OTT

OH

NUREG-0585

Young

Mick Kay

TMI-2 Lessons Learned Task Force Final Report

Office of
Nuclear Reactor Regulation

U.S. Nuclear Regulatory
Commission

Available from

GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

NUREG-0585

TMI-2 Lessons Learned Task Force Final Report

Manuscript Completed: October 1979
Date Published: October 1979

Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington. D. C. 20555

ABSTRACT

In its final report reviewing the Three Mile Island accident, the TMI-2 Lessons Learned Task Force has suggested change in several fundamental aspects of basic safety policy for nuclear power plants. Changes in nuclear power plant design and operations and in the regulatory process are discussed in terms of general goals. The appendix sets forth specific recommendations for reaching these goals.

CONTENTS

CONTENTS (Continued)

TMI-2 LESSONS LEARNED TASK FORCE
FINAL REPORT

1. INTRODUCTION

In May 1979, the Office of Nuclear Reactor Regulation formed an interdisciplinary team of engineers and scientists from various offices of the U.S. Nuclear Regulatory Commission to begin work on the identification and evaluation of safety concerns originating from the accident at Three Mile Island Unit 2 (TMI-2). In July 1979, this team, the TMI-2 Lessons Learned Task Force, issued NUREG-0578 ("TMI-2 Lessons Learned Task Force Status Report and Short-Term Recommendations," Ref. 1) recommending short-term actions to be taken on operating plants and on pending license applications. These short-term recommendations are now being implemented.

In contrast to the short-term recommendations in NUREG-0578, which were of a more narrow, specific, and urgent nature, this report deals with safety questions of a more fundamental policy nature regarding nuclear plant operations and design and the regulatory process. The report addresses these topics in three chapters; each chapter identifies policy elements the Task Force considers to be important and in need of change or improvement. The discussions in these chapters are goal oriented rather than prescriptive in nature, since there may be a number of ways in which the objectives can be achieved. Some objectives would cause significant changes in the nuclear industry and in the regulatory process and should be considered deliberately when choosing the best means of implementation. For others, particularly those related to operations, actions should be initiated without delay since they would introduce a needed and stepwise improvement in safety.

To stimulate discussion and speed the deliberative process, the Task Force has developed a number of specific recommendations toward accomplishing the policy objectives and safety goals described in this report. The specific recommendations are summarized in Appendix A. The Task Force considers the thrust of the modifications it has outlined to be of fundamental importance to nuclear safety, and urges that immediate steps be taken to complete the deliberative process and initiate implementation of these specific recommendations. We envision the deliberative process to include review by the Advisory Committee on Reactor Safeguards; formulation of an action plan by the Office of Nuclear Reactor Regulation in consultation with the Offices of Inspection and Enforcement, Nuclear Regulatory Research, and Standards Development; and approval of the action plan by the Commission. We urge that the action plan address all of the specific recommendations in Appendix A, but we recognize that some may be improved upon in the course of staff, ACRS and Commission review.

We believe that the technical foundation for our specific recommendations is solid, but the recommendations could be affected by the results of studies and investigations that continue inside and outside of the NRC, especially because our scope of responsibility has been narrow in comparison to some of those other efforts. Therefore, the management of NRC will have to exercise some balancing of interests in deciding upon which actions to take now and which actions to study further before regulatory requirements are promulgated. Two

especially important considerations in this balancing of interests, in addition to the improvements in safety inherent in our recommendations, are the need to give prompt and careful consideration to the recommendations of the President's Commission on Three Mile Island and the need to recognize that the bulk of Federal and industry resources are already committed to the timely implementation of shorter term requirements flowing from reviews of the TMI-2 accident and other safety requirements of NRC. The Task Force has given some thought to these factors in developing its suggestions of ways in which implementation could proceed on the specific recommendations in Appendix A. Our judgments on the timing of implementation are stated within the recommendations themselves.

