's siting of a high-level nuclear waste repository at Yucca Mountain in southern Nevada. As part of its oversight role, NWPO has contracted for studies designed to assess the socioeconomic implications of a repository and of repository-related activities.

This study was funded by DOE grant number DE-FG08-85-NV10461.

This report is an interim work product of the Nevada Socioeconomic Study. It has not been specifically reviewed by the Technical Review Committee.

TABLE OF CONTENTS

1. Introduction

Despite the evident importance of the subject, no comprehensive analysis of human factors in spent fuel transportation has occurred. A reason for this may be the assumption that potential human contributions to spent fuel transportation risks are negligible [Nuclear Regulatory Commission 1980]. There are several characteristics of spent fuel and other high-level radioactive waste transport, however, that suggest that human actions may indeed contribute significantly to both actual and perceived risk of the system.

First, the transportation of spent fuel involves a number of stages and phases, all of which depend on effective, safe, and reliable human performance. Improper or inadequate human actions may occur during all phases and activities of a transportation system, including design, implementation, operations, maintenance, and accident recovery. Human actions also are often separated in both time and space from their effects. Similarly, those entities that must respond to events caused by "upstream" human actions, are often separated both spatially and sectorally from the sources of the errors. Improper or inadequate human actions which are not perceived and responded to across time and space, however, may initiate or contribute to system failures or exacerbate adverse consequences at later times thus creating constraints to effective response to risk events.

Second, even minor risk events in the transportation system for spent fuel have the potential for contributing to the social amplification of risk. Prior experiences in both hazardous material transportation and nuclear power industries suggest that the public is very sensitive to such

risks. Human actions have the potential for exacerbating such concerns by initiating minor risk events in the system as well as increasing the probability of severe accidents.

Third, the transportation system for spent nuclear fuel will be comprised of several organizations. In particular, carriers will mainly be from industry where human reliability issues have received inadequate attention in the past. Although extensive regulatory oversight of spent fuel transportation activities is intended to reduce the frequency of risk events, the size of the reduction will depend directly on the effectiveness of inspection and quality control programs. Evidence suggests that such programs have not been completely effective in eliminating human errors in the transportation of spent nuclear fuel in the past. Moreover, concerns over quality control and human reliability have concentrated mainly on operational activities and neglected equally important issues in design, implementation, maintenance, and accident recovery phases.

Fourth, human actions have been shown to be major causes of system failures in many complex technological systems, including the operation and maintenance of nuclear power plants [Meister 1971, Turner 1978, Rasmussen 1980, Bellamy 1983, Miller and Swain 1987]. In addition, human errors have been estimated to account for at least 62% of hazardous material transportation accidents [Office of Technology Assessment 1986].

Thus, we agree with recent suggestions that relationships between human activities and system failures in the transportation of spent fuel need to be evaluated more thoroughly than has occurred in the past [Nuclear Regulatory Commission 1986, Hamilton et al 1986]. The

importance of human reliability analyses becomes even more urgent as planning begins for a federal repository. The opening of such a site will greatly affect the magnitude of manufacturing, operational, and maintenance activities. Although there have been no accidents that have harmed the public to date, the potential for adverse events arising out of human actions will increase as the magnitude of the transportation system grows.

Human participation in complex technological systems may be advantageous or disadvantageous, depending on the particular circumstances. In this report, human reliability refers to two different but related aspects of human interaction with technological systems. The first involves those aspects of human interventions in the system that may lead to or exacerbate the consequences of an incident, which we have called "human errors". Although many human errors may be seen as events where an individual or group actually does something wrong, it is more useful to characterize them as resulting from mismatches in a human-task or human-machine system.

The second type of interactions are those purposeful human interventions that prevent or mitigate the consequences of an incident. While such actions may be performed outside of a pre-established system framework (e.g., emergency response) they are generally conditioned by other types of administrative or managerial programs (e.g., personnel training programs). Two methods may be used to eliminate unwanted effects of human actions and improve human reliability in technological systems: 1) programs may be instituted to reduce the probability of human errors in the design phase of a transportation system, or 2) the

effects of human errors may be eliminated, mitigated, or reversed by effective management control strategies. We call these methods "transportation risk management programs". They should be designed to reduce risks, reduce uncertainties, allow adaptable and flexible responses to events, and reduce the social impacts of unforeseen events.

This report is intended to:

1) describe the regulatory environment and risks associated with spent fuel transportation. Previous experiences, problems, and incidents in the transportation of spent nuclear fuel and other high-level radioactive waste are discussed in the context of: 1) stages and phases in the transportation system, and 2) risk management strategies that have been implemented to avoid them.

2) describe our conceptual approach which is based on a socio-technical perspective of the transportation system and on theories and methods from the field of human factors. With respect to the broad socio-technical perspective taken in this report, we have also discussed the organizational and social aspects of human error. "Human errors" are defined as human-task mismatches between 1) perceived system state and dynamics and 2) actual system state and dynamics.

3) contrast our approach with previous studies that assess human error in the transportation of spent nuclear fuel.

4) review databases that contain information about human error in transportation risk events and assess how the data might be mobilized to improve human reliability evaluations.

5) discuss the application of our approach in the identification and evaluation of human errors and explore its relevance to effective transportation risk management. To facilitate this, a "human reliability matrix" is developed which supports the pre-identification and post-incident analysis of human-task mismatches and helps to identify the types of risk management options that may be employed to control them. This approach enables us to identify key issues related to the prevention, mitigation, and recovery of human-task mismatches through programs related to management structure and decision making protocols, data collection, error reporting systems, personnel training, operational procedure development, accident and incident[1] analyses, and quality assurance and quality control.

6) recommend specific actions that both Nevada and the federal government may wish to implement to reduce the risks associated with human-task mismatches in the transportation system for spent nuclear fuel.

2. Overview of the Transportation System

To date there have been no severe incidents or accidents resulting in significant releases of radioactivity during spent fuel shipments. Indeed, several successful shipment campaigns for spent nuclear fuel have been completed. For example, Duke Power Company has shipped spent fuel

[1] In this report we use the customary definitions for "accident" and "incident". "Accident" refers to a vehicular accident. "Incident" refers to any event which results in a release of material. While we believe that these definitions may be inadequate distinctions, we use the accepted definition to avoid confusion.

assemblies between two reactors [Rasmussen 1986] and Virginia Power has shipped spent fuel to the Idaho National Energy Laboratory [Ruska and Schoonen 1986]. The success of a limited number of spent fuel shipment campaigns, however, does not obviate the need for careful risk management. The potential certainly exists for human-task mismatches to result in severe problems because 1) the number of shipments to date is small compared with the expected numbers after a repository opens, and 2) these shipment campaigns were heavily regulated and closely observed to assure operational safety and system reliability. Careful consideration of human-task mismatches is likely to lead to much higher estimated transportation risks resulting from the shipment of spent fuel to a repository than those estimated in prior risk assessments.

"Human errors", or human-task mismatches, can affect risks in basically five ways. They may:

1) initiate risk events: this is the most widely considered effect of human error, although not necessarily the most important. Initiating events result in immediate effects. Examples of initiating events in the transportation system include mistaken removal of spent fuel from a cooling pool during loading or a driver falling asleep while transporting a truck shipment of spent fuel.

2) contribute to risk events: human errors may contribute to incidents or accidents when they interact with other initiating events [Figure 1]. Their control and identification in human reliability assessments are very important because they may result in unforeseen causal sequences leading to system failures.

Examples include improper welding of casks during fabrication or improper securing of casks on truck-beds or rail-cars.

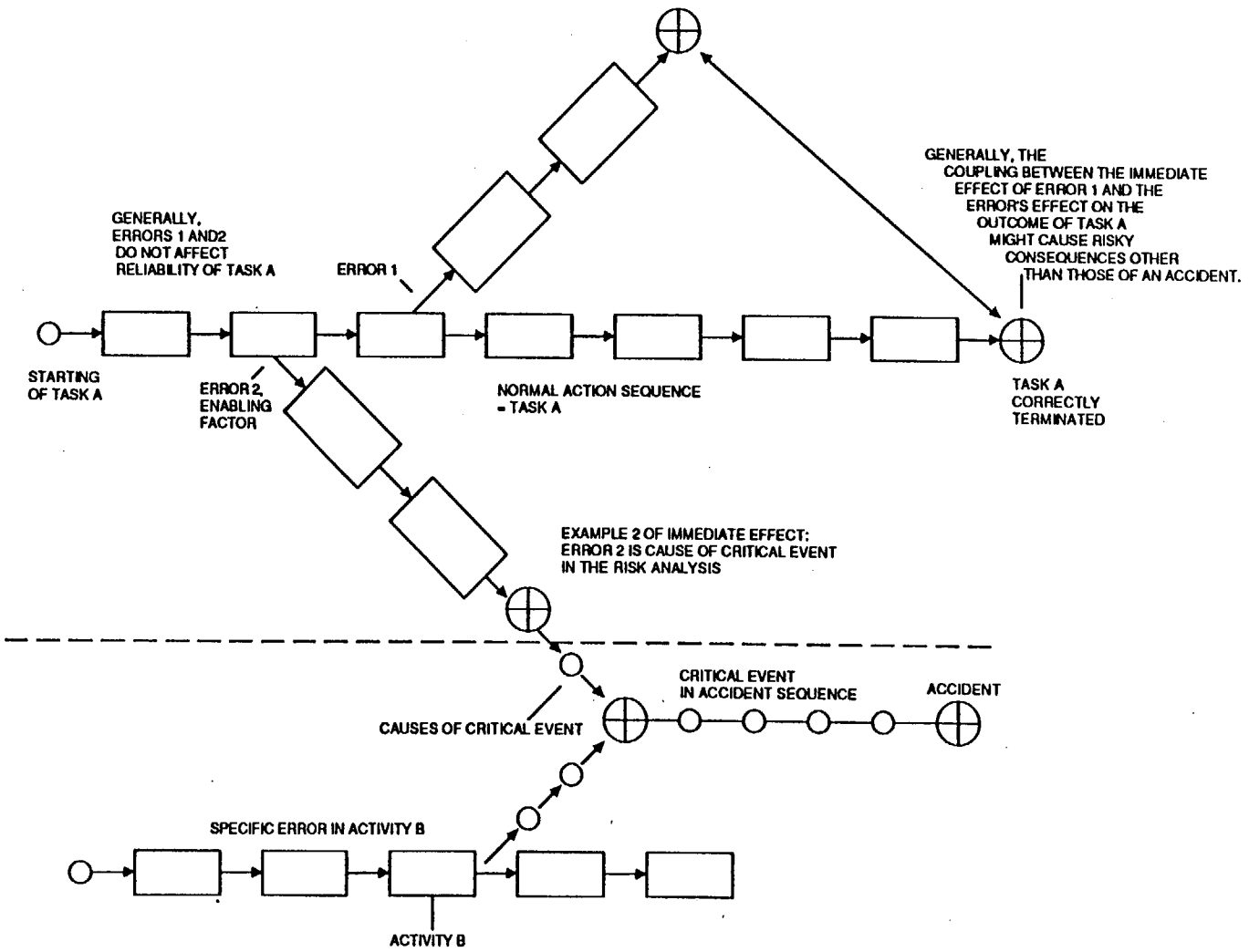
3) alter the frequency of risk event sequences: the frequency of events (some of which may be considered acceptable) may be affected by human errors. Examples include the use of improperly designed cask valves which can lead to a greater frequency of cask integrity failures or truck driver accidents that increase the rate of severe accidents.

4) affect the structure of risk event trees by changing intervention strategies and reliability: if events limit intervention to control a hazard sequence, overall risk will be increased because recovery activities will not be as effective as assumed. Examples of such events include ineffective or nonexistent emergency response plans in situations where they were assumed to exist.

5) affect couplings and interactions between subsystems and components: these events are the most difficult to identify although they may be controlled by making system interactions as observable and reversible as possible Frequently such interactions and couplings are affected because their connections were not known. They have occurred in many industrial accidents including Bhopal and previous spent fuel transportation incidents.

FIGURE 1

HUMAN ERROR AS A CONTRIBUTORY FACTOR TO ACCIDENTS



SOURCE: Adapted from Pedersen (1985)

Prior analyses have generally focused on failures related to cask usage (e.g., cask closure, maintenance, valve operation), although other important sources of human error can affect cask integrity. For example, failures in vehicle and other support equipment operation (e.g., cranes) and failures during quality control can also lead to incidents involving casks [see Appendix B for a review of prior analyses]. In fact, small failures in human-task systems at any point in the system have the potential for creating immediate effects and vulnerabilities at later times and in distant places. For example, the primary effect of a human error may be associated with a single shipment, a single cask, or a specific cask design. Previous analyses examined only the first category, and consequently they assume 1) that errors are randomly distributed among all shipments, and 2) there is a low probability of human error and severe accidents events occurring simultaneously. On the other hand, if an error affects a cask design or a particular cask, errors are <u>not</u> randomly distributed across all shipments and, therefore, may affect multiple shipments.

In addition, the magnitude of transportation activities for a national repository will be both larger and more complex than anything previously attempted. Estimates suggest that rail shipments will increase from currently less than 50 annually to more than 250 shipments per year by the year 2000, which could result in up to five accidents per year involving rail shipments of spent fuel [Office of Technology Assessment 1986: 105]. Similarly, truck shipments are estimated to increase to 750 per year for a newly opened repository (without an MRS) and to result in up to five accidents per year [Office of Technology Assessment 1986: 105].

These estimates are based on prior operational experiences with a much more limited transportation system. Many components of the system, however, will be substantially affected by such growth. As an example, labor market data suggest that there may not be enough qualified and well-trained truck drivers available to work in the truck transport industry in general. It is not clear how the spent fuel transportation system would attract those that are competent and available. In addition, cask fabrication has been proceeding at a very slow rate and even under these slack conditions there have been many problems. Needs for up to 200 casks are predicted, implying that capacities for cask fabrication, inspection, and maintenance will have to increase dramatically. Whether the expected magnitude and complexity of the new system will result in changes in human error and accident rates is an important issue.

2.1. Operational Risks

Operational risks in the transportation of spent nuclear fuel and other high-level wastes may lead to a wide range of incidents, accidents, and adverse consequences. We have previously classified these operational risks into four categories [Kasperson and Renn 1987, Golding et al 1988]:

- normal conditions: workers and members of the public will be exposed to radiological and non-radiological risks from the operation of a nuclear waste transportation system. Even under "normal" or "incident-free" operating conditions (with an assumed absence of accidents, poor quality control, sabotage, terrorism, or theft), radiation will be emitted from even the best designed and

maintained casks under even the most stringent quality control programs.

- accident conditions: accidents include "internal events" or system failures (such as vehicular and loading accidents or events that originate "outside" the waste transportation system). Both radiological and non-radiological consequences may be associated with such accidents.
- sabotage: intentional human-made initiating events of sabotage, terrorism, and theft have been of much concern to experts and the public. Therefore, in general they are treated separately from accidents. This category is not specifically treated in this report because human error is not considered to be the result of intentional actions.
- defective quality control: human errors in quality control have been a continuing problem in the nuclear industry and hazardous material transportation. In the transportation system, defective quality control may lead to both radiological (e.g., improper cask closure leading to excess exposure) and non-radiological (e.g., crane accidents) consequences. Defective quality control and human errors are treated separately because of their importance. They can, however, affect risk under both normal and accident conditions.

In order to identify and control human reliability-related operational risks in the transportation system, a transportation risk management system must consider the entire sequence of activities from the selection of fuel for shipment to the unloading of the material at the final

destination. A sequential view of the shipping procedure is a useful aid in the identification of potential hazards [Figure 2].

The transportation process actually begins with the characteristics of spent fuel (e.g., age, cladding condition, burn-up rate) for shipment because these may influence the integrity of the fuel during transport activities, the selection of casks for shipment, and the handling, inspection, and emergency response needs at a repository [Appendix C]. The inspection of casks prior to packaging are also important to determine if they are defective (e.g., leaking, warped).. There have been numerous examples of human errors during this stage of the transportation system, including [Appendix C, Resnikoff 1983, Nebraska Energy Office 1987]:

- incorrect fuel selection resulting from the use of outdated mathematical fuel-selection equations. The use of an improper equation led to the incorrect choice of fuel to transport in a particular cask.
- failure to properly drain pool water from casks. In one case this occurred when the incorrect valve was opened because of the absence of color-coded labeling on the valves.
- improper dry shipment of spent fuel.

The packaging of material into casks is completed underwater in cooling pools, with personnel remotely controlling automated equipment with the use of video cameras and robotic equipment. These types of activities are of particular concern from a human reliability perspective because the observability and control of actual activities are limited. The second stage of loading casks is completed with the securing and inspection of the casks on a transport vehicle (e.g., truck-trailer or rail-car) and the

completion of all required routing and labeling requirements (e.g., pre-notification, placards). Examples of errors that have occurred at this stage are [Appendix C, Resnikoff 1983, Nebraska Energy Office 1987]:

- incorrect placarding of shipments,
- incorrect filling out of shipping papers,
- improper securing of casks on truck beds,
- surface contamination of cask and trailer,
- improper pre-departure inspections of casks and vehicles,
- improper loading of spent fuel into casks, and
- damage to fuel during loading.

The third stage of the transportation process is the actual material transport by truck or rail. This may include temporary stowage or transshipment as a result of modal mixing. Human reliability concerns at this stage are centered on driver performance, enroute inspections and maintenance, and security. Several road accidents have occurred during truck shipments, which fortunately did not result in releases. Specific errors which have occurred include [Appendix C, Resnikoff 1983, Nebraska Energy Office 1987]:

- drivers' failure to adhere to preplanned routes,
- rail shipments being "lost" and ending up in unprotected train yards,
- co-drivers sleeping at unauthorized times,
- inoperative driver communication equipment,
- collapsing truck beds due to cask weight,
- lack of proper escorts due to improper notification,
- failure to notice radioactive contamination of equipment,

- transport vehicle breakdowns and improper repairs, and
- a truck-trailer overturned during transit.

The final stage of the transportation process occurs when the shipment reaches its final destination and is unloaded and inspected. Human reliability concerns at this stage are similar to those at the originating site, and similar types of human errors (e.g., improper cleansing, inspection, and maintenance of casks and vehicles) have occurred.

2.2. Design, Implementation, Maintenance, and Emergency Response Risks

The description above demonstrates that human reliability issues in spent fuel transport extend well beyond vehicle operation and cask loading. Consideration must be given to human activities at all phases of the transportation system, including technical designs, fabrication of equipment, management, maintenance, and emergency response. Unfortunately, risks from all activities have generally not been considered in prior risk assessments of the spent fuel transportation system. Most prior analyses and risk estimates, for example, have assumed that casks are properly constructed and maintained [Office of Technology Assessment 1986: 29]. There are serious questions, however, as to whether these are correct assumptions [Appendix B, Appendix C, Nebraska Energy Office 1987]. We turn now to a review of the issues associated with each phase [Table 1 lists a selection of more specific activities associated with each phase].

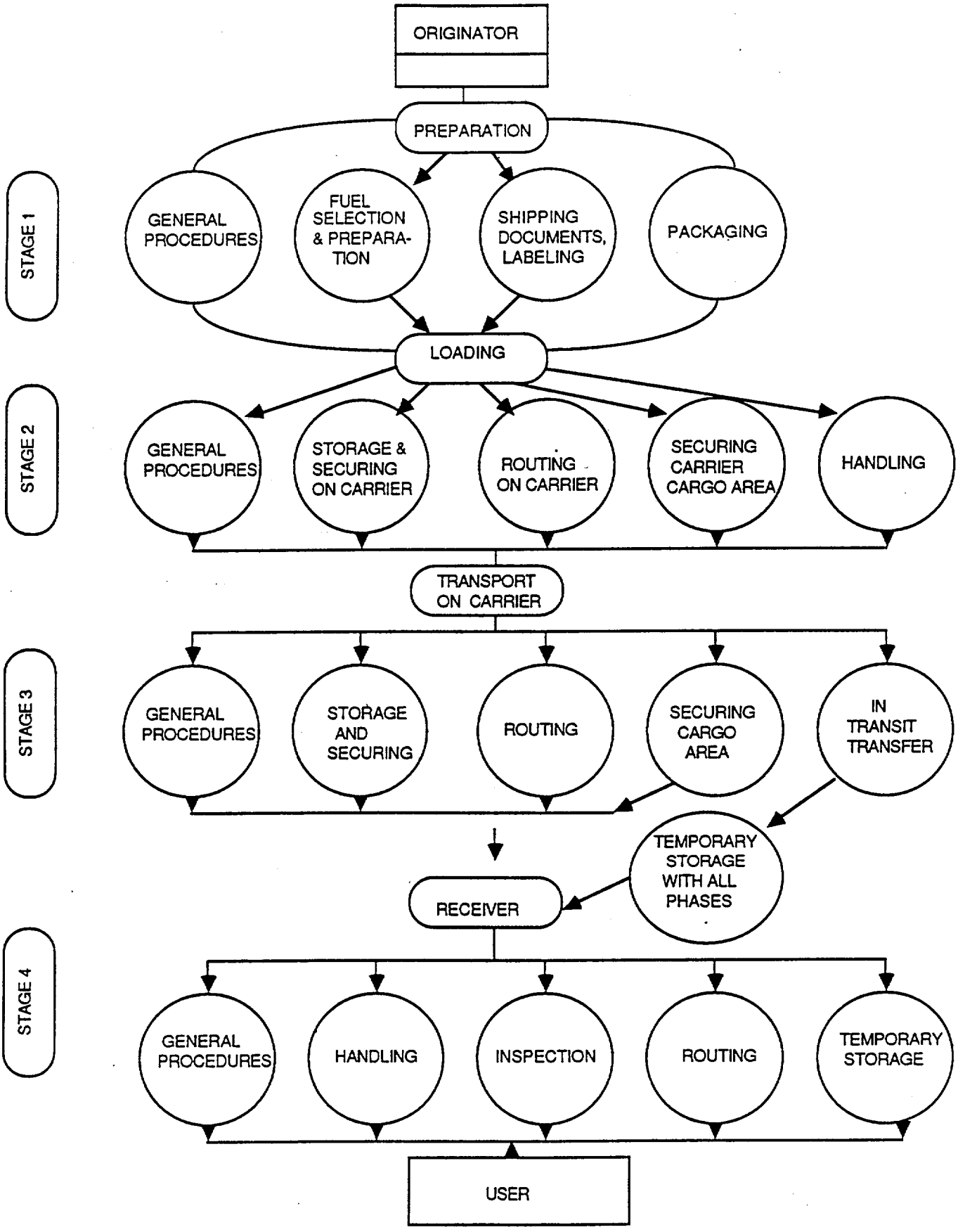


FIGURE 2. THE STAGES OF SPENT NUCLEAR FUEL TRANSPORTATION

The design phase includes the activities that develop the characteristics of the specific transportation system. These include the development of institutional structures through legislative action and regulatory promulgation, the design of equipment and manufacturing standards, and the design of accident prevention and response methods. Many of the human errors that have occurred in the transportation system can be traced back to situations where insufficient consideration has been given to human factors issues in this phase. Specific problems include [Appendix C, Resnikoff 1983, Nebraska Energy Office 1987]:

- errors in the analysis of spent fuel cask baskets,
- drop, puncture, and fire test standards for the most severe accident conditions are not based on historical data,
- improper estimation of rail cask weight,
- cask trailer designs that are inadequate to hold heavy loads resulting in buckling during use,
- designs not tested for maintainability or ease of inspection,
- documentation errors related to cask designs and fabrication,
- methodological errors in risk assessments,
- errors in simulation data inputs, and
- mathematical errors in stress analysis.

The implementation phase involves the development of the transportation system components, such as the fabrication of equipment, the training of personnel, and the implementation of inspection, enforcement, and emergency response programs. Errors have included the use of inadequate testing and licensing procedures for drivers. Other

errors have occurred during cask fabrication that involved [Appendix C, Resnikoff 1983, Nebraska Energy Office 1987]:

- the installation of defective valves and rupture disks,
- the use of improper welding materials and defective bolts, and sealant,
- the use of improper cask welding
- the defective installation of shielding,
- the improper installation of valves,
- the use of a defective shell on an outer cask body, and
- the continued use of casks after the breakdown of quality assurance programs at the manufacturer.

The operations phase includes all the activities and decisions involved in the actual movement of spent fuel and other high-level waste from an origin to a repository. This phase was described previously in section 2.1.

The maintenance phase occurs when equipment requires either scheduled or unscheduled repairs and is simultaneous with the operations phase. Specific activities include inspection, repair, calibration, testing, and verification. Human errors in this phase have included [Appendix C, Resnikoff 1983, Nebraska Energy Office 1987]:

- improper repairs using improper materials,
- inspection failures (i.e., faulty equipment not identified),
- required repairs not performed on vehicles,
- failure to properly perform cask leak tests,
- failure to properly decontaminate casks and equipment,
- failure to routinely replace cask lid seals, and

• replacement of faulty cask valves with other faulty valves.

The accident recovery phase is initiated after either an incident or accident occurs in the transportation system. Specific activities range from the actions and decisions made at the very onset of an emergency (e.g., notification) and extends through long term monitoring and clean-up activities as needed. Errors involving the improper placarding and notification have previously resulted in inadequate emergency response measures being undertaken [Appendix C, Resnikoff 1983, Nebraska Energy Office 1987]. In one case emergency response personnel did not attempt to put out a fire resulting from an accident because they were erroneously led to believe that radioactive materials were involved.

There are also problems in the interface between different phases. In particular, problems may continue to exist in the transportation system because those in authority are not well informed about the problem or are incapable of initiating a response. For example, an incident occurred in 1980 that questioned whether the use of air (rather than inert gases) in casks holding spent fuel actually kept it cool enough not to require water in the cask [see Appendix C for a more detailed discussion]. In this incident an assembly containing damaged rods self-heated in transit sufficiently to reoxidize fuel pellets into a fine powder that was released when the cask was opened. A private spent fuel pool, a worker, and the cask were contaminated. When confronted with this information three years later, the head of the NRC cask certification department and two NRC experts were not well-informed about the incident. Moreover, only because of external pressure for more than a year did the NRC eventually recognize the problem and order such shipments to use inert gases.

TABLE 1

SPENT FUEL TRANSPORTATION SYSTEM PHASES AND ACTIVITIES

DESIGN	IMPLEMENTATION	OPERATION	MAINTENANCE	ACCIDENT RECOVERY
regulatory environment (legislation) institutional structure (resp. authority, objectives) planning criteria (e.g. routing, mode) hazard communication quality control site selection cask design equipment design	<u>Organizational</u> management control system registration programs, licenses, certification rules and tarrifs emergency resp. system enforcement & inspection maintenance programs <u>Technical</u> cask fabrication testing quality control markings construction testing quality control <u>Personnel</u> training staffing (drivers, support, emergency resp., maintenance, management)	oversight inc. error investigations & data collection & analysis reporting (shipping papers, etc.) route selection notifications security arrangements procurement of casks selection of fuel packaging handling labeling freight acceptance loading placarding securing monitoring/inspections transport tracking (inspection, security transshipment unloading decontamination inspection	<u>Technical</u> inspection repair calibration testing quality control monitoring verification <u>Personnel</u> training testing monitoring <u>Data</u> collection analysis	notification situation assessment command & communication system setup control over material recovery process radiological monitoring clean-up removal of equipment accident investigation liability issues support equipment

2.3. The Regulatory Environment

A complex regulatory environment exists to control spent nuclear fuel and other high-level radioactive waste shipments. Although human reliability considerations are not usually specifically addressed by regulation, some relevant regulations have been developed for all phases of the transportation system that include some types of human reliability activities. These include DOE and NRC review of human factors considerations in cask design, employee training programs, employee operating requirements, inspection and enforcement programs, and emergency response plans and personnel training. The adequacy of the regulatory response to manage the wide range of human reliability issues, however, is an open issue.

Even in the much emphasized area of cask design and fabrication, human factors considerations and principles are either not well-formalized or are not comprehensive [Fischer 1988]. Over the years, cask design has followed two basic tenets: 1) meet the extant regulatory standards and 2) make the cask functional for the reactor operators. Some effort is also being made to incorporate additional human factors considerations into current cask designs by both the NRC and DOE [Lake 1988].

There is little evidence that any authority has systematically attempted to track and eliminate failures in various activities (e.g., loading, handling, maintenance, inspection). The main approach to correcting human reliability issues in past cask handling problems has been "administrative controls" (i.e., a document detailing a suggested new procedure). In cases where the problem is perceived as potentially widespread, "regulatory guides" may be issued that attempt to translate a

rule into acceptable practice. This approach has sometimes been criticized by DOE officials as little more than a "technical band-aid" that sometimes compounds the original confusion.

The DOE is currently planning a study on human error in the safety of nuclear waste transportation [Lake 1988]. The scope of the study is still unclear, although the primary focus will most likely be the identification and evaluation of databases already in place and additional information needs for human error analyses. The study is to focus on human errors in operational activities (e.g., mode selection, intermodal transfer, loading, transit) although, as it now stands, unloading at the repository is not included (this is to be covered by other DOE work). Later phases of this study will likely include the identification of human factors issues that are unique to the transportation system for spent nuclear fuel.

In general, federal agency activities reflect the belief that human error is not a significant contributor to risk in the transportation system. In fact, some individuals, interviewed by the authors, within the relevant regulatory agencies are not even convinced that human error in the transportation of spent fuel is an issue worth further study. It is often assumed that quality assurance programs are adequate to maintain proper adherence to procedures and regulations, although there have not been any evaluations of actual performance. On the contrary, the historical record suggests that quality assurance programs are often not very effective [see above, sections 2.1 and 2.2].

The general neglect of human error issues arises from the assumption that the probability associated with simultaneous human and technical failures leading to major accidents is negligible. The two

important prior assessments, however, on which this conclusion is based (i.e., Battelle Pacific Northwest Laboratories 1978, Nuclear Regulatory Commission 1980) contain many methodological errors and faulty data. Specific problems include [see Appendix B for a more detailed discussion]:

- underestimation of worst-case human error consequences, possibly by several orders of magnitude,
- incomplete and incorrect use of unreliable data sources,
- absence of some previous and potential future error types.

The lack of concern about the effects of human errors is in marked contrast to government and industry concern over human errors and recoverability in the operation and maintenance of nuclear power plants. The primary rationale for this limited attention is that the transportation system is viewed as a much simpler system that does not require complex monitoring and problem solving tasks. This assumption, however, ignores the issue of emergency response related decisions and ambiguous cask monitoring procedures. In addition, it is generally assumed that cask technology is sufficient to ensure against the release of radiation under extreme accident conditions and that, therefore, human errors will not be able to create severe enough conditions to cause cask failure. This assumption, however, is based on three other important, but highly suspect assumptions:

1) cask designs are adequate to withstand even the most severe accident conditions,
2) casks are fabricated perfectly according to these design standards, and

3) casks are used and maintained properly with respect to design standards.

The lack of attention also undoubtedly arises from a skepticism among technical people toward the methodologies and potential contributions of the "soft science" of human factors research and from the prevailing "engineering ethic" of the regulatory agencies. In addition, there is a strong belief that technological features (e.g., cask integrity under severe accident conditions) and the reliability and thoroughness of regulatory requirements (e.g., route selection, equipment maintenance, inspection) will ensure system safety and reliability. Other potential reasons include: a mindset that there are no severe problems, a lack of systematic data collection and analysis that limits the ability to perceive patterns of problems, and a reluctance to assess the probabilities of multiple simultaneous events in addition to isolated failings in risk assessments.

2.3.1. Responsible Agencies and Organizations

The main regulatory agencies with jurisdiction over spent fuel transportation are the Department of Transportation [DOT], Department of Energy [DOE], and the Nuclear Regulatory Commission [NRC]. Several other agencies have jurisdiction and responsibilities over specific areas, including OSHA, FEMA, private and other public organizations (e.g., utilities, shippers, carriers), and state agencies Thus, responsibilities and control in the transportation system are distributed across organizational and political sectors. [Table 2, Appendix D of this report provides a detailed listing of authorities and responsibilities of governmental agencies and other

organizations responsible for transporting spent nuclear fuel to a repository].

The DOT is the lead federal agency for establishing and enforcing hazardous materials transportation regulations. Specific activities are based on the Hazardous Materials Transportation Act and include: vehicle inspections, personnel testing and training, data collection and analysis, and emergency response. In the rail industry, for example, the DOT requires a comprehensive set of operating rules, written tests, continual monitoring and training of personnel, and effective means of discipline. Efficiency tests by field inspectors are used to monitor the performance of crews according to rail operating rules (e.g., radio transmissions, train speeds).

The NRC is the lead agency in regulating and certifying spent fuel casks. The issuance of cask certifications are based in part on the implementation of quality control programs developed during the design process. However, according to individuals interviewed by the authors, the inspection of the quality assurance programs are usually limited to comparing the table of contents of the procedures with those required in NRC guidelines--no review of specific procedures actually takes place. The NRC also requires shippers, carriers, and other nuclear facilities, such as utilities, to hold licensees as temporary possessors of spent fuel.

The DOE is the main federal agency responsible for designing and deploying the spent fuel transportation system to a national repository and derives its responsibilities from the Nuclear Waste Policy Act [1982] and amendments. Beginning in 1998 the DOE will take possession of the fuel at utilities and be the shipper for such materials. The DOE will also be

responsible for hiring carriers and ensuring their safe and reliable performance. To ensure such human reliability, the DOE will rely on "thorough on-going training" as part of its quality assurance programs.

Other federal agencies are primarily concerned with employee safety and emergency response [Table 2]. Moreover, states have varying requirements for prenotification of shipments, shipment inspections, and driver license requirements [Department of Energy 1983, Battelle Columbus Laboratories 1985]. Particularly significant problems result from the fragmented nature of emergency response capabilities across political, organizational, and geographic boundaries.

Private organizations also play an important role in the transportation system. In particular, utilities and carriers have primary responsibility for hiring and ensuring the safe and reliable performance of their employees. It should be noted that much of the training for positions related to spent fuel transportation in these industries is completed "on the job". In addition, cask manufacturers and carrier firms have training programs for utility personnel involved in loading and handling activities. Utilities also train personnel in the use of cask handling and loading procedures and equipment.

Many problems have already occurred due to ambiguous or inadequately implemented regulations that do not comprehensively cover all activities in the transportation system. One major problem is the division of power among the three main federal agencies, each with a differing outlook on regulatory interpretation and enforcement. Although several Memoranda of Understanding have been developed, gaps in regulatory authority still exist. Specific examples of such gaps include NRC,

DOT, and DOE security arrangements and routing requirements, and DOT and NRC cask restraint and tiedown requirements [Appendix C]. For example, the NRC presently approves each route used by its licensees prior to shipment. On the other hand, the DOE is governed by DOT's requirement that routes be delineated after completion of a shipment. While the NRC has disapproved routes because of security deficiencies in the past, the DOT has done very little to police DOE shipments. The DOE's use of non-interstate highways when interstates were available and required is an example of such conflicting oversight authority. Similar issues arise in the requirements for cask restraints on vehicles. NRC regulations require that the tiedowns be able to restrain the cask under much larger forces than those required by DOT.

Regulatory inadequacies exist even within specific agencies. The NRC has no staff or system dedicated to monitoring problems with specific casks. Instead, responsibility is divided between a central certification staff that concentrates on design, and a diffuse, inadequately staffed inspection department (consisting of about a half dozen employees) with quality assurance duties for all nuclear equipment, most of which has little to do with transportation. NRC inspectors rarely actually observe casks during production. Instead, they have focussed on the paperwork history of the manufacturing process prior to issuance of cask certificates of compliance.

Similar issues exist for the DOT regulation of hazardous material carriers. The DOT provides no advice on driver training and has fairly general training and testing requirements. In fact, DOT officials have stated that most training occurs on the job [Resnikoff 1983]. DOT

requirements for high-level radioactive waste transportation are supposed to be consistent with those for cryogenic (very cold) liquids; however, regulations for cryogenic liquids were never implemented [Resnikoff 1983]. Rail training requirements are even less specific, although rail employees are often considered to be better trained by their employers than employees of truck carriers. In fact, truck drivers may actually obtain licenses to handle tractor-trailers without special tests in nineteen states (pending federal legislation may close this loop-hole).

The DOT is also responsible for carrier inspections. Like the NRC, it has a very small inspection staff. Therefore, some have argued that its monitoring capacities are inadequate [Insurance Institute for Highway Safety 1985, Office of Technology Assessment 1986, Waller 1988]. Frequently, drivers use multiple licenses and logs to avoid penalties. Additional problems are related to hours-of-service regulations: Bureau of Motor Carrier Safety research suggests that these regulations should be changed, but no action has been taken to date. As a result these avoidable risks continue [Page 1988]. Although the transportation system for spent fuel will probably be more closely watched than other transportation systems, there is cause for concern about the ability of DOT or DOE under current regulations and implementation strategies to inspect adequately all shippers and carriers involved with shipments to a repository.

An additional source of inspection inadequacies (in both the NRC and DOT) arises from the unavailability of reliable incident and accident data. This may become an especially severe problem when rates of cask production and use grow rapidly to accommodate the expected increase in the volume of shipments to a new repository. In the past, it has been the

industry itself that has frequently identified and corrected errors, rather than the regulatory agencies. According to DOE statements carriers will be private haulers of hazardous materials. The ability of carriers to maintain effective and reliable risk management programs, however, is open to question. It is unclear whether such firms (or their employees) are sufficiently sensitive to the special nature of high-level radioactive materials and the special handling and human reliability requirements involved.

3. A Socio-Technical Systems Approach

Ultimately, any analysis of the spent nuclear fuel transportation system must be concerned with both adverse radiological and non-radiological consequences to humans and the environment that may occur during both normal and accident conditions. The main line of defense to any accidental release of radiation hinges on the integrity of the spent fuel casks. However, cask failure may result from a variety of causes at different stages and phases of the transportation system. Thus, our concern is over incidents and accidents arising from human errors during all phases of the spent fuel transportation system [see Table 1 above]. Our perspective is one of a "system" in which individual components are not only analyzed individually, but as interacting dynamic components that must be examined in their totality. If interactions of different subsystems are not taken into account in transportation risk management activities, the result may well be the failure to effectively implement many proposed control strategies.

