Parker

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

AUG 8 1979

MEMORANDUM FOR: E. Kevin Cornell, Staff Director
NRC/TMI Special Inquiry Group

FROM: C. O. Miller, Consultant
NRC/TMI Special Inquiry Group

SUBJECT: OUTLINE OF POSSIBLE INSTITUTIONAL ISSUES ILLUSTRATED BY TMI

Throughout the TMI investigation, it has been quite obvious that certain institutional issues have arisen. For purposes of this discussion an institutional issue is one which is illustrated by the accident in question but which also has fundamental accident causation or prevention potential in other nuclear power situations. Furthermore, an institutional issue usually pertains to management functions not only for the host agency (e.g., NRC), but also for other nuclear power system participants (e.g., the utility, the facility contractors, subcontractors, and even the Congress).

Clearly, all of the task groups within the SIG will have an impact on the definition and resolution of institutional issues. However, in the interest of posing questions and perhaps structuring a portion of the report to emphasize such issues or what might otherwise be called the safety management posture of NRC, the attached outline has been prepared. Like Mr. Frampton's draft of the Outline of the Final Report dated July 30, the attached outline tries not to prejudge the results in view of the voluminous information yet to be obtained. Nevertheless, many of the problems implied by the outline seem to be well established, at least to my mind, based upon material I have reviewed thus far.

The logic of the outline follows certain basic functions of management but adapted to the instant situation as follows:

1. Statutory Base

2. Policy

3. Planning

4. Requirements and Enforcement

5. Tasks

REFERENCE DOCUMENT

6. Implementation, Evaluation and Followup

7. Organization

All categories are amplified by the term "safety" so as to restrict the scope of the issues to that aspect (e.g., Statutory Base for Nuclear Safety, Safety Policy, etc.).

I would welcome the opportunity to discuss the outline further in whatever forum you deem advisable.

C. O. Miller

C. O. Miller, Consultant
NRC/TMI Special Inquiry Group

Enclosure:
As stated

cc: M. Rogovin
G. Frampton
R. DeYoung
B. Doyle
Group Leaders

OUTLINE

INSTITUTIONAL ISSUES

1.0 STATUTORY BASE FOR NUCLEAR SAFETY

1.1 Did the Energy Act of 1974 influence NRC's actions with regard to TMI in a manner adverse to safety by the Act's:

1.1.1 Failure to cite nuclear safety in the introductory parts of the bill as being a Federal responsibility?

1.1.2 Failure to delineate total Federal safety responsibilities between NRC and ERDA (later DOE) while concentrating only on separating nuclear energy promotion/development from regulation?

1.1.3 Failure to identify specific safety tasks beyond the regulatory function such as accident/incident investigation?

1.1.4 Being overly definitive in mandating three elements of the organization NRR, NMSS and RES thereby laying the foundation for safety management fragmentation at NRC?

1.1.5 Failure to specify a role for the Commissioners either singularly or collectively in terms of day by day management of NRC? (Did the Commissioners' equality lead to management by committee?)

1.1.6 Emphasis on risk assessment as distinguished from accident prevention to the highest degree consistent with a viable nuclear power system in the public interest? (Undue emphasis on risk assessment tends to make people stop thinking once they've established a low order of probability for an accident.)

1.1.7 Failure to acknowledge that catastrophic losses in resources without loss of life or injuries should also be a safety objective? (i.e., recognize the real-world importance of the "save the shutdown" syndrome.)

1.2 Has the Congress failed to step up to certain basic safety issues as:

1.2.1 Authorization for Federal control of nuclear power installations at times of site emergencies? (This assumes such control is feasible timing-wise and technically which is open to considerable question.)

1.2.2 Authorization for NRC to demand specific management structure and practices at utilities and possibly at certain contractors as a prerequisite to licensing?

1.2.3 Endorsement of an "intelligent assumption of risk" policy vis-a-vis "assessment of risk," and a requirement for accident prevention, system safety program elements to go with it? (This might better be argued as being an Executive Branch action rather than one for Congress.)

1.2.4 The limitations of the regulatory process as implemented through administrative law channels in development of a comprehensive safety program? (Persuasion must supplement rule-making and certain aspects of safety cannot be legislated.)

1.2.5 The Price-Anderson legislation diminishing utility company's motivation towards safety too much? (i.e. the company is not going to be rapped hard enough when they are truly negligent.)

This has been discussed extensively

- Act -

2.0 SAFETY POLICY

2.1 To what extent, if any, did the following NRC policies influence the occurrence of and response to the events at TMI:

2.1.1 The "design basis" accident concept

2.1.2 Distinction between safety systems and other systems

2.1.3 Emphasis on risk assessment rather than a total accident prevention approach as illustated by regulating only "credible" events

2.1.5 Emphasis that "the utility has the responsibility for safety of plant operation"

2.2 What has been the NRC policy in the following:

2.2.1 The scope of the term "design" as might be used in "design criteria" or "design error" (e.g., did it include the software beyond technical specifications and drawings?)