The principal conclusion of the Task Force is that, although the accident at Three Mile Island stemmed from many sources, the most important lessons learned fall in a general area we have chosen to call operational safety. This general area includes the topics of human factors engineering, qualification and training of operations personnel; integration of the human element in the design, operation, and regulation of system safety; and quality assurance of operations. Specifically, the primary deficiency in reactor safety technology identified by the accident was the inadequate attention that had been paid by all levels and all segments of the technology to the human element and its fundamental role in both the prevention of accidents and the response to accidents. Thus, our policy recommendations and our specific ideas for stimulating and accomplishing change concentrate heavily on operations reliability and the associated design and licensing review measures that support or augment operations reliability. But an important qualifier must be added to this conclusion. That is, if the basic responsibility for public safety is to remain in the private sector, in the hands of the individual licensees for commercial nuclear power plants, then significant change in the attention to operations reliability must take place in the licensed industry. Operations is a "hands-on" concept and high operations reliability can only be achieved in practice by those responsible for "hands-on" functions.

The Task Force has given considerable thought to the basic mission of reactor regulation after Three Mile Island. We are not alone in these efforts; many people have called for a clearer articulation of NRC's role and mission since March 28, 1979. However, the Commission and this Task Force recognized soon after the accident that there was a compelling need for short-term, immediate consideration of presently operating plants and steps that needed to be taken to increase their safety. The results of our short-term work and the various other efforts within the NRC and industry have undoubtedly initiated needed improvements in nuclear reactor safety. But much more is needed beyond these reactionary steps. The Task Force acknowledges and appreciates the unique opportunity it has to stand back and look broadly at the past and the future of reactor safety regulation. This opportunity has led us to a critical scrutiny of NRC safety policy. What we have found is that prescriptive and narrow licensing requirements only add to the quiltwork of regulatory practice and do little to directly address the nation's heightened concern for the safety of nuclear power plants. What seems to be missing is the common denominator of an articulate and widely noticed national nuclear safety policy with which to bind together the narrow and highly technical licensing requirements. The Commission has alluded to a more definitive safety policy by taking actions that, in effect say, "no more Three Mile Islands." But the feasibility and the adequacy of such a policy must be critically examined and an opportunity

should be provided for thorough and widespread public input. Such dialogue and debate at a widely comprehensible level will enable the NRC to realize its leadership role in nuclear safety and diminish our partially deserved image as a reactionary body that is both defensive and apologetic of nuclear power. The need to articulate our basic safety policy is compelling. It need not wait for a new statutory mandate, and it should not be a de facto stepchild of future events.

2. IMPROVEMENTS IN NUCLEAR POWER PLANT OPERATIONS

2.1 Introduction

The Task Force believes that operational safety merits paramount attention by NRC as a result of the accident at TMI-2. Although perhaps not everyone would agree with this preeminent emphasis, it is unlikely that anyone would disagree that improvements are overdue.

During its deliberations, the Task Force considered the various factors that can and do affect the safety of nuclear power plants. These include the design, the design basis, the conduct of operations, the industry, and the scheme of regulation. The essence of the conclusion of our broad and fundamental examination is that there are no such separate things as "safe design" and "safe operation." A good design can be unsafe if put into the hands of a poorly qualified and trained operations organization. The converse is, of course, equally true. We believe, and it is undisputed, that in the past the overwhelming emphasis in commercial nuclear power plant safety has been on producing a safe design, whereas not enough emphasis has been placed on safe operation. Therefore, our conclusion that operational safety merits paramount importance does not mean that it is more important than design, only that it has not received the attention it requires. And, as evidenced by our short-term report and in other sections of this final report, a new emphasis on safe operations does not mean that current designs do not require improvement. Only by the long-overdue emphasis on operational safety and the awareness and attention to the nexus of design and operation can we achieve a high level of safety.

The Task Force believes that an example involving technology's most challenging day-to-day experience with public safety would be helpful to illustrate the point. That experience is, of course, automobile safety. Since the late 1960's and the passage of major Federal legislation, increased attention has been given to automobile safety. It is interesting to note that the increased attention has gone almost exclusively to design factors in achieving safety improvements in automobiles. The intent of Federal standards has been to markedly improve the safety of automobiles through standards for tires, steering stability, brakes, windshield wipers, etc., and, at the state government level, to require periodic inspections to maintain mandated safety levels. The automobile industry, responsive to this public concern and to legal requirements, now recalls its products when unsafe design defects are found. Of course, it is apparent that automobile accidents will still happen, and the response of the automotive industry has been to change automobile designs to achieve "crash worthiness," such as the addition of seat belts, safety glass, padded dash boards, collapsible steering wheels, and air bags. In other words, make the car safe from the user by design measures to prevent and mitigate accidents. Much less attention has gone to upgrading the incentives or enforcement actions for human or operations aspects of automobile safety, and remarkably little attention has been given to improvements in the operability of automobiles, or the man-machine interface. It seems clear that better training of drivers (including off-normal conditions), stricter licensing standards, and requirements for retraining and requalification would achieve a significant improvement in automobile safety. Similarly, the man-machine interface could also bear attention in achieving better visibility, better instruments, and fewer distractions for the operator.