TABLE 2

RESPONSIBILITIES AND ACTIVITIES OF FEDERAL AND STATE AGENCIES AND PRIVATE ORGANIZATIONS

	DRIVERS	CASK MANUFACTURE	INSPECTION	ENFORCEMENT	QA/QC MAINTENANCE	REGULATIONS	EMERGENCY RESPONSE	OTHER SUPPORT	PRENOTIFICATION	SECURITY	INVESTIGATIONS
NRC		X	X	X	X	X	X		X	X	X
DOE		X	X	X		X	X		X	X	X
DOT	X		X			X					
AAR	X				X						
FEMA							X				
NRT							X				
NTSB											X
INPO							X				
UTILITIES (ORIGINATOR)					X			X			
SHIPPERS			X					X		X	X
CARRIERS	X							X		X	X
STATES	X		X			X					X

The approach we utilize evaluates the spent fuel transportation system from a human factors and socio-technical perspective to identify the types of human actions that may affect system risks and how they may be eliminated or their effects mitigated. Human Factors is an interdisciplinary field concerned with improving the relationships between humans and technical systems (e.g., effectiveness, efficiency, safety). "Its goal has been to design systems that use human capabilities in appropriate ways, that protect systems from human frailties, and that protect humans from hazards associated with operation of the system" [National Research Council 1988:12].

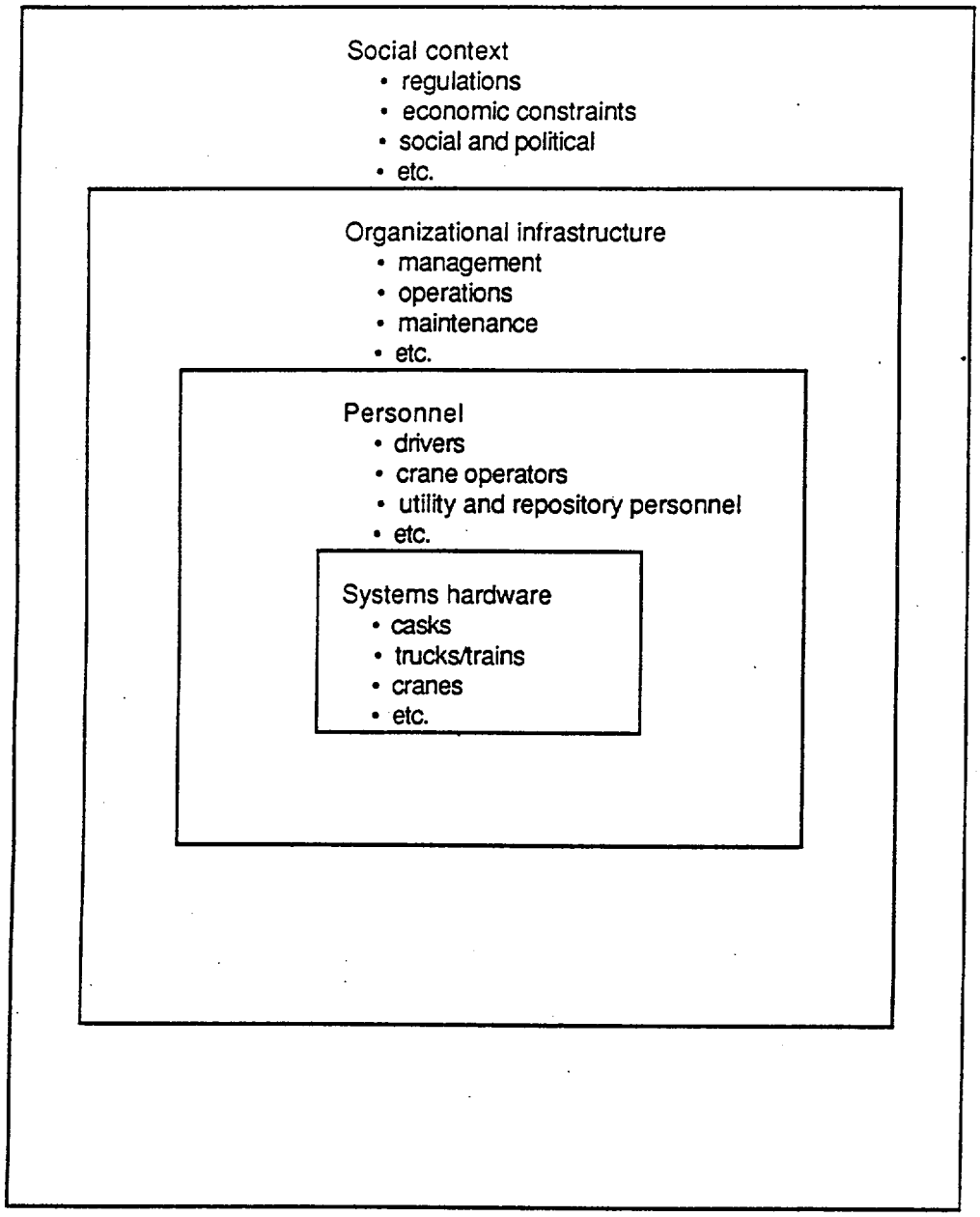
Until recently the focus of human factors has generally been on the narrow interactions of individuals and machines with which they interact while broader organizational and social factors were ignored [Bellamy 1983]. However, system failures may also result from organizational and social effects on decision making and operational behavior. To incorporate these issues into our analysis, we view the transportation system broadly as a socio-technical system, similar to a recent approach to the analysis of safety in commercial nuclear power plants [National Research Council 1988]. In the context of this work, socio-technical system refers to interacting components of system hardware (e.g., spent fuel casks, trucks, cranes), personnel (e.g., drivers, crane operators, managers), organizational infrastructure (e.g., operations, maintenance, administration), and social factors (e.g., regulations, economics, culture) [Figure 3]. A broad socio-technical systems perspective "has great potential for delivering results that yield useful recommendations for safety improvements" [National Research Council 1988].

One particularly important aspect of this perspective is the need for closed-loop feedback from risk assessment to risk management. Risk assessments of technical systems are based on theoretical models and assumptions concerning human behavior during system operations and maintenance. Consequently, these models of behavior and their underlying assumptions must be incorporated into operating specifications and procedures and must provide a basis for risk management control strategies. In addition, error detection and analysis should be based on an awareness of safety constraints and accepted levels of risk identified in risk assessments. Such evaluations should form a closed loop based on actual operating experience to reassess the results and assumptions of risk assessments [Figure 4].

Using the concept of a socio-technical system we have developed a comprehensive methodology for identifying and evaluating the scope and types of human error sources in a spent nuclear fuel transportation system. In particular, a "human reliability matrix" is used to provide a framework for 1) the identification of previous and potential future human errors in the transportation system, and 2) the identification of risk management options that can be implemented to prevent, mitigate, or recover from human errors and their consequences.

FIGURE 3

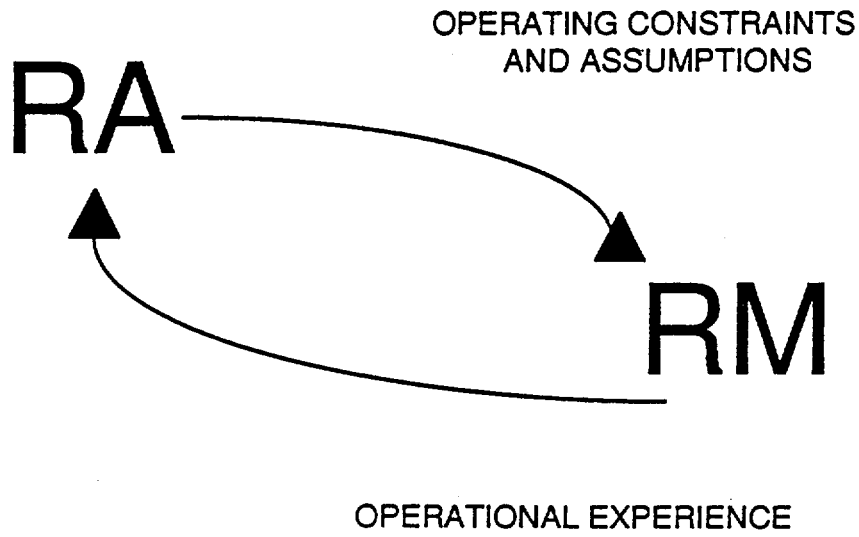
A SOCIO-TECHNICAL VIEW OF THE HIGH LEVEL RADIOACTIVE WASTE TRANSPORTATION SYSTEM



SOURCE: Adapted from National Research Council (1988)

FIGURE 4

INTEGRATED RISK ASSESSMENT - RISK MANAGEMENT



Many prior discussions of human error generally focus on individuals and their interactions with a task or machine (i.e., the interface between the system hardware and personnel identified in the innermost levels of Figure 3). Because the source of actions and goals in many activities are partly the result of subjective criteria, the identification of an error frequently becomes contradictory and closely associated with the assignment of blame and responsibility. In addition, the assignment of blame and responsibility is often related to the power structures within institutions so that the identified "causes" may actually have little to do with the deeper reasons behind failures.

However, interindividual interaction (e.g., group decision making) is also an important feature of activity in the transportation system and is included in the interface between system hardware and personnel as well as at the organizational level. Similarly, because organizational and social factors form the context in which the transportation system operates, they may have significant influences on the safety and reliability of the system. In particular, management can directly or indirectly affect safety and reliability in performance. These influences are also discussed in this report and are believed to be important in human error causation and control.

To provide an understanding of the theory and concepts of our approach, a review of the nature of human errors is discussed in the following sections. These sections summarize the more extensive review provided in Appendix A.

3.1. Individual Errors

The web of interactions between system hardware and the personnel subsystem of a socio-technical system makes defining "human error" a difficult task. Attempts at a unifying definition have often lead to ambiguities and improper characterizations. The definition of "human error" is important, however, because of the underlying basis it provides for any approach to human reliability assessment. Several definitions and cognitive models have been developed, each providing insight into the complexity of the problem, and each becoming more sophisticated in their attempts to include the multiple relationships of human capabilities and task characteristics.

In human-machine systems analysis, variable goals or intentions are incorporated by the conceptualization of "human error" as the behavior of a person transgressing multiple criteria for acceptable performance [Sheridan 1983]. For example, the immediate goals of transport personnel involved in operational tasks (e.g., loading, handling, driving) will vary as the environment moves from one of normal to emergency conditions. Similarly, "acceptable" performance is subjective and related to a variety of criteria, including technical and economic efficiency, system reliability, and public safety, and immediate perceived needs.

In another definition, developed in systems and reliability engineering, a human error is defined with reference to four criteria [Rasmussen 1982]:

1) it is a cause of deviations from a standard;

2) it appears on the causal path to the effect;

3) it is acceptable as a reasonable explanation; and

4) it is such that a cure is known.

These definitions suggest four important factors absent from earlier definitions of human error:

1) multiple externally defined objectives may be relevant to a particular action,

2) the assessment of error depends on being able to identify it,

3) multiple causes may exist, and

4) the source of analysis influences the identification of an error.

These factors are important because the identification of a specific cause of failure frequently depends on how far back in time incident analyses look for root causes; in other words, identification of causes depends on the "stop rule" applied to identify root causes of an incident [Rasmussen 1982, Svenson 1986]. For example, in a hypothetical transportation incident involving spent nuclear fuel, the root cause may be identified as the truck going off the road, the incorrect closure of the cask, or the inadequacy of inspection and quality assurance personnel performance prior to shipment departure, after cask maintenance, or during cask fabrication. The DOT HMIS database would only identify the incorrect closure of the cask because its stop rule is the "actual primary cause of package failure". The other human errors may be relevant, however, for identifying the most effective risk management intervention strategy.

Although some of the tasks in the transportation system for spent fuel involve manual control and have little problem solving or inferential needs, many do have a cognitive component. Tasks requiring memory, attention, interpretation, and problem solving occur in detection, diagnosis,

and recovery activities (i.e., during planning, maintenance, inspection, transport, and accident recovery related activities). Failures in such activities are considerably more difficult to characterize than action errors because cognitive behavior is more ambiguous than proceduralized actions and cognitive processes are not necessarily decomposable.

In particular, there are several difficulties in attempting to observe and understand the cognitive processes and reasons, or subjective rationale, of individuals making decisions, inferences, or judgments. Part of the ambiguity arises because individuals may use multiple decision making strategies and they may not be aware of switching among them. In addition, decisions are not necessarily discrete events in time or place, nor are they distinct from other individual and group activities [Poole and Hirokawa 1986]. Still another ambiguity arises because "effectiveness" is not necessarily the only desired outcome: additional "non-decision" functions include justifying procedures, distributing blame or success, and fulfilling role expectations. "Effective" choices may actually be of secondary importance relative to other goals.

Empirical observations of human problem-solving and decision making have shown that people do not generally use prescriptive decision analysis techniques. In fact, novices are the only ones who generally use such techniques. Moreover, in complex technological systems, such as that of spent fuel transportation, many decisions are "dynamic." "Dynamic decision" environments refer to problem situations where a series of interdependent decisions are required, task specifications and the environment are dynamic, available information may be dependent on prior decision outcomes, and decisions modify the environment [Slovic et

al. 1977, Brehmer 1987]. Severe problems may result because while people are generally capable of understanding causal chains of system processes, they have difficulty understanding the dynamics of complex processes [Bainbridge 1984]. There is no normative theory of problem solving, however, for these dynamic decision environments, as opposed to "static decision" environments (i.e., decision problems are sequential, do not depend on prior outcomes, and the environment is stable).

To simplify a complex world and guide their judgments, humans develop biases and heuristics in their information processing and decision making [Tversky and Kahneman 1974, Svenson 1979, Svenson 1981, Fischhoff 1986, Rasmussen 1987b]. In general these processes work to people's advantage, but in certain situations they can cause the selection of inappropriate choices or actions and lead to predictable biases.

Consequently, individual cognitive biases and heuristics call into question the whole concept of "rational" decision making that is often assumed in planning, judgmental, and inferential situations. These problems have been confronted with the notion of "bounded rationality" that refers to informational and time constraints that force people to make choices based on limited information [Simon 1955]. Similarly, unconscious heuristics learned over time may create problems in novel situations where they suddenly become irrelevant or even detrimental [Svenson 1979]. In many cases, decisions may be "rational" but made in incorrect contexts [Perrow 1984].

Prior research on human cognitive processing, decision making behavior, and cognitive models, suggests that analyses of human-task systems cannot be based solely on task characteristics. For example, the

occurrence of failure is closely associated with human variability resulting from stochastic behavioral properties, learning, and adaptability. In fact, it is now believed that most types of successful and unsuccessful human performance can be explained by a common, limited set of underlying cognitive mechanisms and their interaction with task characteristics and situational factors [Rasmussen 1987b, Reason 1987a]. Failures are closely associated with the system characteristics of observability of system state and dynamics and the reversibility of system behavior [Appendix A.2].

Other human factors research suggests that human errors may have significant effects on accident probabilities and consequences in the transportation system for spent fuel. Such research has been conducted on fatigue, monitoring tasks, decision times, illumination, noise, vibrations, and other ergonomic issues [Kantowitz and Sorkin 1983, Salvendy 1987]. Many of these effects have been studied in the context of truck transportation [Waller and Li 1979, Insurance Institute for Highway Safety 1985, Hertz 1987, Jones and Stein 1987, Waller 1988]. On the other hand, very little human factors research has been conducted specifically for railway transportation (most human factors research in this area is related to railway construction and maintenance tasks, such as lifting). One of the more important results from transportation related studies is the relationship among hours-of-service rules, fatigue, and accident probabilities--accident probabilities increase along with driving times and driving schedules that are not compatible with drivers' 24-hour, circadian sleep cycles [Waller 1988].

3.2. Group Errors

In many technological systems groups of people must interact to perform a task and failures can result from their interactions. Interindividual interactions may have especially important implications in planning and decision making situations and affect performance in the personnel subsystem and its interactions with system hardware and system infrastructure interactions with the social environment [Figure 3]. For example, in the spent nuclear fuel transportation system, groups may plan routes, two drivers may operate a truck, a number of individuals may be involved in deciding how to respond to an incident or accident, and environmental activists may influence public policy. Consequently, the dynamics of group decision making, and in particular the effects of faulty group decision making, need to be incorporated into our conceptualization of human error.

Faulty group decision making can often be traced directly or indirectly to communicative and social influences of individuals. Five factors that have been suggested as leading to faulty decisions are [Hirokawa and Scheerhorn 1986]:

- improper assessment of situation,
- establishment of inappropriate goals and procedures,
- improper assessment of attributes of alternatives,
- establishment of faulty information base, and
- faulty reasoning.

Important factors affecting the quality of group decisions are conflict and group biases [see Appendix A.5]. These factors can enable faulty decisions by facilitating the occurrence of errors such as misinterpretations

and incorrect conclusions during different stages of the decision making process. Conflicts may arise in regard to substantive issues in a group task, procedural methods, and affective issues between members [Putnam 1986]. Group biases result from interindividual interactions that may affect behavior and lead to faulty decisions. They include:

- the "risky shift" phenomena in which a group chooses more risky alternatives than its individual members;
- group polarization, whereby the choice of a group is more extreme than the individual choices;
- groupthink, where a group arrives at a consensus decision without adequately evaluating all alternatives;
- false consensus, where individuals of a group falsely believe that a consensus has been reached; and,
- pluralistic ignorance, where group members believe they are alone in their beliefs.

In the transportation system the form of consensus generated by groupthink is of particular concern because it may also contribute to more risky decisions (e.g., "risky shift") and may lead to especially severe consequences in hazardous situations such as those that may result from spent nuclear fuel transportation accidents. The major factors contributing to such behavior are the uniformity of members, the size and isolation of a group, norms, cohesiveness, and personalities [Reason, 1987b]. In groups experiencing groupthink, "the powerful forces of perceived 'togetherness' act in concert to render the possibility of failure unthinkable--and if not unthinkable, then certainly unspeakable" [Reason 1987b: 124]. This behavior, characteristic of '"mindsets", is frequently seen in risk research

and hazard and accident response planning by the frequently mistaken belief that catastrophic accidents are not credible events and that response organizations are well prepared [Gray and Quarantelli 1984].

3.3. Social and Organizational Factors

The field of human factors has rarely focused on errors connected to social or organizational characteristics in high-risk technological systems although these aspects of socio-technical systems have been identified as contributory causes to many accidents [Turner 1978, Bellamy 1983, Perrow 1984]. Moreover, organizational design is frequently ignored in safety analyses in contrast with construction and personnel considerations [Nordic Liaison Committee for Atomic Energy 1985, Bjordal 1987].

The dynamics of interindividual interaction are partly a result of the understanding of system behavior by personnel that arise through the framing effects of affective, cultural, and social forces by which people understand, interpret, and infer things about the world around them. In addition, dynamics depend partly on the work environment (e.g., management-employee relations, job requirements) and organizational structure (e.g., authority, hierarchy, communication system). Thus, organizational and social factors affect the conceptualization of human errors in two primary ways:

1) group and individual perceptions and actions can be influenced by organizational, social, and cultural factors. These may lead to "operational errors" where incorrect actions were performed or correct actions not performed because of "framing effects" or other constraints on behavior.

2) Organizational and social factors may diminish effective decision making capacity of individuals and groups within an organization. This effect may lead to decision and planning failures ("policy errors") within organizations. The hazards of spent fuel transportation, however, demand very low failure rates in management and planning.

The reliability of organizational behavior is measured with respect to the efficiency and effectiveness of prevention and detection of, and recovery from, threats to system safety. Organizational and policy errors can result from both the dynamics of interindividual interaction and organizational structure. These factors not only affect the reliability and effectiveness of actions and decisions, but also provide the context for "rational" reasons that in hindsight are determined to be faulty. Table 3 lists potential organizational and social factors contributing to failures.

TABLE 3

Social and organizational factors contributing to system failures

- Pressure
  - group, social, authority, heavy responsibility
- Job requirements
  - ill-defined job requirements
  - multiple personnel use same equipment
  - multiple tasks--work overload leads to selective attention by decision-makers and workers
  - lack of resources--inadequate access or distribution
- Conflict
  - substantive
  - procedural
  - affective
- Assumptions related to tasks or roles conflict
  - management vs. designer
  - management vs. operating personnel
- Rigid organizational beliefs and assumptions
- Rules and procedures not maintained
- Communication system
  - assumed reliable when it is not
  - delayed
  - noisy
  - informal
  - blocked
  - hierarchical--information distorted, not passed, or reinterpreted
  - reporting of messages not completed or incorrect
- Organizational authority
  - overlapping responsibilities
  - hierarchical structure
  - slow learning and adaptation to new or changing environment
  - inconsistent and conflicting objectives
- Quality of work environment
- Framing effects
- Industrial actions
  - strikes
  - slowdowns
- System considered unreliable or untrustworthy by personnel

Frequently, issues of influence and power play important roles in decision-making behavior in organizations. For example, the roles of managers is crucial to safe and reliable system operation because they can affect safety both directly and indirectly. The managers create and maintain an organizational culture that reinforces safety and reliability considerations (i.e., "culture of safety"), implementing effective decision making protocols and shaping the impact of regulations and social constraints on operational activities [National Research Council 1988]. In the spent fuel transportation system, management must be adept at working within a complex system of federal and state regulations that can affect system flexibility in operations. Similarly, if the public is highly skeptical of the DOE's ability to operate the transportation system or repository, the operations must be as safe and failure-free as possible and the response to incidents must be immediate and effective. Members of the public, it needs to be remembered, measure safety and reliability largely through their perceptions of safety and reliability [LaPorte 1988].

On the other hand, the actual behavior of managers can exacerbate problems inherent in organizational behavior. In particular, managers often spend considerable time in low priority activities, perform with self-serving biases, lack interest in the implementation phase of policy, and concentrate on appeals to the legitimacy of outcomes and processes [Crecine 1986]. In public organizations, management frequently attempts to shape employee behavior and operations to externally-, constraint-oriented managerial strategies or ignores task performance in organizational design [Cook 1988]. Organizational structure is often created and maintained to ensure an organizational culture that promotes

economy, ease of management, and organizational survival. Similarly, technological designs and choices are frequently a result of attempts to reinforce or reproduce existing structures [Perrow 1983, Noble 1986, Cook 1988].

In spite of framing effects, subunit goals, perceptions, and values of large and complex organizations may be very differentiated. In fact, organizations tend not to be coherent wholes, but resemble collections of subunits and specialists with their own objectives and conflicting choice making techniques. Subgroups may develop informally and provide information bases other than those derived from formal authority structures. These subgroups may contribute to failures because of barriers to information gathering, sharing from social habits, and established patterns of routine interaction. On the other hand, individual and subgroup diversity is an important mechanism for coping with the complexities of the real world.

One of the reasons organizations develop centralized control structures and rigid procedures and rules is to ensure that individual behavior is true to organizational "desires". In particular, lack of central control has been observed to lead to confusion, delays, competition for power, and a management void [Sorensen and Vogt 1987]. On the other hand, the central control provided by hierarchies is assumed to ensure continuity of knowledge and processes, to direct actions, and to create shared perceptions, assumptions, and methods. All of these allow the smooth functioning of the organization. Such organizational constraints, however, may also contribute to the occurrence of failures [Appendix A.6]. For example, organizations may create or amplify unintended sequences in

surprisingly ordered ways by virtue of these common understandings and normal administrative processes [Turner 1978].

Another method of dealing with the tensions between subgroup behavior and organizational "desires" is the implementation of standard operating procedures [SOP]. Such procedures are developed to match personnel with both work requirements and the environment. SOP's, however, reduce the variability and "richness" of information internally and do not usually provide adequate guidelines for actions necessary for safe and reliable performance. Gaps in such procedures are filled by organizational culture and motivational incentives. The absence of SOP's for many important situations suggests the need for knowledgeable decision making and flexibility by personnel other than at managerial and policy levels of an organization. Unfortunately, most individuals and subgroups in complex technological systems are not trained, encouraged, or necessarily capable of utilizing substantial rationality in decision situations.

Many of the social and organizational factors that lead to system failures can be understood by the behavior that organizations generate in groups and individuals. In fact, most disasters within organizational settings do not occur as the result of single actions by a single individual, but rather from complex interactions of a number of individuals or groups. One approach to modeling the dynamics of failures in organizational environments, which recognizes the special characteristics of organizational decision making, is based on a "sociological definition of disaster as a challenge to existing cultural assumptions" [Turner 1978: 84, Appendix A.7]. It is a time phase approach to describing organizational awareness of

divergences between its perception of the world and the actual state of the world.

In this view, an unnoticed set of events at odds with accepted beliefs about hazards and how they may be avoided accumulate during an "incubation period". These events enable system failures at a later time by setting the stage whereby a single event can precipitate a major disaster. These events may not be observed because of erroneous assumptions, poor and delayed communication, and cultural lag in existing precautions, as well as other individual, group, and organizational factors described above. In particular, when norms of correct and incorrect behavior are related to the performance of standardized procedures, negative interactions or errors may not be readily observable when the "correct" procedures are followed. Moreover, the knowledge and understanding of events may be limited by the distribution of power, control of resources, and social constraints. Thus, even though the information exists, knowledge may be limited with respect to the consequences of potential choice alternatives and the events that occur as a result of choices.

These ideas correspond to the notions of observability and reversibility in individual errors described earlier. Observability of events and failures are limited by the nature of group and organizational behavior, barriers in the flow of information, and the distribution and control of authority. In addition, design strategies of multiple defenses create situations where many errors may appear in the system but remain unnoticed. Their identification may only occur when independent events cause a failure or change in system behavior [Perrow 1984, Rasmussen 1987d]. The reversibility of failures (single or accumulated) are further

limited by these constraints, and also by normal group and administrative processes that can actually amplify their consequences.

3.4. Errors as Mismatches

The confluence of research resulting from both theoretical and applied work on human error suggests that defining human errors as mismatches that derive from the total human-task system is an appropriate approach for the analysis of complex human-task systems (such as the transportation of spent nuclear fuel). Failures caused by "human errors" in such an approach, occur when a system goes outside of its acceptable boundaries of behavior due to human-task or human-machine interactions (i.e., they result in undesirable consequences). In many cases, errors can be thought of as the inappropriate match between an individual's mental representation of a task or system and the actual state and dynamics of a task or system. Consequently, there is a need to include subjective reasons, external environmental factors, characteristics of human information and cognitive processing, and task characteristics in any reasonable definition of "human error" in complex technological systems.

One way of doing this is by conceptualizing errors as human-task or human-machine "mismatches." Thus, "human error" may be defined as the result of a mismatch between perceived and actual system state and dynamics in human-machine or human-task systems. Mismatches occur as a result of human variability, technical variability or failure, and required interactions that are incompatible with general human cognitive

limitations or organizational constraints. This perspective on human error incorporates the important issues shown in Table 4.

In the case of frequent mismatches, the cause can be attributed to design errors, resulting in an inappropriate match between the content and organization of tasks with respect to human capabilities. For example, misperceptions of system designers can create task requirements that are incompatible with human capabilities, both in normal and emergency operating situations. Design errors can induce failures at a later time because task demands were not matched to human capabilities.

On the other hand, errors can result from the inability of humans to match themselves adequately to a task. Infrequent mismatches can be viewed as resulting from variability on the part of the system or humans during operational phases. Errors result from divergent operator perceptions of system state and dynamics and actual system state and dynamics. Thus, mismatches may occur even in systems that have been designed to avoid the occurrence of human errors. Often such mismatches are due to inadequate feedback and excessive demands on human cognitive capabilities--characteristics closely associated to the concepts of observability and reversibility discussed in section 3.1.

Although it is true that there are some errors in function that can be attributed solely to technical components or to human operators, many result from the interaction of these two worlds. In the past there have been attempts to remove human participation in technological systems as a way of reducing the frequency of errors and improving performance. Where they have not been removed, it has usually been because humans possess special capabilities that cannot be matched by technical

components in the system. In particular, humans are adaptable and flexible. The need for these characteristics frequently occur in systems where judgmental, inferential, problem solving, and decision making capabilities are needed. Humans are particularly adept at such behavior, whereas machines are not.

These same characteristics, however, also affect human variability and may create the conditions that push systems beyond acceptable limits of performance. Human variability results in complex, multidimensional relationships between a task or machine and human operators. This variability can affect the probability of errors in two major ways [Rasmussen 1987a]:

1) human variability causes system behavior to transcend acceptable boundaries of continued system function; or,
2) human variability is insufficient to maintain acceptable system behavior when the system itself changes.

In the human factors literature, nonpersistent factors, or events that are recognizable as distinct in space and time are usually described as causes of failure in technological systems [Rasmussen 1982]. Yet the information processing and behavioral characteristics of individuals and groups are affected by many different persistent phenomena and characteristics of the decision environment. Persistent conditions are referred to as "performance-shaping factors" and include affective, social, organizational, and physiological features of the work environment (e.g., noise, fatigue, illumination, time pressures, emotional stress, communication protocols, management-employee relations) [Rasmussen 1982, Embry 1984, Rasmussen 1987c, Gael 1988]. "Such factors will not

directly appear in the causal chain of events but may influence it by changing human limits of capability, subjective preferences in choice of mental strategies and goals, etc." [Rasmussen 1982: 20]. They influence the behavior of a system by affecting the interactions of people in a system and the cognitive processes involved in setting priorities, planning, selecting goals, and generating and testing hypotheses. Fatigue and stress are performance-shaping factors that have been shown to affect greatly decision behavior. They may be particularly relevant to the spent fuel transportation and transshipment system because costs due to failure may be very high.

Fatigue may significantly affect risk of transportation accidents by decreasing operators' abilities to respond to hazardous driving situations. Fatigue may result from two different but related causes: 1) length of driving time, and 2) time of driving (although the effects of fatigue are discussed in terms of truck transport, it is also relevant for rail engineers). The duration of driving a truck may affect accident probabilities because such an activity has very few stimuli that maintain levels of alertness. The time of driving may also affect the level of fatigue because humans operate on 24-hour, circadian, sleep cycles. If a person attempts to drive at times during which they normally need sleep, their level of alertness will be low. Changing roadway conditions and maneuverability difficulties, however, require not only truck operating experience, but a high degree of alertness for safe operation [Page 1988].

Emotional stress may occur in decision tasks because of threats of negative consequences, individual anxiety, or conflict. Fear and depression may influence how an individual deals with uncertainty and performs

tasks and may increase subjectively experienced workload, thereby decreasing performance. Lack of knowledge or uncertainty in decision situations may contribute to emotional stress because people are unable adequately to evaluate alternatives.

Time pressure also contributes to stress and may occur in emergencies or routinely system requirements (e.g.,. delivery schedules). Individual decision making and problem solving becomes more difficult with the introduction of time pressure, which can drastically increase the mental workload experienced by an individual. Time pressure may also increase cognitive strain and emotional stress because of the awareness that events may be unavoidable. Similarly, time pressure may induce stress because a decision maker may not be able to identify or evaluate all the important information.

Failures occurring in group or organizational environments are well suited to a conceptualization as human-task mismatches. Enabling or initiating events may be caused by interindividual interaction (e.g., group or organizational) as well as individual actions that can accumulate to cause system wide failures or disasters. The concept of an "incubation period" describes how the perceptions of system state and dynamics by personnel may diverge from actual system state and dynamics, thereby creating a "mismatch" [Appendix A.7]. For example, perceptions of operating characteristics by management and operators may differ significantly from actual design features and assumptions because of communication constraints. Such differences can lead to improper use of equipment and, consequently, to failures. In the transportation system for spent fuel, such failures could occur in the use of spent fuel casks and

loading equipment and procedures. These dynamics are partly a result of the understanding of system behavior by personnel that arise through affective, cultural, organizational, and social forces by which people understand, interpret, and infer things about the world around them. These factors not only influence actions and decisions, but also provide the context in which "rational" reasons for certain actions in hindsight are determined to be faulty.

4. Transportation Risk Management

When the transportation system is viewed broadly, it is clear that numerous control strategies for improving human reliability exist at all phases of the transportation system and at all socio-technical levels of the system. Ideally such control strategies should entirely eliminate causal chains leading to incidents or accidents through effective design. In many cases, however, this is not feasible, especially in the case of human-task mismatches that cannot always be foreseen or in tasks which are not formalized. Consequently, transportation risk management programs should also focus on increasing the observability and reversibility of human-task mismatches and mitigating their adverse consequences. The focus of mitigating and recovery strategies are on incident and accident control, clean-up, and monitoring. Figure 5 illustrates the relationship between these transportation risk management approaches and a generalized transportation incident or accident sequence.

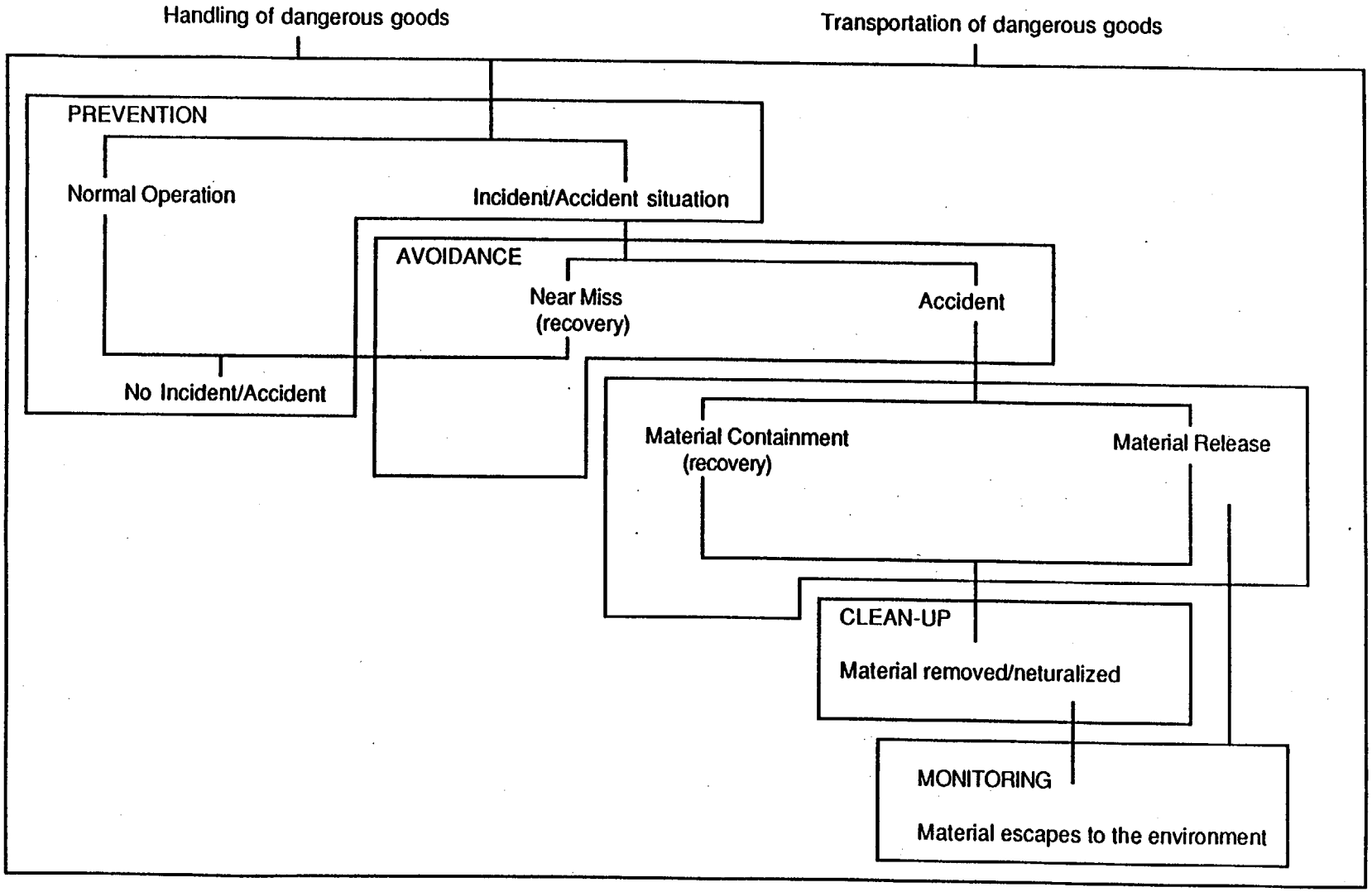
TABLE 4

Human error as human-machine or human-task mismatches

- removes the attribution of blame on individual or group operators in many instances where the task was not well designed;
- failures may be due to differences in externally prescribed standards of interaction, procedures, and objectives to those of operating personnel (e.g., design phase vs. operating phase);
- faulty decision making can be caused by interindividual interactions in groups and organizations and can enable or initiate system failures;
- performance-shaping factors affect human-task interactions and human behavior, including affective, social, and organizational influences;
- recoverability from system failures depends on human characteristics of variability and adaptability; and,
- recoverability from system failure dependent on (technical) characteristics of observability and reversibility .

FIGURE 5

RISK MANAGEMENT APPROACHES TO TRANSPORTATION INCIDENTS/ACCIDENTS



SOURCE: Adopted from Martin et al. 1986

While the primary focus of transportation human reliability risk management programs is generic, specific concerns may vary. In particular, there are several aspects of a transportation system for spent fuel that must be managed because of differences among: casks, other support equipment (e.g., trucks, cranes), transport workers (e.g., truck drivers), and other personnel (e.g., cask loaders and handlers, managerial staff, maintenance staff). Moreover, the formalization of a task affects the choice of risk management approach. Planning and design tasks, for example, are more ambiguous and their causal sequences less open to analysis. On the other hand, cask handling and loading is completed at a nuclear reactor site where personnel are presumably well-trained to respond to incidents and accidents. Accordingly, different activities call for different types of transportation risk management approaches. For example, during actual transport, respondents to an accident may not even know that radioactive materials are involved, which suggests the importance of inspections to verify pre-notification and placarding requirements.

4.1. Control Options

Table 5 provides a suggestive list of possible transportation risk management control options that could be used in the transportation system. They are divided roughly into socio-technical levels, although it should be noted that many control strategies can appear at more than one level, affect more than one phase, or affect the interactions among phases. A broad view is essential in that it suggests a number of possible interventions in causal event sequences leading to failures. This broad

view for identifying transportation risk management strategies is even more important because the system in question is a new one. Thus, risk can be affected at not only system hardware and personnel levels (as is the most common approach), but also in infrastructural and social levels that may be more effective in eliminating risks rather than mitigating their consequences.

In the transportation system, technical design strategies can reduce human-task mismatches by formally incorporating human factors considerations in the development of regulatory requirements and making equipment "goof proof". These strategies are important because errors are frequently a direct result of defective designs.

Control strategies during implementation can do much to ensure proper fabrication of equipment and effective training of personnel. Control strategies should include thorough review and inspection before casks and other critical equipment become operational. Similarly, human factors considerations should assist in the implementation of effective and reliable decision protocols.

Control strategies during the operations and maintenance phases should emphasize effective human error data collection and analysis and quality control inspections to evaluate actual performance. Similarly, human errors may be reduced by improving the quality of the work environment and by promoting a higher sense of professionalism. Control options include greater employee participation in planning activities, increased work incentives, and the establishment of a "culture of safety".