2.2.2 Promotion of nuclear safety by NRC using techniques beyond the regulatory process (e.g., other methods of influencing utility or contractor management).

2.2.3 NRC's view of DOE's responsibility for nuclear safety compared to its own

2.2.4 Public health and safety requirements of NRC's enabling legislation in possible competition with public interest in available electrical power during the current energy crisis.

2.2.5 The need for a utility to "save the shutdown"

2.2.6 The objective of NRC's safety efforts

2.2.7 THe objective of NRC accident/incident investigations

2.2.8 The accountability of management for safety

2.2.9 I&E's role in NRC's nuclear safety efforts

2.2.10 Discretionary limits that are to be observed by I&E in day-to-day enforcement activities

2.2.11 Quality Assuance Program's relation to NRC's nuclear safety issues

2.2.12 Autonomy of Office Directors in decisions clearly related to safety efforts

2.2.13 Priority of Commission in terms of matters to be brought before them

2.2.14 Sabotage as a safety issue

2.2.15 Confidential reporting of hazards

2.3 Does NRC, as viewed from the perspective of the Commissioners and/or Office Directors believe:

2.3.1 It is NRC's role to take "intelligent risks" in trade-offs between safety performance, cost and schedule?

2.3.2 In view of TMI, that safety efforts within NRC have been fragmented?

2.3.3 In view of TMI, that nuclear safety efforts on a broader scope than NRC have been fragmented (i.e., uncoordinated) between the government, utilities and the contractors?

2.3.4 That man in the nuclear reactor control is a positive or negative factor in nuclear safety?

2.3.5 That safety improvements always cost money?

2.3.6 That the current L.E.R. system or any other means exists to document actual or potential human errors?

2.3.7 I&E's accident/incident investigation role can satisfy both enforcement and accident prevention needs?

2.3.8 A difference in philosphy and operation exist between "licensing" and "regulation"

2.3.9 Differences have existed on how NRC has treated nuclear power reactor safety compared to AEC?

2.3.10 That safety technology has been applied within NRC as a technical speciality?

3.0 SAFETY PLANNING

3.1 To what extent were the following safety plans in existence at the time of TMI:

3.1.1 National nuclear power accident prevention program plan?

3.1.2 Safety engineering plans?

3.1.2.1 In the form of requirements by NRC

3.1.2.2 As issued or implemented by Met-Ed

3.1.2.3 As issued or implemented by B&W

3.1.3 Operational safety plans?

3.1.3.1 In the form of requirements by NRC

3.1.3.2 As issued or implemented by Met-Ed

3.1.4 Accident/incident emergency response plan?

3.1.4.1 As applicable to NRC actions

3.1.4.2 In the form of requirements by NRC for others

3.1.4.3 As issued or implemented by the others (Met-Ed, B&W, States, etc.)

3.1.5 Accident/incident investigation plans

3.1.5.1 NRC

3.1.5.2 Other Federal and State Agencies

3.1.5.3 Others (e.g., Met-Ed, B&W, etc.)

3.2 With respect to the above plans to what extent did they:

3.2.1 Identify the personnel responsible for the plan and/or the chain of command implicit in its implementation

3.2.2 Delineate a notification process of appropriate personnel for carrying out the plan?

3.2.3 Provide an opportunity to exercise, evaluate or otherwise test the efficacy of the plan? (e.g., were there structured review times or simulated emergencies?)

3.2.4 Require specific qualifications for personnel assigned to carry out the plans?

3.2.5 Specify the communications system that would be used in implementing the plan?

3.2.6 Plan for risks that could not readily be quantified nor defined precisely?

3.2.7 Account for varying levels of authority one participant may have had over another for successful implementation of the plan?

4.0 SAFETY REQUIREMENTS AND ENFORCEMENT

4.1 Considering safety requirements in general:

4.1.1 Are safety requirements structured so as to "save the shutdown" as well as protect against physical injury to persons or property?

4.1.2 Which ones, if any, are aimed at mitigating the effects of unpredictable hazards and those hazards whose probabilities are extremely small?

4.1.3 Does risk assessment necessarily have to be accomplished before requirements are defined?

4.1.4 Are safety requirements performance requirements or task requirements, or both?

4.1.5 How are safety requirements documented when they apply to NRC personnel (i.e., what are the tasks and to what acceptable performance level must they be accomplished)?

4.1.6 Are the minimum standards that must be met to allow licensing the same ones which, if enforced, satisfy the mandate to the NRC to regulate the nuclear power industry so as to assure public health and safety?