The national choices with regard to automobile safety have been to accept the many challenges to the design that occur, and the very high risk in terms of injury and deaths, rather than more vigorously attacking operational safety. An analogous approach in the field of nuclear energy is unacceptable because of the magnitude of risk involved, the unequal distribution of the risks and the benefits, and the apparent public rejection of significant risks of radiation health effects. Historically, we have traveled a path in commercial nuclear power of attempting to develop a fail-safe machine. Not only have plants been designed to place low reliance on the operator for short-term response in times of emergency, but past policy has also limited the operator involvement through the use of automatic systems, interlocks, and fail-safe features. With this emphasis on system design, we have been inattentive to the broader implications of the human element in reactor safety. Lacking emphasis on operational safety and on the integration of operational and design safety, we are left with a line of defense that is too susceptible to poor operations performance.

Accepting the premise that there is a need to increase our consideration of operational safety, two possible goals become clear: reduce challenges to the plant safety systems and provide maximum capability to mitigate the challenges that inevitably occur. Reduction of challenges stems not only from reliable operation itself, thus avoiding off-normal situations, but also from recognizing precursors to off-normal operation and neutralizing them before they develop into, or recur under different circumstances as, direct challenges to plant safety systems. Proper operator reaction to challenges requires sufficient understanding of the plant design and its dynamic response to upset conditions to diagnose the problem, to recognize when the plant safety systems are functioning effectively, and, in situations where they are not, to take additional corrective actions, including utilization of all available plant systems, to minimize the consequences. Attendant to these functions is assurance at all times that the status of plant systems is known and that the systems are in their required configuration.

The complementary goals of reducing the rate of challenges and maximizing the response to challenges can be achieved through a vigorous commitment to improve the various elements of what can be thought of as an operations matrix for normal and emergency operations. This matrix encompasses personnel qualifications, training, and procedures; the personnel environment, including staffing and the design of the man-machine interface; provisions for verification of correct performance of operating activities and feedback of operating experience; and commitment by management to operational safety through personal responsibility and accountability. Attainment of requisite performance levels throughout the matrix, and integration with plant design, may change today's frequently asked question of how to account for operator error to the question of how much credit to allow for operator action (see Recommendation 7.4).

2.2 Roles of NRC and Industry

With these general goals of operational safety defined, and before moving on to the question of specifically how one attains these goals, it is appropriate to elaborate on our views of the respective roles of the NRC and the regulated industry.

The Task Force believes that the improvement and maintenance of operational safety is a fundamental responsibility of licensees. That is, the licensees must assure day-to-day awareness of, and attention to, not only the letter but also the spirit of operational safety principles. The accident at TMI-2 shows that the financial risk associated with accidents is substantial so that the dual public safety and energy production missions of an electric utility are not necessarily in conflict, as some have suggested in the past. The NRC role should be to provide minimum acceptance criteria, detailed guidance where necessary, and any additional incentives that are necessary to attain the goals for operational safety. In this regard, one of our short-term recommendations in NUREG-0578 was to formulate a new requirement for a "Limiting Condition for Operation" requiring plant shutdown in the event of human error leading to a complete loss of safety function. Embodied in this recommendation is the expectation that licensees will demonstrate the necessary initiative to reduce human errors to avoid the precipitative requirement for plant shutdown. The Task Force is thus recommending that the NRC challenge its licensees to attain a step improvement in operations reliability. Notwithstanding the challenge to licensees provided by our earlier proposed increase in the incentive for good operations management, which we still support, the Task Force has also concluded that the NRC staff must give increased attention to the detailed methods of obtaining improvements in operational safety.

Appendix A contains our specific recommendations with respect to improvement in operational reliability and improvement in operational response to off-normal accident situations (see Recommendations 1 through 7). The recommendations are directed to both licensees and the NRC staff and are included in terms of what the Task Force considers to be the basic underlying causes of problems in the operations area. The list of recommendations is not intended to be all-inclusive because it is expected that a large segment of the licensing staff will begin further work in this area and licensees will exhibit the initiative to obtain the onsite management and organizational ingredients required for significant improvement in operational safety.