Control strategies for ensuring effective and reliable accident recovery occur during design, implementation, and actual response

activities. They may affect ultimate recovery performance by ensuring proper maintenance of response equipment, training of response personnel, and timely access to equipment. Interagency coordination and well thought out decision protocols can also affect accident response capabilities.

Three additional strategies for transportation risk management are important because of the general perspective that they provide for the identification and evaluation of potential human-task mismatches. They are discussed in the following sections and include:

1) job and task analyses,
2) a comprehensive risk assessment-risk management approach, and
3) effective human error data collection and analysis programs.

TABLE 5

TRANSPORTATION RISK MANAGEMENT OPTIONS

SYSTEM HARDWARE
- Choice of technology (e.g., mode)
- Design of technology (e.g., automation, manual, maintainability)
- Quality control
  - Testing (ongoing)
  - Inspection
  - Repair

PERSONNEL
- Procedures and protocol development
- Training
- Staff qualifications, including management
- Job analysis
- Task analysis
- Incentives/discipline (e.g., motivation)
- Quality control
  - Testing (ongoing)
  - Inspection

ORGANIZATIONAL INFRASTRUCTURE
- "Culture of safety"
- Data collection and analysis
  - Error investigations
  - Accident investigations
- Organizational structure (e.g., decision protocols, communication channels)
- Safety committees, quality circles
- Labor union/employee management relations
- Enforcement

SOCIAL FACTORS
- Enforcement
- Coherent and comprehensive regulations
- Economic and political incentives and constraints
- Risk communication

4.1.1. Job and Task Analyses

Job and task analyses provide an important approach for pre-identifying critical tasks and potentially critical errors in transportation related activities. Moreover, such analyses may be used to support evaluations and modifications of transportation risk management control strategies. Jobs are collections of tasks assigned to a single person, whereas tasks consist of specific activities that an individual must perform. The characteristics of both tasks and jobs have important impacts on human performance. Thus, their assessment and design should be on-going activities in the transportation system.

Many different methodological processes fall under the rubric of job and task analyses [Pedersen 1985, Embry 1986, Gael 1988]. Discussing their qualities or selecting a "best" method is, however, beyond the scope of this report. Each can provide different types of information relevant to the design and operation of a spent fuel transportation system [Table 6]. In fact, specific approaches will vary, depending on the characteristics of the job or task under analysis (e.g., well-structured, formalized, policy-oriented, cognitive), who is performing the analysis, and the availability of empirical data, time, and resources.

Human error research suggests that inadequacies exist in all cognitive models and taxonomies of human error. Generally, they are not adequate to support analysts in the comprehensive pre-identification of all important error modes and evaluation of behavior at all cognitive processing levels in all task situations. One important difficulty that analysts have is in the use of models and taxonomies for predictive, rather than descriptive, purposes. On the other hand, models are unquestionably useful in suggesting the types of questions analysts should ask, error

modes needing analysis, and psychological mechanisms that cause errors [Embry and Reason 1986, Bellamy 1988, Kirwan 1988].

Whichever analytical process is employed, all potential factors affecting human behavior need to be considered and the analyses need to be based on the knowledge of cognitive and motor capabilities of humans. One method that suggests the range of issues that need to be considered is the Failure-Mode-Effect taxonomy [see Appendix A.9.3 for a review]. The Failure-Mode-Effect taxonomy, is concerned with what and how error events occur [Figure 6]. This method is based on the view that human errors are a result of total human-task system behavior rather than specific characteristics of humans or tasks. Consequently, the taxonomy reflects different factors influencing the interactions of humans and tasks: task characteristics, performance-shaping factors, and human motor control and cognitive mechanisms, cognitive error modes, and external events. Although questions exist as to the underlying cognitive model of this approach [see Appendix A.4.2], it provides a general framework for determining the range of issues to consider and the relationships among them. The failure-mode-effect approach has been used to evaluate well-structured tasks (i.e., scheduled, familiar tasks with unchangeable procedures) in process control plants [Pedersen 1985].

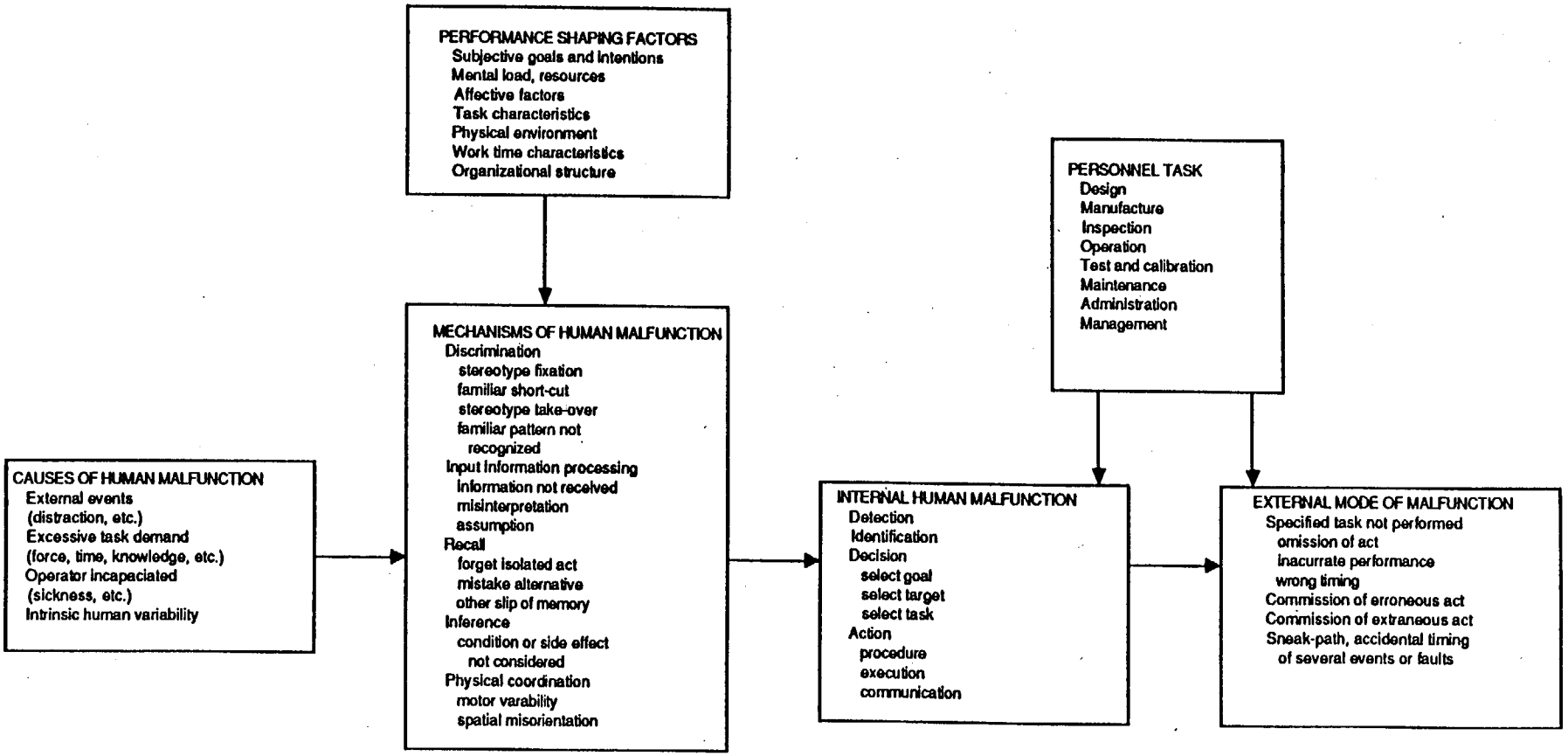
TABLE 6

USES OF JOB AND TASK ANALYSIS INFORMATION

1. Job and Task Description
2. Job and Task Classification
3. Job Evaluation
4. Job and Task Design/Restructuring
5. Personnel Requirements/Specifications
6. Performance Appraisal and Standards
7. Worker Training
8. Worker Mobility
9. Efficiency
10. Safety and Error Reduction
11. Manpower/Workforce Planning
12. Legal/Quasi-Legal Requirements
13. Design/Evaluation of Procedures
14. Communication Requirements and Procedures
15. Human, Machine Task Allocations

FIGURE 6

FAILURE-MODE-EFFECT TAXONOMY FOR DESCRIPTION AND ANALYSIS OF EVENTS INVOLVING HUMAN MALFUNCTION



SOURCE: RASMUSSEN 1982

4.1.2. The Risk Assessment-Risk Management Loop

The second general transportation risk management strategy is the creation of an integrated, feedback driven process of risk assessment and risk management [Figure 4]. Here, analyses of system performance identify the inevitable discrepancies between design assumptions in a risk analysis and actual operational behavior. Transportation risk management programs need to evaluate and correct these failures before they occur.

One approach is for detailed error or accident investigations to be performed after all human-task mismatch events. It should be noted that error investigations are distinct from accident investigations--errors may not actually lead to accidents or incidents in all cases although their potential impact may be great. Both types of investigations are important because they can lead to more effective design and operating strategies that could eliminate or mitigate the effects of other types of errors in the future. The impact of knowledge gained by both types of investigations, however, will only be gained if the results are incorporated into risk assessments and if design, fabrication, or operating procedures are modified.

4.1.3. Human Error Data Collection

The third general strategy is the effective and timely collection and evaluation of human error data to support job and task analyses and accident investigations. This strategy drives the effectiveness and efficiency of all other types of transportation risk management strategies by providing vital evaluative information. To implement effective system designs and modifications, an understanding of how events occurred, as

well as knowledge about what occurred, is essential. This requirement also applies to the use of quantitative data in human reliability assessments.

Consequently, detailed data must be collected during error and accident investigations to support human factors analyses. Structured descriptions of events are needed, based on the sequence of cognitive functions and human behavior prior to, during, and in response to events [Bainbridge 1984]. For effective evaluation, investigators will need to know both the causal flow of events and their underlying control mechanisms. Various methodologies have been proposed for structuring the types of data to be included in such investigations. The most appropriate method needs to be evaluated, but could be based on prior approaches suggested for nuclear and chemical processing industries [e.g., Rasmussen 1980, Lucas 1987]. In addition, simulations and exercises can be used to collect data on specific tasks [National Research Council 1985]. Table 7 lists specific methods for data collection. The data may either be quantitative or qualitative, depending on the approach and the difficulty of measurement.

The collection of experiential, human error data from personnel is fraught with difficulties because current reporting systems typically are often associated with the assignment of blame and responsibility. The NRC has recently proposed an "unobtrusive, voluntary, anonymous, third-party managed, nonpunitive human factors data gathering system" for the nuclear power industry [Nuclear Regulatory Commission 1985a, Nuclear Regulatory Commission 1985b, Nuclear Regulatory Commission 1985c]. The system is designed to encourage the reporting of incidents, accidents, and other unreported, but significant events related to human reliability

and the data are intended for use in identifying and quantifying factors that can degrade safety and reliability. The approach developed by the NRC closely resembles the successful Aviation Safety Reporting System [ASAR] system utilized by the FAA for the reporting of air-traffic errors and failures. Although problematic policy issues exist concerning control and access to information, such an approach provides a potentially effective method for identifying human-task mismatches in the transportation system and should be carefully assessed.

4.2. Human Error Databases

Because of the importance of human error data for both the identification of human error types before they occur and modes of control after they occur, the adequacy of existing transportation databases is discussed in this section. Accordingly, we address questions relating to the accuracy, completeness, and usefulness of transportation related human error data in federal and state agencies and private institutions.

The main sources of information about human errors during non-operations phases in the transportation system for spent fuel are inspection and maintenance reports. Sources for such information include the DOT, NRC, DOE, state inspection agencies, utilities, and carriers. For example, NRC data has been used to summarize prior inspection activities [Grella 1985]. Other data sources are provided by incident investigations when some type of failure occurs during non-transit operational activities. Specific information available from these sources includes data on manufacture, use, and maintenance of casks and transportation equipment (e.g., vehicles, cranes) and personnel qualifications.

TABLE 7

Data Collection Methods

- Observation
  - direct observation by trained personnel
    - error and accident investigations
    - simulations and exercises
  - work diaries
  - critical incident reports
  - work sampling
    - maintenance reports
    - inspection reports
  - indirect methods
    - audio-visual equipment
    - computer monitoring
- Interviews
  - individual
  - group
  - technical conferences with supervisors, managerial staff, and experts
- Questionnaires
  - structured
  - activity checklists
  - open-ended
  - surveys

A newly developing database system to support the Motor Carrier Safety Assistance Program is the SAFETYNET Inspection System under the auspices of the Federal Highway Administration. SAFETYNET is designed to monitor the safety performance of interstate and intrastate commercial motor carriers [Appendix E.3]. It is to be implemented by the states (it is currently being demonstrated in Colorado, Michigan, North Carolina, and Oregon) and will allow users to [Department of Transportation 1986]:

1) input truck driver-vehicle inspection data,
2) monitor carrier inspection histories,
3) identify carriers failing to certify correction of vehicle defects,
4) satisfy MCSAP reporting requirements, and
5) profile inspector workloads.

Consequently, when implemented nationally, it will allow the identification and evaluation of DOT inspection programs and carrier responses to defective vehicles.

Illinois is a unique state in that it has an extensive database of spent fuel rail and truck shipment inspections. Since 1983 the Illinois Department of Nuclear Safety has performed inspections on casks, vehicles, and drivers of all shipments passing through the state [Appendix E.4]. In addition, the Illinois Commerce Commission has performed pre-departure inspections of all rail shipments. Specific problems that have been identified for both rail and truck shipments through Illinois are listed in Table 8.

TABLE 8

ILLINOIS SPENT FUEL TRANSPORTATION INSPECTION DATA BASE

RAIL SHIPMENTS

- Rather common paper work and labelling deficiencies.
- Security problems at an Illinois rail yard, involving a bomb threat.
- Security problems caused by media coverage, which included following a TMI spent fuel shipment with a helicopter.
- Potential security problems at another Illinois rail yard due to negligence.
- A rail/automobile collision (a 25 mph train-speed) in Missouri shortly after the train crossed the Illinois/Missouri border. No damage to the cask occurred.
- The buffer car between the casks in one shipment had a defective flange; the train had to be delayed for repair.

TRUCK SHIPMENTS

- Common paper work and labelling deficiencies.
- Vehicle problems, including a lost wheel in Indiana, misadjusted brakes, unoperable tail lights, several cases of air leaks in brakes, unoperative emergency flashers, and unsafe rear tires. In one case the trailer failed the safety inspection and the shipment was cancelled.
- Driver related problems, including a case where the driver was found sleeping in the cab, and expired training dates.
- Several cases of incorrect highway route plans.
- Security problems, including several failures to notify state authorities, security guards leaving the truck unattended, and several cases of inoperable mobile phones in trucks.

Previous reviews of federal, state, and private transportation accident and incident databases suggest that there are major generic inadequacies in the data they contain for supporting evaluation efforts [Office of Technology Assessment 1986]. For example, reporting compliance of transportation incidents is clearly not 100%, there is no centralized authority for transportation related data collection and analysis, and no uniformity exists in the types of data collected and definitions used.

Although one might suspect that the problems would not be as severe for the more heavily regulated spent fuel transportation system, this is not necessarily the case because of the multiple agencies involved and the ineffectiveness of existing inspection programs. For example, spent fuel transportation related incidents are not complete in the DOT or DOE databases and, when events do occur, they may not be entered immediately. Similarly, access to data is not always easy--for example, the NRC did not even start separating out data on transportation related issues from on-site inspection reports until 1981.

Aside from the generic problems of data reporting and availability, specific problems arise in the data relating to human error. In fact, such data are less adequate for comprehensive analyses than other transportation related data (e.g., property damage, injury rates) because of the ambiguity of human error itself, difficulty in its evaluation, and the general disregard of causal information (i.e., only accident consequences need to be reported in many cases). This suggests in part why data in the Battelle and NRC reports on human error were substantially defective [see section 2.3 and Appendix B]. Table 9 lists federal, state, and private

databases that contain human error related information. The following paragraphs briefly describe them.

The Office of Hazardous Materials Transportation [OHMT] of the the DOT maintains the Hazardous Materials Information System. It requires the reporting of all vehicular accidents and incidents (i.e., releases) during transport related activities (e.g., during packaging, loading, temporary storage, unloading) involving hazardous materials. This database is concerned with the "actual, primary causes" of releases in the transportation of hazardous materials and uses four causal categories--human error, package failure, vehicular accident, and "other".

The actual primary causes are extracted from information reported by carriers on Form F5800.1 [Appendix E.1]. Although the form is accompanied by general guidelines for reporting information, there are no examples related to human errors and no requirement for identifying environmental conditions or contributory causes. In fact, the form does not specifically identify human error as a primary cause of packaging failure. If data entry personnel believe the "remarks" or "packaging failure" sections suggest human error as the primary cause, they may enter it as the causal factor even though the reported information does not specify it. One problem created by the carrier reporting requirements is that the carriers are not involved or present for all transportation related activities (e.g., packaging). Additional problems are specific to the identification of the type of high-level radioactive material involved in events--in particular, only the class of radioactive material needs to be noted so that events involving spent nuclear fuel and other high-level wastes are not necessarily separable.

TABLE 9

HUMAN ERROR/INCIDENT/ACCIDENT DATA BASES

DATABASES	KEPT BY	YEARS	MODES
Hazardous Materials Information System	DOT, Office of Hazardous Materials Transportation, Research and Special Programs Administration	1971 to present	All
Radioactivie Materials Incident Report	Department of Energy, Oak Ridge National Laboratory	1971 to present	All
National Transportation Safety Board File	National Transportation Safety Board	—	All
Monthly Accident/Incident Reports	DOT, Federal Railroad Administration	1957 to present	Rail
Railroad Accident File	Association of American Railroads	1973 to present	Rail
SAFETYNET	DOT, Federal Highway Administrator, Motor Carrier Safety Assistance Program	Demonstration only	Highway
Truck and Rail Inspections	Illinois, Department of Nuclear Safety	1983 to present	Rail, Highway
Washington State Accident File	Washington State Utility and Transportation Commission	1978	Highway
Hazardous Material Spill Database	North Carolina, Department of Environmental Management	1978 to present	Highway
Inspection Reports	NRC, DOE, DOT	—	All

Recently an evaluation was completed on the HMIS database [Office of Technology Assessment 1986, see Appendix B for a review]. It found that "human error" was identified as the primary cause of 62% of accidents and incidents contained in the database. The next most cited cause was package failure, and the next, vehicular accidents. The specific reasons for the occurrence of hazardous material transportation incidents indicate that the dominant cause of failure varies considerably by mode, although loose and defective fittings and external puncture were frequently observed. Other "primary cause" categories included handling, corrosion and rust, package failure, loading and unloading, and metal fatigue, suggesting that human errors occurred during manufacture, maintenance, inspection, and operation. The category of "miscellaneous information" in the study is defined to include events that also suggest certain types of human error (although this is not possible to verify in all cases).

Two databases are maintained specifically for railroad-related information. The Federal Railroad Administration [FRA] publishes yearly summaries based on monthly accident and incident reports. The FRA reporting forms include "human error" in its list of "cause codes" although there are no specific guidelines on how to identify human error as either a primary or contributory cause of rail accidents or incidents [Appendix E.2]. On the other hand, the forms request both primary and contributory causes of incidents and accidents and the environmental conditions when they occurred.

The Association of American Railroads [AAR] also maintains a database on hazardous material railway accidents and incidents, the Hazardous Materials Accident/Incident Database. It uses information filed

on DOT form F5800.1, CHEMTREC reports, and by Hazardous Materials Systems Field Force Inspectors. Unlike the HMIS, no specific field is used to designate human factors as the cause of an accident or incident. Inferences can be drawn from the data, however, that suggest human error as the cause of an event. For example, "tank car leaking from the manway due to loose bolts or no gasket" would suggest the occurrence of a human error.

The Department of Energy maintains two databases specifically related to the transportation of radioactive materials. The Radioactive Materials Incident Report (it was at SANDIA, but has recently been moved to Oak Ridge National Laboratory) contains publicly available data on all accidents, incidents, and handling mishaps during radioactive materials shipments from 1971 to the present. Because the data are derived predominantly from the HMIS, NRC, and state radiological control offices, there is attention is given to human errors as primary and contributory causes than in the DOT and NRC reports.

Another database maintained by the DOE, the Radioactive Material Routing Report, also contains some information that may be useful for human error analyses of the transportation system. It includes descriptions of completed highway shipments by DOE, NRC, and NRC licensed shippers. If the data are accurate, the database may allow analyses of routes taken during spent fuel shipments. Prior analyses of these databases have resulted in reports summarizing operating experiences [McClure and Emerson 1980, McClure and Tyron-Hopko 1985].

The National Transportation Safety Board [NTSB] is the only government agency that performs detailed accident investigations

including human factors experts. Although, the NTSB is only required to investigate accidents which result in fatalities, more than $500,000 in property damage, or occur in the commercial aviation system, one NTSB analyst stated that accidents involving spent fuel and other high-level radioactive waste would also be investigated. Other studies may also be relevant to the transportation system for spent fuel; for example, previous studies have been issued concerning hazardous material transportation through urban areas and interagency coordination during hazardous material accidents [National Transportation Safety Board 1979, National Transportation Safety Board 1983].

Other states currently have their own inspection or incident/accident reporting systems (e.g., Illinois, Maryland, New York, Pennsylvania, Washington). In these systems most investigations and reports are completed by state police personnel and provide very limited data. According to one state DOT agency employee interviewed, because investigators usually have no human factors experience, they frequently assume human error as the cause if mechanical failures cannot be identified. In addition, according to another interviewee, inspections of shipments containing radioactive materials are not always performed by state agencies, even when required. He believes that inspectors tend to shy away from such shipments because of fear about radiological exposure.

North Carolina is one state that maintains an accident and incident reporting system that can support some level of human error analysis. A study of the data showed that human error was specifically reported as leading to 22.9% of hazardous material spills in the state. In the data human error was defined as occurring from four causes: negligence (17%),

accidental (60%), deliberate (14%), and vandalism (9%). Other spills suggesting human error causes occurred from mechanical failure (36.5%) and traffic accidents (26.2%), although there was usually insufficient information about the causes of traffic accidents and maintenance histories to assign cause.

4.2.1. Lessons From Prior Experience

Although the historical experience from spent fuel and other high-level radioactive wastes is limited, some specific lessons related to human reliability are apparent. In particular, significant problems in cask usage and transportation activities have resulted from insufficient attention to human factors issues in the design of equipment and procedures.

With respect to casks, design induced problems result from a number of causes [Appendix C]:

- lack of a central cask certification authority,
- use of cask integrity standards as the only criteria for cask design,
- lack of incorporation of maintainability engineering criteria,
- lack of attention to human-cask interface design,
- incomplete verification of all design input data,
- lack of requirement for full-scale testing,
- lack of independent multi-disciplinary review.

Many other problems during the transportation of spent fuel and other hazardous materials noted in this report result during non-design phase activities. Specifically, many cases of improper shipping paper, labeling, and placarding requirements, and hardware (e.g., vehicles, casks) maintenance, inspection, and mechanical failures have occurred.

Unfortunately, available data on particular hazardous material transportation incidents or accidents cannot support detailed error or accident investigations. The frequency of such failures in general transportation systems, however, suggests that meticulous attention needs to be focused on inspection and enforcement programs, operator training, and quality control.

4.3. Human Reliability Matrix

The previous discussion of human error definitions, causes, and identification suggests that their total elimination is not possible because of human and system variability and the designers' inability to predict all potential situations. Although attempts should be made to eliminate human-task mismatches where possible, attention must also be focussed on making the effects of human-task mismatches more benign, controllable, and reversible.

The conceptualization of the transportation system as a socio-technical system suggests that human-task and human-machine interactions may be controlled at many different levels. In particular, specific activities [Table 1] can be controlled by different risk management strategies at different phases of the transportation system. Table 5 (see above) suggests possible transportation risk management control strategies, including:

- data collection and reporting,
- employee training,
- work procedure and regulatory framework development,
- quality control and quality assurance, and

- accident analyses.

Our approach to the identification of transportation risk management control strategies is to systematically relate transportation activities to risk management options [Figure 7]. This approach specifically allows error producing conditions for each transportation activity to be related to error reduction and control methods at all socio-technical levels. The vertical axis identifies the various phases of the transportation system (these are the phases identified in Table 1]. The horizontal axis identifies the types of transportation risk management options available; the figure shows major categories from Table 5 and the specific control options discussed in sections 5.1.1 - 5.1.3.

Because organizational failures are clearly an important source of previous risk events in complex socio-technical systems (including the transportation of spent nuclear fuel), a sound method for identifying and characterizing such failures is essential. Our method for doing this uses the notion of the incubation period. When an incident is analyzed and potential mismatches identified, their sources or causes in earlier system phases (e.g., design, manufacture, maintenance, operations) need to be identified. In many cases, the underlying factors will probably not extend very far back in time (e.g., inspection, operation, calibration phases) or will be obvious in hindsight. Where mismatch causes are based on more fundamental design and manufacture features, useful suggestions on system redesign may be possible.

FIGURE 7

HUMAN RELIABILITY MATRIX

TRANSPORTATION RISK MANAGEMENT OPTIONS

TRANSPORTATION PHASES/ACTIVITIES	Job/task Analyses	RA/RM	Data collection and analysis	System hardware	Personnel	Infrastructure	Social factors
Design							
Implementation							
Operation							
Maintenance							
Accident Recovery							

In this process, a "stop-rule" is required to identify how far back in time and activity the incubation period should stretch. One proposal, described earlier [section 3.1], seeks that point in a causal sequence that can be accepted as an explanation and where effective control interventions can be implemented [Rasmussen 1982]. Another approach, based on the conceptualization of human errors as mismatches between perceptions and actuality, is to stretch the analysis back to that point at which the mismatch occurs. Then, if possible, the source of the mismatch can be removed, while other intervention points may be identified which can mitigate its consequences or reverse the process of divergence between perceptions and actuality. This second approach is, in our view, the preferable one because it always leads to the identification of the source of a mismatch, so the analyst becomes aware of its existence even if it cannot be eliminated. Moreover, it may lead to the identification of unexpected couplings and other potential effects not suggested by the first approach.

The following sections describe the application of our approach to both the pre-identification and post-incident analysis of human-task mismatches in spent fuel transportation. Specific scenarios are used in each case to highlight the methodology.

4.3.1. Mismatch Pre-identification

To pre-identify potential human-task mismatches and control strategies, the following three steps should be performed. To highlight our approach, an sample scenario is discussed. We use the pre-identification of errors and control strategies for the reduction of human-task mismatch potential in the loading of a cask with spent fuel. Spent fuel is loaded into

potential in the loading of a cask with spent fuel. Spent fuel is loaded into casks under water in a spent fuel pool. The handling of the fuel and cask (e.g., lifting) is done with cranes and may be done remotely (i.e., operators may use video cameras to monitor operations). After spent fuel assemblies are placed into the cask, the lid is sealed, the cask removed from the pool, and water pumped out of the cask.

The first, step is to perform a comprehensive analysis of all tasks. Job and task analyses can assist in the identification of potential critical errors in each task. Not all human-task mismatches, however, have the potential for affecting performance of human-task systems. Thus, critical errors refer to those errors that have the potential for initiating or contributing to severe accidents or incidents in the transportation system. As described earlier [section 2] attention must be given to the potential for human errors to:

1) initiate risk events;
2) contribute to risk events;
3) affect the frequency of risk event sequences;
4) affect the structure of risk event trees by changing points of reversibility or recoverability; and,
5) affect couplings and interactions between subsystems and components.

When using the various approaches to identify error modes, the number of behavior-affecting factors used will depend on the purpose of the analysis. For reliability and risk analysis, only the external mode of behavior need be identified in order to estimate failure rates. To create designs and programs for training, the cognitive functions and error

mechanisms of humans must be included in the analysis to understand the dynamics of human-task interactions. And to evaluate the work environment, all factors should be assessed in order to understand the complex interactions among tasks, humans, and the environment in the performance of system activities.

The final result of these analyses should be the identification of "task-error taxonomies" for each activity. In other words, the specific set of critical errors that could affect human-task performance should be classified. Frequently, they will fall into a generalized taxonomy [see Appendix A.9 for a review]:

- errors of omission (i.e., not performing action correctly),
- errors of commission (i.e., performing action incorrectly),
- extraneous acts (i.e., performing action that should not have been performed),
- errors of sequence (i.e., performing action out of sequence), and
- errors of timing (i.e., too early, too late, or not within specified time constraints),
- errors of communication (i.e., during sending, receiving, and transmission of messages),

Usually, almost all task related errors will fall into one of these categories. If this is not the case, however, additional categories could be added. The error taxonomies are very important because they assist:

- the identification of clusters of human-task mismatches in transportation activities,
- the analysis of system sensitivity to actual (as opposed to designed) task characteristics and demands, and

- the evaluation of the effectiveness of various transportation risk management control options.

When performing such analyses, the impossibility of identifying all possible problems and error modes in each task must be recognized. In fact, their identification is only limited by the imagination of the analyst. Thus, the composition of the analytical team and the knowledge of the assessors is of critical importance. Accordingly, the investigative team should be inter-disciplinary, including human factors specialists, cognitive psychologists, technical specialists, management personnel, system designers, and experienced workers. The importance of worker participation in the analytical process should not be underestimated as they are the ones who both know how the task is actually performed and the constraints under which they actually operate. Moreover, error modes and conditions that occur in other systems with similar conditions (e.g., heavy truck transportation) may suggest underlying causal factors behind failures in the transportation system for spent fuel.

Second, after critical error forms are identified by a task-error-taxonomy, control strategies for the elimination, reversibility, or mitigation of adverse consequences need to be identified. The human reliability matrix suggests the range of risk management control strategies that may be used for each case, although only a subset will actually be relevant.

Specific control strategies will be suggested by the analyses of the first step. In particular, questions related to the effects of performance-shaping factors and the cognitive and motor requirements of workers will suggest how to eliminate "bad" performance-shaping factors and to reduce individual or group cognitive and physical workloads. Inferences as to the

best control strategies to use should be based on experience and empirical data where available. Where such information is not available, in spite of the predictive problems associated with human information processing models, they may be used (carefully) to identify error mechanisms in relation to cognitive functions. For example, in the scenario under consideration, control strategies could include:

- a deeper cooling pool,
- cask redesign,
- improved human-machine interface (e.g., monitors, controls),
- improve observability and reversibility of actions and effects,
- improved operator training (e.g, use of simulators),
- improved activity procedures (e.g., checklists), and
- improved cask-robotic equipment interface.

Third, before selected control strategies are implemented or redesigned for the activity under analysis, the potential effects of proposed modifications need to be determined for the entire system. In our example, the potential effects of proposed control strategies need to be assiduously assessed for the design process, maintenance and inspection activities, and emergency response procedures. This step is important to ensure the coherence between control strategies at all stages and phases of the transportation system. Examples from our scenario include the effects of greater demands on resources (e.g., simulators, training programs) and trailer redesigns due to cask redesign.

Finally, specific control strategies identified from the previous steps should be implemented. Their final selection should depend on a variety

of factors including perceived effectiveness, costs, resource constraints, and difficulties of implementation.

4.3.2. Post-Incident Analysis

To ensure effective transportation risk management for spent fuel, on-going evaluations of performance are essential. A necessary component in the evaluation process is the analysis of human errors and incidents during all stages of the transportation system. Such investigations will also provide information about control strategy performance during particular activities. Ideally, part of the transportation risk management strategy should be to investigate all incidents, accidents, and errors because important knowledge may be gained from even minor events. Practically, however, such an approach is impossible due to resource and time constraints. Thus, it is important to develop formal criteria for the types of events to investigate. For example, one approach might be to investigate all errors or incidents identified in the task-error taxonomy or which might contribute to the social amplification of risk.

The steps in the process of post-incident evaluation are similar to those of pre-identification; they are described in the following paragraphs. To highlight the methodology, a hypothetical accident scenario is used: a truck shipment of spent fuel in a remote area is involved in a vehicular accident in which the driver is killed. During the accident, a cask valve fails and radiation is released to the environment. Because of inspection inadequacies, the shipment is allowed to leave the utility site with incomplete shipping papers, incorrect placarding, and no pre-notification to the state.

The first step in post-incident evaluation involves an accident or error investigation. Methodologies and issues relating to such investigations were discussed previously in section 5.1.3. Questions that should be asked in the investigation relate to what specific events occurred and how they happened. They directly depend upon the task-error taxonomies developed during pre-identification analyses. In the above example, answers might include driver fatigue, bad brakes, inadequately maintained cask, faulty cask valves, defective quality control, and poor cask design that made inspections difficult.

We propose a detailed and multidimensional classification scheme for the reporting and analysis of future events. By identifying the information that is needed for an in-depth analysis of an event, the information for extensive human reliability analyses will slowly become more available and useful. This step should support risk assessment and risk management integration by providing useful feedback of actual system, procedure, or task performance to the design and assessment process.

The second step is to identify the set of control strategies that directly affect performance during the incident. The human reliability matrix assists in this process by relating risk management control strategies to the activities in the transportation system. Control strategies may either affect the impact of performance-shaping factors, task characteristics, or even cognitive performance. In this case, they might include driver hours-of-service regulations, shipment scheduling, worker training, and pre-departure cask, vehicle, and reporting inspection.

Third, because sources of mismatches may occur during activities other than those where the actual failure occurred, previous activities that

affect the design, implementation, and operation of the task should be evaluated. In particular, relevant control strategies that could block a causal chain leading to the incident should be identified. This process is assisted by an accident investigation analyzing how the failure occurred and the causal sequence of events (the causal "chain" of hazard) leading to the actual failure. The focus at this stage should be on how to eliminate the sources of mismatches and how to make system dynamics more observable and reversible. Effective control strategies in our example might include cask inspection and maintenance procedures, cask design for maintainability, quality control during valve fabrication, scheduling requirements, promulgation of regulatory standards (e.g., cask tests, driver hours-of-service rules), and reporting mechanisms for employees to report management abuses. This process suggests that effective and reliable communication processes among individuals at different socio-technical levels and different phases of the transportation system are key ingredients to effective risk management in the transportation system.

Similarly, activities that might have controlled the effects of the incident should be identified, and control strategies that could improve their effectiveness evaluated. In this way, methods to mitigate consequences to recover effectively from failures can be identified. In our example, these might include escorts for shipments and effective emergency response systems.

Fourth, the most appropriate control strategies for eliminating errors during the activity should be assessed. The potential effectiveness of the control option, as well as related political, economic, and social factors, should be addressed. As the transportation system becomes more

established, for example, modification and implementation of control strategies at outer socio-technical levels (e.g., organizational infrastructure and social factors) will be more difficult.

Consequently, it may be intrinsically difficult to eliminate human-task mismatches at their source. As a result, methods should be identified for improving the effectiveness of potential transportation risk management control strategies and developing new ones for event prevention, exposure reduction, consequence mitigation, and recovery.

6. Major Findings and Recommendations

Humans are a central ingredient in a successful transportation system for spent fuel. Their roles, if anything, will likely increase in importance as the system progressively takes form and becomes operational. As shown by this report the interactions of humans with complex high-risk technological systems, such as spent fuel transportation, may both cause or contribute to risk events, and prevent or mitigate their likelihood or consequences. Here we identify the major findings from our work and state our specific recommendations to the state of Nevada for developing a comprehensive and effective approach to the prevention and mitigation of effects from human-task mismatches. Recommendations relevant to each major finding are listed after a brief summary of the major finding.

Finding 1. The effects of human-task mismatches in the spent fuel transportation system are separated temporally, spatially, and sectorally from their causes. This is a fundamental reality in

designing the transportation system and managing its risks. Human-task mismatches may occur at any phase or activity of the transportation system although their consequences may not be manifested until later times or distant places. Similarly, because the transportation system is not location specific the consequences of human errors may be manifested within different organizational, political, and geographical contexts than those within which the actual errors occur. Constraints created by such divisions pose significant challenges to the implementation and coordination of emergency response capabilities and may greatly affect the social amplification of risk.

Recommendation 1: The state of Nevada should initiate investigations and exercise oversight over reliability and safety during all phases and stages of the transportation system for spent fuel. Events which occur during "upstream" operational activities or during other system phases, including design, implementation, and maintenance, will substantially affect the occurrence of risk events within the state's boundaries.

Recommendation 2: The state of Nevada should adopt a comprehensive approach to assessing the causes and patterns of human error in the transportation system and develop the requisite capabilities to implement the approach. An important aspect of this recommendation is the use of multi-disciplinary teams to perform and evaluate

transportation system designs and oversight. In particular, human factors specialists, experienced workers, and public representatives need to be incorporated into many transportation design and implementation activities.

Finding 2. Human-task mismatches will be a major contributor to transportation risk. Although previous transportation experience with spent fuel has not resulted in major accidents involving radioactive releases, events involving human-task mismatches that have affected the reliability and safety of the system have occurred and will do so again. Previous analyses suggesting that the contribution of human errors to risk is negligible have failed to consider quality assurance programs throughout all phases of the transportation system. Instead, they have focussed primarily on the probability of severe accidents. Human-task mismatches may have a major impact on both actual and perceived risk because they are important contributors not only to severe accidents, but also to the social amplification of risk.

Recommendation 3: The state of Nevada should initiate studies to clarify the relationship between various risk events in the transportation system and the social amplification of risk. Publics in the state of Nevada and elsewhere in the United States are highly concerned over the hazards of nuclear materials transportation. Media coverage and public perceptions have a large potential for amplifying risk

events and eroding confidence in the transportation system. The spent fuel transportation system both shares the network system with members of the public and performs its activities within or sufficiently near population centers so that mishaps are readily observable. Since members of the public measure safety and reliability largely through their perceptions of safety and reliability, system performance must be as safe and failure-free as possible and human error kept to a minimum.

Recommendation 4: The state of Nevada should insist that judgments setting risk acceptability in the transportation system be sensitive to the high levels of public concern and the social inequities in waste transportation. As we stated in the Transportation Needs Assessment, when establishing a risk management system it must be recognized that acceptable levels of risk cannot be derived from an isolated and formal analytical process and that the public often views risks differently than technical experts. To accommodate this divergence, a broad approach to standard setting and widespread public participation and consultation will be necessary to determine which risks are or are not acceptable.

Finding 3. No comprehensive risk analyses have been performed that thoroughly assess the potential human contribution to risks at all phases and stages of the transportation system. The focus of current transportation risk management programs in the spent fuel transportation system is narrowly on the integrity of

technical safeguards (i.e., spent fuel casks). The reliance on technical safeguards, however, gives insufficient attention to the possibility of human errors during the design, manufacture, or use of the technology.