4.2 In the interpretation of design requirements:

4.2.1 To what extent do "design" requirements extend into software that precedes, accompanies and follows the actual making and release of drawings?

4.2.2 Design goals are expresssed in what manner?

4.2.3 Who chooses the "design basis" accidents or "credible event" and what methods are used to validate or otherwise approve such a choice?

4.2.4 How and by whom is the line drawn between safety and non-safety systems ... what methods are used to validate or otherwise approve that choice?

4.3 When enforcing requirements that have been imposed upon the utility or contractor:

4.3.1 What discretion is allowed the inspector in initiating punitive action?

4.3.2 What informal channels as well as formal ones are used in practice to resolve differences of opinions?

4.3.3 To what extent may I&E inspectors amplify or extend requirements promulgated by NRR ... to what extent can they mitigate them?

4.3.4 Does I&E look for responsibility for a rule infraction in a vicarious sense or do they only cite the person whose acts were proximate to the violation?

4.3.5 Has I&E management been satisfied with both the quantity and quality of personnel available to perform the enforcement function?

4.3.6 Have Met-Ed, B&W et al been satisfied in the past with the quantity and quality of NRC enforcement actions?

4.3.7 Does the NRR/IE coordination memo of June 29, 1979 (signed by Mr. Denton) accurately reflect how safety requirements have been delineated, coordinated and enforced or how they should be? (NRR concentrates on observation, inspection, evaluation, reporting and enforcement.)

5.0 SAFETY TASKS *

5.1 The analysis task

5.1.1 What discrete phases of hazard analysis can be identified through the life cycle of a typical nuclear power plant licensed by NRC?

5.1.2 What distinctions, if any, are made between Hazard Mode and Effects Analysis (HMEA) and Failure Mode and Effects Analysis (FMEA)?

5.1.3 How does the establishment of design bases limit or otherwise control HMEA/FMEA's?

5.1.4 What analysis techniques are applied to the "incredible" events?

5.1.5 To what exent do the HMEA/FMEA's not only identify hazards but also describe symptoms thereof and control mechanisms available to keep the hazard from maturing to an accident.

5.2 Safety communications

5.2.1 In what manner do NRC, the utilities, the contractors et al document and store for ready retrieval the bitter lessons of past accidents and incidents (the known precedent concept)?

---

* Safety tasks in this connotation are those efforts beyond planning and the implementation of requirements which follow NRC accident prevention policy and use modern safety technology techniques.

5.2.2 In what manner do NRC, the utilities, the contractors et al effect liaison among themselves and other industries in matters germane to accident prevention?

5.2.3 What discrete methods are available to generate safety research, study or testing when a question arises during the development of a new system?

5.2.4 What attitudes prevail and what methods are available for persons within NRC, the utilities or the contractors to obtain objective and perhaps confidential review of perceived hazards, including those in which the individual played a part?

5.2.5 What methods are used to assure that emergency procedures are a product of combined efforts of the system designers, the operators, and those who moniter the results of past accident/incident investigations?

5.3 Safety awareness and attitude development

5.3.1 WHat programs in nuclear safety awareness and attitude development have been applied to:

5.3.1.1 NRC Commissioners?

5.3.1.2 NRC supervisors?

5.3.1.3 NRC engineers, scientists, attorneys, inspectors, etc.

5.3.1.4 Met-Ed and B&W personnel equivalent to the above?

5.3.1.5 Members of Congress?

5.3.1.6 The public?

5.3.2 To what extent have the programs noted above been accomplished in the sense of:

5.3.2.1 Education ... teaching people to think

5.3.2.2 Training ... skill development for a particular task

5.3.2.3 Indoctrination ...in application of the education and training to a particular situation

5.3.2.4 Motivation ...personal commitment

5.4 Accident/incident/event (AIE) investigations *

5.4.1 Who are the investigators?

5.4.2 What training have the investigators received in investigation techniques?

5.4.3 How practical is it to have "SWAT" or "GO" teams to respond on short notice to critical AIE's?

5.4.4 In what manner are NRC-recommended AIE investigation procedures documented for use either by NRC personnel or others?

5.4.5 What is the objective of AIE investigations; cause, recommendations for remedial action or enforcement?

5.4.6 What statutory or administrative rules exist which provide appropriate control at the AIE site?

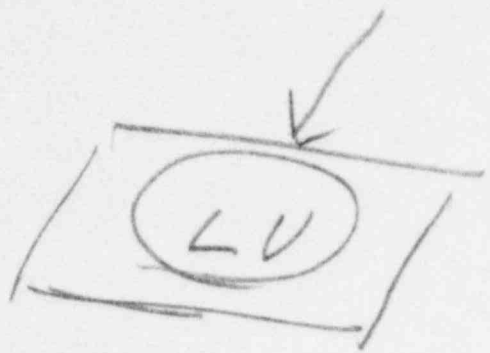
5.4.7 What provision for training and procedures exist to minimize hazard to investigating personnel at the scene of an AIE?