To meet a goal of significantly improving operational safety, an effective mixture of regulatory and financial incentives and of Federal and industry standards must be established for the commercial nuclear power program to achieve an acceptance of personal responsibility for safety at all levels throughout the private sector. In the Naval Nuclear Propulsion Program, Admiral Rickover has insisted that there be acceptance of personal responsibility throughout the program and that the designer, draftsman, or workman, and their supervisors and managers are responsible for their work and, if a mistake is made, it is necessary that those responsible acknowledge it and take corrective actions to prevent recurrence. This concept applies equally to the commercial nuclear power program, but it has not yet been achieved.

2.3 Achievement of Goals

Our general conclusions on major components of the overall matrix of operational safety are provided below and our specific recommendations are included in Appendix A.

2.3.1 Management Commitment

For the goal of significant improvement in operational safety to be achieved, nuclear utility management must show a commitment to the goal through positive action. Corporate managers must accept prime responsibility for assuring an acceptance of responsibility for public safety throughout their operations organizations. This requires, among other things, involvement of top managers in operational safety matters and a commitment to upgrade the knowledge of the fundamental technology and the hazards of nuclear power at all levels of their organization. These comments apply equally to the top management of the NRC in assuming additional responsibility for operations safety matters and involvement in operations regulation. Utility corporate management involvement in training and qualifications of operations personnel is addressed in Recommendation 1.1 of Appendix A.

There are signs that the nuclear utility industry intends to commit new resources and the attention of its managers to achieving a significant improvement in operational safety. The establishment of the Institute for Nuclear Power Operations (INPO) is a step in that direction. We have been told that INPO will:

(1) Establish industry-wide benchmarks for excellence in the management and operation of nuclear power plants.
(2) Conduct independent evaluations to determine that the benchmarks are being met.
(3) Review nuclear power operating experiences for analysis and feedback to the utilities. Incorporate lessons learned into training programs. Coordinate information reporting and analysis with other organizations.
(4) Establish educational and training requirements for operations and maintenance personnel and develop screening and performance measurement systems.
(5) Accredit training programs and certify instructors.
(6) Conduct seminars and generic training for various utility employees, including instructors, utility executives, and upper management, to ensure quality in the operation of nuclear power programs.
(7) Perform studies and analyses to support development of criteria for operation, for training, and for the human factors aspects of design and operation.
(8) Provide emergency preparedness coordination for the nuclear utility industry.
(9) Exchange information and experience with operators of nuclear power plants in other countries.

These are necessary and important objectives, and they should be pursued with vigor. The NRC must soon decide what reliance, if any, to place in the future effectiveness of INPO in achieving these objectives. There are two motives for industry participation in INPO, namely, public safety and corporate finances. The NRC will need to understand to what extent the safety interests can be satisfied by this industry group and what other areas or criteria need to be addressed independently by the NRC (see Recommendations 1.4, 1.5, and 1.8).

2.3.2 Qualification of Personnel

A prerequisite to improved operational safety is an improvement in the qualifications of personnel. Nuclear power is a complex technology that demands highly competent personnel at all levels.

The accident at TMI-2 raises a number of questions about the technical qualifications of electric utilities to safely operate reactors. Many different groups have been addressing this subject in general cognizance of one another. For example, the staff is implementing the Lessons Learned Task Force recommendation in NUREG-0578 that the presence of a shift technical advisor be required so that the crew in the control room has the opportunity and the capability to better understand and diagnose complex nuclear plant transients. The Office of Nuclear Reactor Regulation has also provided recommendations in Commission Paper SECY 79-330E (Ref. 2) for upgrading the qualifications of licensed operators and senior operators through a program that includes increased training and testing in the areas of thermal-hydraulics and reactor transient response; increased use of simulator training and testing; higher passing grades on licensing examinations; and increased emphasis on retraining and reexamination. The Office of Nuclear Reactor Regulation is also conducting an overall review and is developing licensing criteria for the management and technical resources available to utilities who own and operate nuclear power plants to handle and support the response to unusual events or accidents. Another task force in the Office of Nuclear Reactor Regulation is reviewing new emergency procedures and training at all operating plants for small break loss-of-coolant accidents pursuant to a number of NRC Bulletins and Orders issued to licensees since the accident at TMI-2. The Office of Standards Development is revising and upgrading Regulatory Guide 1.8, "Selection and Training of Personnel." The ANS-3 Standards Committee is redrafting its basic personnel standard to upgrade qualification requirements. The ANS-3 Committee is also revising the standard that addresses minimum capabilities of simulators for use in operator training programs.