Recommendation 5: The state of Nevada should insist that responsible federal agencies conduct a comprehensive and thorough risk assessment for the national transportation system for spent fuel and should mount a searching independent review of its adequacy. In our work for the Transportation Needs Assessment, we identified the components of a comprehensive transportation risk assessment, including the evaluation of the complete range of initiating events and likely consequences at each stage of the transportation sequence. In addition, the range of contributory causes of risk events and their likely consequences must be assessed. Because they may enable failures or cause unsuspected interactions, specific attention should be focused on the potential impacts of human-task mismatches on the transportation system.

Recommendation 6: The state of Nevada should conduct its own comprehensive and detailed risk assessment of the state-specific portion of the spent fuel transportation system. As in recommendation 5 above, the full range of initiating and contributory risks should be assessed. This risk assessment should be as detailed as possible, including specific routes, repository and inspection sites, and driver

regulations. Similarly, specific attention should be focused on the potential impacts of human-task mismatches on the transportation system. Not only will this provide an important baseline document for the state, but it will enlarge state capabilities for monitoring and also help validate the assessments conducted by federal agencies.

Recommendation 7: The state of Nevada should obtain assurance that the comprehensive risk assessment becomes a "living document", integrating new information that becomes available as the transportation system is implemented. Although successful spent fuel shipment campaigns have been completed, the expected rapid growth in the transportation system after a repository opens may significantly change current assumptions. The magnitude of the system will likely impact cask fabrication, maintenance, and driver training capabilities. Mistakes in the design, implementation, and operation of the spent fuel transportation system are inevitable. Thus, risk assessments and risk management programs need to form a "living", integrated system where system modifications can be assessed and implemented effectively and rapidly.

Finding 4. A large gap between state-of-the-art human reliability assessment methodologies and the assessment of human reliability in the transportation system for spent fuel currently exists. Although current methodologies are limited in their

ability to predict comprehensively types of human error and effective methods for their reduction, they are much more sophisticated than the current approaches that are applied to the transportation system for spent fuel. In spite of the fact that a federal repository will not open for at least ten years, basic design and operational decisions are being made now about fundamental technical, organizational, and regulatory issues. Thus, a state-of the-art approach to human reliability in the transportation system is of major importance.

Recommendation 8: The state of Nevada should require that state-of-the-art methodologies for human reliability assessment be incorporated into the structure of risk assessments and should use such methodologies in its own independent reviews and studies. A comprehensive approach for the identification of critical errors at all phases of the transportation system and methods for error reduction should be implemented. One possible approach (albeit not the only one) to incorporating issues of human reliability into all phases of the transportation system is the "human reliability matrix" developed in this report.

Finding 5. Current monitoring programs and databases for the spent fuel transportation system are inadequate to support well-founded risk assessment or risk management needs. Monitoring systems (e.g., inspections) do not perform effective oversight on all

critical system components (e.g., driver performance). Neither monitoring or other data collection systems treat information of all critical system aspects, including human error, for comprehensive risk assessments and risk management program evaluations.

Recommendation 9: The state of Nevada should recommend that the DOE establish a national real-time shipment monitoring and tracking system and should participate in its design. This issue is discussed in some detail in the Transportation Needs Assessment. Such a system should be capable of providing real-time information about the locations, amounts, and attributes of all shipments and the state of preparedness of key emergency response capabilities.

Recommendation 10: The state of Nevada should recommend that DOE and DOT develop substantially improved and integrated databases needed for the design, evaluation, and monitoring of a safe and reliable spent fuel transportation system. Currently accident and incident databases are fragmented and distributed among federal agencies. To ensure comprehensiveness and accuracy in databases, a centralized data storage and collection system needs to be implemented specifically for the spent fuel transportation system.

Recommendation 11: The state of Nevada should recommend that the DOT and NRC initiate a new institutional mechanism for timely and ongoing

assessments, to include on-site field investigations of accidents and notable human errors. Much useful information about the relationships between actual and expected system performance can be learned from detailed investigations. In particular, the impact of human participation in the transportation system can be more effectively evaluated. Such investigations can also provide detailed and reliable data which can be incorporated into the design and evaluation of effective risk management control strategies (see recommendation 7). While the responsibility for funding and implementing such an accident and error investigation system should be at the national level, it should include active state participation. Moreover, the investigation system should be managed independently from federal regulatory authorities.

Recommendation 12: The state of Nevada should recommend the implementation of an effective unobtrusive, voluntary, anonymous, third-party managed, and nonpunitive human factors data gathering system at the national level. The system should be designed to encourage the reporting of incidents, accidents, and other unreported, but significant events related to human reliability by system personnel. Data developed from such sources have proved to be very useful for identifying and quantifying factors which can degrade safety and reliability in other complex, high-risk technological systems. In a manner similar to recommendation 11, the implementation of such an

accident and error investigation system should be at the national level, include state oversight, and be independent of federal regulatory authorities.

Finding 6. Federal regulatory and transportation risk management programs, as currently configured, are obviously flawed and inadequate. Regulatory authority for the transportation of spent fuel is divided primarily among three federal agencies--the DOT, DOE, and NRC--with additional responsibilities scattered among other federal and state agencies. Such a fragmented approach has led to many administrative problems and regulatory ambiguities. In addition, the management programs specific to particular agencies are deficient in a number of respects. In particular, NRC and DOT inspection capabilities are inadequate to ensure the reliability of spent fuel casks, transport vehicles, and personnel. State roles in the system are limited and inadequate to ensure safety within their borders.

Recommendation 13: The state of Nevada should call forth a searching congressional review of the gaps and fragmentation in the regulatory structure pertaining to the transportation of spent fuel. Although there are severe inadequacies in individual agency risk management programs, some blame for regulatory gaps and ambiguity rests with the enabling legislation and resulting regulatory structure. A more comprehensive and integrated socio-technical systems approach should be used in amending or developing new regulations for

spent fuel transportation. In addition, any new regulations should consider human factors issues in regulatory statutes, technical design standards, and task and procedure design requirements.

Recommendation 14: The state of Nevada should develop an effective and reliable state inspection program for all spent fuel shipments at state borders and subsequent random inspections within the state. Because "upstream" events are critical to safety within the state (see recommendation 1), inspection programs should be instituted at the state border to consider cask integrity, vehicle repair, and driver performance. If shipments should fail inspections, the state of Nevada should have the option of prohibiting the shipment from crossing its borders until all problems are rectified. Similarly, the state of Nevada should initiate random inspections of shipments within its territory to ensure regulatory compliance by drivers and vehicles (e.g., adhering to hours-of-service regulations, following preplanned and accepted routes). The state should develop effective emergency response capabilities to respond rapidly should accidents occur.

Finding 7. The regulatory system for quality assurance of spent fuel transportation is currently narrow and piecemeal. The existing approach toward quality assurance implemented by the NRC has focussed inordinately on casks although many problems have

occurred in other components of the transportation system. The NRC has given little attention to quality assurance at other levels or phases of the transportation socio-technical system.

Recommendation 15: The state of Nevada should insist that the NRC, DOT, and DOE quality assurance programs are substantially upgraded and improved. In particular, inspection programs and capabilities should be substantially upgraded and less reliance placed on the "self-policing" aspects of the system. A particularly major deficiency at this time is the size and frequency of enforcement penalties. To address this we recommend that fines should be increased to create effective incentives for safety and reliability.

Recommendation 16: The state of Nevada should recommend that a comprehensive approach be developed for relating the occurrence of errors and system failures to effective transportation risk management and error reduction strategies. This issue was discussed previously in recommendation 8.

Recommendation 17: Industry should develop effective model training programs and requirements. Personnel at all levels and phases of the transportation system need to be trained effectively to respond to both normal and accident conditions. Moreover, training programs should be on-going and actual personnel performance closely monitored and evaluated. Training programs are particularly important in the

transportation system because of the hazardous nature of spent fuel and because of the many different organizations involved.

6. References

Bainbridge, L. 1984. "Diagnostic skill in process operation". Paper presented at the International Conference on Occupational Ergonomics, Toronto, Canada, 7-9 May 1984.

Battelle Columbus Laboratories 1985. "Assessment of state and local notification requirements for transportation of radioactive and other hazardous materials". Report prepared for the U.S. Department of Transportation, BHARC-300-85-001.

Battelle Pacific Northwest Laboratories 1978. "An Assessment of the risk of transporting spent nuclear fuel by truck". PNL-2588, Richland, VA

Bellamy, L. 1983. "Neglected individual, social, and organizational factors in human reliability assessment". Proceedings of the Fourth National Reliability Conference 6-8 July, 1983, Volume 1, National Centre of Systems Reliability, Birmingham, England.

Bellamy, L. 1988. Personal communication.

Brehmer, B. 1987. "Models of diagnostic judgments", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Bjordal, E. N. 1987. "Risk from a safety executive viewpoint", in W. T. Singleton and J. Hovden, Eds., Risk and Decisions, NY: John Wiley and Sons.

Crecine, J. 1986. "Defense resource allocation: garbage can analysis of C3 procurement", in J. March and R. Weissinger-Baylon, Eds., Ambiguity and Command: Organizational Perspectives on Military Decision Making. MA: Pitman Publishing Inc..

Cook, B. 1988. Personal communication.

Department of Energy 1983. "State statutes and regulation on radioactive materials transportation". Report prepared by Sandia National Laboratory, SAND83-7437.

Department of Energy 1986. "Yucca Mountain Environmental Assessment". DOE/RW-0073, Washington, DC: USGPO.

Department of Transportation 1986. "SAFETYNET: The Motor Carrier Safety Information Network, Program Manager's Guide", Washington, D.C.: Federal Highway Administration.

Embry, D. 1984. "Human reliability", Paper presented at the 1984 Summer School of the Italian Physical Society, Human Reliability Associates, Ltd., Parbold, England.

Embry, D. 1986. "SHERPA: A systematic human error reduction approach". Paper presented at the International Topical Meeting on Advances in Human Factors in Nuclear Poser Systems, Knoxville, TN, 20-23 April, 1986.

Embry, D. and Reason, J. 1986. "The application of cognitive models to the evaluation and prediction of human reliability". Paper presented at the International Topical Meeting on Advances in Human Factors in Nuclear Poser Systems, Knoxville, TN, 20-23 April, 1986.

Fischer 1988. Personal communication.

Fischhoff, B. 1986. "Judgment and decision making", in R. Sternberg and E. Smith, Eds., The Psychology of Human Thought, New York: Wiley, in press.

Gael, S. (Ed.) 1988. The Job Analysis Handbook for Business, Industry, and Government. NY: John Wiley and Sons..

Gray, J. and Quarantelli, E.L. 1984. "Research findings on community and organizational preparation for and response to acute chemical emergencies (DRC Preliminary Paper 91). Newark, Delaware: Disaster Research Center, University of Delaware.

Grella, A. 1985. "NRC inspection activities on recent shipments of spent fuel 1983-present". Office of Inspection and Enforcement, U.S. Nuclear

Regulatory Commission. Unpublished speech at the Spent Nuclear Fuel Transportation Seminar, Chicago, Illinois, 1 August, 1985,

Golding, D., Kasperson, R., Ratick, S., Renn, O., and Tuler, S. 1988. "Risk Assessment and Risk Management of Nuclear Waste Transportation". Unpublished report prepared as part of the Transportation Needs Assessment, Mountain West Research.

Hamilton, L., Hill, D., Rowe, M., and Stern, E. 1986. Toward a Risk Assessment of the Spent Fuel and High-Level Nuclear Waste Disposal System. Report number BNL-51972, Brookhaven National Laboratory, Upton, NY.

Hertz, R. 1987. "Sleeper berth as a risk factor for tractor-trailer driver fatality". Paper presented to the American Association for Automotive Medicine, New Orleans, September 1987.

Hirokawa, R. and Scheerhorn, D. 1986. "Communication in faulty group decision-making", in R. Hirokawa and M. Poole, Eds., Communication and Group Decision-Making, CA: Sage Publications.

Insurance Institute for Highway Safety 1985. "Big Trucks and Highway Safety". Washington, DC: Insurance Institute for Highway Safety.

Jones, I. and Stein, H. 1987. "Effect of driver hours of service on tractor-trailer crash involvement". Washington, DC: Insurance Institute for Highway Safety.

Kantowitz, B. and Sorkin, R. 1983. Human Factors. NY: John Wiley and Sons.

Kasperson, R. and Renn, O. 1987. "Risk assessment of spent fuel transportation. Progress report". Unpublished manuscript. Worcester, MA: CENTED, Clark University.

Kirwan, B. 1988. Personal communication.

Lake, B. 1988. Personal communication.

LaPorte, T. 1988. Personal communication.

Lucas, D. 1987. "Human performance data collection in the nuclear industry". Paper presented at the Conference on Human Reliability in Nuclear Power, London, England, 22-23 October, 1987.

Martin, M., Matthews, M., and Rucker, L. 1986. "Developing a plan for R&D in dangerous goods transport", in Recent Advances in Hazardous Materials Transportation, Washington, D.C.: Transportation Research Board, National Research Council.

McClure, J.D. and Emerson, E. 1980. A review of U.S. accident/incident involving the transportation of radioactive material (RAM), 1970-1980. SAND 80-0899C, TTC-0100. Albuquerque: Sandia National Laboratories.

McClure, J.D. and Tyron-Hopko, A. 1985. Radioactive material transportation accident analysis. SAND 85-1016. Albuquerque: Sandia National Laboratories.

Meister, D. 1971. Human Factors: Theory and Practice. NY: John Wiley and Sons.

Miller, D.P. and Swain A.D. 1987. "Human error and human reliability", in G. Salvendy, Ed., Handbook of Human Factors. NY: John Wiley and Sons.

National Research Council 1985. Human Factors Aspects of Simulation. Committee on Human Factors, National Research Council, Washington, D.C.: National Academy Press.

National Research Council 1988. Human Factors Research and Nuclear Safety. Committee on Human Factors, National Research Council. Washington, D.C.: National Academy Press.

Nebraska Energy Office 1987. "A review of the effects of human error on the risks involved in spent fuel transportation". Lincoln, Nebraska: Nebraska Energy Office.

National Transportation Safety Board 1979. "On-scene coordination among agencies at hazardous material accidents". NTSB-HZM-79-3, Washington, DC: USGPO.

National Transportation Safety Board 1983. "Multiple vehicle collisions and fire, Caldecott Tunnel, Near Oakland, California, April, 7, 1982". NTSB-HAR-83-01, Washington, DC: USGPO.

Noble, D. 1986. Forces of Production. NY: Oxford University Press.

Nordic Liaison Committee for Atomic Energy 1985. "Organization for safety", Report LIT(85)3, Statens Vattenfallsverk, Fack, S-162 82 Vallingby, Norway.

Nuclear Regulatory Commission 1980. Transportation of radionuclides in urban Environs: Draft Environmental Assessment. U. S. Nuclear Regulatory Commission, NUREG/CR-0743.

Nuclear Regulatory Commission 1985a. Nuclear power safety reporting system. U. S. Nuclear Regulatory Commission, NUREG/CR-4132.

Nuclear Regulatory Commission 1985b. Nuclear Power Safety Reporting System. U. S. Nuclear Regulatory Commission, NUREG/CR-4133.

Nuclear Regulatory Commission 1985c. Specification of a Human Reliability Data Bank for Conducting HRA Segments of PRA for Nuclear Power Plants. U. S. Nuclear Regulatory Commission, NUREG/CR-4010.

Nuclear Regulatory Commission 1986. Shipping Container Response to Severe Highway and Railway Accident Conditions. U. S. Nuclear Regulatory Commission, NUREG/CR-4829.

Office of Technology Assessment 1986. The Transportation of Hazardous Materials. OTA-SET-304, Washington, DC: US Government Printing Office.

Page, E. 1988. Personnel communication.

Pedersen, O.M. 1985. "Human risk contributions in process industry: guides for their identification in well-structured activities and for post-incident analysis". Report number RISO-M-2513, Riso National Laboratory, Denmark.

Perrow, C. 1983. "The organizational context of human factors engineering". Administrative Science Quarterly, December 1983.

Perrow, C. 1984. Normal Accidents. NY: Basic Books, Inc.

Poole, M. and Hirokawa, R. 1986. "Communication and group decision-making: a critical assessment", in R. Hirokawa and M. Poole, Eds., Communication and Group Decision-Making, CA: Sage Publications.

Putnam, L. 1986. "Conflict in group decision-making", in R. Hirokawa and M. Poole, Eds., Communication and Group Decision-Making, CA: Sage Publications.

Rasmussen, J. 1980. "What can be learned from human error reports?", in K. Duncan, M. Gruneberg, D. Wallis, Eds., Changes in Working Life, NY: John Wiley and Sons.

Rasmussen, J. 1982. "Human errors. A taxonomy for describing human malfunction in industrial installations", Journal of Occupational Accidents, 4:311-333.

Rasmussen, J. 1987a. "Definition of human error and a taxonomy for technical system design", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Rasmussen, J. 1987b. "Cognitive control and human error mechanisms", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Rasmussen, J. 1987c. "Mental models and the control of actions in complex environments", Report number RISO-M-2656, Riso National Laboratory, Denmark.

Rasmussen, J. 1987d. "Human error mechanisms in complex work environments", Report number RISO-M-2679, Riso National Laboratory, Denmark.

Rasmussen, R.W. 1986. "Duke Power Company spent fuel storage and transportation experience". Nuclear Safety, vol. 27, no. 4., pg. 512-518.

Reason, J. 1987a. "A framework for classifying errors", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Reason, J. 1987b. "Collective planning and its failures", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Resnikoff, M. 1983. The Next Nuclear Gamble. NY: Council on Economic Priorities.

Ruska, M. and Schoonen, D. 1986. "Virginia Power and Department of Energy Spent Fuel Transportation Experience". Report (EGG-2491) prepared for the Department of Energy by EG&G Idaho, Idaho Falls, Idaho.

Salvendy, G. 1987. Handbook of Human Factors. NY: John Wiley and Sons.

Sheridan, T. 1983. "Measuring, modeling, and augmenting reliability in man-machine systems", Automatica,19(6), 637-645.

Simon, H. A. 1955. "A behavioral model of rational choice", Quarterly Journal of Economics, 69, 99-118.

Slovic, P., Fischhoff, B., and Lichtenstein, S. 1977. "Behavioral decision theory", Annual Review of Psychology, 28, 1-39.

Sorensen, J.H. and Vogt, B.M. 1987. "Emergency planning for nuclear accidents: Contentions and issues." Paper prepared for the symposium: Nuclear Radiation and Public Health Practice and Policies in the Post-Chernobyl World. September 18-19, 1987.

Svenson, O. 1979. "Process descriptions of decision making", Organizational Behavior and Human Performance, 23, 86-112.

Svenson, O. 1981. "Are we all less risky and more skillful than our fellow drivers", Acta Psychologia, 47, 143-148.

Svenson, O. 1986. "A psychological perspective on accident evolutions and how to arrest them in nuclear power plants". Paper presented at the

Society for Risk Analysis Annual Meeting, Boston, Massachusetts,. 9-12 November, 1986.

Turner, B. 1978. Man-made Disasters. London: Wykeham Publications, Ltd.

Tversky, A. and Kahneman, D. 1974. "Judgment under uncertainty: heuristics and biases", Science (185):1124-1131.

Waller, P. 1988. Personal communication.

Waller, P.and Li, L. 1979. "Truck Drivers: Licensing and monitoring". Report to the DOT, National Highway Traffic Safety Administration, Bureau of Motor Carrier Safety, December 1979.

Appendix A

Human Errors, Causes, and Taxonomies: A Conceptual Review

TABLE OF CONTENTS

A.1 Introduction

In the context of complex technological systems, such as the transportation of spent nuclear fuel and other high level wastes, ambiguities exist that create difficulties in the definition and identification of "human errors". Definitions of "human error", "human reliability", or "unacceptable performance" of human-machine or human-task systems are very complex and depend on the purpose of an analysis. In particular, purposes of analyses determine whether direct and indirect causes are incorporated into failure analysis and how far back one goes in an accident evolution to assign cause. Definitions also depend on disciplinary perspectives and the extent to which a system includes only individual or organizational and social objectives. The identification of failure and success in human behavior is further complicated because they are closely related and actions cannot be identified as errors until after they are performed.

This paper reviews research on "human error" and assesses the factors that contribute to their occurrence. It has three main parts:

- First, various definitions of "human error" are discussed. Human cognitive models help explain how both human motor control and decision failures occur in technological systems. They also suggest how they are related to successful performance.
- Second, the effects of group, organizational, and social processes on human behavior are discussed. Such factors may influence both the causes and types of errors that can occur in a spent fuel transportation system.

• The third part of the paper reviews taxonomies that treat human error types. The differences in classificatory frameworks are seen to reflect both the desired uses of the taxonomies and their underlying cognitive models.

A.2. Definitions of Human Error

The web of interactions in complex human-task systems makes defining "human error" a difficult task. Attempts at a unifying definition have often lead to ambiguities and improper characterizations. The definition of "human error" is important, however, because of the underlying basis it provides for any approach to human reliability assessment. Several definitions have been attempted, each providing insight into the complexity of the problem, and each becoming more sophisticated in their attempts to include the multiple relationships of human capabilities and task characteristics.

An early definition derives from human reliability engineering, a field that analyzes the performance of the human component of technological systems and human-machine interfaces. A fundamental assumption of this perspective is that the human component of a system can be analyzed in much the same way as its technical components. This early and restrictive approach defines "human error" as the "failure to carry out a specified task or performance of a forbidden action that could lead to disruption or damage" [Dhillon 1986]. This is similar to the definition used for the description of a failure of a technical component with the exception that human intention is also included.

This approach to human reliability analysis bases much of its theory on the assumption that error characteristics and frequencies are transferable among situations. It concentrates, therefore, on modeling the task rather than the total human-task system and the performance of tasks by humans is viewed as the aggregation of proceduralized actions. Thus, error frequencies and types are quantified with respect to features of the task and external human behavior. Consequently, this mechanistic view, exemplary of early human reliability assessment methods, employed little psychological theory [Embry 1984].

Such a restrictive definition may not be sufficient in complex situations because it fails to incorporate the fact that individuals and organizations may have variable intentions and goals. Moreover, it is questionable whether data from one context can be effectively used in the analysis of another human-task work environment. Consequently, such an approach offers little predictive power.

From the perspective of cognitive psychology, a definition has been proposed that directly incorporates the variability of intentions and goals: "human error" or failure refers to an action that is counter-productive relative to the subjective intentions or goals of a person [Reason 1987c]. In human-machine systems analysis, variable goals or intentions are incorporated by the conceptualization of "human error" as the behavior of a person transgressing the multidimensional bounds of acceptable performance [Sheridan 1983]. This approach, which broadens the conceptualization of human error, is important because subjective or externally defined intentions or goals may change as conditions change; for example, the immediate goals of transport personnel will be very

different as the environment moves from one of normal to emergency conditions. Similarly, "acceptable" performance is related to a variety of criteria, including technical and economic efficiency, system reliability, and public safety.

In another definition, developed in systems and reliability engineering, a fault is defined with reference to four criteria [Rasmussen 1982]:

1) it is a cause of deviations from a standard;

2) it appears on the causal path to the effect;

3) it is acceptable as a reasonable explanation; and

4) it is such that a cure is known.

These latter definitions suggest four important factors absent from earlier definitions:

1) multiple externally defined objectives may be relevant to a particular action,

2) the assessment of an error depends on being able to identify it,

3) multiple causes may exist, and

4) the source of analysis influences the identification of an error.

These factors are important because the identification of a specific cause of failure frequently depends on how far back analyses of incident evolution look for root causes; in other words, identification of causes depends on the "stop rule" applied to identify root causes of an incident [Rasmussen 1982, Svenson 1986]. For example, in a hypothetical transportation incident involving spent nuclear fuel, the root cause may be identified as the truck going off the road, the incorrect closure of the cask, or the inadequacy of inspection and quality assurance personnel

performance prior to shipment departure, after cask maintenance, or during cask fabrication. The DOT HMIS database would only identify the incorrect closure of the cask because its stop rule is the "actual primary cause of package failure". The other human errors may be relevant, however, for identifying the most effective intervention strategy.

A.3. Decision and Judgement Failures

Failures in decisions or judgments are covered by the above definitions, but are considerably more difficult to characterize than action errors. Although the definitions may suffice for highly proceduralized tasks (e.g., assembly lines) in which human goals and required actions are externally defined and readily observable, decision making and problem solving behavior are more ambiguous and not necessarily decomposable. In particular, there are several difficulties in attempting to observe and understand the cognitive processes and reasons, or subjective rationale, of individuals making decisions, inferences, or judgments. Some attempts have been made to define verbal protocols and to elicit reasons from decision makers although there is much debate over whether elicited information accurately represents the reasons why people make certain choices [Nisbett and Wilson 1977, Svenson 1979].

Part of the ambiguity arises because individuals may use multiple decision making strategies and they may not be aware of switching among them. In addition, decisions are not necessarily discrete events in time or place, nor are they distinct from other individual and group activities [Poole and Hirokawa 1986]. Still another ambiguity arises because "effectiveness" is not necessarily the only desired outcome. Additional "non-decision" functions include justifying procedures, distributing blame

or success, and fulfilling role expectations. "Effective" choices may actually be of secondary importance relative to other goals.

Empirical observations of human problem-solving and decision making have shown that people do not generally use prescriptive decision analysis techniques. In fact, novices are the only ones who generally use such techniques. Moreover, in complex technological systems, such as that of spent fuel transportation, many decisions are "dynamic." "Dynamic decision" environments refer to problem situations where a series of interdependent decisions are required, task specifications and the environment are dynamic, available information may be dependent on prior decision outcomes, and decisions modify the environment [Slovic et al. 1977, Brehmer 1987]. Unlike "static decision" environments (i.e., decision problems are sequential, do not depend on prior outcomes, and the environment is stable), there is no normative theory of problem solving.

Thus, to simplify a complex world and guide their judgments, humans develop biases and heuristics in their information processing and decision making [Tversky and Kahneman 1974, Svenson 1979, Svenson 1981, Fischhoff 1986, Rasmussen 1987b]. In general these processes work to people's advantage, but in certain situations they can cause the selection of inappropriate choices or actions and lead to predictable biases. As Niels Bohr once said to Einstein, "just because you are using logic, does not mean you are thinking." Many different biases and heuristics have been identified; some important examples are listed in Table A.1.

Because biases and heuristics usually serve the important function of allowing people to operate in complex environments, they cannot be

dismissed as dangerous or useless. However, these biases and heuristics call into question the whole concept of "rational" decision making that is often assumed in planning, judgmental, and inferential situations. These problems have been confronted with the notion of "bounded rationality" that refers to informational and time constraints that force people to make choices based on limited information [Simon 1955]. Similarly, unconscious heuristics learned over time may create problems in novel situations where they suddenly become irrelevant or even detrimental [Svenson 1979]. In many cases, decisions may be "rational" but made in incorrect contexts [Perrow 1984]. The selection of contexts, in which an individual acts, is made prior to a decision episode and depends upon social and organizational constraints and previous experiences. In addition, during laboratory experiments, decision outcomes have been shown to depend on the order in which information is presented to decision makers [Slovic and Lichtenstein 1971].

TABLE A.1

Individual Cognitive Biases and Heuristics

- overconfidence in estimation, inferences, predictions, and hindsight
- underestimation of time constraints
- attempt to verify previously held beliefs by searching for and accepting confirmatory evidence and ignoring or forgetting contradictory evidence
- exaggeration of personal immunity from threats
- oversimplification of others' behavior
- use of limited examples to make statistical inferences
- use of representative samples to make statistical inferences
- difficulty of assessing probabilities and exponential processes
- ignorance of subtleties
- over use of labor saving heuristics
- tendencies toward conservatism
- thinking in causal series, not causal nets, thus ignoring side effects and considering only primary linkages
- previous experiences often used as basis for future choices
- options not readily apparent may not be considered

A.4. Human Cognitive Models

Various attempts have been made to develop models that can describe the complexities of individual cognitive processes. They are used both as descriptors and predictors of human behavior and decision processes. Predictive power is especially important in the design of new tasks in which humans are an integral part: cognitive models should be used where possible to design a task or machine around human capabilities, instead of forcing people to adapt to "unnatural" task demands that can contribute to the occurrence of "human errors".

A behavioristic model of human behavior suggests that errors frequently remain unnoticed because there is no feedback from which to learn [Sheridan 1983]. In many systems the consequences may not be noticeably severe and a trial and error approach suffices. Unfortunately, this method of decision making can be very dangerous when a correct decision is necessary the first time, as in responding to incidents in the transportation of spent fuel. Within this framework, therefore, it is important to provide information to decision makers in a timely fashion and in a form that can be understood. The behavioristic model, however, provides little understanding of how decisions are made.

An additional approach to describing problem solving behavior and human-task interactions is through the concept of "mental models" [Gentner and Stevens 1986, Sheridan et al. 1986, Rasmussen 1987c]. In many technological systems, information about system structure and behavior is indirect and abstract. Information may be limited for two reasons: 1) some data may not be directly measurable or observable, and 2) designs are based on system models that may explicitly or implicitly

assume the range of decisions likely to be made and the range of potential system behavior [Brehmer 1987]. Because of these constraints on direct knowledge of a system, personnel must develop "models" of how the system works. These mental representations, or models, are based on previous experiences and information and derived from various representations of the system (e.g., means-end, part-whole). They are analogs of a real system, support problem solving activities, and offer predictive capabilities in unfamiliar situations.

Although there is no one accepted definition, the concept of "mental model" has been used to refer to the knowledge base used by humans to represent properties of a task and its relationship to the environment. Depending on the mental models brought to bear on a particular problem, different questions and actions may result because of framing effects. Failures are thought to result when inappropriate or incorrect models are used. Moreover, errors may result from interactions of different representations being applied simultaneously to a particular task and incompatible representations applied by people with different levels of training and specializations.

From the above discussion of human cognitive processing, decision making behavior, and cognitive models, it is clear that analyses of human-task systems cannot be based solely on task characteristics. The occurrence of failure is closely associated with human variability resulting from stochastic behavioral properties, learning, and adaptability. It is now believed that most types of successful and unsuccessful human performance can be explained by a common, limited set of underlying cognitive mechanisms and their interaction with task characteristics and

situational factors [Rasmussen 1987b, Reason 1987a]. This section reviews two models that attempt to describe human cognition and behavior and have been used to describe human errors [see below, sections A.9.2., A.9.3].

A.4.1. The attentional-schematic model

This model is based on theoretical research in cognitive psychology. This approach assumes that all internal and external human actions are controlled by the interaction of two modes of control--attentional and schematic [Reason 1987a, Reason 1987c]. The information processing capabilities of the attentional mode of control are powerful and feedback-driven. It is required for performance in novel situations, but is slow, sequential, limited, and difficult to sustain. The schematic mode of control can rapidly process large amounts of familiar information in parallel. This particular model relates three components of cognition and their complex interactions:

- working (attentional) database includes information used for a particular planning process. This database has limited capacity, its content is highly variable, and it is difficult to apply for long periods of time.
- mental operations (e.g., selection, judgment, and decision making) that control the working database.
- schemata are the memory structures that form the long term knowledgebase. Schemata contribute selected and uncalled for information to the working database. The schemata available to the working database appear as a result of association with plan elements, environmental triggers, or affective factors.

This cognitive model allows an expanded understanding of the relationships between limited rationality described by Simon [1955] and planning failures [Reason 1987a]:

- Bounded rationality refers to the attention that can be brought to bear on a problem--it is limited and consequently the information used to plan will be limited. The result may be the oversimplification of a problem and is similar to Simon's [1955] use of the term.
- Imperfect rationality refers to limitations of the schematic knowledge base (i.e., the collection of theories possessed by humans to deal with the world through different cognitive domains). "Mistakes" may arise from imperfect rationality by the application of often used but inappropriate judgmental and inferential heuristics. Errors in low level control, referred to as "slips", occur in a similar fashion in human actions [Reason and Mycielska 1982]. They result from the inappropriate application of low level control processes in similar but different situations. The result is that actions and planning can be too rigid and conservative.
- Reluctant rationality results from the interaction of the attentional and schematic modes of control. In the past, mistakes in this category have been blamed on "cognitive strain". This limitation in rationality can lead to the excessive use of cues and previous experiences.

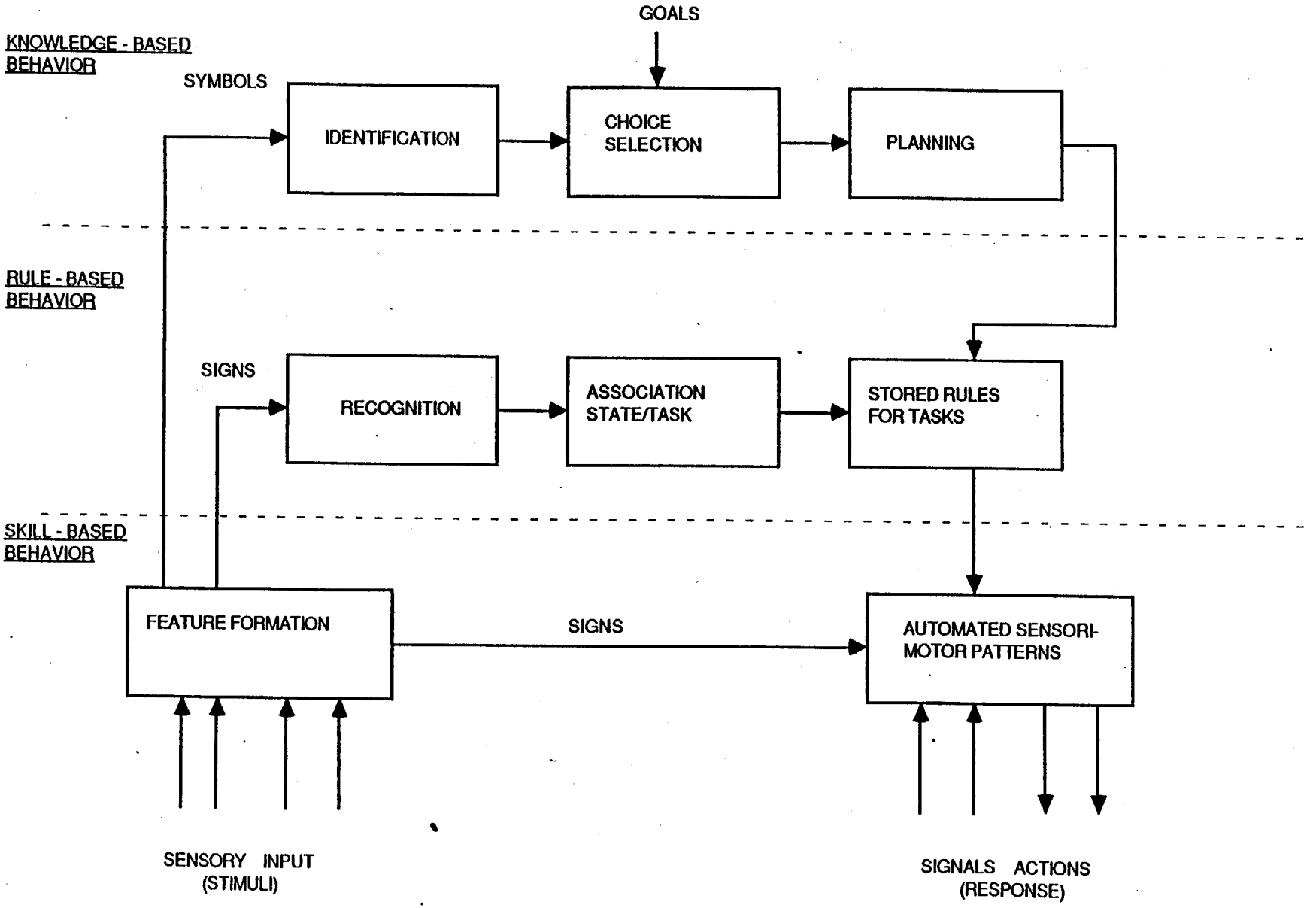
A.4.2. The skill-, rule-, and knowledge-based model

This model was developed to describe operator behavior in process plants and industrial accidents [Rasmussen 1982, Rasmussen 1987b]. It is based on the relationships of human cognitive control and decision making behavior and actions to internal psychological processes. Three modes of control were identified that are related to the norms used for error judgment and attribution: skill, rule, and knowledge based domains of behavior [Figure A.1]:

- skill-based behavior includes automated or routine activities. Performance is controlled by stored patterns of behavior and errors are related to variability in time or space coordination and of force.
- rule-based behavior includes behavior in familiar situations with specified stored rules of action. Rule-based behavior is goal oriented rather than goal controlled. The identification of errors depends on whether correct rules were recalled and used. Errors are related to incorrect classification or recognition, forgetting procedures, and erroneous association of tasks.
- knowledge-based behavior includes behavior related to the performance of new and unfamiliar tasks. At this level, decisions are made and planned on the basis of functional and physical system properties as well as goals. The information processing characteristics are very person- and situation-dependent. Errors must be defined relative to subjective goals.

FIGURE A.1

SKILL-, RULE-, KNOWLEDGE-BASED COGNITIVE MODEL



SOURCE: RASMUSSEN 1982

According to this model, minor deviations from standard procedures and known rules support, intentionally or subconsciously, learning processes and the refinement of skills [Rasmussen 1987c]. The development of skill-based behavior, for example, requires the continuous updating of sensory-motor schemata to time-space features of a task environment. For rule-based behavior, by contrast, the development of heuristics depends on the application of potential short cuts and the identification of signs to aid in the recognition of conditions without analytical diagnostics. At the knowledge-based level, the testing of hypotheses is important in problem-solving tasks.

The development of skills through the replacement of knowledge-based behavior by rule-based, and then skill-based behavior, creates the conditions whereby errors may occur. Automated responses and behavioral patterns develop while tasks are controlled and supervised by higher levels. As lower levels of automatic control develop, errors may result from the interference of deteriorated higher level controls and undeveloped lower level control [Rasmussen 1987c, Rasmussen 1987d].

Although this conceptualization has proven useful to some researchers, others believe it is inadequate to account for the nature of cognitive behavior and support design decisions by specialists [Bainbridge 1984]. In particular, Bainbridge questions the validity of the assumption that to test hypotheses individuals either proceed automatically (skill-based behavior) or by thinking causally (knowledge-based behavior). While she believes the model may be useful for providing basic information about cognitive processing to non-specialists, she makes two specific criticisms of the model.

First, there may be more than three distinct types of processing levels in human cognition. Instead of using a taxonomy of cognitive processing based on cognitive mechanisms, it may be more appropriate to classify cognitive functions (e.g., attention, memory, selection, recall, compare, explain). Cognitive functions may be more appropriate for design considerations because they suggest specific capabilities and limitations in memory functions, while the identification of skill-, rule-, or knowledge-based behavior does not necessarily provide the same information.