5.4.8 To what degree, if any, are lines of authority at the scene of AIE's spelled out in statutes or administrative rules or procedures?

5.4.9 Which persons during AIE investigations are authorized to provide information to the media or other outside agencies (e.g., Congress) and what constraints do they operate under?

---

* An accident means injury or significant damage has occurred. An incident is an event which, except for a fortunate input, serious injury or damage would have occurred. An event is a deviation from the norm, the consequences of which are arguable.


∠V

6.0 SAFETY IMPLEMENTATION, EVALUATION AND FOLLOWUP

6.1 Assuming implementation of safety tasks (ref. 5.0):

6.1.1 Are they seen as separately identifiable functions or corollary to existent duties and functions of the Commissioners, EDO, NRR, IE, NMSS, RES, etc.

6.1.2 Are they seen as always adding program cost and if so, on what accounting basis?

6.1.3 What is the impact on accomplishment of these tasks from the multiple NRC facilities in the Washington, D. C. area?

6.2 Considering day-to-day project management activities

6.2.1 What forms of communications and documentation are used to forward safety decisions, warnings or similar indicators of action related to safety?

6.2.2 What priority system is used to identify and record the safety significance of a given action?

6.2.3 To what extent is the hazard being protected against described in the action documentation?

6.2.4 What variables are most frequently encountered that enter into the action decision process in matters related to safety?

6.2.5 Are risk assessment studies sufficiently comprehensive to provide confidence that the hazard being discussed (and presumably acted upon) is thoroughly understood?

6.2.6 What proportion of the activities related to safety can be identified with the licensing process compared to the regulatory process? (Any difference between two?)

6.2.7 To what extent are group dynamics applied in the resolution of safety problems, specifically through:

6.2.7.1 An NRC Safety Board, Counsel or Committee?

6.2.7.2 Program review meetings?

6.2.8 What process is followed to record and track reported safety deficiencies, including action taken and followup thereto?

6.2.9 To what extent are safety surveys or staff assistance visits used with utilities or contractors as distinguished from inspections?

7.0 SAFETY ORGANIZATION

7.1 Considering organization at NRC to achieve its objectives towards nuclear safety:

7.1.1 What path does the line (or decision-making) safety function follow?

7.1.2 What persons or organizational segments provide the staff (advisory) safety function?

7.1.3 What role is played by the Commissioners, singly and collectively in both the line and staff safety functions?

7.1.4 Who is the "Chief Safety Officer of NRC" in the line and staff sense; that is:

7.1.4.1 Who is most responsible for decisions related to safety?

7.1.4.2 Who is most responsible for advice related to safety?

7.1.5 What is the definition of "Systems" as used in the "Division of Systems Safety"? (Was it ever intended to be synonymous with "system safety" as used by DOD, NASA, etc.?)

7.1.6 Is NRC's fundamental approach to management that of program/project management utilizing a matrix concept of staffing for major efforts? (Alternattively, may each major office function autonomously?)

7.1.7 In what manner are tasks related to safety assigned to a given office?

7.1.8 Which organizational segments are concerned with man's input to nuclear safety? (There are easily identified areas for site safety, the reactor plant systems, etc.)

7.1.9 What organizational segments are concerned with ensuring effective organization and management at the utilities and their contractors and how is it accomplished?

7.1.10 Do any formal or informal safety boards or safety councils exist within NRC and at what levels of the organization?

7.1.11 What NRC personnel participate in interagency safety activities and what are these activities (both government and non-government)?

7.1.12 To what extent does the organization of NRC parallel the organizations at utilities and their contractors? (Could a person in one activity readily find an "opposite number" in the other?)

7.1.13 Organizationally, how does NRC provide for its employees' health and safety?

7.2 Reflecting on the development of the present NRC organization:

7.2.1 Any reason why some offices have "safety" in their titles (or something close to it) while others do not?

7.2.2 Why has the accident/incident/event investigation task been assigned to IE and how long ago was this done?

7.2.3 Had any studies been made prior to TMI exploring the possibility of a staff safety office for NRC/AEC in addition to safety tasks being assigned to other organizational segments?

7.2.4 Had any studies ever been made prior to TMI to establish an accident investigation function independent of the principal offices of NRC?

7.2.5 In what organizatonal segments of AEC did one find personnel most active in accident prevention?

7.2.6 In what organizational segments of NRC does one find personnel most active in accident prevention?