Most of these efforts are directed toward areas in which weaknesses can be readily identified and for which corrective action is easily agreed upon. We believe that all of these efforts are appropriate, but the activities are not well coordinated and there is no generally accepted goal to bind them together. The Commission should assure that the NRC has an effective plan to take the lead in articulating a coordinated approach and a generally accepted goal for technical qualifications for both onsite and offsite personnel and for both normal and accident conditions.

The specific additional recommendations of the Task Force in this area are contained in Appendix A and include (1) increasing NRC staff resources for review of utility operations capabilities and the assignment of responsibilities within the staff for an integrated licensing effort (Recommendation 1.5); (2) initiating a long-term program for raising the qualifications of shift supervisors and senior reactor operators (Recommendation 1.6); (3) examining licensee technical and management support cabilities (Recommendation 1.7); and (4) establishing licensing requirements for utility operations personnel besides the reactor operators and senior operators (Recommendation 1.8).

2.3.3 Training

In determining the qualifications of personnel, academic education, experience, health, and training are taken into account. A principal element in achieving the desired level of competence is training. Once a level of competence is achieved, it must be continually reinforced. Thus, training should be an ongoing process. Utility management must assure itself that personnel occupying all positions are able to perform the tasks required of them in normal and accident situations. The Task Force recommends that each licensee should be required to review its training program, using a position task analysis for all operations personnel, and to justify the acceptability of training programs on the basis that they provide sufficient assurance that safety-related tasks will be carried out effectively (Recommendation 1.2). It is expected that completion of this review will lead to the identification and correction of weaknesses where they exist in present training programs. We also see, in both government and industry, that there is a need to include the expertise of professional educators in improving reactor operations training programs (see Recommendation 1.5).

2.3.4 Emergency Operating Procedures

The use of properly prepared procedures in plant operations is another important ingredient in the matrix of operational safety. Attention must be given to both normal and emergency operating procedures. Although the Task Force recognizes the importance of normal operating procedures, it has, because of limits on time and expertise, directed its attention primarily to emergency operating procedures. Emergency operating procedures should consider system interactions and be written in such a manner that they are unambiguous and useful in crisis control. They should be based on thorough engineering evaluation and realistic analyses of the dynamic response of the nuclear power plant. The Task Force has found the NRC review process for emergency procedures to be inadequate and is recommending that present practice be changed to provide for interdisciplinary review of emergency procedures as part of the operating license review process (see Recommendation 4). Past practice was not sufficient because it did not specifically investigate the compatibility of emergency procedures with the design bases of the systems involved, nor was the discipline of human factors involved. The reviews should also include consideration of experience outside the commercial nuclear industry in the use of written procedures for crisis mitigation.

2.3.5 Working Environment and Operational Aids

The first line of reliance for safe operation of a nuclear power plant is the reactor operators and their immediate control room supervisor. Operator action in accordance with improved training and better operating procedures can prevent a number of challenges to safety systems and thus prevent potential accidents. In the event that safety systems fail and procedures do not apply, the operators are also the last line of reliance; i.e., they are the key component in contingency decisions and accident mitigation strategies if the design basis for the plant is exceeded. To diagnose and respond to plant disturbances, the operators must be well-qualified and their human actions must be integrated with the machine actions of the plant design. Control systems and related displays should also be integrated and easily identified

for the operators. In short, the operators must be provided with the knowledge and information necessary to fulfill their responsibilities, and an environment that keeps them alert and fit to respond to an emergency at all times, despite the routine of normal operations. Considerations for change include better management and technical staff support, more consideration of the man-machine interface in the redesign of existing control rooms and the design of future control rooms, improved training, increased staffing, improved working conditions, improved operating procedures, and better regulatory support. The Task Force has provided recommendations in these areas in Appendix A (see Recommendations 1, 2, 3, 4, and 7). These recommendations recognize the need to have operators ready to deal with the unusual and the need for frequent reinforcement of that readiness by retraining and requalification.