Second, in Rasmussen's cognitive model all information processing routes are from stimuli to response. This may be misleading, however, as the complexity and flexibility of human cognition is not necessarily accounted for [Bainbridge 1984]. For example, human cognition includes feedback, recursion, mental stimulation and anticipation, working memory and multiple goals.

A.5. Group Decision Making

Thus far the discussion has focused on interactions or failures involving a single person. However, in many technological systems groups of people must interact to perform a task and failures can result from their interactions. These may have especially important implications in planning and decision making situations. For example, in the spent nuclear fuel transportation system, groups may plan routes, two drivers may operate a truck, and a number of individuals may be involved in deciding how to respond to an incident or accident. Consequently, faulty group decision making needs to be incorporated into our definition of human error.

Group decision making and problem solving is often characterized as the aggregation of individual behavior and interactive processes [Davis and Hinsz 1982]. Consequently, group behavior can be viewed as a social process centered around a problem and involving the collective perception of a choice making situation.

Although some group processes resemble those of individuals, this is not totally correct. Human error characteristics and frequencies differ for individuals and groups. Formal and informal modes of communication within a group and with others outside of it create additional problems relating to attention, activity, values, conflict resolution, and information flows. On the other hand, they help to reduce some problems, such as workload.

Faulty group decision making can often be traced directly or indirectly to communicative and social influences of individuals. They can enable faulty decisions by facilitating the occurrence of errors such as misinterpretations and incorrect conclusions during different stages of the decision making process. Five factors that have been suggested as leading to faulty decisions are [Hirokawa and Scheerhorn 1986]:

- improper assessment of situation,
- establishment of inappropriate goals and procedures,
- improper assessment of attributes of alternatives,
- establishment of faulty information base, and
- faulty reasoning.

The model on which these concepts are based suggests that individuals can prevent decision errors by counteracting the negative influences otherwise leading to faulty decisions (e.g., convince others to

reject flawed beliefs, perceptions, and inferences) and by influencing a group to accept correct conclusions before negative influences occur.

Just as biases affect the information processing of individuals, there also exist biases that may affect group behavior and lead to faulty decisions. They result from the dynamics of interindividual interactions and include:

- the "risky shift" phenomena in which a group chooses more risky alternatives than its individual members;
- group polarization, whereby the choice of a group is more extreme than the individual choices;
- groupthink, where a group arrives at a consensus decision without adequately evaluating all alternatives;
- false consensus, where individuals of a group falsely believe that a consensus has been reached; and,
- pluralistic ignorance, where group members believe they are alone in their beliefs.

The strength of the effects from these biases depend on the characteristics of a group and the environment in which they interact. The important group characteristics affecting behavior may be divided into four categories [Swap 1984]:

1) composition (e.g., size, personalities),
2) leadership (e.g., emergence, centrality, style),
3) task (e.g., structure, timing, interdependencies), and
4) decision rules and processes (e.g., reversibility, criteria, social context).

In the transportation system the form of consensus generated by groupthink is of particular concern because it may also contribute to more risky decisions (e.g., "risky shift") and may lead to especially severe consequences in hazardous situations such as may result from spent nuclear fuel transportation accidents. The major factors contributing to such behavior are the uniformity of members, the size and isolation of a group, norms, cohesiveness, and personalities [Reason, 1987b]. In groups experiencing groupthink, "the powerful forces of perceived 'togetherness' act in concert to render the possibility of failure unthinkable--and if not unthinkable, then certainly unspeakable" [Reason 1987b: 124]. This behavior, characteristic of '"mindsets", is frequently seen in risk research and hazard and accident response planning by the belief that catastrophic accidents are not credible events and that response organizations are well prepared [Gray and Quarantelli 1984].

An additional important consequence of interindividual interaction is conflict in a decision process [Putnam 1986]. Conflicts may arise in regard to substantive issues in a group task, procedural methods, and affective issues between members. Although often viewed as a negative factor in group decision making, if managed properly, conflict can actually be a positive function by promoting effective decision making and avoiding premature consensus. For example, conflict may expand the range of alternatives considered, increase the scrutiny of considerations and assumptions, or enhance group cohesiveness. However, if not managed effectively, conflict can result in dysfunctional behavior and weak performance. For example, decision makers frequently explain time delays in communication in hierarchical organizations by attitudes or

incompetence instead of their actual functional causes [Rasmussen 1987c]. The result may be affective conflict and the reluctance to delegate authority and control over tasks.

Putnam [1986] has identified three types of conflict:

- Substantive conflict is the result of disagreements or differences of opinion concerning the ideas or content of a group task. When members in a group experience substantive conflict they may revert to using old work habits that may not be appropriate to the situation. This behavior is avoidable if members are responsive to suggestions and ideas of others.
- Affective conflict results from personality differences, self-oriented needs, personalization of differences of opinion, and emotional aspects of interaction. Affective conflict may increase anxiety and decrease openness to alternative perspectives. The detrimental effects of affective conflict may be reduced by the realization that conflicts are a result of differences in positions, not the sentiments of a person.
- Procedural conflict emerges from differences concerning a group's procedural rules. These may include disagreements over decision rules, the running of meetings, and work and task routines. Procedures provide a means of withdrawing from conflict and may be used in constructive ways to manage substantive and affective conflicts--they may help to reduce uncertainty and equalize member power differences. On the other hand, "the use of powerful people to prevent conflict from surfacing stifles the free

expression of ideas, a fundamental condition for effective decision making" (Putnam, 1986, 185).

A.6. Organizational and Social Factors

The field of human factors has rarely focused on errors connected to social or organizational characteristics in high-risk technological systems although these aspects of socio-technical systems have been identified as contributory causes to many accidents [Turner 1978, Bellamy 1983, Perrow 1984]. Moreover, organizational design is frequently ignored in safety analyses in contrast to the areas of construction and personnel [Nordic Liaison Committee for Atomic Energy 1985, Bjordal 1987].

The dynamics of interindividual interaction are partly a result of the understanding of system behavior by personnel that arise through the framing effects of affective, cultural, and social forces by which people understand, interpret, and infer things about the world around them. In addition, dynamics depend partly on the work environment (e.g., management-employee relations, job requirements) and organizational structure (e.g., hierarchy, communication system). Thus, organizational and social factors affect the conceptualization of human errors in two primary ways:

1) group and individual perceptions and actions can be influenced by organizational, social, and cultural factors. These may lead to "operational errors" where incorrect actions were performed or correct actions not performed because of "framing effects" or other constraints on behavior.

2) Organizational and social factors may diminish effective decision making capacity of individuals and groups within an organization. This effect may lead to making decision and planning failures ("policy errors") within organizations. The hazards of spent fuel transportation, however, demand "failure-free" management and planning.

The reliability of organizational behavior is measured with respect to the efficiency and effectiveness of prevention, detection, and recovery of threats on system safety. Organizational and policy errors can result from both the dynamics of interindividual interaction and organizational structure. These factors not only affect the reliability and effectiveness of actions and decisions, but also provide the context in which "rational" reasons that in hindsight are determined to be faulty. Table A.2 lists potential organizational and social factors contributing to failures.

Organizations often experience conflict and ambiguous preferences; ignore information they possess, request more information, and then ignore it; and, buffer processes of thought from processes of action [March 1981]. Adaptation and learning process are frequently slow and incremental. Group as well as individual misperceptions and bad choice selections may result from pressures in high stress environments, interindividual conflicts, rigid organizational beliefs and practices, restrictions of the social and cultural environment, political and economic interests, institutional constraints, and communication problems [Turner 1978]. Unreliable behavior may be exacerbated during industrial disputes (i.e., strikes, slowdowns) and if the system is considered unreliable or untrustworthy by personnel.

Frequently, issues of influence and power play important roles in decision making behavior in organizations. For example, the role of managers is crucial to safe and reliable system operation because they can affect safety both directly and indirectly. They are responsible for creating and maintaining an organizational culture that reinforces safety and reliability considerations (i.e., "culture of safety"), implementing effective decision making protocols, and shaping the impact of regulations and social constraints on operational activities [National Research Council 1988]. In the spent fuel transportation system, management must be adept at working within a complex system of federal and state regulations that can affect system flexibility in operations. Similarly, if the public is very skeptical of the DOE's ability to operate the transportation system or repository, the operations must be as safe and failure-free as possible and the response to incidents must be immediate and effective--the only way members of the public can measure safety and reliability is through their perceptions of safety and reliability [LaPorte 1988].

On the other hand, the actual behavior of managers can exacerbate problems inherent in organizational behavior. In particular, managers often spend considerable time in activities that have few consequences beyond acknowledging the importance of others and themselves, perform with self-serving biases, have little interest in the implementation phase relative to the policy making phase, and attempt to show the legitimacy of outcomes and processes [Crecine 1986]. In public organizations, management frequently attempts to shape employee behavior and operations to externally-, constraint-oriented managerial strategies or they ignore task performance in organizational design [Cook 1988].

Organizational structure is often created and maintained to ensure an organizational culture that promotes economy and ease of management and ensures organizational survival. Similarly, technological designs and choices are frequently a result of attempts to reinforce or reproduce existing structures [Perrow 1983, Noble 1986, Cook 1988].

Many of the social and organizational factors that lead to system failures can be understood by the behavior that organizations generate in groups and individuals. In prior research, organizational decision making has been viewed as coordinated sets of linked individual and group decision processes; decision making behavior is viewed as a social process. Much research also assumes that organizational decision making is rational in that [March 1981]:

- alternatives are known unambiguously,
- consequences of alternatives are known at least up to a probability distribution,
- a consistent preference ordering of consequences exists, and
- a decision rule is available.

However, just as individuals are described as having "bounded rationality" so are organizations [Simon 1957, March 1981]. In the organizational context, bounded rationality is a function of informational and computational constraints in institutional decision making.

TABLE A.2

Social and organizational factors contributing to system failures

- Pressure
  - group, social, authority, heavy responsibility
- Job requirements
  - ill-defined job requirements
  - multiple personnel use same equipment
  - multiple tasks--work overload leads to selective attention by decision-makers and workers
  - lack of resources--inadequate access or distribution
- Conflict
  - substantive
  - procedural
  - affective
- Assumptions related to tasks or roles conflict
  - management vs. designer
  - management vs. operating personnel
- Rigid organizational beliefs and assumptions
- Rules and procedures not maintained
- Communication system
  - assumed reliable when it is not
  - delayed
  - noisy
  - informal
  - blocked
  - hierarchical--information distorted, not passed, or reinterpreted
  - reporting of messages not completed or incorrect
- Organizational authority
  - overlapping responsibilities
  - hierarchical structure
  - slow learning and adaptation to new or changing environment
  - inconsistent and conflicting objectives
- Quality of work environment
- Framing effects
- Industrial actions
  - strikes
  - slowdowns
- System considered unreliable or untrustworthy by personnel

Consequently, the variability and richness of information internalized by an organization is frequently reduced and simplified. Social perspectives of organizational decision making suggest that social and cultural values are important factors in behavior and error generation. Decision making as a social process also implies that personnel in organizations need to have shared understandings of information, objectives, and procedures in order to coordinate effectively [Turner 1978, March 1981, Crecine 1986]. In addition, it is often assumed that they develop shared values, assumptions, and expectations and operate with similar notions of rationality. Organizations form intentional systems and members are frequently subject to framing effects in the ways that they perceive events internal and external to the organization. Individual mental models are created and modified by "group" and "organizational" mental models [Tuler 1987].

Consequently, organizational characteristics result in important dynamics and constraints that differ from those in individual decision making; in organizations [Crecine 1986]:

- information is more important in choice processes and is more formalized and less varied;
- alternatives are discarded from the possible choice set at an earlier stage in the decision process;
- decisions are less likely to be given up once chosen;
- simpler coordination structures are used and hierarchical structures are prevalent because they reduce coordination and communication costs;

- pre-existing routines and processes are more dominant and inappropriate routines are less likely to be given up;
- decisions and problem solving take longer;
- a greater tendency exists to deal with partial definitions of problems, especially those that can be dealt with by subunits;
- multiple justifications for decisions are typical;
- simpler strategies are employed for dealing with uncertainty; and,
- in the short run, actions are constrained by activities previously encountered, previously rehearsed by subunits, or for which standard operating procedures can be easily modified.

In spite of framing effects, subunit goals, perceptions, and values of large and complex organizations may be very differentiated. In fact, organizations tend not to be coherent wholes, but resemble collections of subunits and specialists with their own objectives and choice making technologies that often conflict. Subgroups may develop informally and provide information bases other than those derived from formal authority structures. These subgroups may contribute to the occurrence of failures or adverse consequences because of barriers to information gathering and sharing from social habit and established routine patterns of interaction. On the other hand, individual and subgroup diversity is an important mechanism for coping with the complexities of the real world.

One of the reasons organizations develop centralized control and authority structures and develop rigid procedures and rules is to ensure that individual behavior is true to organizational "desires". In particular,

lack of central control has been observed to lead to confusion, delays, competition for power, and a management void [Sorensen and Vogt 1987].

The central control provided by authority and decision hierarchies are assumed to ensure continuity of knowledge and processes, to direct actions, to create shared perceptions, assumptions, and methods, and to allow the smooth functioning of the organization. Such organizational constraints, however, may also contribute to the occurrence of failures. Organizations may create or amplify unintended sequences in surprisingly ordered ways by virtue of these common understandings and normal administrative processes [Turner 1978].

In hierarchical organizations most downward flow of information is in the form of orders, instructions, and information. The information that flows upward is generally in the form of requests for assistance and resources, descriptions of system state, and suggestions for action. Information that flows up through an organizational structure is likely to be distorted, delayed, or lost so that decision makers at the top levels are distanced and not in control of information concerning system states. In addition, role status differences can create flow barriers and differentiation may be exacerbated by time stress [Bellamy, 1985]. Consequently, formal hierarchies exacerbate already existing tensions between an organizations responsiveness and adaptability to new situations and knowledge and the accountability for actions and decisions within an organization.

Another method of dealing with the tensions of subgroup behavior and organizational "desires" is the implementation of standard operating procedures [SOP] developed and implemented to match personnel with

both work requirements and the environment and reduce the variability and "richness" of information internally. The behavior that such proceduralization promotes has been referred to as "functional rationality", in which a sequence of actions is designed that leads to a selected objective [Turner 1978]. SOP's, however, do not usually provide adequate guidelines for actions necessary for safe and reliable performance in all situations. Gaps in such procedures are filled by organizational culture and motivational incentives. The absence of SOP's in many situations suggest the need for knowledgeable decision making and flexibility derived from insights not only at the managerial and policy levels of an organization.

In particular, flexibility derived from insights into the interrelationships between events, or "substantial rationality", is of critical importance. In fact, to improve safety and reliability and make effective decisions when needed, employees should be encouraged to question (and therefore accept) the logic behind technical, managerial, operational, and policy aspects of system operation and control [Turner 1978, Nordic Liaison Committee for Atomic Energy 1985, National Research Council 1988]. Unfortunately, most individuals and subgroups in complex technological systems are not trained, encouraged, or necessarily capable of utilizing substantial rationality in decision situations.

This view corresponds to that of Rasmussen discussed above. He suggests that to improve skills and knowledge people constantly deviate from rules and procedures to identify short-cuts, develop heuristics, and test hypotheses. "Substantial rationality" is just one factor needed to assist this behavior and increase the likelihood that intentional and subconscious "experiments" do not lead to failures. This is an especially important

feature in complex or hazardous technological systems, such as spent fuel transportation, where potential consequences of failure are great. An example where substantial rationality is needed in the spent fuel transportation system is the routing of shipments: procedures are developed for this process and personnel are not supposed to deviate from them. However, because of their experiences or substantial rationality they may identify procedural modifications for task improvement (e.g., in safety or efficiency). An additional example of the need for substantial rationality is for the identification, diagnosis, and response to emergency or novel situations.

A.7. A Model of Organizational Failures

Most disasters within organizational settings do not occur as the result of single actions by single individuals, but rather from complex interactions of contributory behavior of a number of individuals or groups shaped by the institutions and organizations within which they operate. One approach to modeling the dynamics of failures in organizational environments, which recognizes the special characteristics of organizational decision making, is based on a "sociological definition of disaster as a challenge to existing cultural assumptions" [Turner 1978: 84]. It is a time phase approach to organizational awareness of divergences between its perception of the world and the actual dynamics and state of the world. The six stages from the initiation of divergence to reconvergence are:

> Stage 1) accepted, "normal", starting points of initial cultural beliefs about the world and hazards, and associated precautionary norms delineated in laws, regulations, mores, and social constraints.

Stage 2) "incubation period" of an accumulated, unnoticed set of events that are at odds with the accepted beliefs about hazards and the norms for their avoidance.

Stage 3) precipitating event that forces itself to attention and transforms general perceptions of stage 2.

Stage 4) onset of the immediate consequences where the collapse of cultural precautions become apparent.

Stage 5) rescue and salvage: the first stage adjustment in which the immediate post-collapse situation is recognized in ad hoc changes that permit the work of rescue and salvage to begin.

Stage 6) full cultural readjustment of beliefs and precautionary norms to fit the newly gained understanding of the world.

In this view, it is the events during the incubation period that enable failures at a later time by setting the stage whereby a single event can precipitate a major disaster. These events may not be observed because of erroneous assumptions, poor and delayed communication, cultural lag in existing precautions, as well as other individual, group, and organizational factors described above. In particular, when norms of correct and incorrect behavior are related to the performance of standardized procedures, negative interactions or errors may not be readily observable when the "correct" procedures are followed. Moreover, the knowledge and understanding of events may be limited by the distribution of power, control of resources, and social constraints. Thus, even though the information exists, knowledge may be limited with respect to the consequences of potential choice alternatives and the events that occur as a result of choices.

These ideas correspond to the notions of observability and reversibility described earlier. Observability of events and failures are limited by the nature of group and organizational behavior, barriers in the flow of information, and the distribution and control of authority. In addition, design strategies of multiple defenses create situations where many errors may appear in the system but remain unnoticed. Their identification may only occur when independent events cause a failure or change in system behavior [Perrow 1984, Rasmussen 1987d]. The reversibility of failures (single or accumulated) are further limited by these constraints, by normal group and administrative processes that can actually amplify their consequences, and the characteristics of dynamic decision environments in which environmental constraints are affected by decision processes and prior decision outcomes.

The process of reversibility is heavily influenced by organizational adaptability and learning. In organizations, the role of information, and hence communication processes, is crucial. In particular, the availability, form, and timing of information in the possession of decision makers frequently affects their ability to use information about potential failures and in emergencies. Thus, a complicated tension results between the need for flexibility and adaptation and the need for control and an organizational culture to constrain employee behavior.

Prior organizational research suggests that new alternatives are sought in the neighborhood of those previously known or attempted. Hence processes of adaptation to environmental (i.e., social and regulatory) change is slower than routine adaptation to changing conditions within the context of current rules (e.g., new operating procedures and technologies)

[March 1981]. In fact, "most organizational adaptation consists in monitoring the environment and the organization for familiar messages about the state of the world, and doing what is appropriate (according to the rules) given the situation" [March 1981: 222].

As in the case of individuals, the removal of all sources of errors is neither desirable or possible. The relationships between institutions and the external world constitute a continuous cycle through the development and modification of assumptions and the identification of their limits [Turner 1978]. Large scale technological failures can be the result of "organizational experiments" in unkind environments. Such "experiments" may result from a need to perform in competitive environments or the need to increase the efficiency of production and performance [Rasmussen 1987d]. Rasmussen has also recently suggested that an "analogy can be drawn between the adaptive mechanisms involved in the skill attainment of the individual...and the role of management decisions...in the adaptation to the requirements of functional effectiveness" [Rasmussen 1987d: 15].

A.8. The Identification of Human Error

Frequently, human errors are only identified as such because they occur in work environments that do not allow for recovery from inappropriate or variable human actions. On the other hand, errors that are identified and rectified before they result in unacceptable system behavior are not usually identified as "human errors". Thus, the characteristics of human behavior in technological systems and methods of error attribution can result in severe biases in the identification of causal factors as "human errors".

The identification of an error often occurs after the fact and with the use of hindsight. Those analyzing an action are typically not the ones who performed it and analysts and operators may not have access to specific intentions or goals. Because the source of actions and goals are partly subjective criteria, the identification of an error frequently becomes contradictory and closely associated with assignment of blame and responsibility. In addition, the assignment of blame and responsibility is often related to the power structures within institutions so that identified "causes" may actually have little to do with the deeper reasons behind failures.

Consequently, it is critical that reference norms of behavior be understood by both those conducting the analysis and those performing the activity. Norms for human actions in technological systems may be defined in two ways, depending on the familiarity of the system [Rasmussen 1982]. When the results of human actions are readily apparent, the definition of error is related to the outcome of an activity relative to a norm. On the other hand, when the effects of human actions are not readily or immediately apparent, error is related to the performance of standardized procedures, which provide the only reference for judging actions.

A.9. Human Error Taxonomies

Many different taxonomies of human error have been proposed and used. Their differences are a result of the questions being asked of them and their underlying models of human behavior. In particular, there are different ways of looking at failures depending on the ultimate objective:

behavioral, contextual, and conceptual [Reason 1987c]. These taxonomies refer to what happened, how it happened, and why it happened, respectively. For the assessment of human reliability causes and effects in the transportation system for spent fuel it is important to understand what errors occurred and how they came about.

The state-of-the-art in human error research is such that inadequacies exist in all cognitive models and taxonomies of human error. In particular, they are not adequate to support analysts in the comprehensive pre-identification of all important error types and evaluation of behavior at all cognitive processing levels. One important difficulty that analysts have is in the use of models and taxonomies for predictive, rather than descriptive, purposes. On the other hand, they are very useful in that they suggest the types of questions analysts should ask, error modes for analysis, and psychological mechanisms that cause errors [Bellamy 1988, Kirwan 1988]. Thus, the identification and evaluation of human errors is as much art as science--although a very useful and much neglected art.

The following sections review some example taxonomies. It should be noted that they are primarily concerned with the behavior of individuals and not with group or organizational tasks.

A.9.1. Taxonomies of What

Many classifications of failures at the behavioral level have been developed that refer to the external characteristics of the failure: what happened? They are based on the mechanistic assumptions of human reliability engineering and do not specifically incorporate the notion of

"mismatch", although their associated analytical models may incorporate environmental factors. One widely used taxonomy has its origins in human reliability assessment of nuclear power plant operations [Nuclear Regulatory Commission 1980]. Its five categories are:

- errors of omission (i.e., not performing action correctly),
- errors of commission (i.e., performing action incorrectly),
- extraneous acts (i.e., performing action that should not have been performed),
- errors of sequence (i.e., performing action out of sequence), and
- errors of timing (e.g., too early, too late, or not within specified time constraints).

In systems where individuals must interact and plan, an additional important category is errors of communication. Such errors include failures by individuals and groups in the sending of messages, receiving of messages, and the transmission of messages.

When analyzing specific systems, external characteristics of failures may also be defined in the context of system requirements and activities. Examples in the transportation of spent nuclear fuel may include:

- casks improperly sealed,
- driver accident,
- improper labeling,
- vehicular accident, and
- improper notification.

The requirements of reporting failures in technological systems can promote such classification schemes. For example, the ease of defining human errors and of developing reporting formats for such classificatory

schemes can be key ingredients. Unfortunately, by themselves they provide little information about the underlying causes of failures and thus little predictive power for the pre-identification of error sources.

Theoretical and empirical research suggests that many similar behavioral effects are caused by very different underlying cognitive mechanisms, whereas many different behavioral effects are caused by the same underlying causal factors. "Human errors" frequently occur because of desired qualities of human variability, learning, and adaptability in a technical system. For example, failures may occur as a result of too much human variability during normal system operations, too little human adaptability during abnormal or unfamiliar operations, or general constraints of human cognitive and motor capabilities. "To explain man-system mismatch we must therefore look at the control of human behavior, to find mechanisms behind variability during normal, familiar situations and mechanisms limiting adaptability in unfamiliar situations when the system changes" [Rasmussen 1987a: 25]. Accomplishing this goal requires the modeling of human behavior during normal and familiar situations. The following taxonomies exemplify different attempts to incorporate these needs and ideas by using cognitive models of human information processing.

A.9.2. A Taxonomy of How and Why

One classification scheme is based on the attentional-schematic model of human cognition [section A.4.1]. This model and the resulting taxonomy rests on the belief that "predictable error and correct performance are two sides of the same coin, and hence demand common

explanatory principles" [Reason 1987c: 14]. This model of human behavior is based on the interactions of the working (attentional) database, mental operations, and schemata.

The interactions of these components may result in two basic types of errors--1) slips (action failures) and 2) mistakes (planning failures). The interaction of incorrect or unwanted schemata and limited attention may result in failures of action from absent-mindedness [Reason and Mycielska 1982]. The interaction of heuristics, information processing limitation, and schemata characteristics contribute to the formation of detrimental biases that can result in planning failures [Reason 1987a].

The taxonomy based on this cognitive model is represented by a matrix whose axes are "basic error tendencies" and "cognitive domains" and whose elements are "primary error groupings" [Figure A.2]. Basic error tendencies are assumed to be the underlying mechanisms of most systematic varieties of human error. Although each mechanism is required for normal psychological functioning, they are capable of inducing certain types of errors. The mechanisms are: ecological constraints, change enhancing biases, resource limitations, schema properties, strategies and heuristics. The cognitive domains form the second matrix axis and represent different stages of human cognition: sensory registration, input selection, temporary memory (including prospective memory), long-term memory, recognition processes, judgmental processes, inferential processes, and action control.

The interactions that produce primary error groupings are classified as Primary and Secondary Nodes. Primary nodels represent points in the information processing sequence where basic error tendencies are known

to exert a strong influence. On the other hand, secondary nodes are points of less certain interaction or where basic error tendencies exert an influence that depends on a primary effect at an earlier stage of information processing. Eight primary error groupings have been identified and are influenced in different ways depending on task characteristics:

- false sensations are discrepancies between subjective perceptions of the world and objective characteristics where features of the physical world are distorted or misrepresented by sensory apparatus. Some of the ways they occur are: during and immediately after exposure to steady state inputs; conditions of simultaneous and successive contrast; viewing two-dimensional representations of three-dimensional objects; during and immediately following exposure to inertial rearrangement; and when viewing large-scale moving visual scenes.
- attentional failures are failures in a universal although limited control resource fundamental to the initiation and guidance of mental activities. Attentional failures are divided into the following contextual groups: coping with distraction; processing simultaneous inputs; focusing attention of one of two concurrent messages; dividing attention between the performance of two concurrent tasks; tasks providing limited opportunity for the appropriate combination of object features; and monitoring, custodial, and verification tasks.
- memory lapses result from volatile memory, the cognitive domain associated with this type of failure, and refer to short-term

memory, working memory, and prospective memory (remembering things to do). Based on different contextual factors, these error groupings are characterized as: forgetting list items; forgetting intentions; and loosing track of previous actions.

• inaccurate recall is a feature of recollection processes. Categories include misremembering sentences, stories, places, faces, and events and blocked recall.

• misperceptions occur when incorrect interpretations are placed on sensory inputs. They often occur when sensory input is incomplete or ambiguous. They are divided into the categories of: experimental manipulations; mishearing speech; misreading text; misreading signals and instruments; misperceptions in routine actions; and misperceptions of people.

• errors of judgement are divided as follows: psychological misjudgments; temporal misjudgments; misconceptions of chance; misconceptions of covariation; misjudgments of risk; incorrect diagnoses; fallacies in probability judgements; and erroneous social assessments.

• inferential errors are divided into the following categories: errors in deductive reasoning; errors in propositional reasoning; reasoning with positive and negative instances; reasoning with concrete and abstract instances; errors in concept formation; and errors in hypothesis verification.

• unintended actions refer to slips (absent minded deviations of actions, words, and signs from their intended path) in the failure of execution of plans rather than from faulty or inadequate plans.

They are divided contextually as: slips of the tongue; slips of the pen; slips of the hand (in sign language or body language); slips of actions; and Freudian slips.

Different error forms result from localized interactions of primary error groups with situational factors. "Predictable error forms" result from the interaction of primary error groups and situational factors that may initiate or enable their occurrence. "A predictable error form is one for which it is possible to specify (in a probabilistic rather than a deterministic fashion) both the circumstances that will promote its occurrence and the likely form it will take" [Reason 1987c: 6]. Individual factors such as age and pathological dispositions to commit certain errors are assumed not to produce unique error forms. Performance shaping factors only enhance the likelihood of the occurrence of already identified forms--they do not cause them.

FIGURE A.1

MATRIX FOR CLASSIFYING PRIMARY ERROR GROUPINGS

Basic Error Tendencies

COGNITIVE DOMAINS	ECOLOGICAL CONSTRAINTS	CHANGE ENHANCEMENT	RESOURCE LIMITATIONS	SCHEMA PROPERTIES	STRATEGIES HEURISTICS
SENSORY REGISTRATION	False sensations: X	X			
INPUT SELECTION			Attentional failures: X	X	O
VOLATILE MEMORY			Memory lapses: X	X	O
LONG-TERM MEMORY			Inaccurate recall: O	X	X
RECOGNITION PROCESSES	Misperceptions: O	O	X	X	X
JUDGEMENTAL PROCESSES		Errors of judgement: X	X	X	X
INFERENTIAL PROCESSES			Reasoning errors: X	X	X
ACTION CONTROL			Unintended words/actions: X	X	O

X = PRIMARY NODE O = SECONDARY NODE

SOURCE: Adapted from Reason (1987c)

A.9.3. A Taxonomy of What and How

An alternative approach to classifying human errors, the Failure-Mode-Effect taxonomy, is based on the behavioral and contextual levels of analysis [Rasmussen 1982, Rasmussen 1987a]. This method is based on the view that human errors are a result of total human-task system behavior rather than specific characteristics of humans or tasks. Consequently, the taxonomy reflects different factors influencing the interactions of humans and tasks: task characteristics, performance shaping factors, and human motor control and cognitive mechanisms. Therefore, this approach suggests that error data collected during routine task situations are not necessarily applicable to novel situations that the approach of human reliability engineering may not be appropriate in complex technological systems.

Because the taxonomy has its roots in the analysis and prevention of industrial process plant accidents, it is intended to provide a method for describing and analyzing the causal path of events leading to an accident. The multi-faceted failure-mode-effect taxonomy has six dimensions [Figure A.3]:

1) task of personnel: the specific types of tasks in which the human is involved. Knowledge of the task is important for determining the circumstances of a failure.

2) external mode of malfunction: the external characteristics of human failure. These correspond to immediate and observable consequences of human failure in the performance of a task. The purpose of this category is to identify system sensitivity to the

failure of a limited number of subtasks. This information can be useful for reliability and risk analyses.

3) internal human malfunction: the internal mental function of a person's decision making that was not performed, or performed inadequately, during a task. This category is based on the assumption that human decision making is a rational sequence of events.

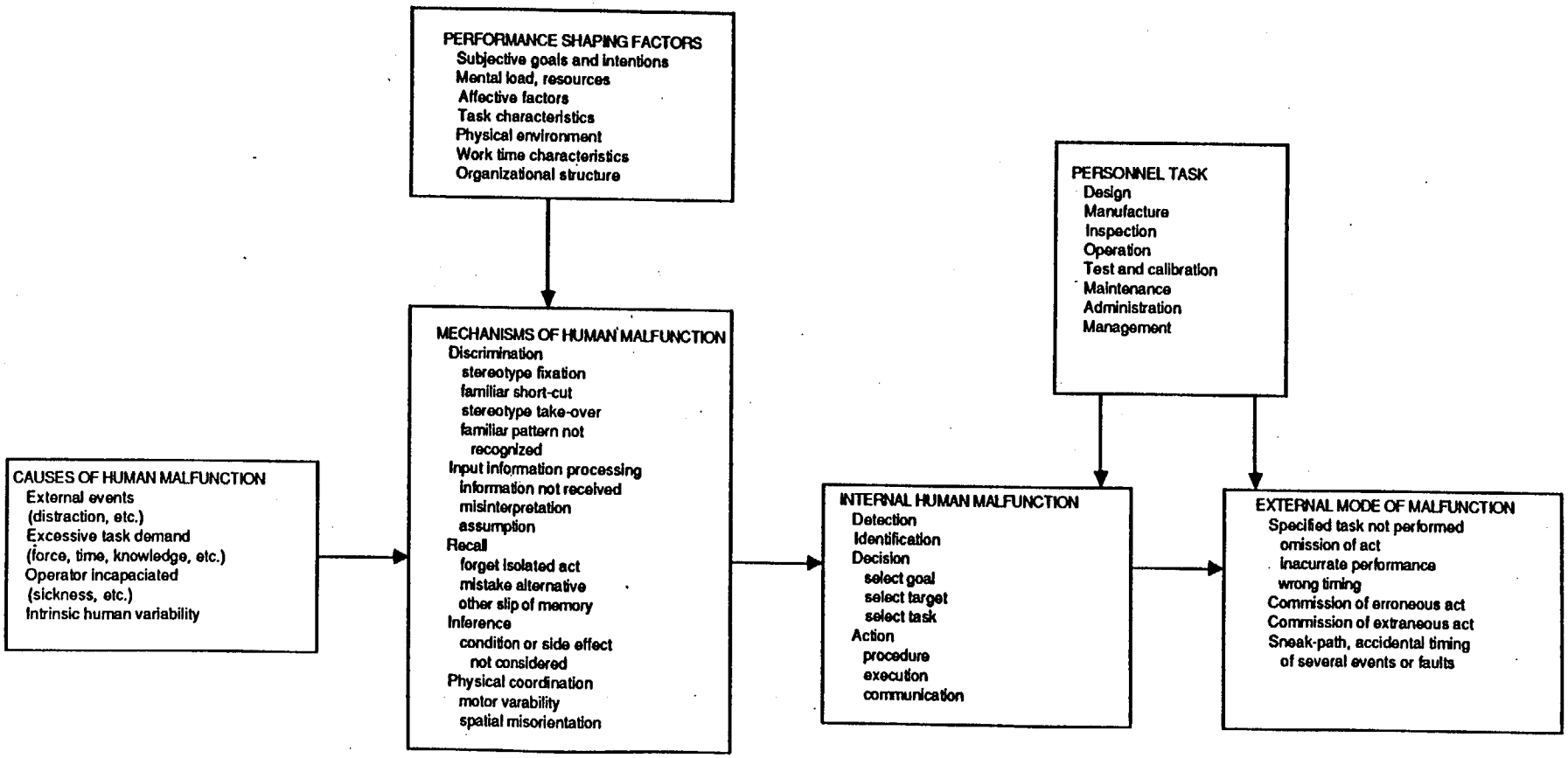
4) mechanisms of human malfunction: the level and mechanisms of cognitive control that help explain a human-task mismatch. This taxonomy is based on the three level cognitive model incorporating skill-, rule-, and knowledge-based behavior described in section A.4.2. Errors are considered in terms of hierarchical cognitive control domains.

5) causes of human malfunction: the identification of possible external causes of human failure. They are events recognizable as distinct in time and space unlike performance shaping and situational factors. These causes may be due to spontaneous internal human variability or a change in the external task.

6) performance shaping factors: general persistent features of the human-task environment that may influence error probabilities, but which do not directly cause errors. Performance shaping, or situational factors, do not appear explicitly in the causal chain of events leading to an accident, but they influence them by affecting human capabilities and subjective preferences and strategies. Such factors include affective, motivating, and environmental influences, different types of stress, and ergonomic designs.

FIGURE A.3

FAILURE-MODE-EFFECT TAXONOMY FOR DESCRIPTION AND ANALYSIS OF EVENTS INVOLVING HUMAN MALFUNCTION



SOURCE: RASMUSSEN 1982

Table A.3 lists some error types identifiable from this taxonomy and the skill-, rule-, and knowledge-based model of human cognition. This approach is based on the belief that errors are intimately connected to the cognitive control of behavior. During attempts to design safer systems using the failure-mode-effect taxonomy, errors were found to be clustered in four categories related to cognitive processing mechanisms [Rasmussen 1987d]:

1) Inadequate resources: inadequate knowledge or cognitive capacity exists to reason about complex systems. Errors in this category result when causal conditions and complex interactions are not considered properly.

2) Control structure interferences: often more than one task must be performed simultaneously. Consequently, internal control structures, such as skill controlled behavior, attention, and mental models, may interfere with each other, thus creating errors such as forgetting, incorrect recall, stereotype takeover, and false analogies.

3) Learning processes: learning and adaptation processes by individuals are complex and continuous. Errors in this category result from attempts to test hypotheses and develop shortcuts.

4) Human variability: unlike the others that describe systemic errors, this group is related to variability in human motor and cognitive control. Although it is not always possible to eliminate such errors, their consequences can often be mitigated through proper design.

The taxonomy described in the previous section and the failure-mode-effect taxonomy share similar structures. In particular, the

dimension of "basic error tendencies" is similar to the category of "internal error mode" in the failure-mode-effect taxonomy. In addition, "predictable error forms" are similar to the category of "error mechanisms" at all levels of cognitive processing. Finally, the "predictable error forms" and analyses utilizing the failure-mode-effect taxonomy help to identify the errors that result from the interactions of an operator, the environment, and the task. The similarity of research results from systems and reliability analyses of empirical data and theoretical cognitive psychology is suggestive that errors defined as mismatches and deriving from the total human-task system is appropriate for the the analysis of complex human-task systems, such as the transportation of spent nuclear fuel.

TABLE A.3

Error Types in Failure-Mode-Effect Taxonomy

Knowledge-based behavior
- causal conditions not considered
- interactions not considered
- false analogies

Rule-based behavior
- improper shortcut
- fixation ("tunnel vision")
- forget isolated item
- mistake among alternatives
- incorrect recall

Skill-based behavior
- stereotype takeover
- motor control variability
- topographic misorientation

A.10. References

Bainbridge, L. 1984. "Diagnostic skill in process operation". Paper presented at the International Conference on Occupational Ergonomics, Toronto, Canada, 7-9 May 1984.

Bellamy, L. 1983. "Neglected Individual, Social, and Organizational Factors in Human Reliability Assessment". Proceedings of the Fourth National Reliability Conference 6-8 July, 1983, Volume 1, National Centre of Systems Reliability, England.

Bellamy, L. 1985. "How people's behavior shapes your plant operation", Process Engineering, July, 1985, pg. 27-28.

Bellamy, L. 1988. Personal communication.

Brehmer, B. 1987. "Models of diagnostic judgments", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Bjordal, E. N. 1987. "Risk from a Safety Executive Viewpoint", in W. T. Singleton and J. Hovden, Eds., Risk and Decisions, NY: John Wiley and Sons.

Cook, B. 1988. Personal communication.