2.3.6 Verification of Correct Performance of Operating Activities

Human beings make errors no matter how qualified they are. Better systems of verifying correct performance of operating activities are needed to provide a means of detecting human errors and thus improving the quality of normal operations by reducing the frequency of occurrence of situations that could result in or contribute to accidents. The Task Force has provided a recommendation for more effective verification by licensees of correct performance of operating activities (see Recommendation 5).

2.3.7 Feedback of Information

Another essential component of improved operational safety is learning from experience. The Task Force has provided two recommendations in this area (Recommendations 6.1 and 6.2). The first recommendation concerns the integration of the new NRC and utility programs for evaluating operating experience. In order to assure that lessons are learned from operating experiences, there should be a structured, systematic, and coordinated national plan. The end-product of this process, the area of the second task force recommendation, is that the lessons learned must be fed back to the operators and other affected operations personnel and that changes in regulatory requirements must be accomplished in a timely manner.

2.3.8 Preparation for the Unusual

Everyone connected with nuclear power technology must accept as a fact that unusual situations can occur and accidents can happen. Operations personnel in particular must not have a mindset that future accidents are impossible. The experience of Three Mile Island has not been sufficient to erradicate that mindset in all quarters and the effects of that experience will fade with time. This is probably the single most important human factor with which this industry and NRC has to contend. We have no easy answer to suggest, but attitudes, through training and policy actions, must be changed.

Many of the preceding sections deal with preparations for the unusual and include recommendations for improvements in training, emergency procedures, and the man-machine interface. Two areas are worth reemphasizing. First, in the area of training, the Task Force recommends that each licensee be required to review its training program with respect to conducting in-plant drills and that a schedule be developed for in-plant drills as a part of a disciplined

training program for each station (see Recommendation 1.3). Second, one of the most important lessons learned from the Three Mile Island accident is that there is a need to rapidly improve the human factors engineering in the design and layout of existing and future control rooms (see Recommendations 7.1, 7.2, 7.3 and 7.5). The most highly skilled and trained operators are likely to make errors in a fast-moving situation if their instrument readings are ambiguous, or if the instrument displays are not quickly and easily understood. The use of best available technology to integrate and display data to give the operators a clearer understanding of the plant condition is an important step in improving the response capability for abnormal situations.

Control systems and related displays should be integrated and easily identified to improve operator response during off-normal and emergency operations. Also, process displays indicating the parameters of the plant, such as coolant temperature, pressure, and subcooling, should be integrated and readily viewable from normal stations and by the control room supervisor and shift technical advisor in accident situations. Operator aids, such as the process computer, can also be better utilized in off-normal situations to gather plant sensor data, analyze and format the data for hard copy print or video display to the operator, and serve as a concentrated summary of plant status. Additional operator aids, such as electronic systems for automatic status monitoring of safety systems, and possibly computer-based monitoring and analysis of plant disturbances to identify causes of disturbances, might also be used to enhance plant safety. We have tied a number of these elements together in our principal recommendation in the area of man-machine interface. It is the year-long safety review of all control rooms that is described in Appendix A (see Recommendation 7.1).

Related to the safety review of control rooms is a Task Force recommendation concerning plant safety system status monitoring (see Recommendation 7.2.). The objective of this recommendation is to provide a set of concentrated information that is easily available to the operators to enable rapid, continuous assessment of the safety status of the plant. It is expected that these two recommendations (7.1 and 7.2) will be tied together; licensees should develop the minimum set of plant parameters that defines the safety status of the plant as a part of the control room review, and that set of parameters should be concentrated in one location in the control room.

3. IMPROVEMENTS IN PLANT DESIGN

3.1 Introduction

Although the Task Force believes that operational safety merits primary emphasis by the NRC, means of improving or supplementing current plant designs should not be overlooked. Even though the radiological consequences experienced by the public at TMI-2 were small and well within the guideline values of 10 CFR Part 100, the performance and reliability of some of the engineered safety features at TMI-2 indicates to us that there are weaknesses in the current design requirements. The accident also involved a sequence of events more severe than those included in current design basis events, and thus it raises the question of whether other events should be included or whether additional accident mitigation features should be required. Having considered the policy aspects of these questions and available engineering evaluations of the feasibility and need for changes, the Task Force finds that there is a need to supplement current design requirements (Recommendations 8 and 9) and to include certain design features for mitigating accidents that are not provided by the set of design basis events (Recommendation 10).

3.2 Design Requirements

Current regulatory requirements for system design are of two kinds: performance and reliability. Performance is specified through the use of acceptance criteria for a set of design basis events that are evaluated according to approved analysis methods. Reliability, in its broadest sense, is specified through a set of overall requirements in the General Design Criteria that address quality assurance, seismic and other natural phenomena, and environmental qualification and missile protection. These requirements are supplemented by a requirement to comply with national codes and standards that specify materials; design, construction and inspection methods; inservice surveillance; and requirements for independence, separation, redundancy, and diversity.

All of these requirements are deterministic in form and are based primarily on engineering evaluation and judgment. The design basis events are not realistic descriptions of all of the numerous and varied events that could occur at nuclear power plants. Rather, they are representative of classes of events that have been judged to be of significant severity and sufficient likelihood to require consideration. Similarly, the associated analysis methods and acceptance criteria are also not realistic, but are conservative, convenient, or bounding representations of actual or expected conditions. Thus, current performance requirements are intended to encompass a broad spectrum of likely events, system responses, and ultimate consequences. The current reliability requirements are not direct translations of quantified statistical reliability criteria, but are methods and procedures derived from general engineering and design experience, supplemented by the special requirements of nuclear safety that are judged necessary and capable of assuring highly reliable components, equipment, systems and structures. Such specific, unambiguous deterministic requirements have been found to be a workable and necessary form for regulatory requirements. There remains, however, the possibility that significant event sequences have been overlooked and not included within the current design basis events, or that the deterministic design requirements are incomplete or inadequate for some events and systems.

There are two particular weaknesses in the current deterministic design requirements illustrated by the accident at TMI. The first weakness is illustrated by the recent review of auxiliary feedwater systems of some operating reactors, which was motivated by the TMI-2 accident. The review was conducted with the use of system reliability methods. It revealed some relatively low system reliabilities in particular designs because the existing single failure criterion excludes some passive failures and some operator errors. Better identification of these types of design inadequacies, if they exist in other systems, can be gained through systematic, integrated, quantitative evaluations of potential accident sequences and system responses. Probabilistic assessment techniques, including event and fault tree analysis, are powerful tools for accomplishing such evaluations. The Reactor Safety Study (WASH-1400, Ref. 3) was the first comprehensive application of this technique to nuclear power plants, but it was limited to two specific nuclear power plant designs. The technique has since been applied to additional designs.

The Task Force believes that probabilistic analysis has now been sufficiently developed to provide an effective method of assessing some aspects of reactor design and should be used to supplement current evaluations. However, although it is theoretically possible, the use of probabilistic analysis directly as a licensing requirement does not seem practical or worthwhile. In some areas, the technique is not valid. In other areas, the uncertainty in the estimates of reliability are so large as to make the analysis not useful. The technique requires substantially more effort to apply, on the part of both an applicant and the licensing staff, than do the deterministic criteria. The technique is best used for relative comparisons requiring the use of uniform methods and quantitative input data. However, the application of the technique by a multiplicity of applicants using various methods and sources of data would not be uniform. The Task Force concludes that uniform application of probabilistic assessment to a broad range of representative designs by one group, within the NRC, to assess the adequacy of specific designs, to identify systems with relatively low reliability, and to develop or modify current deterministic criteria would be the most effective use of this technique at this time. Our specific recommendation in this regard is provided in Appendix A (see Recommendation 8).

The second weakness in the current deterministic design requirements is the system used for classification and qualification of equipment. Current practice in the licensing of nuclear power plants is to apply design requirements to one class of components, equipment, systems and structures, the so-called safety-grade class, but not to another non-safety-grade class. This system of classification is based on the premise that things can be classed either as important to safety (that is, the function is credited in the analysis of a design basis event or is specified in the regulations) or not important to safety. Such a clear and distinct separation does not really exist; in fact, modifications of this classification have evolved in past practice to meet specific situations. Thus, for example, the functioning of some components that are not seismically qualified (a general requirement of safety-grade equipment) has been credited in the analysis of some events that are not initiated by an earthquake. Another example is that in some designs the function of non-safety-grade equipment is credited in the analysis of anticipated transients but not in the analysis of lower probability accidents.