Crecine, J. 1986. "Defense Resource Allocation: Garbage Can Analysis of C3 Procurement", in J. March and R. Weissinger-Baylon, Eds., Ambiguity and Command: Organizational Perspectives on Military Decision Making. MA: Pitman Publishing Inc..

Davis, J. and Hinsz, V. 1982. "Social Interaction as a Combinatorial Process in Group Decision", in H. Brandstatter, J. Davis, G. Stocker-Kreichgauer, Eds., Group Decision Making. Academic Press.

Dhillon, B. S. 1986. Human Reliability, Elmsford, NY: Pergamon Press.

Embry, D. 1984. "Human Reliability", Paper presented at the 1984 Summer School of the Italian Physical Society, Human Reliability Associates, Ltd., Parbold, England.

Fischhoff, B. 1986. "Judgement and Decision Making", in R. Sternberg and E. Smith, Eds., The Psychology of Human Thought, New York: Wiley, in press.

Gentner, D. and Stevens, A. (Eds.) 1983. Mental Models. NJ: Lawrence Erlbaum Publishers, Inc.

Gray, J. and Quarantelli, E.L. 1984. "Research findings on community and organizational preparation for and response to acute chemical emergencies (DRC Preliminary Paper 91). Newark, Delaware: Disaster Research Center, University of Delaware.

Hirokawa, R. and Scheerhorn, D. 1986. "Communication in faulty group decision-making", in R. Hirokawa and M. Poole, Eds., Communication and Group Decision-Making, CA: Sage Publications.

Kirwan, B. 1988. Personal communication.

LaPorte, T. 1988. Personal communication.

March, J. 1981. "Decisions in Organizations and Theories of Choice", in A. H. Van De Ven and W. Joyce, Eds., Perspectives on Organization Design and Behavior, NY: John Wiley and Sons.

National Research Council 1988. Human Factors Research and Nuclear Safety. Committee on Human Factors, National Research Council. Washington, D.C.: National Academy Press.

Nisbett, R. and Wilson, T. 1977. "Telling more than we can know: Verbal reports on mental processes", Psychology Review, 35, 613-624

Noble, D. 1986. Forces of Production. NY: Oxford University Press.

Nordic Liaison Committee for Atomic Energy 1985. "Organization for Safety", Report LIT(85)3, Statens Vattenfallsverk, Fack, S-162 82 Vallingby, Norway.

Nuclear Regulatory Commission 1980. Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications. U.S. Nuclear Regulatory Commission NUREG/CR-1278

Perrow, C. 1983. "The organizational context of human factors engineering". Administrative Science Quarterly, December 1983.

Perrow, C. 1984. Normal Accidents. NY: Basic Books, Inc.

Poole, M. and Hirokawa, R. 1986. "Communication and Group Decision-Making: A Critical Assessment", in R. Hirokawa and M. Poole, Eds., Communication and Group Decision-Making, CA: Sage Publications.

Putnam, L. 1986. "Conflict in Group Decision-Making", in R. Hirokawa and M. Poole, Eds., Communication and Group Decision-Making, CA: Sage Publications.

Rasmussen, J. 1982. "Human Errors. A Taxonomy for Describing Human Malfunction in Industrial Installations", Journal of Occupational Accidents, 4:311-333.

Rasmussen, J. 1987a. "Definition of Human Error and a Taxonomy for Technical System Design", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Rasmussen, J. 1987b. "Cognitive Control and Human Error Mechanisms", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, NY: John Wiley and Sons.

Rasmussen, J. 1987c. "Mental Models and the Control of Actions in Complex Environments", Report number RISO-M-2656, Riso National Laboratory, DK 4000 Roskilde, Denmark.

Rasmussen, J. 1987d. "Human Error Mechanisms in Complex Work Environments", Report number RISO-M-2679, Riso National Laboratory, DK 4000 Roskilde, Denmark.

Reason, J. 1987a. "The Psychology of Mistakes: A Brief Review of Planning Failures", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, John Wiley and Sons.

Reason, J. 1987b. "Collective Planning and its Failures", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, John Wiley and Sons.

Reason, J. 1987c. "A Framework for Classifying Errors", in J. Rasmussen, K. Duncan, and J. Leplat, Eds., New Technology and Human Error, John Wiley and Sons.

Reason, J. and Mycielska, K. 1982. Absent-Minded? The Psychology of Mental Lapses and Everyday Errors, Englewood Cliffs, NJ: Prentice-Hall, Inc.

Sheridan, T. 1983. "Measuring, Modeling, and Augmenting Reliability in Man-Machine Systems", Automatica,19(6), 637-645.

Sheridan, T., Charny, L., Mendel, M., and Roseborough, J. 1986. "Supervisory control, mental models, and decision aids". Unpublished manuscript, Cambridge, MA: MIT Man-Machine Systems Laboratory, Massachusetts Institute of Technology.

Simon, H. A. 1955. "A Behavioral Model of Rational Choice", Quarterly Journal of Economics, 69, 99-118.

Simon, H. A. 1957. Administrative Behavior. (2nd edition). NY: MacMillan.

Slovic, P., Fischhoff, B., and Lichtenstein, S. 1977. "Behavioral Decision Theory", Annual Review of Psychology, 28, 1-39.

Slovic, P. and Lichtenstein, S. 1971. "Comparison of Baysian and regression approaches to the study of information processing in judgement", Organizational Behavior and Human Performance, 6, 649-744.

Sorensen, J.H. and Vogt, B.M. 1987. "Emergency planning for nuclear accidents: Contentions and issues." Paper prepared for the symposium:

Nuclear Radiation and Public Health Practice and Policies in the Post-Chernobyl World. September 18-19, 1987.

Svenson, O. 1979. "Process Descriptions of Decision Making", Organizational Behavior and Human Performance, 23, 86-112.

Svenson, O. 1981. "Are we all less risky and more skillful than our fellow drivers", Acta Psychologia, 47, 143-148.

Svenson, O. 1986. "A psychological perspective on accident evolutions and how to arrest them in nuclear power plants". Paper presented at the Society for Risk Analysis Annual Meeting, Boston, Massachusetts,. 9-12 November, 1986.

Swap, W. 1984. Group Decision Making, CA: Sage Publications.

Tuler, S. 1987. "Human Behavior in Time-Pressured Distributed Decision Systems", Masters Thesis, Man-Machine Systems Laboratory, Massachusetts Institute of Technology, Cambridge, MA.

Turner, B. 1978. Man-made Disasters. London: Wykeham Publications Ltd.

Tversky, A. and Kahneman, D. 1974. "Judgement under uncertainty: Heuristics and Biases", Science, (185):1124-1131.

APPENDIX B

B.1. Prior Research

Four studies that have evaluated human errors in spent fuel transportation are reviewed in the following sections.

B.1.1. PNL-2588, An Assessment of the Risk of Transporting Spent Nuclear Fuel by Truck, Chapter 7: "Conditions of Spent Fuel Casks During Transportation" [Battelle Northwest Laboratories 1978].

In this study a survey of industry cask handlers was used to determine the conditions of the casks during spent fuel transportation. This information was ultimately to be used in risk analyses. The report attempts to estimate error types and rates in loading, packaging, and normal transport of spent fuel in both truck and rail casks during the period of 1970-1977. Five companies (both commercial and non-commercial) participated in the study; none, however, were commercial power plants that are regulated by strict Nuclear Regulatory Commission [NRC] regulations of oversight and reporting. Three of the companies were regulated by the DOE that requires fewer oversight and reporting activities than does the NRC. These more lenient reporting requirements could lead to the underestimation or misidentification of errors. In addition, the survey was only concerned with normal, "incident-free", transportation, although unexpected and accident situations may

create additional sources and types of failures that, therefore, would not be not identified in the report.

Another limitation of this study resulted from the assumption that the quality control and quality assurance requirements that were strengthened by the NRC after 1971 resulted in "a significant reduction in package errors." However, they offer no proof for this claim. In fact, since 1978 the frequency of exterior cask contamination has been observed to be much higher than assumed in this study [Nebraska Energy Office 1987].

The survey approach was to collect anecdotal information concerning human errors in the use of casks. Because observations were from personal recollections, the time period of observations is uncertain. This anecdotal approach was a major weakness of the study, because it did not include all the incident types that had been reported in other databases. In addition, the range of potential consequences of the errors identified in the survey does not cover the range of more recently observed consequences from human errors. Significantly, errors that were assigned a very low probability in their risk analysis have already occurred in the transportation of spent fuel and other high level radioactive waste.

B.1.2. Transportation of Radionuclides in Urban Environs

(NUREG/CR-0743), Chapter 4: "Environmental Impacts from Human Errors and Deviations from Accepted Quality Assurance Practices" [Nuclear Regulatory Commission 1980]. This report concludes that the potential contribution of human error to severe accidents is negligible. This conclusion results from the assumption that a circumferential crack in a cask is the mode of radioactivity release in an

accident, and that "human error...would not create the kinds of forces necessary to cause a circumferential crack in the cask wall". This is not the only route, however, by which radioactivity can be released from a cask [Resnikoff 1983]. Moreover, the analysis is based on an assessment that did not incorporate sophisticated approaches to human reliability assessment and on a faulty database.

In this study the transportation related activities within which human error was assumed to be a potential contributor to accident probabilities were: packaging, labeling, temporary stowage, handling, securing, routing operations prior to movement, in-transit transfers, and movement by receiver to final destination. Traffic accidents were considered separately and human error as a causal factor was not specifically analyzed (i.e., accident rates were assumed to include human error rates). Although human error was defined to occur "when there is a reduction or potential reduction in system reliability or safety", the increased vulnerability of an incorrectly designed, manufactured, or maintained cask was not considered.

A major problem of the report concerns the data on which its results are based. The primary source of data was from PNL-2588 and DOT and NRC incident reports. However, this data cannot support the claim of a "detailed error analysis" because the PNL-2588 survey lacked rigor and its results were incomplete. Moreover, for unspecified reasons, not all of the available human error data from the survey was used. Similarly, other known cases of human errors in cask inspection, maintenance, and handling were not included in the analysis [Resnikoff 1983].

The data from PNL-2588 was also used inappropriately. In fact, if used properly, more than twice the number of errors would have been identified [Nebraska Energy Office 1987]. These deficiencies of the survey data affect parameters that were crucial to the attempt to show that the contribution of human error to accidents is statistically negligible. The full range of human error types are not identified and, therefore, accident probability estimates are too low. Consequently, the report's conclusions are seriously flawed.

This is a significant problem because the report forms the basis of the evaluation of human error in spent fuel transportation for the worst case transportation accident- and transportation risk-analysis in the Nuclear Waste Policy Act [NWPA] Yucca Mountain, Nevada Environmental Assessment [DOE 1986]. When it was suggested that human error was not treated adequately in the Environmental Assessment transportation analysis, the DOE response stated that: "The DOE has considered the potential for human error in the assessment of transportation risks...The results [of NUREG/CR 0743] indicate that the risks from human errors or deviations form accepted QA practices are extremely small (i.e., 0.00012 latent-cancer fatality per shipment year for packages tested to accident conditions), and thus it is not meaningful to include these risks in the radiological risk analysis for transportation" [Department of Energy 1986: Appendix C.2.4.1.23].

B.1.3. A Review of the Effects of Human Error on the Risks Involved in Spent Fuel Transportation [Nebraska Energy Office 1987]. In this study the emphasis was on human error in spent fuel cask

design, construction, use, and maintenance. This study examines problems caused by a variety of human error types, including errors of judgment. It also addresses the issue of imperfectly fabricated casks and errors in cask use due to human error, which had received little attention in the past relative to the efforts made to assess the effects of impacts and fires on casks. An important part of this study is an extensive review of PNL-2588 and NUREG/CR-0743 that identifies many of the problems listed above. This study takes an important step toward a more sophisticated evaluation of human errors related to spent fuel casks.

The primary effect of a human error may be associated with a single shipment, a single cask, or a specific cask design. Previous analyses examined only the first category, and consequently they assume 1) that errors are randomly distributed among all shipments, and 2) there is a low probability of human error and severe accidents events occurring simultaneously. On the other hand, if an error effects a cask design or a particular cask, errors are <u>not</u> randomly distributed across all shipments and, therefore, they may affect multiple shipments.

To show the potential effects and occurrence of human errors, the report includes example lists of design, manufacture, maintenance, inspection, and normal and accident handling errors with casks. Both actual and hypothetical problems are included. Although, the list of errors is admittedly incomplete, as the real record is unknown, it does provide a broad range of human error types related to cask fabrication, use, maintenance, and repair. Other types of human errors, however, are not emphasized (e.g., driver caused incidents, such as unauthorized deviations from preplanned routes).

This study was not intended to determine the frequency of human error events, or to develop an approach for their prevention or for the mitigation of consequences. The final section, however, offers some illustrative examples for factoring human error effects into accident probability estimates. For example, it suggests the use of safety factors in probability estimates to take into account human error effects. This approach is relatively unsophisticated and is not based on proven methodologies developed in human reliability analysis.

B.1.4. Transportation of Hazardous Materials, Chapter 2: "Data and Information Systems for Hazardous Materials Transportation" [Office of Technology Assessment, 1986]. This study is not specific to spent nuclear fuel, but reviews hazardous materials transportation in general. It aids in the identification of the possible range of error types in the transportation of spent fuel. Based on a review of the DOT Hazardous Materials Incident System [HMIS] database, this study identified human error as a major cause of hazardous materials transportation accidents. Risk management programs that were considered to be of prime importance were training of emergency response and enforcement personnel, improving the coordination and comprehensiveness of federal and state regulations, increasing the availability of public information about hazardous material transportation, and improving the regulation of containers.

The approach of this analysis was to count all incidents reported to the DOT that had "human error" identified as the primary cause, a factor reported as the cause of 62% of the accidents and incidents reviewed. The

next most cited cause was package failure, and the next, vehicular accidents. The specific reasons for the occurrence of hazardous material transportation incident indicate that the predominant cause of failure varies considerably by mode although loose and defective fittings and external puncture were frequently observed. Other "primary cause" categories included handling, corrosion and rust, package failure, loading and unloading, and metal fatigue which suggest that human errors occurred during manufacture, maintenance, inspection, and operation. The category of "miscellaneous information" in the study is defined to include events that also suggest certain types of human error although this is not possible to verify in all cases.

The HMIS database, maintained by the DOT, provides one source of information about transportation accidents and incidents although it is not completely reliable. The OTA study found that compliance rates of reporting were not 100% (i.e., when a reportable incident or accident occurred it was not always reported to DOT). The estimates of human error rates are probably underestimated for this reason and because human error is only identified when it was a primary cause of failure and not when it was a contributory cause.

Appendix C

A REVIEW OF

HUMAN RELIABILITY ISSUES

IN THE TRANSPORTATION

OF SPENT NUCLEAR FUEL

prepared by:

Lindsay Audin,
nuclear transport consultant

prepared for:

Delos Associates
RR 1, Joy Road
Woodstock, CT 06281

May 8, 1988

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Human reliability is of significant importance in spent fuel transportation. Small errors at various stages can create vulnerabilities assumed non-existent in analyses of accident consequences.

Opportunities for human errors stretch far beyond the driver of the transport vehicle, from the system designer to the maintenance staff, and from the fuel handler at the reactor to the cask handler at the repository. All parties perform functions that could initiate and/or complicate serious incidents. There is a need to examine such opportunities and eliminate them by better design, testing, inspection, maintenance and enforcement.

Previous failures fall into two general categories: conceptual and mechanical.

Conceptual errors arise from:

- confusing, seemingly contradictory and incomplete regulations by agencies with different approaches to the same problems
- underestimation of human error potential by immature risk analysis methods, making serious accidents appear to be nearly impossible
- gaps in knowledge and communication of the potential consequences of human error, both between and among regulators and their staff.

Mechanical errors are more specific in nature:

- failures in cask design due to incomplete verification data and a lack of both rigor in analysis, and independent confirmation of the design
- creating opportunities for errors in fabrication and handling by failing to anticipate and avoid them
- deficiencies in procedures for fuel and cask handling, and the absence of electronic detection of internal cask conditions resulting from such errors.

Human reliability can be heightened without major alteration to the present structure. Improvements fall into four general areas:

- better fuel and cask management and tracking, preferably by a computerized database
- fail-safe designing that assumes human error at every turn, and seeks to avoid it
- more precise cask/vehicle design criteria and rigorous testing
- better oversight and inspection methods, both human and electronic, to detect errors as they occur, instead of years later.

To implement these criteria, several general initiatives are needed:

- a funding mechanism to support an office dedicated to improving spent fuel handling and transportation
- development of resources, both human and electronic, to collect, digest and act on data related to spent fuel, transport equipment and their interactions
- adoption of an approach of "constructive initiation and intervention" in the regulatory and technical processes covering design, handling, maintenance, etc.

By adopting an aggressive, informed and positive perspective - and maintaining the courage to pursue it - Nevada will be in an excellent position to significantly influence this aspect of the confrontation with federal policies on nuclear waste disposal.

EXISTING MANAGEMENT SYSTEMS INVOLVED IN SPENT FUEL TRANSPORTATION

The movement of spent nuclear fuel utilizes a number of systems, all of them involving human interaction. To fully understand their interplay, it is necessary to understand the spent fuel transport process.

THE FUEL

Spent fuel consists of small cylindrical pellets of uranium oxide, a portion of which has been converted, during the nuclear reaction, into potentially hazardous radioactive substances. These pellets are housed inside zirconium alloy tubes (called "cladding") which are, in turn, held in frames to form assemblies. A typical assembly for a pressurized water reactor (PWR) will hold about 200 tubes (called "fuel rods" when filled with pellets) and weighs about half a ton, most of it being uranium oxide. The rods are sealed and pressurized with an inert gas (usually helium). Coating the surface of the rods is a fine powder (called "crud") consisting of irradiated materials released into the reactor by corrosion of the inside of the reactor core vessel.

When the fuel is removed from the reactor, it is still highly radioactive and hot for many years (due to conversion of some uranium into fission products) and is usually kept under water in a separate pool while it cools off. Water acts as both coolant and radiation shield, while allowing continuous removal (via filtration) of particles and gases that may leave the fuel during storage. When ready for shipment, the fuel is typically loaded into a cask that has been submerged in the spent fuel pool. Remote control cranes, handling tools and TV cameras allow operators to load fuel without approaching it.

Most spent fuel is not damaged when placed into the spent fuel pool, but a small percentage does leak due to cracks and holes in the

cladding. Such fuel is usually packaged in a sealed steel cylinder to reduce the chance of leakage into the cask during transit, or upon arrival and unloading. This process is referred to as "canning." Movement of such fuel may involve special "baskets" (which hold spent fuel in the cask) and perhaps (as in the case of fuel from the damaged Three Mile Island reactor) even specially designed casks.

Commercial power reactors were initially designed to hold only a few years of fuel discharges. It was assumed (up to 1978) that fuel would be reprocessed to harvest the remaining enriched uranium, and possibly the plutonium, for re-use in new fuel. When commercial reprocessing was abandoned in this country, reactor operators were forced to hold onto their fuel until other storage facilities become available. In some cases, utilities with multiple power plants "transshipped" spent fuel from a full pool to an empty one, but most have instead installed new racks to hold assemblies closer together in existing pools. There is a limit to the packing density of recently discharged (i.e., 3 years or less out of the reactor) fuel assemblies, however: loss of pool water surrounding high density racks for an extended period (about 12 hours) such as during a plant accident could cause the fuel to self-heat and ignite. The zirconium cladding will burn in air when it reaches a temperature above 1600°F, giving off sufficient heat to raise the temperature of nearby assemblies. The rods would burst, the pellets re-oxidize (i.e., form a fine powder) and a very difficult situation would arise as the debris began to settle to the bottom of the dry pool (ref 1).

Re-racking typically "bought" another ten years of storage for older reactors and more time for later reactors erected with larger pools. That time is now running out at an increasing number of plants. however, so utilities have begun installation of special storage casks or other above-ground facilities that contain spent fuel in a dry, air-filled environment. Such dry storage does not require any mechanical cooling and is modular, thereby allowing continuous expansion until a final repository is available to receive the fuel.

Depending on the age of the fuel, it may reach temperatures exceeding 600°F in a dry cask. While this temperature is not high enough to damage the fuel, it is high enough to loosen the crud on the fuel rods, (ref. 2) gradually oxidizing the cladding (long term effects are not well known) and re-oxidize any fuel pellets exposed to air through damaged cladding. Re-oxidized fuel contains the dangerous fission products in a aerosable (i.e., breathable) form (ref. 3).

After dry storage for probably at least ten years, the fuel will be transferred (again by remote control) into transport casks. Some storage casks have also been designed for transport, but it is unclear if many will be used for this purpose due to their extreme weight and the variety of non-transportable storage systems becoming available. Such dual use casks would require careful inspection prior to transport after being is constant use for a decade or more.

In addition to re-racking and dry storage, utilities have begun to explore an additional option to store more fuel in available space. Consolidation of spent fuel assemblies involves disassembly (removing the rods from their framework) and packing them into a space roughly half the volume of a typical assembly, usually in a sealed can. Such a technique also roughly doubles the capacity of a spent fuel cask. The same concerns (e.g., crud and fission product release) would exist during canning at the power plant: the cans would require thorough inspection prior to packing into a transport or storage cask. The age of consolidated fuel is also a concern: still in the pilot testing stage, this procedure assumes that fuel has cooled sufficiently to avoid raising the temperature of the rods closest to the center to a point where they could be damaged.

To summarize, the transport process actually starts with the characteristics of the spent fuel: its time out of the reactor, the condition of the cladding, the type and duration of its storage, its surface cleanliness, and the consolidation of its rods. Other factors, such as reactor type (pressurized or boiling water), burn-up

rate, enrichment level, and cladding type (steel or zircalloy) could also influence (to a generally lesser degree) the integrity of the fuel under stress. Finally, it must be recalled that a final repository will likely receive a variety of fuels from older or non-commercial reactors as they are decommissioned. While involving a much smaller quantity of fuel, the variations in fuel types (i.e., composition, shape, cladding, etc.) present some unique challenges to handling, inspection and emergency preparedness personnel.

THE CASKS

Spent fuel casks vary in design and construction but are similar in nature. A typical design (ref. 4) consists of two concentric cylinders with a dense gamma ray shielding material (lead or depleted uranium) sandwiched between them. The outside of the cask may be coated with an organic material (such as a resin) to reduce the escape of neutron radiation. Older casks utilized a water jacket for this purpose. One end of the cask is welded to the main body while the other end is removable to allow loading and unloading. The fuel is held in an adapter (the "basket") that conforms to the cylindrical interior of the cask while securely holding the square assemblies. Older truck casks could hold only one or two assemblies (depending upon reactor type) due to the heavy shielding required for "young" fuel (less than one year out of the reactor), but new models will likely hold double this amount due to the reduction in radiation output when the fuel is 5 or more years out of the reactor.

When loaded in the spent fuel pool, the cask fills with water which must be drained and replaced (in casks presently licensed by NRC) with an inert gas such as helium or nitrogen. To perform this function, casks may have drain, fill and vent valves: the fill valve allows air to enter the cask to force water out through the drain valve, and the vent valve allows the cask to be dried by creating a vacuum (any remaining water vaporizes and is withdrawn with the air). The fill valve then allows the cask to be filled with the required inert gas.

Depending on the design, only two valves may be needed since the filling and venting functions may be accomplished at one valve port. It is also possible to replace the drain valve with a pipe plug. Older casks also had pressure relief valves that could open during a fire to avoid overpressurizing a water-filled cask (water was previously used to help cool young fuel while still in the cask). Such relief valves may not be needed on newer gas-filled casks.

The cask lid is mated to the cask body at a metal or teflon-like seal. Such seals are crucial to maintenance of an airtight environment and are often inspected prior to each shipment. They must be capable of maintaining a seal even after the cask has been involved in a severe impact and fire.

The ends of the cask are covered and protected by shock absorbers (called "impact limiters") often consisting of a thin aluminum shell filled with crushable wood. When bolted to the cylindrical cask, the impact limiters give the unit a dumbbell-like appearance. At the ends of the cask, large pins extend perpendicular to the main body to allow the cask to be lifted by a separate harness and crane. Called "trunnions", these pins also serve to restrain the cask when mounted on a trailer and attached to the trailer's "tiedowns" (brackets or chains connected to the trailer bed).

The trailer itself may also be required to be equipped with devices to disable its movement (e.g., by bursting its tires), depending upon resolution of a proposed 1984 rulemaking on physical security.

LOADING AND HANDLING PROCEDURES

Various procedures exist to facilitate proper loading and handling of spent fuel and casks. The first effort involves determining which fuel is appropriate for shipment. Fuel records are examined and a calculation is performed to determine that the heat and radiological outputs do not exceed the cask specifications. The fuel is then

removed from the main pool and placed into a separate clean water bath for a short period, during which tests (called "sipping") are performed on the water to determine if the fuel rods are leaking. If found acceptable, the fuel is then available for placement into the cask.

The cask may be inspected upon arrival to determine the condition of its valves, seal, basket, impact limiters, etc. Surface wipe tests (called "swipes") may be done prior to acceptance into the pool area to determine if any loose or excess surface contamination exists. If all is found acceptable, the cask is immersed in the pool and opened, and assemblies are inserted. As mentioned previously, the cask is then closed, drained, evacuated, backfilled with an inert gas and pressure-tested for leakage. It is washed, swipe-tested and loaded onto a trailer. The impact limiters and tiedowns are attached, and a final inspection is made, usually by an agent of the shipper.

Upon arrival, checks are made on the cask similar to those made prior to acceptance, whereupon it is admitted and may be filled with distilled water for a check of interior contamination, or may be directly immersed into the pool. The lid is removed, the fuel withdrawn, and the cask drained, washed and swipe-tested. Valves and seals may be checked prior to loading onto the trailer and any regular maintenance performed, as detailed in the cask license (called the "certificate of compliance").

As can be seen from the above, human reliabililty concerns in spent fuel transport extend far beyond the driver of the vehicle, reaching back to the reactor official who chooses which fuel to ship, and forward to the repository maintenance staff that must test, inspect and maintain the container's replaceable parts. In the next section, it will become obvious that human reliability concerns extend even further beyond the actual transportation process: into the realms of regulation, design, manufacturing and routing.

DEFICIENCIES IN CURRENT METHODS FOR ASSURING HUMAN RELIABILITY

BACKGROUND

Recent changes to the Nuclear Waste Policy Act (NWPA) (ref. 5) have clouded the role of the U.S. Department of Energy (DOE) in handling the movement of spent fuel between nuclear facilities and a final repository. The NWPA amendments mandate use of casks certified by the Nuclear Regulatory Commission (NRC) and require prenotification of states prior to shipments, as per existing NRC rules. The amendments do not, however, address the physical security, inspection or routing requirements for the shipments. While a U.S. Department of Transportation (DOT) rule requires that DOE utilize a physical security plan "equivalent" to that of the NRC, this has not always been the case in the past and the two agencies presently allow different levels of security when traversing urban areas, and different security-related equipment of the transport vehicles. Similarly, it is not clear when NRC is empowered (or required) to examine containers and procedures to ascertain if DOE, as a shipper, is complying with the NRC cask license. There is also a potential conflict over routing regulation: NRC requires advance approval of routes, but DOE shipments are presently governed by DOT rules, which require no advance approval.

A recent (April, 1988) interview with DOE and NRC officials (ref. 6) by this writer indicates that the Office of Civilian Radioactive Waste Management (OCRWM), DOE's branch dedicated to handling commercial spent fuel, will act and be treated as "just another licensee; like Duke Power, for instance." If this interpretation is maintained, the present NRC practices (which are generally better than those of DOE) will cover all OCRWM transport activities. In the past, however, DOE has strongly resisted NRC control of any of its actions and may again seek to do so if not bound by specific law. Similarly, NRC has avoided holding DOE to account for its technical and regulatory failures even when NRC was aware that DOE was using deficient containers (ref. 8).

DOE VS. NRC VS. DOT: THE REGULATORY MAZE

The first major gap in overseeing human reliability is the division of power in this area among three large federal agencies, each with a differing outlook on regulatory interpretation and enforcement. While some clarifications have been made on the final authority in some areas, there are still major gaps and uncertainties. The general framework of transportation regulation involves chapter 49 of the Code of Federal Regulations (CFR) but also chapter 10, parts 19 and 71 (and occasionally other chapters). These regulations often appear as a changing patchwork to shippers, carriers and enforcers (which includes most states that have adopted parts of the CFR into their own bodies of law). While an occasional attempt has been made to translate them from "technicalese" into useable English, such a translation has not been issued recently and (in the past) has also contained serious gaps (such as exactly where to take radiation measurements to ascertain compliance of a loaded cask).

The interface of regulations between one agency and another has also led to problems. For example, NRC presently approves each route used by its licensees prior to shipment (ref. 9). But DOE is governed by DOT's routing rules that only require delineation of routes after completion of a shipment (ref. 10). While NRC has disapproved routes because of security deficiencies in the past, DOT has done very little to police DOE's shipments, as evidenced by DOE's use of non-interstate highways when interstates were available and required (ref 11). At present, NRC cannot halt a DOE shipment on an improper route since DOE need not inform it of the route in advance.

A second area of conflict is in radiation safety policy. NRC recently (1987) codified the ALARA principle ("As Low As Reasonably Achievable") into its radiation protection regulations (ref. 12). This means that handlers of radioactive materials must, whenever more than one option exists, choose the one that reduces exposure to a minimum, despite slight extra cost. DOE and DOT have, in the past,

allowed a different standard to apply: certain levels are considered "safe enough" and nothing more need be done even if the increase in cost is minor (ref. 13). When faced with such variations, different handlers and enforcers may decide to opt for different methods to perform the same task, opening the door to misunderstanding and error.

A problem of even more specific nature involves the cask restraints. NRC regulations require that the tiedowns be able to hold onto the cask against a force of 10 g's (ten times the weight of the cask) along its length, 5 g's up or down, and 2 g's from a side impact (ref. 14). But other federal rules require that the restraint be able to hold onto the trailer against a force of only 1.8 g's in any direction (ref. 15). It is thus possible to generate a cask restraint system that will hold securely onto the cask but break easily away from the vehicle, and still comply with all relevant rules, due to the division of control between NRC and DOT at the vehicle boundary.

RISK ANALYSIS VS. REALITY: ERRING IN THE ASSESSMENT OF HUMAN ERROR

Probability Risk Assessment (PRA) is a young science used to determine which of several options may present the least risk. When used in an absolute way, it allows comparison between the probability of very different hazards, such as being hit by a car or falling off a ladder. When used in a relative way, it may compare the hazard of one shipping route with another. When used in the area of spent fuel transport, it is still an imprecise tool that may lead to questionable conclusions and questionable policies.

PRA has been used to calculate the risk (i.e., the mathematical product of probability and consequences of an undesired action, such as routine exposure or a serious accident) of reactor operations. As these analyses have been fine-tuned, the calculated probability of a serious accident has increased dramatically. Yet such events as Three Mile Island and Chernobyl were still considered extremely unlikely (if not nearly impossible) due to the near absence in the analysis of

realistic assessments of human error. PRA for spent fuel transport is still many years behind where it is for reactor operations and, once again, human error has been all but ignored as a significant source of risk. But routine decisions are still based on PRA, regulations depend on its findings, and courts accept it as a viable means upon which to render a judgment.

Only one effort has been made to incorporate human error into a PRA, that being a study (NUREG/CR-0743) (ref. 16) which depended on a brief survey by another study (PNL-2588) (ref. 17). The Environmental Assessment (EA) for the NWPA relied on these studies to assess the impact of human error and, to the degree that these studies fail the task, so does the NWPA EA. A detailed analysis of the human errors listed (and missing) in the survey and how they were utilized by NUREG/CR-0743 was done by this author in 1986 under contract with the State of Nebraska (ref. 18). That analysis found:

- the NUREG analysis greatly underestimated the worst possible impact of human error, possibly by several orders of magnitude
- the PNL survey statistically misused data on some errors, was missing many others, and depended on very limited, variable and possibly unreliable data sources
- both studies were grossly outdated due to human errors of a much more serious nature that happened subsequent to either of them (and therefore were not considered by them).

The State of Nebraska study concluded: "The probabilities derived by 0743 are incorrect, the consequences are incorrect and thus the risk analysis is incorrect."

There is a strong need both to advance this analytical method, and to limit its application where great uncertainties exist concerning its accuracy. The present unreliability of such a decision tool allows it to be used by differing parties to come to whatever conclusions they desire. The lack of any equally powerful analytical resources leaves such a fallible procedure unchallenged until reality proves it to be erroneous, possibly via a disaster.

GENERALISM VS. EXPERTISE: GAPS IN THE KNOWLEDGE OF THE REGULATORS

It is this writer's perception, gained over 14 years of experience in this area, that the level of knowledge of officials and decision makers on some technical matters is often sufficiently spotty (or non-existent) as to present opportunity for serious gaps in human reliability. Several incidents have occurred that show how variations in knowledge between upper and lower staff have increased (or maintained) avoidable hazards.

In 1980, an incident occurred (detailed later in this chapter) that brought into question the use of air (rather than inert gases) in casks holding spent fuel cool enought not to require water in the cask. An assembly containing damaged rods self-heated in transit sufficiently to re-oxidize fuel pellets into a fine powder that was released when the cask was opened. A private spent fuel pool, a worker and the cask were contaminated, resulting in multi-million dollar lawsuits (ref. 19). When confronted by this information three years later, the head of NRC's cask certification department, plus two of his experts, demonstrated marked ignorance of the re-oxidation phenomenon at a private meeting with this writer (ref. 20). All three believed the rate of re-oxidation to be so slow as to be irrelevant during the brief time of a shipment. Despite provision to them of official past studies on the subject, these officials took no action until formerly petitioned under NRC rules to examine the situation. Eight months after the meeting (and four years after the incident), a study by lower-level technical staff showed the matter to be sufficiently serious to require use of only inert gases in all spent fuel casks (ref. 22). The problem continued to exist due to technical ignorance by the people in charge and the lack of any routine requirement to assess the potential risk of an actual incident.

There may be similar problems today. For example, the potential exists for a serious crush environment during a train derailment,

according to a 1980 NRC-sponsored study, and the forces involved could exceed those experienced in the existing hypothetical tests (ref. 23). NRC considered the likelihood of such forces to be low, however, and took no action. The advent of trains carrying numerous casks increases the chances for a collision between two casks during a derailment, but this scenario has never been examined in a publicly available study. Once again, policy is being made at one end of the authority spectrum (the MRS plan involves numerous rail shipments, each involving multiple rail casks) while a void exists on the impacts of such policies from a technical standpoint.

There also appears to be a missing link between the reportage of problems by licensees and the perception of a trend by those receiving such data. Investigations of human errors in cask maintenance (ref. 18) found that valve problems and excessive surface contamination were routinely reported by users of the same casks but no action was taken to discern the problems. While the individual incidents presented no immediate problems or hazards, each had the potential for greatly complicating a minor accident. In one case, valves had been installed backwards (due to confusing instructions) (ref. 24) and came open in transit. In a separate series of incidents, the surface contamination resulted in "hot spots" on the outside of the cask and trailer (ref. 25). In a minor accident, police or emergency personnel could easily interpret either type of event as a leaking container, leading to an unnecessary (and likely hazardous) evacuation, and possible panic. Only after seven incidents of excess surface contamination with the same cask did NRC authorities take any action (ref. 26) (the valve situation was solved after several occurrences by a utility employee; no action was taken by NRC officials).

Such failure to appreciate possible hazards stems from at least three sources:

- a complacent litany, preached for so long that is easy to believe that there really are no problems
- unless one assumes that there could be multiple simultaneous

errors, it is not hard to conclude that an isolated failing is of no concern

- the lack of a systematic collection and presentation of data on minor incidents precludes perception of any patter of failure.

It is this writer's experience that the often repeated statement that "a cask has never leaked" is believed by many in high circles despite the fact that such incidents have occurred (though they are both poorly documented and did not occur near populated areas). Such statements were heard numerous times before Three Mile Island and are still heard after Chernobyl. Belief in such absolute statements is a convenient form of denial. Similarly, common daily experience does not support the notion that "everything that can go wrong will go wrong" very often, so there is little impetus for always assuming the worst case scenario unless there is a requirement to do so. Finally, NRC did not even start separating out data on transport-related problems from its on-site inpsection reports until 1981. It also has no staff or system dedicated to "tracking" problems with particular containers. Instead, responsibility is divided between a central certification staff concentrating on design and a diffuse inspection staff with quality assurance duties for all nuclear equipment, most of which has little to do with transportation.

ACCURATE DESIGN VS. DEFECTIVE DESIGN: FAILURES AT "SQUARE ONE"

Cask design is a relatively straightforward task involving generally accepted mathematical methods, easily verified by certification staff. Unfortunately, the design process can become complicated by faulty input data not easily verified by federal licensing authorities. Simplifying assumptions can also mask secondary interactions between container materials or potential vulnerabilities of fabrication techniques (e.g., assuming all welds are perfect). The end result can be a "perfect" cask design that will not react properly once

manufactured in the real world. Conservatism is often built into a design to handle possible deficiencies in materials, fabrication or design methods, but it is no guarantee of safety.

One area that requires extreme care is the control of "criticality." In order for uranium to yield its energy, it is necessary to shape it into a configuration that results in a certain concentration of escaping neutrons. When that task is achieved, the fuel puts out radiation that, upon striking a medium such as water, is useable as heat to create steam. Controlling criticality is the essence of harnessing atomic power. Forcing uncontrolled criticality in a very small space is the essence of detonating a nuclear weapon. Accidental criticality is the essence of something in between. There are several cases where criticality control could have been lost due to design errors.

NRC checks the numbers in all design calculations that are part of the application for a cask license. The design study demonstrating regulatory compliance, called the Safety Analysis Report for Packaging (SARP), includes data on stress, temperature, materials specifications, etc. and is often several inches thick. Review time is measured in months and is an iterative process often involving additions to documentation and sometimes changes to design. Rarely, however, does it involve any verification of projected weights for cask parts. In one episode involving a rail cask, the weight of the fuel basket (several tons) was incorrectly estimated by the manufacturer (ref. 27). The casks were in use for seven years before the error was uncovered, not by NRC, but by the designers themselves. They concluded that (in the hypothetical drop test), the basket would buckle, possibly forcing the assemblies together in a configuration conducive to uncontrolled criticality. The net result could have been rapid overheating, severe disruption of the cladding, mixing of the now damaged fuel with the cask water, overpressurization, and opening of the relief valve (dispersing the water as steam, carrying some of the fuel and released gases). Fortunately, the original analysis was

so grossly oversimplified that this error was not large enough to overcome the limits of those calculations. A more sophisticated method, not used in early cask designs, showed that, while the fuel basket would be damaged, it would still maintain its shape sufficiently to avoid criticality. The casks in question were used for nearly 400 shipments before the error was found.

DOE is also empowered to license containers for radioactive materials and must follow certifying procedures "equivalent" to those of NRC. It, too, allowed design problems to occur, some involving criticality, and (again) years passed before the problems were found. DOE certified a dozen spent fuel container designs for its licensees (mainly federal labs and weapons facilities) between 1975 (when DOE's parent, ERDA, was created) and 1982. All were offered to NRC licensees for their use if NRC co-certified the containers. Instead, NRC technical staff found numerous open technical items, analytical errors, documentation deficiencies and other problems. NRC declined to certify <u>any</u> of DOE's casks (ref. 28). A plutonium container was also refused when actual drop tests indicated that its structure could collapse, allowing several inner containers to come into contact during an accident involving a multiple container shipment (typical in plutonium transit) (ref 29). A criticality in such a container could have been catastrophic since the plutonium was often in powder form, ideal for dispersal.

When confronted by these problems, the two agencies agreed to drop the issue; NRC would no longer criticize DOE's containers if DOE simply withdrew its requests for co-certification (ref. 30). NRC did <u>not</u> report these deficiencies to DOT, which has overall responsibility in container regulation. Two years later, DOE again tried to obtain NRC approval for a cask, slated to move spent fuel through New York City. NRC again declined, citing technical issues which DOE attempted to address through design changes to the cask. DOE then initiated use of the container without waiting for NRC to comment on the changes. Only an uproar raised by environmentalists acting through their

Congressional and City officials brought the issue before the DOT, which also has final authority over NRC and DOE in transportation matters. DOT ordered DOE to suspend the container until NRC's prior questions were answered (ref. 31). Not only was DOE unable to do so, but two of its own labs later confirmed that the cask would not maintain its seal under hypothetical accident conditions (ref. 32). Thirteen shipments were made with the modified cask through the City and across the country to Idaho. Even more had been made previously in the South, prior to any alterations. Any one of them could have placed the cask under stresses exceeding its capabilities, due to faulty design. DOE eventually withdrew all of its remaining spent fuel casks from use (as of September, 1987).

The root causes of these various design failures stem from at least five concerns:

1. A lack of a central certification authority - DOE (as of January, 1986) has now withdrawn certification powers from its nine regional offices and centralized it in one Washington office. NRC has its own certification office, and DOT is also empowered to certify (and has done so, though not for spent fuel casks).

2. Use of cask standards as the sole driver of cask design - As long as the regulatory standards are met (i.e., drop, fire and other tests), the designer is free to approach the problems as he sees fit, without any other regulatory specification to meet.

3. Incomplete verification of all design input data - Much of the data submitted in the SARP is accepted as correct (though material specifications, such as yield stresses, may be checked against standard values) since it may be difficult to verify prior to fabrication. Emphasis after fabrication, however, is on completeness of documentation, adherence to design drawings and the integrity of fabrication techniques.

4. Lack of any requirement for full scale testing of an actual cask to the point of failure - Tests are done on scale models (usually checked for perfection in fabrication prior to testing) or by computer models.

5. Lack of any independent multi-disciplinary review group whose purpose is to find flaws and deficiences - Such a group is usually convened only to investigate an accident.

EXPEDIENT DESIGN VS. SAFE DESIGN: ELIMINATING OPPORTUNITIES FOR ERROR

Cask design over the years has appeared to follow two basic tenets: meet the regulatory standard, and make the cask functional for the reactor operators. At no time has there been an effort to make the containers "goof proof." Instead, when problems in handling have arisen, an "administrative control" (i.e., a document detailing a procedure) has been put forth as the answer. In cases where the problem is perceived as potentially widespread, a "regulatory guide" may be issued. Such a guide attempts to translate a rule into an acceptable practice (such as use of a given mathematical formula) but has been sometimes criticized by DOE officials as little more than a "technical band-aid," often compounding the original confusion.

To accommodate the need to drain, fill, vent and relieve a cask, valves on the cask body were introduced despite the fact that each hole drilled for a valve, and each weld for its attendant internal piping, could compromise containment in an accident (if not done perfectly). Similarly, casks were designed using steel and lead (or depleted uranium) sandwiches instead of heavier solid steel or iron walls that would not be heir to the problems of lead (and uranium) casting, but could require special overweight vehicles and permits.

An examination of the proposed cask designs in the Yucca Mountain EA indicates this pattern may be continuing. Instead of utilizing European experience on cast iron casks, DOE again proposes a steel and cast uranium sandwich (ref. 33). This is especially noteworthy since the only firm experienced with large uranium casting left the cask manufacturing business over 5 years ago (ref. 34). Bidders on such a cask design will thus be inexperienced in this area, at least for the early casks they produce. Lead castings have caused problems as well,

but still appear likely to be used if no uranium casting is available.

No attention appears to have been paid to the difficulty in inspecting the cask during or after manufacture. A careful reading of all of NRC's manufacturing reports and related documentation by this writer reveals the following:

- very few casks were ever inspected; usually only the "paper trail" of welder's certificates, materials specifications and drawings was followed
- almost casks were on the road prior to any detailed inspection of the manufacturing facilities or paperwork
- a complete breakdown in one fabricator's quality assurance program occurred, but the casks he produced were allowed to remain on the road (until their defects were discovered years later)
- important welds could not be verified because it is difficult to examine interior welds once a lead or uranium casting is in place; it shields the weld from the inspector's scrutiny, even with electronic equipment.

Other problems also occurred which are related to the design and to resultant fabrication techniques needed to match the cask to the design. For example, in 1979 two casks were found to have bowed inner cavities (the interior layer of the steel and lead sandwich) (ref. 35) but this was only discovered during a routine measurement taken by a utility considering purchase of one five year old container from another user. NRC felt the problem serious enough to permanently withdraw the containers from use. Other fabricating errors have occurred that should have been found in the paperwork. A lead-shielded cask was found (again by a purchaser, not the NRC) to have copper plates welded to its exterior to correct shielding deficiences in the lead casting (ref. 36). Such copper plating was not only not allowed in the cask license, but could have compromised the outer shell's integrity in a fire (due to a reaction between copper and steel at high temperatures). It is unclear how this obvious surface repair also escaped on-site inspections of the cask.

Even when an inspector-in-residence was maintained during recent (1985) production of the casks used to ship damaged fuel from Three Mile Island, numerous cases of non-compliance were later uncovered in the paperwork. A potentially faulty weld was also found on a radiograph and required a special team of experts to analyze it (ref. 37). Their conclusion did not come until the casks were already being loaded for their maiden shipment, which occurred only five days after the weld problem was resolved. NRC had already licensed the container, with the defect, and a major controversy would have erupted if it had been necessary to withdraw certification.

Other defects have been found in the various valves on casks. Some were occasional, but one instance involved a generic failure of an entire production run of special pressure relief valves for a group of rail casks. It appears that defective valves, already replaced once, were replaced again by <u>other</u> defective valves which had never been tested (ref. 38). To settle the problem, the casks were restricted to dry shipments, but only after nearly 400 shipments had been made with defective valves. The valves had been certified operational by the manufacturer but never verified by a third party, such as NRC.

NRC maintains only a small vendor inspection staff (in its Texas office) which is responsible for inspecting all parts and materials for all nuclear operations in the country. Emphasis is given to reactor operations because of the problems and immense safety-related systems at such facilities, so it is not surprising that so many cask-related problems escaped attention. In essence, the nuclear transportation industry is self-policing and uncovers many errors on its own. It is therefore likely that many go unreported to NRC, leading one to the conclusion that such errors are probably more prevalent than indicated by the available documentation.

Designers assumed that anything that could be designed could also be made perfectly (every time), and convenience and flexibility were at

least as important as safety. If any difficulty in handling occurred, it was simply the problem of the cask user and was not a concern for the cask designer.

SLIPS IN THE PROCEDURES

Loading and handling of spent fuel and casks involves a number of steps where human reliability is crucial. As previously indicated, these include choosing the fuel to be shipped, fuel testing, cask inspection and maintenance, and cask loading and testing; vehicle inspections and possible testing are also important. Failures have occurred in all these areas, with varying implications for transport safety. While it is difficult to generalize about these deficiencies, it is safe to say that few have resulted in any effort to eliminate their causes. When a problem appears in the field, an administrative procedure is implemented to handle it; there is very little evidence that any authority has attempted to "chase down" the problem to its source and end it.

One case where some effort was made is the "cask weeping" situation. Weeping is a troublesome phenomenon for cask handlers but rarely affects the public. It involves the release of spent fuel contaminants from the cask surface after it has been washed and inspected. British studies found that a film of traffic dirt adheres to the cask body and absorbs radionuclides from the pool water (ref. 39). During transit, the vibration and exposure to the elements gradually loosens some of this material to the point that it may settle onto the vehicle or collect in cask crevices or surface defects. Swipe tests at the cask receiving facility then show inordinately high contamination levels (sometimes over 100 times greater than the regulatory limit).

This problem can result in a misinterpretation that the cask is leaking (especially when the weeping occurs at the crevices near the cask lid seal or near a valve) and, in one extreme case, caused a

release of radiation to the environment. In that instance, an ill-conceived attempt to affix the contaminants to the cask surface by painting it went awry. During a rainstorm, the paint on the moving cask began to dissolve (it was not waterproof) and it removed the contaminants, resulting in dispersal of contaminated paint on a major interstate highway (ref. 40). While the drivers were aware of the dripping paint, it meant little to them and they continued on to their destination, dispersing the radiation over several hundred miles of roadway, where it washed across the highway shoulder as runoff. No formal action was taken and no fines were levied on this incident, but several meetings between NRC, DOT and cask officials attempted to define the problem. The primary results were suggestions to better clean the cask and, especially, to refine the way in which swipe tests were handled to avoid "overestimation" of removable surface contamination. In Europe, on the other hand, the problem was handled by research into stronger cleansing agents and methods, and the use of a disposable watertight cask "condom" that protects the cask's outer surface while it's immersed in the pool.

Weeping may become more pronounced with future casks since the proposed DOE design shows the organic neutron shield (probably a slightly porous rubber-based compound) residing on the surface of the cask, thereby opening the door to even greater (and possibly cumulative) surface contamination. Neither the DOE Transportation Business Plan (which includes a vague specification for new cask designs) nor any other publicly available document addresses this potential problem.

A different federal approach was seen after pressure by environmentalists, however, when the "near miss" occurred with the 1980 shipment of damaged fuel. As previously discussed, an assembly with cracks in its cladding self-heated in an air environment, causing the fuel pellets to re-oxidize into a fine powder. The problem was a direct result of an error in the choice of fuel to be shipped (ref. 41). The cask license specifies the allowable heat output of an

assembly and the involved plant officials used an accepted NRC formula for calculating the assembly's output. The formula was outdated, however, and the updated version was not known to the plant operators. Had it been available, the operators would have found that the damaged fuel could not be shipped dry. Instead, a serious incident arose which, if accompanied by a failed valve (one was removed from the cask just prior to this shipment), could have yielded a release of radiation without a vehicular accident.

NRC did nothing about this problem until pressed by the author and the Sierra Club. Four years after its occurrence, the problem was diminished considerably by eliminating the air atmosphere from all commercial spent fuel casks and requiring seriously damaged fuel to be sealed in welded cans (fuel with only pinholes can still be shipped uncanned) (ref. 42).

A problem that did not fare as well as either of the above involves proper draining of pool water from casks. At least two cases are detailed in NRC correspondence and inspection reports that involved incomplete or total failure to drain casks, one empty and one loaded. The importance of this procedure arises when one considers the potential for leakage during an accident, especially due to a failed valve or seal. While spent fuel pool water is continuously filtered, it always contains radioactive contamination that could be dispersed as a liquid or as aerosable particles if vaporized during an accompanying fire. While in the cask, the water can also pick up surface crud from the fuel, which can be loosened at relatively low temperatures (above 212°F). The interior of a well-used cask may also contain "hot spots" where past contamination has settled and could be released by water sloshing in the container during transit.

In the first case, contrary to the cask's license (which called for dry shipment), fuel was shipped wet due to accidental reversal of the drain and vent lines during the draining procedure (ref. 43). This error was ascribed to the lack of color-coded labelling on the valves

(the paint had worn off). To avoid this problem in the future, the reactor operator (not the cask owner) inscribed valve numbers onto the cask surface and keyed them to the written procedure for hooking up the lines. Since no verification testing is required, however, the problem could still recur. The particular cask involved was designed to always be shipped dry and the presence of water with a "young" fuel assembly could have resulted (during a fire) in pressurization of the cask, opening the relief valve and venting of the contaminated water as steam.

The case concerning an empty cask involved the same container previously seen in the re-oxidation incident. Having been extensively decontaminated after that problem, the empty cask was shipped to another reactor. Upon opening a valve, a cask handler was contaminated by the excess water left in the container. Later analysis found that a small sample of the cask water gave off very high radiation readings (over 100 r/hr). Note that the cask was empty, so it was under no travel or reporting regulations. Recall that this cask had recently had a defective valve replaced, so again there was potential for a release without a vehicular accident (had the valve not been changed prior to this incident). The cask water proved to be a further problem due to the inexperience of the handler (an employee of the cask owner) who, in violation of normal procedures, drained the fluid into a plastic bag. Unable to fit the bag into a shielded waste holder, he punctured the bag with a screwdriver, allowing release of contamination into the air (he wore no breathing apparatus) and spilling the fluid (ref. 44). One wonders how this action would have been perceived if the cask fluid were found to be leaking in transit. In this case, fines were levied, not against the cask owner, but against the utility since it did not properly supervise the situation. But the problem can still recur.

Another problem related to handling is the potential for damaging fuel in loading and/or in transit. At least seven such incidents (two in the U.S.) (ref. 45) have occurred and the damage was only discerned

upon arrival of the fuel. None of the fuel was damaged prior to loading, so there was no need for it to be canned. As previously mentioned, the release of loose or powdered fuel to the cask interior can create the potential for a release to the environment if accompanied by a failed valve or seal, or a very serious accident that could open a valve or damage a seal. While all present commercial casks require non-air atmospheres, this rule has not been codified (it exists only in the individual licenses of six casks, two of which are no longer available for spent fuel shipments). Unless required by NRC in all new licenses, the potential exists for re-oxidation of fuel that overheats in a future air-filled cask.

Other possible loading scenarios exist that have not occurred (at least to the knowledge of this author). For example, one could imagine a mislabeled gas canister, containing pure oxygen instead of helium. Filling a cask with such a gas could greatly accelerate re-oxidation (and possibly other problems) instead of eliminating that hazard. There is a need - prior to cask licensing - for a full examination of a cask's loading procedures to ascertain all possible errors and design fail-safe procedures or equipment to avoid, or at least detect, the problems before they create a serious potential for risk.

The same need pertains to addressing problems during incidents in transit. Situations have occurred (some not involving spent fuel) that resulted in the mistaken belief that a leak had occurred. In one case, a fire was allowed to contact a container of radioactive gas for over two hours because firefighters had been unnecessarily evacuated from the area (ref. 46). This action calls into question the assumption of a 30-minute fire (one of the cask standards), which is based on an active effort to extinguish (not avoid) a blaze.

Vehicles have also been subject to poor inspection and/or maintenance. Despite design efforts to make a cask trailer strong enough to handle its heavy load, a trailer bed buckled in transit only several days

after an inspection (ref. 47). Trailers are also expected to remain upright during normal transport. In March, 1988, a trailer with an empty cask overturned while making a right angle turn at only 10 mph. Shipments with that cask-vehicle combination have been suspended pending investigation (ref. 48).

Many of the above problems can be ascribed to poor training, poor documentation, poor inspection, poor maintenance, etc. but such answers beg the question: most (if not all) are really the result of a lack of effort to anticipate possible human error and seek ways to eliminate, through planning and equipment design, the ability to cause those errors. While no system can eliminate all human error (some systems even add new opportunities for error), there are ways to reduce the variety of errors and detect others before they are allowed to combine in the manner of a Three Mile Island or a Chernobyl.

CRITERIA AND PROPOSALS FOR IMPROVING HUMAN RELIABILITY SYSTEMS

To overcome all of the deficiencies covered above may not be possible within an acceptable budgetary framework. The following is, however, an unconstrained list of ways that many such deficiencies could be reduced or eliminated, without regard to a specific funding limit.

CRITERIA FOR A SYSTEM TO IMPROVE HUMAN RELIABILITY

1. fuel handling must be overseen and assemblies tracked more closely over their lifetime to ascertain any vulnerabilities, and to verify the appropriateness of their shipment date and containment

2. fuel should be managed to reduce potential leakage and crud dispersal in transit

3. cask designs should assume human failures will occur in fabrication and seek to minimize and simplify human involvement in manufacturing

4. cask design should incorporate ease of use, minimization of maintenance, and limitations on the ability to err during cask handling

5. design criteria in the form of testing standards must be supplemented by more precise requirements to enforce the best design

6. an independent oversight body should have access to all transportation-related facilities and documentation to foster very vigorous enforcement of regulations and specifications

7. computer and scale model testing should be supplemented by actual testing (to failure) of a cask directly off the assembly line

8. manufacturing inspections must be expanded to include closer oversight of fabrication while in progress

9. each cask must be "tracked" from fabrication through use to verify and oversee regular maintenance and problem handling

10. certification authority must be centralized in an agency not responsible for maintaining shipping schedules or budgets

11. simplified and expedited procedures for challenging regulatory actions must be easily accessible to concerned parties

12. cask contents and conditions should be remotely monitorable by cask handlers, drivers and emergency preparedness personnel

13. conflicting regulations and areas of authority or coverage should be eliminated and the highest attainable level of safety be sought as an ongoing goal

14. vehicle standards and quality assurance (QA) must be incorporated under the same QA procedures as the casks so the container and

transporter are dealt with as an integrated unit

PROPOSALS TO IMPLEMENT THE ABOVE CRITERIA

A. create a self-funding mechanism (such as repository and/or shipment fees) dedicated to minimizing risks of both transportation and stationary operations

B. establish an independent "watchdog" panel to maintain an ongoing investigatory presence around all federal agencies and private contractors in this area

C. set up a database and "tracking" system to monitor fuel and casks through their life cycles

D. utilizing independent contractors, develop and press for improved cask testing and design standards and a cask specification that pays attention to avoiding problems in design, manufacturing, maintenance and operation

E. seek adoption of highest radiation protection standards (i.e., ALARA) and seek ways to implement them

F. press to incorporate QA standards for vehicles in the cask license

G. call for development of a transponder <u>inside the cask</u> to radio information on cask contents and conditions prior and during shipment

H. urge that standards for cask and fuel cleanliness be part of the cask license

I. press for an improved cask fire standard and inclusion of an on-board automatic fire suppression system for transport vehicles (especially for rail transport)

J. lobby for a realistic crush test that simulates collision of two rail casks

K. supplement some of NRC's inspection functions with state personnel to expand container oversight at all stages

L. if OCRWM will not mandate full-scale cask tests, purchase a typical cask and trailer and test them to failure

M. create a transportation "cookbook" covering cask inspection, maintenance, and all other aspects of transportation, for state enforcement and emergency personnel to utilize as an independent, simplified resource for aggressively maintaining compliance

N. develop state laws and regulations that "fill in" any gaps or gray areas in federal regulations

O. obtain and utilize a mobile enforcement van/lab for hazardous materials handling and shipping; use it to perform random, very detailed checks on containers and vehicles as well as emergency response

P. set up an impoundment facility to hold containers and vehicles that do not comply with regulations, and utilize it to document infractions.

RECOMMENDATIONS TO THE STATE OF NEVADA

All of the above proposals can be considered as suggestions for actions by the State of Nevada over the long term. Most, however, require an approach by the State to begin preparation for "aggressive compliance enforcement." Such a stance does not in any way connote acceptance of Yucca Mountain as a home for a final repository. Rather, it creates a set of goals for handling hazardous materials transportation simply passing through the state.

Once a decision has been made to take this approach, the first step is to establish a nuclear materials transportation engineering office in the appropriate state agency to focus and collect the technical resources necessary to deal with transportation issues specific to this area.

A legal approach must also be taken to determine all areas of regulation open to the state beyond the usual minimum often stated by U.S.D.O.T.

Enaction of a shipments tax is essential to fund these activities and has already been upheld by DOT in the case of Illinois, despite challenges by DOE.

The aggressive approach and these three suggestions are essential to implementing any of the more detailed proposals in this report. Nevada is in an excellent position to seize the initiative in this arena, especially in light of the shift in control from DOE to NRC. While NRC is far from perfect, it is more sensitive to well developed technical and political pressures than DOE and has rules and a history of vulnerability open to public intervention.

Nevada should begin to marshal and expand its forces on this issue so it will be in a leadership position when the cask design process begins in earnest over the next few years. By taking a positive approach to spent fuel transport now, the State will find numerous avenues for legal intervention open to it in the future.

REFERENCES

1. "Beyond Design-Basis Accidents in Spent Fuel Pools," Brookhaven National Laboratory, January, 1987 (draft, no NUREG number assigned)

2. NUREG/CR-0163, "Comments on Fuel Crud as a Safety and Operational Factor of Independent Spent Fuel Installations," November, 1978

3. NRC Research Information Letter No. 139, March 5, 1984

4. Safety Analysis Report for Packaging, Docket No. 71-6698, NAC-1 cask, 1972

5. OCRWM Bulletin, DOE/RW-0153, December, 1987/January, 1988

6. telephone communication between Lindsay Audin and Lake Barrett and William Lake of OCRWM, April 28. 1988

7. DOE letter to DOT and accompanying legal memo, March 7, 1980

8. DOE letter to NRC, May 31, 1983

9. NUREG-0561, "Physical Protection of Shipments of Irradiated Nuclear Fuel," June, 1979

10. 49 CFR 173.22(d)

11. RAMRT printout report, DOT, Nov. 3, 1986

12. "Standards for Protection Against Radiation," Federal Register, 51FR1092, June 9, 1986

13. "Decision on Appeal from denial of non-preemption determination," DOT Docket No. NPDA-2, p. 11, December 23, 1986

14. 10 CFR 71.45(b)(1) (January 1, 1986 edition)

15. 49 CFR 393.100(c)

16. NUREG/CR-0743, "Transportation of Radioactive Materials in Urban Environs," draft environmental assessment, Sandia National Laboratory, 1979

17. PNL-2588, "An Assessment of the Risk of Transporting Spent Nuclear Fuel by Truck," Battelle Pacific Northwest Laboratory, November, 1978

18. "A Review of the Effects of Human Error on the Risks Involved in Spent Fuel Transportation," Nebraska Energy Office, December, 1986

19. NRC Inspection Report 50-206/80-26, January 21, 1981

20. meeting between Lindsay Audin and Charles MacDonald, NRC chief of cask certification, and two techical assistants, September, 1983

21. "Uranium Dioxide: Properties and Nuclear Applications, Atomic Energy Commission, circa 1960

22. NRC Decision DD-84-9, April 13, 1984

23. NUREG/CR-1588, "Potential Crush Loading of Radioactive Materials Packaging in Highway, Rail and Marine Accidents," October, 1980

24. letter to NRC from Wisconsin Electric Power Co., June 21, 1977

25. NRC Inspection Report 50-219/81-03, April, 1981

26. NRC Order to Show Cause, Docket No. 71-6698, July, 1981

27. GE letter to NRC, Docket No. 9001, September 7, 1982

28. "A Review of the Effects of Human Error on the Risks Involved in Spent Fuel Transportation," Nebraska Energy Office, December, 1986

29. NRC letter to DOE, Docket No. 71-4960, March 13, 1980

30. DOE letter to NRC, May 31, 1983

31. DOT letter to DOE, March 23, 1985

32. NRC meeting memo, "Summary of Meeting Concerning MH-1A Cask Design", November 29, 1985

33. DOE/RW-0073, Yucca Mountain Environmental Assessment, May, 1986, Appendix p. A-13

34. Complaint in U.S. Claims Court, No. 229-83C, filed April 7, 1983

35. NRC Order to Show Cause, Docket No. 71-6698, April 4, 1979

36. NRC Inspection Report 99900331/79-01, August 31, 1979

37. NRC memo, Docket no. 71-9200, July 16, 1986

38. GE letter to NRC, Docket no, 9001, June 2, 1981

39. "Contamination Studies on Pond-Loaded Casks," PATRAM '83, p. 929

40. letter to NRC from Nuclear Assurance Corp., Docket no. 71-6698, April, 1979

41. "Airborne Contamination Released During Unloading of a Failed PWR Spent Fuel Assembly," PATRAM '80, p. 646

42. NRC Decision DD-84-9, April 13, 1984

43. letter to NRC from Duke Power Co., Docket no. 71-9010, December 1, 1981

44. NRC Inspection Reports 50-213/80-20 and 50-219/80-38. April 1981

45. Preceedings of PATRAM '83, p. 806, May, 1983

46. National Transportation Safety Board Study NTSB-HZM-79-3, p. 8, November 13, 1979

47. NUREG/CR-0744, "Identification and Assessment of Social Implications of Transportation of Radioactive Materials in Urban Environs," 1979

48. letter to NRC from Nuclear Assurance Corp., Docket no. 71-9010, March 14, 1988

Appendix D

Summary of regulatory and private institution responsibilities in the transportation of spent fuel and other high level radioactive wastes.

D.1. Acronyms

AAR - Association of American Railroads
BMCS - Bureau of Motor Carrier Safety (DOT)
CERCLA - Comprehensive Environmental Responsibility, Compensation, and Liability Act (1980)
DOD - Department of Defense
DOE - Department of Energy
DOT - Department of Transportation
EIS - Environmental Impact Statement
EPA - Environmental Protection Agency
ERDA - Energy Research and Development Administration
FAA - Federal Aviation Administration (DOT)
FEMA - Federal Emergency Management Agency
FHA - Federal Highway Administration (DOT)
FIA - Freedom of Information Act
FRA - Federal Railway Administration (DOT)
GAO - Government Accounting Office
HMIS - Hazardous Material Information System (DOT)
HMTA - Hazardous Materials Transportation Act (1972)
IAEA - International Atomic Energy Association
ICC - Interstate Commerce Commission
IMO - UN International Maritime Organization
INPO - Institute for Nuclear Power Operations
MCASP - Motor Carrier Safety Assistance Program
MTB - Materials Transportation Bureau (DOT)
NRC - Nuclear Regulatory Commission
NRT - National Response Team
NWPA - Nuclear Waste Policy Act (1982)

OCRWM - Office of Civilian Radioactive Waste Management (DOE)
OSHA - Occupational Safety and Health Administration
OTA - Office of Technology Assessment
RAMRT - Radioactive Materials Routing Report
RSPA - Research and Special Programs Administration (DOT)

D.2. Design Phase

D.2.1. institutional structure

• Federal - radioactive shipments treated in much the same manner as other hazardous wastes. Reliance on technical safeguards - containers. Using this rationale, regulators need not impose any significant treatment on handling and transportation of radioactive materials.
• CERCLA - 1980 - provides the authority for Federal emergency response assistance when major hazardous materials disasters occur.
• DOT - international regulations and standards often used instead of DOT regulations or when no DOT regulations exist. Especially water and air - also because of potential crossing of international boundaries.
• DOT - HMTA, 1975 - "intent to improve regulatory and enforcement activities by providing secretary of DOT with broad authority to set regulations applicable to all modes of transport". DOT has primary responsibility for radioactive materials transport. HMTA authorized both interstate and intrastate regulation but hazardous materials transport intrastate not governed by most regulations.
• RSPA - Materials Transportation Bureau [MTB] is the lead DOT hazardous material agency - except bulk transport by water. This is done by coast guard. RSPA regulations for water transport apply to nonbulk shipments only [49 CFR 176.5]. DOT modal administrations regulate their areas of concern - FRA, FHA, Coast Guard. Since 1976 most regulations have not been changed by MTB. It is responsible for enforcing regulations governing irradiated fuel shipments.
• DOT - reliance on industry and technical input for development and implementation of regulations.
• Federal Railroad Safety Act of 1970 - to promote safety in railroad operations. Includes issues related to nuclear materials safety.

• Coast guard regulates bulk transport by water.
• NRC - three offices concerned with the transportation of radioactive materials: 1) Office of Nuclear Materials Safety and Safeguards, Transportation Certification Branch, evaluates the design of packages for high level radioactive waste and spent fuel; 2) Office of Inspection and Enforcement has responsibility for the inspection program and procedures for the transportation activities of NRC licensees, including fabrication and use of casks. The office also provides training to the inspectors from the regional offices; 3) Office of Nuclear Regulatory Research, Transportation Research Branch, contracts for research and is responsible for writing regulations.
• DOE - NWPA 1982 - will be responsible for movement, storage, and disposal of all commercial high level radioactive waste beginning in 1998. Responsible for moving waste from utility site to repository or MRS facility.
• DOE - Although DOE is required to use standards and procedures equivalent to those of NRC in the container certification process, when DOE has chosen to exercise its own authority to use casks and procedures other than NRC approved, substantial conflict between DOE, states, and concerned citizens has occurred. DOE uses equivalent but not identical procedures for shipments as the NRC's. DOE says that future NWPA shipments will comply with both NRC and DOT regulations.
• DOD - has authority similar to those of DOE to use equipment and procedures equivalent to NRC's. DOD materials transported by government or commercial contractors must be in accordance with DOT and NRC regulations. DOD shipments are subject to DOD rules which are similar to DOT and NRC rules. The RSPA recognizes DOD regulations - 49 CFR 173.7, 177.806
• OSHA - prohibited from exercising authority where other Federal agencies exercise regulatory authority [OSHAct, 29 USC 653 (b)(1)].
• state and local - regulations over transportation and transshipment system mostly preempted by DOT [HMTA] and NRC regulations.

D.2.2. interagency coordination

• DOT modal administrations - FRA, FHA, FAA - Little coordination despite monthly meetings. Appropriate agencies deal with specific modal issues;

and interagency coordination (multi-modal) not effectively coordinated. RSPA is the DOT office responsible for liaison with other federal agencies.

- DOT - NRT [National Response Team] - Memoranda of Understanding provides only formal mechanisms for interagency coordination of regulatory matters.
- NRC-DOT 1973 Memorandum of Understanding - enforcement of cask standards and shipping rules.
- DOT - DOE - The DOT has granted authority to the DOE to approve the packaging and certain operational aspects of its research, defense, and contractor-related transportation of fissile and highly radioactive materials.
- DOT-DOE - memorandum of understanding, 18 Nov., 1985 concerning the transportation of radioactive material under NWPA. It delineates responsibilities and establishes common planning assumptions between RSPA and OCRWM for the implementation of NWPA. The four main points are: transport management under NWPA resides with OCRWM and transportation of nuclear materials will be in compliance with DOT regulations. OCRWM will also comply with state and local laws and regulations not inconsistent with HMTA; the transportation of spent fuel from DOE related activities to any NWPA site will be subject to applicable DOT regulations; RSPA and OCRWM will exchange information and support within areas of interest; and common area of interest is the development of effective transportation safety , regulatory compliance, and inspection policy. Should address preshipment, enroute, postshipment phases and allow utilization of Federal and State resources.
- NRC - DOE - memorandum of understanding concerning spent fuel and high level waste transportation packaging, 14 Nov. 1983. DOE will use packaging approved by NRC for NWPA shipments from NRC facilities to NWPA facilities. Includes procedures for consultation and information exchange to resolve issues on packaging design, testing, and certification.
- DOT-NRC 1979 memorandum of understanding - 44 FR 38690, July 2, 1979. The DOT is responsible for regulating safety in the transportation of all hazardous materials. The DOT is concerned with carriers and the conditions of transport of radioactive materials. The NRC is responsible for regulating safety and the receipt, possession, and transfer of radioactive

materials. In particular, the NRC is concerned with who uses and possess radioactive materials (Type B), and establishment of national safety standards, regulating, reviewing, and certifying designs and manufactured packages used in transportation, and also security. The NRC is the lead agency for investigating the cause of leakage in accidents or incidents and preparing a report of the investigation.

• FEMA / NRT - coordinate emergency response.

D.2.3. federal - state - local consistency procedures

• DOT - HM164 appendix: policy guidance for state and local authorities for establishing requirements consistent with Federal law and regulations (also 49 CFR 107 subpart C).

D.2.4. public participation

• NRC - public provided with access to NRC information (FIA) and opportunities to know about NRC decisions and policies [10 CFR 9]. Requirements for EIS's, environmental reports and administrative procedures for materials licensing, and administrative procedures for public communication [10 CFR 51].

• DOE - requirements under NWPA.

D.2.5. route planning criteria

• RSPA - established national highway routing rule for radioactive material [49 CFR 177.825] Appendix A of 49 CFR 177 provides a DOT policy statement on the relationships between Federal, State, and local routing requirements. Routing rule: DOT Docket HM-164, 19 Jan. 1981, 46 FR 5316. Promulgated to preempt large number of state and local proposed or actual legislation to ban or restrict transport of radioactive material through their jurisdictions. After much public comment DOT decided that "the public risk in transporting these materials by highway are too low to justify the unilateral imposition by local governments of bans and other severe restrictions" [Office of Technology Assessment 1986: 165]. When DOT - HM-164 was issued [49 CFR 177.810] was amended to exclude shipments of radioactive materials so that states could "evaluate the site-specific risks involved over various routes without being hampered by locally imposed constraints which may be counterproductive" [46 FR 5308, 19 Jan. 1981] [Office of Technology

Assessment 1986: 164]. But DOT realized need for minimizing risks from shipments by requiring carriers of all placarded radioactive materials to: operate on routes that minimize radiological risk [49 CFR 177.825(a)]; and carriers of high level radioactive waste must operate over a "preferred" route selected to reduce transit time. Either on interstate highway systems (including interstate bypass if available) or an alternative selected by a state designated routing agency in accordance with DOT guidelines. FHA - states and municipalities are preempted from restricting radioactive waste transport through tunnels used for mass transport despite safety concerns. BMCS requires radioactive materials be exempt from avoiding populated areas, tunnels, etc. [49 CFR 397]. DOT rules governing routing of all radioactive materials replicates NRC general routing requirements and also preempts non-federal regulations/laws which require additional security or safety features: additional guards, prior notification, time constraints, different modes of transportation, extra safety features. Replaced earlier rule [49 CFR 397.9] for all hazardous materials which required avoidance of populated areas whenever possible. Hm-164 exempts radioactive materials. "As a result, all hazardous materials *except* radioactive shipments must avoid urban areas if possible" [Resnikoff 1983: 150]. HM-164 challenged in court by New York City and other ways of preempting it have been tried by Michigan.

- FRA - carriers must forward shipments of hazardous materials within 48 hours after acceptance at originating point, receipt in any yard, transfer station, or interchange point. Also issue of special trains would affect routing (see section D.2.6).
- FHA - general requirement - transport without unnecessary delay from loading at origin to arrival at destination.
- Coast Guard - regulations affecting navigational requirements for inland waters, navigational aids [33 CFR Chapter 1].
- NRC - NUREG-0561 July 1979. Rule concerning routing of rad waste shipments. Avoid certain high population areas, extra security under certain conditions needed, contact with local authorities be established. Rules introduced to decrease likelihood of sabotage. Also safety rationale used.

• US Army Corps of Engineers - regulations concerning navigational activities in waterways [33 CFR part 209].

D.2.6. transport mode selection criteria

• ICC - intervened on special train issue because of illegal constraints on interstate shipping. ICC rules desired by ERDA and nuclear industry. Court decisions (ICC, ERDA, and utilities against railroad companies) affirm common carrier status for spent fuel transportation and eliminate AAR and railroad recommendations and requirements for special trains.

• Association of American Railroads, AAR - recommended special trains. Railroads and rules governing their use have been suggested. Companies are planning to use them and issuing special regulations. Court decisions (ICC, ERDA, and utilities against railroad companies) affirm common carrier status for spent fuel transportation.

D.2.7. hazard communication

• DOE - requirements under NWPA.

• DOT hazard classification assumptions: most accidents involve fire, only acute health effects need to be considered, only people nearby accident affected. Hazard classifications provide essential information about cargo to emergency response personnel. The agency has rules for designs, provision, and affixing placards, requirement to specify UN/NA identification number on some placards.

• UN International Maritime Organization (IMO) - establish requirements for classification. International Maritime Dangerous Goods [IMDG] Code. Used for marking, labeling, and placarding.

D.2.8. repository and temporary storage site design and selection

• DOE - requirements under NWPA.

D.2.9. emergency response system planning

• Federal government offers no guidance about who offers what kind of training for emergency response or how much it will cost.

• DOE - maintain authority for planning and program development for emergency response, notification, technical assistance and advice, and involvement in response activities for radiological spills. DOE has 30 regional response teams for responding to radiological incidents.

• NRC has no rules governing local emergency response preparedness for transportation of spent fuel.
• NRT (National Response Team) - Federal coordinating group with primary concern for emergency response. Composed of representatives from 12 federal agencies with environmental and health responsibilities. NRT is chaired by EPA and Coast Guard is vice-chair. 13 regional response teams formed by NRT regional representatives of NRT agencies and states - provide the regional mechanism for emergency response planning and coordination of technical assistance during response activities.
• FEMA - In 1979 FEMA published a guide on local emergency response plans for a transportation accident. Compliance is voluntary. Other than publishing guides and handbooks the role of the federal government has been small (some training). Federal Radiological Preparedness Coordination Committee - formed by FEMA in 1982 . 10 Regional Assistance Committees to help state and local authorities develop emergency plans. Federal Emergency Response Plan [FRERP - 49 Federal Register 35896, 12 Sept., 1984].
• FEMA - responsible for establishing Federal policies for, and coordinating, all civil emergency planning, management, mitigation, and assistance mechanisms of Federal executive agencies. Coordination of Federal and State participation in emergency response procedure development [Executive Order 12148, 20 July, 1979]. Responsibility for development of interim Federal Radiological Emergency Response Plan [49 FR 35896]. FEMA established the Federal Radiological Preparedness Coordinating Committee [FRPCC] to assist State and local agencies in developing emergency response plans. The subcommittee on Transportation Accidents (DOE, NRC, FEMA, other Federal and State agency representatives) issued the guidance document Guidance for Developing State and Local Radiological Emergency Response Plans and Preparedness for Transportation Accidents in 1982. It provides a basis for state and local governments to develop emergency plans and improve preparedness for transportation accidents involving radioactive materials.
• State and local governments have primary responsibilities under FEMA's response plan. Federal assistance to be made available only if specifically requested.

• DOE - OCRWM Bulletin, Sept. 1987 has info on transportation emergency response capabilities.
• state and local - focus mostly on accident prevention , emergency response, and public safety. Focus on routing, permits, and licenses and on highway and railroad.

D.2.10. research - standard development

• DOE
• NRC
• DOT
• national laboratories
• contractors

D.2.11. cask design

• DOT - hazard classification assumptions affect design standards.
• DOT - regulations allow DOE or NRC certified casks for commerce. 49 CFR 173.398 - performance criteria for accident conditions for Type B containers - drop test, puncture test, thermal exposure, water immersion. Spent fuel Type B package designs require prior approval by the NRC [49 CFR.393(a)]. Regulations recently revised [10 CFR 71, 5 August, 1983] so Type B standards to be consistent with IAEA 1973 guidelines. Following international guidelines, Type B containers are used for spent fuel transportation. Based on performance standards. Type B containers are required to withstand severe accident conditions - provide safety largely independent of procedural and other controls on the shipment. Properties for packages considered include leak resistance, corrosion resistance, absorption rate, cushioning, and resistance to explosives [49 CFR 173].
• FRA - administrative law judge ruled that DOT has jurisdiction over safety requirements in packaging - in case concerning use of special trains.
• NRC - approve and certify cask designs. Standards for Type B containers, and certify designs used in construction [10 CFR 71]. The Office of Nuclear Material Safety and Safeguard, Transportation Certification Branch evaluates designs. (Performance standards are specified by NRC and used by cask designer for design requirements for the container. They specify how a cask must perform under special conditions, tests, and

environments. Performance criteria for containers - not specific design requirements - to remove need to predict specific accident scenarios and to provide engineering test specifications for impact, puncture, temperature, immersion, and seal that encompass types of conditions that occur in an accident. Requires detailed structural, thermal, and nuclear safety analyses, computer modeling, and scale model or full scale tests. Engineering Test Conditions - encompass real accident conditions. Are supposed to exceed actual accident conditions.).

- DOE must comply with NRC standards.
- IAEA - package design guidelines.

D.2.12. criteria for maintenance and quality assurance

- NRC - is primarily concerned with inspection and enforcement in areas defined by DOT-NRC memorandum of Understanding. Standards for the inspection of cask licensees. Other quality assurance instructions and inspection requirements [10 CFR 71].

D.2.13. design of support and transportation equipment

- DOT modal administrations - general safety requirements.
- coast guard - bulk transport, rules governing design of commercial vessels [46 CFR parts D, I, N, O].
- NRC - standards for licensees
- AAR - among other things publish equipment standards and specifications.

D.3. Implementation Phase

D.3.1. registration programs / licenses / certification

- RSPA - authority to create registration program for hazardous material shippers, carriers, and container manufacturers but has not done it - no complete record of firms regulated or their locations.
- BMCS - provide safety ratings of carriers.
- ICC - motor carriers must have ICC operating authority. ICC regulations vary with type of transportation but generally include certification of rates, adequacy of service, purchases, and mergers. Grants operating

authority (certification and licenses) to freight forwarders, trucking companies, and water carriers. [Relevant regulation CFR Title 49, Chapter 10, Subchapter D].

• NRC - requires carriers, shippers, and other nuclear facilities to hold licenses as temporary possessors of spent fuel. This provides a modicum of control/responsibility allocation during emergencies. Requirements for license applications (package description, package evaluation, quality assurance) [10 CFR 71]. Regulates licensees and certification of shipping casks. Certification of container standard compliance [for performance criteria]. Office of Inspection and Enforcement licenses cask manufacturers and users.

• DOE must comply with NRC procedures for cask certification.

• UN International Maritime Organization (IMO) - establish requirements for certification and description of materials. International Maritime Dangerous Goods [IMDG] Code.

• AAR - certifies construction and repair shops for rail industry.

D.3.2. data collection

• Enforcement agencies - use reported release experience to determine which shippers and carriers to inspect. Validity of criteria depends on reporting compliance.

• DOT - by law annual report on the safety of hazardous material transportation. Includes: statistical compilation of any accidents and casualties involving the transportation of hazardous materials; and an evaluation of the effectiveness of enforcement activities and the degree of voluntary compliance with applicable regulations. Compiles data on completed highway shipments. In addition, DOT maintains the Radioactive Materials Routing Report [RAMRT]. Data may not be recorded as long as one year after shipments because in some cases regulations do not allow release of routing information until after entire shipment completed.

• DOE - maintains list of all high level waste shipments.

• other Federal agencies, modal administrations and state agencies - collect data on flows, vehicular accidents, inspection reports, and hazardous material transport releases and incidents.

D.3.3. rates and tariffs

• ICC - Railroads should offer common carrier service under published rates and subject to the same transportation conditions as any other commodity - such as transport in regular trains with other cargo.
• ICC - regulates economic aspects of interstate surface transportation including trains, trucks, inland waterway and costal shipping, freight forwarders. Must ensure that rates and services are equitable and reasonable. [Relevant regulation CFR Title 49, Chapter 10, Subchapter D].
• ICC - Railroads should offer common carrier service under published rates and subject to the same transportation conditions as any other commodity - such as transport in regular trains with other cargo.

D.3.4. cask fabrication

• DOT - requirements concerning the manufacture and fabrication of packages in radioactive material transportation [49 CFR 171].
• NRC - Most effort of NRC so far has been on cask construction. Make sure quality assurance procedures implemented for manufacturing of casks.
• Private companies - manufacture casks.

D.3.5. cask testing and quality assurance

• NRC - Tests to be applied sequentially - drop, puncture, exposure to heat, and water immersion. Test conditions may be satisfied by computer analyses, model testing, full scale tests, or some combination [10 CFR 71]. The NRC monitors the quality assurance programs of its licensees for the construction of spent fuel shipping casks. The NRC also has regulations to establish procedures and requirements for reporting defects in nuclear components and materials and for non-compliance with manufacturing standards. Manufacturer's and suppliers must identify and report faulty transportation related products [10 CFR 21].
• IAEA - package testing and inspection procedures.

D.3.6. support equipment construction

• BMCS - tank truck manufacture and maintenance.

• FRA - enforces regulations concerning transport of hazardous materials by rail (manufacture and maintenance).
• coast guard - bulk transport, rules governing equipment of commercial vessels [46 CFR parts D, I, N, O].
• AAR - develops standards for railroad industry. Certifies construction and repair shops.

D.3.7. support equipment testing and quality assurance

• DOT - modal administrations. Requirements concerning the testing of packages in radioactive material transportation [49 CFR 171].
• FEMA - Federal Radiological Preparedness Coordinating Committee [FRPCC] to assist State and local agencies in developing and testing emergency response plans.
• AAR - develops testing requirements.

D.3.8. driver training

• DOT - Radioactive waste transportation driver training requirements are fairly general. The DOT provides no advice on training. As supplement to HM-164, regulations were promulgated on driver training requirements. They are supposed to be "consistent with that for cryogenic (very cold) liquids" [Resnikoff 1983: 172]. However, regulations for cryogenic liquids never implemented. Driver training requirements apply to interstate transportation only; there are no specific requirements for driver training for intrastate transportation. BMCS is the bureau within DOT with prime responsibility for motor vehicle driver training authority. Open book written exam required. Passing not required. No provision for driver disqualification based on cumulative record of convictions and apply only to driver of commercial vehicle operations and on-duty offenses. Regulations also require biennial written examinations to be administered by the carrier (not DOT) on DOT radioactive material regulations, properties, and hazards of radioactive materials, and emergency procedures in case of an accident or other emergency. None of the training provided by DOT prepares drivers to protect public health or safety in event of an accident - they are only related to security measures. Unlike NRC, DOT has not written a guide (NRC Regulatory Guides). DOT official has

stated that most training takes place on the job. Drivers must satisfy general requirements in reading and speaking English (read signs and signals, communicate with public), determine status of cargo (tied down properly, located on vehicle properly, etc.), and pass a road test given by the carrier and written exam on Motor Carrier Safety Regulations [49 CFR Part 390-397]. No standardized tests on hazardous materials to supplement other driver training. DOT official stated that it would be discriminatory to ask specific questions about materials that will be transported. Rail and barge training requirements are even less specific [49 CFR Subpart A, 134.7]. FRA is responsible for enforcing DOT rail regulations. US coast guard is responsible for barge. Because all the regulations are nonspecific it would be difficult to determine noncompliance. DOT - RSPA - FHA - drivers of high level rad waste transport are required to receive written training.

- NRC - None of the training provided by NRC prepares drivers to protect public health or safety in event of an accident - they are only related to security measures (just like the DOT). Publish a guide (NRC Regulatory Guides) concerning training.
- States - requirements vary a lot.
- Carrier - responsible for making regulations effective by providing adequate instruction to employees. Regulations also require biennial written examinations to be administered by the carrier (described above, DOT). Road tests are to be administered by carrier. Railroads have been better at training their employees with respect to radioactive waste transportation. The training programs contain elements concerning hazardous materials. Conrail has a rule book, CT 225, which describes the preparation of all types of materials for shipment. Barge carriers are responsible for training their personnel too.

D.3.9. support personnel training

- modal agencies, carriers, and utilities provide training to their employees.

D.3.10. emergency response system implementation

- RSPA - does not respond directly to transportation accidents, but publishes information source, Emergency Response Guidebook.

• DOD teams available, but mainly for responding to nuclear weapons incidents.
• states - responsible for establishing emergency response teams, coordinating communications, and reaching agreements for coordinating procedures with municipalities and neighboring states. [Resnikoff 1983: 234] describes state agency responsibilities for preparedness for transportation accidents. State authority for emergency response is generally fragmented and varies from state to state. Similarly for local level. Rural communities generally give responsibility to fire or police department. Many urban and metropolitan area public safety organizations - fire and emergency service / civil defense - have developed or are in the process of developing special competence to respond to accidents. Local preparations are often limited to dissemination of information to public and having some trained personnel. Urban and metropolitan areas usually have specially trained and equipped teams. Rural areas usually assign such duties to the fire or police department.
• INPO - Institute for Nuclear Power Operations - has established a voluntary agreement including 42 utilities to provide assistance in the event of a radioactive materials accident, including transportation accidents or incidents. It is a nonprofit organization formed by electric ultilities in 1979 after TMI.

D.3.11. emergency response training

• Emergency response and enforcement training programs must be compared with numbers of personnel needing training, funds, and availability of courses in order to determine how effective they really are. Few personnel have actually received training.
• DOT - offers some training courses.
• NRC - through Oak Ridge Associated Universities offers courses in health physics for Federal, state, local, and industry personnel. Discuss radiation accidents, role of health physicist in medical emergencies, personnel decontamination and protection, environmental monitoring, and environmental sample preparation.
• DOE - emergency response training for state and local police and fire personnel.

• FEMA - Offers some training courses for fire, police, and civil disaster personnel, and the maintenance of an Interagency Radiological Assistance Plan formed in 1961.
• NRT - Federal leadership in emergency response training is not available despite interagency communication via NRT. In 1985 NRT established a special training committee to identify gaps, problems, and duplicative activities and to recommend training programs and alternatives.
• States, Local - volunteers are about 85% of firefighters (with about a 25% turnover per year), other 15% are paid employees of municipal, local, or county government. Police personnel are the second largest group involved in emergency response. May be the first on scene of a hazardous materials accident. Health care and civil defense personnel may respond too. Civil defense personnel receive training in radiological response. Do not always have appropriate equipment.
• INPO - Establish industry standards for personnel and training.

D.3.12. maintenance and quality assurance program implementation
• DOE -
• NRC - quality assurance for casks. Require licensees to develop quality assurance programs in fuel handling activities.
• carriers and utilities - must develop quality assurance programs for their employees and equipment. They must also maintain their equipment to federal and state requirements.

D.3.13. enforcement system implementation
• Federal grant programs offer no direct support for local inspection and enforcement programs.
• Motor Carrier Safety Assistance Program [MCASP] - funds state enforcement and regulatory enforcement for highways. Administered by Bureau of Motor Carrier Safety. To help states enforce motor carrier safety regulations and increase safety inspections for commercial vehicles, both interstate and intrastate.
• State activities fragmented - police, terminal inspection, radioactive materials inspection. May become NRC Agreement states: the Agreement

Program grants regulatory and enforcement authority to States over activities (including shipping) related to some types of radioactive materials (byproduct materials - radioisotopes, source materials, small quantities of special nuclear materials).

D.3.14. enforcement training

• Emergency response and enforcement training programs must be compared with numbers of personnel needing training, funds, and availability of courses in order to determine how effective they really are.
• Federal agencies train their own inspectors and enforcement officers. Some Federal training programs are directed at state and local personnel.
• DOT - RSPA - enforcement and inspection focused mostly on container manufacturers, reconditioners, and testers. DOT/RSPA has specific courses for training enforcers and enforcees.
• NRC - Inspectors are in three program areas - reactors, fuel facilities, and transportation related. NRC training courses for transportation and packaging. Training for Federal and State employees. Regional offices and Office of State programs also offer courses on transportation of radioactive materials.
• DOE - as shipper and carrier, provides compliance training for employees. Commercial carriers and other government personnel may attend as space permits.
• DOD - as shipper and carrier, provides compliance training for employees.
• State - activities becoming increasingly important in the area of training highway enforcement personnel and to educate shippers and carriers about regulations because Federal inspection capabilities have been decreasing.

D.3.15. violation reports

• incentive is to avoid civil or criminal penalties. Often insufficient to deter violations.

D.3.16. penalties

• DOT - authorized by HMTA to assess civil and criminal penalties.
• NRC - Authority to impose fines for regulatory violations.

D.4. Operations Phase

D.4.1. contracts

• shippers - contracted by utility and have the responsibility to contract a competent carrier.

• carriers - contracted by shipper. Responsible for complying with state, local, and federal traffic regulations that govern a mode of transportation. Very few regulations directly on carriers by agencies.

• FHA - contract, common, and private carriers regulated.

D.4.2. shipping papers

• DOT - shipping papers to accompany shipment. Special requirements apply to radioactive materials [49 CFR 172.203(d)]. Shipping papers must include a certificate signed by the shipper [49 CFR 172.204]. Carriers may not accept for transport any packages that have not been properly certified by the shipper pursuant to 49 CFR 172.204. Used as evidence that packaging is in accordance with regulations. For nonbulk water transport carriers must prepare dangerous cargo manifest which must be kept in designated holder on or near vessel bridge.

• carriers must prepare and carry appropriate shipping papers based on shippers' shipping papers

• shippers - responsible for paperwork and permits.

D.4.3. route selection

• NRC - approval is required for routes for shipments needing physical protection during transport, but the routes must be compatible with DOT regulations. Shipper and carrier requirements for planning and scheduling, and obtaining approval prior to shipments for routes [10 CFR 73.37].

• carriers must prepare written route plan.

• Shippers - responsible for route selection. Must comply with DOT and NRC regulations.

D.4.4. notification of shipment

• DOT - requires postnotification of many shipments of high level radioactive materials - according to which regulations.

• NRC - congressional mandate made public disclosure of routes twice a year mandatory and governors receive prior notification of certain nuclear shipments [10 CFR 71] and licensees must provide advance notice for certain nuclear shipments. Information must include name, address, and telephone number of shipping organization, and a description of the material, and estimated arrival and departure times at state boundaries Licensees must notify regional NRC offices. Shipper and carrier requirements for prenotification to states along transportation route because of potential for accidents [10 CFR 73.37].
• DOE - notification requirements are much less detailed or explicit than those of the NRC. Shipments involving "national security" are exempt. Problems occur because DOE does not always comply with NRC notification and safety requirements.
• coast guard - bulk transport, dangerous cargo vessels must notify appropriate captain of port in advance of arrivals or departure. Includes large quantities of radioactive material and certain fissile radioactive material.

D.4.5. security

• NRC - requirements for establishment and maintenance of physical protection systems [10 CFR 73]. Includes physical security requirements for radioactive material transport to prevent theft, diversion, or sabotage.. Shipper and carrier requirements for arrangements with law enforcement agencies along transportation route for potential accidents [10 CFR 73.37].

D.4.6. preparation of packages, inspection

• DOT - types of packages used for each hazard class. [49 CFR 178] - general specifications for each package type. IAEA regulations incorporated into DOT regulations by reference with certain modifications. Apply to trade abroad with nuclear materials. Security seal must be on the outside of each package which is not easily broken, as an indication of whether the package has been tampered or opened illicitly [49 CFR 173.393(b)].
• NRC - Make sure quality assurance procedures implemented for operations of casks.

• DOE - The DOT allows DOE approval of packaging for research, defense, and contractor shipments.
• OSHA - accepts DOT packaging requirements.
• UN International Maritime Organization (IMO) - establish requirements for packaging. International Maritime Dangerous Goods [IMDG] Code.
• IAEA - Controls for transport of packages.
• Utility - at the reactor site utility has complete responsibility for materials and is governed by NRC rules and licensing requirements.

D.4.7. handling of materials

• FHA - rules governing handling [49 CFR 177].
• FRA - rules governing handling [49 CFR 174].
• RSPA - nonbulk water, rules governing handling [49 CFR 176.5].
• NRC - standards for handling packages [10 CFR 20]. The NRC is responsible for inspecting its licensees for compliance of applicable regulations - public utilities, universities, nuclear laboratories, and industries that handle radioactive materials.

D.4.8. markings

• DOT - requirements concern packages, freight containers, transport vehicles. DOT specification numbers, shipping name, serial numbers, test inspection dates must be on containers to certify maintenance requirements met. [49 CFR 173.24(c)(i), 49 CFR 172.310, 173.389, 173.393]. RSPA authorized use of IMO International Maritime Dangerous Goods Code for marking most domestic shipments and motor vehicles on port not operating on public street of highway.
• EPA requires special markings for packages of hazardous wastes identifying shipper and saying that Federal law prohibits improper disposal.

D.4.9. labeling

• DOT - Labels are "symbolic representation of hazard associated with a particular material". Required on packages and must be affixed near shipping name. On two opposite sides of the package. [49 CFR 172.403(f), .436-.440]. On the labels the contents, number of curries, and transport index must appear. RSPA has authorized use of IMO International

Maritime Dangerous Goods Code for labeling of most domestic shipments and motor vehicles on port not operating on public street of highway.

D.4.10. freight acceptance

• FHA - Rules governing acceptance of freight [49 CFR 177].
• RSPA - nonbulk water, rules governing freight acceptance [49 CFR 176.5].
• NRC - regulates receipt and possession of spent fuel and other byproduct, source, and special nuclear materials [AEC Act 1954, 42 USC 2011]. 10 CFR Part 71 pertains to requirements for licensees when delivering licensed material to a carrier for transport when materials or quantities exceeding Type A are involved.

D.4.11. loading onto carrier

• FHA - rules governing loading [49 CFR 177].
• FRA - rules governing loading [49 CFR 174].
• RSPA - nonbulk water, rules governing loading [49 CFR 176.5].
• NRC -
• National Cargo Bureau, Inc. - assists coast guard with administration of loading regulations. Made up of government and industry representatives.
• Utility - Loading spent fuel into casks and on truck or rail car by utility employees.

D.4.12. placards

• DOT - Placards, symbols on ends of transport vehicles and freight containers to indicate cargo hazards, are required [49 CFR 172.519]. RSPA has authorized use of IMO International Maritime Dangerous Goods Code for placarding of most domestic shipments and motor vehicles on port not operating on public street of highway.
• Joint responsibility of shippers and carriers. Extremely important for emergency response personnel. Should be highly visible.

D.4.13. securing package onto carrier

• DOT - tiedown standards for vehicles.
• NRC - tiedown standards for casks.
• FHA - segregation and separation chart for hazardous materials [49 CFR 177].
• FRA - segregation and placement of cars [49 CFR 174.81, 49 CFR 174.83 - .93]. Includes number of packages per car.

• RSPA - requirements for placement of packages on vessels
• shippers - responsible for trailer restraints / fasteners.
• carriers -

D.4.14. accident free radiation levels from casks

• DOT - radioactive materials maximum radiation level limitations [49 CFR 173.393(i)(j)]. Shipper must determine in accordance with 10 CFR 71.37-.40 the correct transport Index [T.I.] criteria based on nuclear criticality safety. [DOT booklet]. Surface temperature is also regulated [49 CFR 173.393(e)].
• DOT - regulations based on EPA guidelines - establish upper limits of radiation levels around casks.
• Coast guard - enforce exposure levels during transit.
• MTB - enforce exposure levels during transit.
• FRA - enforce exposure levels during transit.
• FHA - enforce exposure levels during transit.
• NRC - regulations based on EPA guidelines - establish upper limits of radiation levels around casks.
• shippers - Responsible for cask surface contamination standard compliance

D.4.15. occupational and public health and safety

• NRC - requirements for notices, instructions, and reports by licensees to individuals involved in transportation related activities. Individuals must be informed of storage, use, or transfer of nuclear materials, and radiation levels. Procedures for addressing violations. Radiological working conditions and consultations with workers [10 CFR 19]. 10 CFR 20 provides standards for personnel protection from radiation exposure. Includes standards for precautionary procedures, signs, labels, signals, and controls. Operating procedures contained in 10 CFR 71. Standards for transportation worker exposures.
• Carriers - must vouch for safe performance of drivers.
• EPA - guidelines for public radiation protection. Follow international criteria established by the International Commission on Radiological

Protection. Authority to establish environmental standards for the protection of the environment from radioactive material.
• DOT-OSHA memorandum of understanding - DOT established regulations for vehicle operator exposures. No OSHA action.
• IAEA - Guidelines for limiting human exposure.

D.4.16. driving
• Very few regulations directly on drivers by agencies.
• DOT - regulations for drivers.
• carriers - responsible for ensuring safe and reliable performance.

D.4.17. vehicle and equipment operations
• DOT, BMCS - requirements for Federal , state, and local law compliance: parking, surveillance of vehicles, operating requirements (fueling, tires, etc) [49 CFR 397].
• FRA - jurisdiction over all areas of safety includes operating practices. Rail safety regulations contained in 49 CFR 209-236.
• ICC - regulates railroad equipment (e.g. use, control, supply, movement, interchange, and return).

D.4.18. inspections during transport
• DOE - inspectors onboard rail shipments.
• NRC - inspectors present at licensee facilities to monitor the beginning of spent fuel shipment [10 CFR 71].
• States may require inspector to be present at beginning/during transport of spent fuel.
• States - may require inspections prior to crossing state boundaries.
• carriers - inspectors onboard rail shipments.

D.4.19. tracking

D.4.20. general safety, inspections
• DOT modal administrations are responsible for operating, general safety, and hazardous material regulations: FHA (e.g. tolls, bridges, carrier arrangements with States, driver qualifications, reporting of accidents,

motor carrier and shipper facilities, roadside and terminal checks of motor vehicles) [49 CFR 177 and [49 CFR Chapter 3]; FRA (e.g. rail shipper and carrier and freight forwarder facilities, railroad tank and freight cars and bulk container manufacturers) [49 CFR 174]; Coast Guard (e.g. boating safety, anchorages, security of vessels, bridges) [33 CFR Chapter 1]; RSPA (e.g. vessels [49 CFR 176]); and National Highway Traffic Safety Administration (not concerned with nuclear material transportation per se, but affects such transportation through safety procedures concerning shippers and carriers that use national highways) [49 CFR Chapter 5]. They develop and enforce general regulations specific to modes of transport. Jurisdiction over general safety requirements for operators, vehicles, vessels by other federal statutes beside HMTA. Modal Administrations are also responsible for inspection and enforcement activities: FRA is responsible for enforcement and inspections responsibility for rail shipper and carrier and freight forwarder facilities, railroad tanks, freight cars and bulk container manufacturers; the FHA inspects motor carrier and shipper facilities and roadside and terminal checks of motor vehicles; the Coast Guard is responsible for monitoring compliance with general safety and hazardous material regulations for bulk transport in ports and US navigable waters of USA. Maintenance and inspection of commercial vessels and equipment [46 CFR parts D, I, N, O].

- NRC - regulates possession of spent fuel and other byproduct, source, and special nuclear materials [AEC Act 1954, 42 USC 2011].
- DOE - The DOT allows approval of some operational aspects of research, defense, and contractor shipments.
- ICC - Administrative law judge decision - ICC will not allow different standards or additional safety measures to be imposed by railways (i.e. no special trains). It must inspect whether safe and adequate equipment, services, and facilities provided by carriers under ICC jurisdiction
- shippers - Responsible for coordinating the transport.
- American Bureau of Shipping and National Cargo Bureau assists the coast guard in monitoring compliance with general safety and hazardous material regulations. The American Bureau of Shipping and National Cargo Bureau assists in water front and facility inspections.

D.4.21. transshipment inspections

• DOT - must assure that exposure levels from stowage do not exceed certain levels.
• RSPA - nonbulk water, rules governing stowage [49 CFR 176.5].
• FHA - rules governing storage [49 CFR 177].
• FRA - rules governing storage [49 CFR 174].
• NRC - regulates transfer of spent fuel and other byproduct, source, and special nuclear materials [AEC Act 1954, 42 USC 2011] [10 CFR 20].
• IAEA - Controls for temporary (in transit) storage of packages.

D.4.22. unloading and inspection at destination

• FHA - rules governing unloading [49 CFR 177].
• FRA - rules governing unloading [49 CFR 174].
• RSPA - nonbulk water, rules governing unloading [49 CFR 176.5].
• NRC

D.4.23. cask and other equipment decontamination and inspections

• DOT - [49 CFR 173.397] prescribes limits for control of non-fixed radioactive contamination and define "significant removable contamination". In general applicable to any package offered for transportation [49 CFR 173.393(h)] and transport vehicle released after being used exclusively for transport of "full loads" of radioactive materials [49 CFR 173.397(c) 173.389(o)]. FRA regulations concerning decontamination and cleaning of cars after use [49 CFR 174]. Contamination control for vessel compartments used in transportation of nuclear materials [49 CFR 176]. FHA regulations [49 CFR 177]. Rules on package reuse, reconditioning, and maintenance [49 CFR 173].
• NRC - Make sure quality assurance procedures implemented for maintenance of casks.
• shippers - Responsible for cask surface contamination standard compliance.

D.4.24. scheduled maintenance and repair of casks, equipment, and procedures

• FRA - jurisdiction over all areas of safety includes track maintenance and equipment standards. Rail safety regulations contained in 49 CFR 209-236.

• DOT - regulations prescribe requirements before first shipment in which a package is used [49 CFR 173.393(m)] and before each shipment [49 CFR 173.393(n)]. Requirements concerning the maintenance, reconditioning, and repairing of packages in radioactive material transportation [49 CFR 171].
• NRC - requires checks such as leak test prior to each use of casks and monitors the quality assurance programs of its licensees for the operation of spent fuel shipping casks.

D.4.25. unscheduled maintenance and repair of casks, equipment

• FRA - jurisdiction over all areas of safety includes track maintenance and equipment standards. Rail safety regulations contained in 49 CFR 209-236.

D.4.26. violation reporting

• incentive is to avoid civil or criminal penalties. Often insufficient to deter violations.

D.4.27. penalties

• DOT - authorized by HMTA to assess civil and criminal penalties.
• NRC - Authority to impose fines for regulatory violations.

D.5. Accident Response and Recovery Phase

D.5.1. immediate notification

• DOT - carriers must notify the agency in event of fire, accident, breakage, or suspected radioactive contamination. The reporting requirement is not necessarily a means of receiving assistance in the event of a transportation accident.
• National Response Team - staffed 24 hours a day by coast guard. Telephone number not in DOT handbook, Emergency Response Handbook. Carriers required to make immediate report of release by telephone to National Response Team under certain conditions. May satisfy requirement to call by calling some other organization - e.g., CHEMTREC.

D.5.2. setup command, control, and communication systems

• NRT - If states request Federal assistance, EPA and Coast Guard will assume responsibility and control and direct Federal emergency response activities.

• FEMA - Federal Radiological Emergency Response Plan [49 FR 35896]. To provide coordinated Federal response to support state and local governments in the event of accidents in the transportation of spent fuel and radioactive waste.
• EPA - responsible for providing assistance in event of radiological emergencies.

D.5.3. control over material
• NRC - resolved conflict as to whether states have right to take control over waste during/after an accident to ensure public safety by letting states make prior arrangements and become "agreement states" which can obtain NRC Licenses to temporarily possess fuel. Only about half the states are agreement states.

D.5.4. actual recovery processes - fire, medical, police
• FRA - actions following incidents involving leakage [49 CFR 174].
• RSPA - actions following leakage or shifting of packages in vessels [49 CFR 176].
• FHA - actions following accidents [49 CFR 177].

D.5.5. radiological monitoring
• EPA - is to assist DOE in monitoring levels of radioactivity in the environment in event of radiological emergencies and as needed to assist in developing recommended measures to protect public health and safety.

D.5.6. clean-up
• DOT - Vehicles, areas, and equipment may not be placed in service again until they have been surveyed and decontaminated. [49 CFR 174.750, 171.15, 171.16, 175.45,(a)(4), 176.48(b), 177.861(a)].

D.5.7. delayed notification
• DOT - every release of hazardous materials except during marine bulk transport and motor carrier transport during intrastate only business must be reported to RSPA in writing [49 CFR parts 171, 174.45 (rail), 175.45 (air), 176.48 (marine). Carriers must fill out written report on form F5800.1 to report release, within 15 days of discovery. Anybody may file

the report, but carriers are required. Required to report releases that occur during loading, unloading even though that is not their function.

- NRC - Standards and requirements for records, reports, and notification of incidents [10 CFR 20].
- other Federal agencies, modal administrations and state agencies - collect data on vehicular accidents and hazardous material transport releases and incidents.

D.5.8. accident investigations

- Coast Guard - Investigations of accidents and incidents.
- FRA - Investigations of accidents and incidents.
- FHA - Investigations of accidents and incidents.
- NRC - is the lead organization for accident and incident investigations.
- National Transportation Safety Board [NTSB] - promotes transportation safety by conducting independent investigations of accidents and other safety problems and by formulating safety improvement recommendations. May make recommendations for accident prevention and regulations, and safe highway highway transport of nuclear materials. [Relevant regulations CFR Title 49, Chapter 8].

D.6. References

Department of Energy 1986. Transportation Institutional Plan. DOE/RW-0094, Washington, D.C.: US Government Printing Office.

Office of Technology Assessment 1986. The Transportation of Hazardous Materials. OTA-SET-304, Washington, D.C.: US Government Printing Office.

Resnikoff, M. 1983. The Next Nuclear Gamble. NY: Council on Economic Affairs.

Appendix E:
Accident and Incident Database Reporting Forms

DEPARTMENT OF TRANSPORTATION

Form Approved OMB No. 04-5613

HAZARDOUS MATERIALS INCIDENT REPORT

INSTRUCTIONS: Submit this report in duplicate to the Director, Office of Hazardous Materials Operations, Materials Transportation Bureau, Department of Transportation, Washington, D.C. 20590, (ATTN: Op. Div.). If space provided for any item is inadequate, complete that item under Section H, "Remarks", keying to the entry number being completed. Copies of this form, in limited quantities, may be obtained from the Director, Office of Hazardous Materials Operations. Additional copies in this prescribed format may be reproduced and used, if on the same size and kind of paper.

A INCIDENT

1. TYPE OF OPERATION
1 ☐ AIR 2 ☐ HIGHWAY 3 ☐ RAIL 4 ☐ WATER 5 ☐ FREIGHT FORWARDER 6 ☐ OTHER *(Identify)* _____

2. DATE AND TIME OF INCIDENT *(Month - Day - Year)*
_____ a.m.
_____ p.m.

3. LOCATION OF INCIDENT

B REPORTING CARRIER, COMPANY OR INDIVIDUAL

4. FULL NAME

5. ADDRESS *(Number, Street, City, State and Zip Code)*

6. TYPE OF VEHICLE OR FACILITY

C SHIPMENT INFORMATION

7. NAME AND ADDRESS OF SHIPPER *(Origin address)*

8. NAME AND ADDRESS OF CONSIGNEE *(Destination address)*

9. SHIPPING PAPER IDENTIFICATION NO.

10. SHIPPING PAPERS ISSUED BY
☐ CARRIER ☐ SHIPPER
☐ OTHER *(Identify)* _____

D DEATHS, INJURIES, LOSS AND DAMAGE

DUE TO HAZARDOUS MATERIALS INVOLVED

11. NUMBER PERSONS INJURED

12. NUMBER PERSONS KILLED

13. ESTIMATED AMOUNT OF LOSS AND/OR PROPERTY DAMAGE INCLUDING COST OF DECONTAMINATION *(Round off in dollars)*
$

14. ESTIMATED TOTAL QUANTITY OF HAZARDOUS MATERIALS RELEASED

E HAZARDOUS MATERIALS INVOLVED

15. HAZARD CLASS (*Sec. 172.101, Col. 3)	16. SHIPPING NAME (*Sec. 172.101, Col. 2)	17. TRADE NAME

F NATURE OF PACKAGING FAILURE

18. *(Check all applicable boxes)*

☐ (1) DROPPED IN HANDLING	☐ (2) EXTERNAL PUNCTURE	☐ (3) DAMAGE BY OTHER FREIGHT
☐ (4) WATER DAMAGE	☐ (5) DAMAGE FROM OTHER LIQUID	☐ (6) FREEZING
☐ (7) EXTERNAL HEAT	☐ (8) INTERNAL PRESSURE	☐ (9) CORROSION OR RUST
☐ (10) DEFECTIVE FITTINGS, VALVES, OR CLOSURES	☐ (11) LOOSE FITTINGS, VALVES OR CLOSURES	☐ (12) FAILURE OF INNER RECEPTACLES
☐ (13) BOTTOM FAILURE	☐ (14) BODY OR SIDE FAILURE	☐ (15) WELD FAILURE
☐ (16) CHIME FAILURE	☐ (17) OTHER CONDITIONS *(Identify)* _____	19. *SPACE FOR DOT USE ONLY*

Form DOT F 5800.1 (10-70) (9/1/76)
*-Editorial change to incorporate redesignation per HM-112.

STANDARD SAFETYNET INSPECTION DOCUMENT

MOTOR CARRIER SAFETY ASSISTANCE PROGRAM

(State agency name and logo)

DRIVER-VEHICLE EXAMINATION REPORT

GENERAL INFORMATION

1 REPORT NO	2. INSPECTION DATE	3 TIME STARTED
No 016011	M D Y	:

4 INSP LOCATION	5 STATE NO	6 DOT NO	7. ICC DOCKET NO

8 INTERSTATE? Y N	9 NAME OF MOTOR CARRIER

10 STREET ADDRESS	11 CITY	12. STATE	13 ZIP CODE

14 NAME OF SHIPPER	15 SHIPPING PAPER NO

16 DRIVER IDENTIFICATION	17 DRIVER LICENSE NO	18 LIC STATE
Last Name / First Name / MI		

19	20	21
22	23	24
	25	26
	27	28

HAZARDOUS MATERIALS

A – Explosives A
B – Explosives B
C – Explosives C
D – Flammable Liquid
E – Flammable Solid
F – Flammable Gas
G – Nonflammable Gas
H – Corrosive
I – Oxidizer
J – Poison A
K – Poison B
L – Combustible Liq
M – Radioactive Mat
N – Organic Peroxide
O – Irritating Mat
P – Cmb A, B or C
Q – Cmb E
R – Etiologic Agt
S – Blasting Agt
T – Cryogenics
Z – Other

	CODE	RQ?	WGT
29			
30			
31.			

PLACARDS REQUIRED? 32

Y YES N NO

VEHICLE IDENTIFICATION

	UNIT NUMBER	UNIT TYPE	MAKE	CO NUMBER	LICENSE TAG NO & STATE
33	1				
34	2				
35	3				
36	4				
37	5				
38	6				

Unit Type TR - Straight Truck TT Truck Tractor ST Semi Trailer PT Pole Trailer FT Full Trailer DC - Dolly Converter BU Bus OT Other

VIOLATIONS

NO	VIOLATION IDENTIFICATION	UNIT NO	OUT OF SVC	VIOLATIONS DISCOVERED
SEE CONTINUATION SHEET YES NO				

VEHICLE/DRIVER OUT OF SERVICE NOTICE

☐ Pursuant to authority contained in _____ I hereby declare vehicles with defects followed by an "X" in the Out of Service column of this report Out of Service. No person shall remove the out of service stickers applied to these vehicles or operate such vehicles until the out of service defects have been repaired and the vehicles have been restored to safe operating condition.

☐ Pursuant to authority contained in _____ I hereby notify and declare the driver named on this report Out of Service. No motor carrier shall permit or require this driver to drive or operate any motor vehicle until _____

REPORT PREPARED BY	A INSPECTOR CODE	B TIME COMPLETED	COPY RECEIVED BY
		:	

NOTE TO DRIVER This report must be furnished to the motor carrier whose name appears on this report. NOTE TO MOTOR CARRIER Please sign the below certification and return this report to _____ within fifteen days.

The undersigned certifies that all violations noted on this report have been corrected and action has been taken to assure compliance with the _____ shown as they are applicable to motor carriers and drivers.

SIGNATURE OF CARRIER OFFICIAL	TITLE	DATE SIGNED

SPENT FUEL SHIPMENT INSPECTION FORM

☐ TRUCK ☐ RAIL

A. Shipment Route: _____ Shipment Ref. #: _____ Date: _____

Shipper: _____ Carrier: _____ Cask Serial #: _____

Cask Model: _____ Tractor Unit #: _____ Trailor Unit #: _____

B. Cask Radiation Levels (Maximum)	Beta/Gamma (mR/hr) (I.D.N.S.: Shipper)	Neutron (Indicate Unit ___) (I.D.N.S.: Shipper)
a. Surface (Cask) (1000 mR/hr)	:	:
b. 1 Meter (From Cask - TI)	:	:
c. Surface (Vehicle) (200 mR/hr)	:	:
d. 2 Meters (From Vehicle) (10 mR/hr)	:	:
e. Cab (Vehicle) (2 mR/hr)	:	:

C. Contamination Levels (Removable/100 cm^2)	Maximum (DPM) (I.D.N.S.: Shipper)	Average (DPM) (I.D.N.S.: Shipper)
a. Beta/Gamma (2200 dpm)	:	:
b. Alpha (220 dpm)	:	:

D. Cask Labeling/Marking:

a. Transport Index (TI) _____ b. Curie Content _____

c. Radionuclides _____ d. Label Type & (#) _____ ( )

e. Proper Shipping Name _____ f. UN # _____

E. Placarding: a. Type _____ b. 4 Sides _____

F. Shipping Papers:

a. Certification _____ b. Physical/Chem Form _____/_____

c. Matches Shipping Label _____ d. Notations for Fissile III & Hwy Controlled _____

G. Drivers:

a. Driver Name _____ b. Highway Route Plan _____

c. Training Dates _____ d. Emergency Procedures Available _____

H. Inspections and Testing Conducted (Indicate Individual's name):

a. Motor Carrier Safety _____ b. Mobile Phone/CB _____

c. Hazardous Materials Radiation Survey _____

d. IDNS _____ e. NRC _____

f. Security Seals: (1) Cask _____ (2) Bracing _____

I. Comments (DOT violations, escort training, MCS violations, etc.): _____

_____

_____