The interactions between non-safety-grade and safety-grade equipment are numerous, varied, and complex and have not been systematically evaluated. Even though there is a general requirement that failure of non-safety-grade equipment or structures should not initiate or aggravate an accident, there is no comprehensive and systematic demonstration that this has been accomplished. Furthermore, the term "failure" when applied to non-safety-grade equipment has generally been defined as "failure to operate upon demand." There is evidence from Three Mile Island and other operating and licensing experience that the failure modes should also include unintended operation or unusual operation that might result from process or environmental conditions accompanying an event. For example, the high humidity or temperature following a loss-of-coolant accident might cause a relay, control circuit, or other component in a non-safety-grade system to operate or to function in a manner that unacceptably exacerbates the event.

The Task Force concludes that comprehensive studies of the interaction of non-safety-grade components, equipment, systems and structures with safety systems and the effects of these interactions during normal operation, transients, and accidents need to be made by all licensees and license applicants (see Recommendation 9). This would constitute a significant alteration of the current unresolved safety issue concerning systems interaction. The Office of Standards Development has previously been requested to develop a Regulatory Guide that would specify generic requirements for some safety-related systems that do not presently fall within the safety-grade classification. This effort would have to be closely coordinated with the study by licensees that we are now recommending. In the interim, the effects of the abnormal conditions that accompany transients and accidents on the operation and failure of non-safety-grade items should be reviewed by all licensees to determine if there are any probable adverse interactions. The extent of simultaneous interactions considered in this review should reflect the number of non-safety systems simultaneously exposed to conditions for which they were not designed. Equipment identified as the cause of unacceptable interactions should be appropriately modified to reduce the probability of that interaction, or the safety system that is adversely affected should be modified to cope with the interaction. In either event, operating procedures and operator training must be expanded to include consideration of the possible permutations and combinations of non-safety-grade system interactions with safety systems.

3.3 Defense in Depth

In current practice, there are essentially three levels of protection of the public from releases of radioactivity in the defense-in-depth concept. Each of the first two levels of protection has a design objective in the form of a limit on the release of radioactivity of a characteristic frequency. For normal operation, the design objective is to keep the levels of radioactive materials in effluents to unrestricted areas as low as reasonably achievable during conditions that are expected to occur one or more times during the life of the nuclear power unit. For accident conditions, the objective is to limit offsite radiation exposure to well within the guideline values contained in 10 CFR Part 100 following any of a set of design basis accidents that are representative of those events judged sufficiently likely to require consideration, as discussed in Section 3.2. The functions and general characteristics of the equipment, systems, and structures required for these two levels of protection

are specified in the General Design Criteria contained in Appendix A to 10 CFR Part 50 of the NRC regulations.

The third and less completely defined level of protection has as a design objective the reduction of exposure of the public when an accident occurs, including accidents beyond the so-called design basis accidents used in specifying the second level of defense in depth. This protection is provided by the requirements for siting nuclear power plants (i.e., 10 CFR Part 100) and for emergency response plans (i.e., Paragraph 50.34 and Appendix E of 10 CFR Part 50).

Except for actions to upgrade emergency plans and a proposal to modify siting requirements, the recommendations resulting from evaluations of the accident at TMI-2 have, up to now, been generally directed toward improving the first two levels of protection. That is, the actions are generally directed toward the prevention of high-consequence accidents beyond the current design basis, rather than toward mitigation of the consequences of such accidents.

The defense-in-depth concept is based on the premise that there is a limit to the effectiveness of any level of prevention. Unanticipated interactions and interrelationships among and between systems and the operators, and the possibility of undetected common modes of failure are a bound on the assurance of any level of prevention. The TMI accident is illustrative of the point. It was initiated and aggravated by component failures that had been identified in safety evaluations and considered in the plant design, but its ultimate severity resulted from a subtle interaction of elements including incompletely understood system response, inadequate training and procedures, and misleading instrument readings. As a consequence of these interactions, the operators were led to defeat the emergency core cooling function, a well-recognized common failure mode. Although the accident shows us ways to strengthen the current levels of protection, there can never be absolute assurance that only events within the current design basis will occur. Furthermore, even though more operating experience and evaluation will most likely reveal means of improving the systems or operations of current designs, these improvements will be specific to particular designs. It is our judgment that significant safety improvements in design, generally applicable to all designs, must lie in areas not now included in the design basis events. Said another way, within the current licensing design basis, and given the operational safety changes mandated by TMI-2, we believe that we have reached a point of diminishing returns in significantly reducing the probability of events outside of the current design basis. If a general imporvement in safety beyond that level is required, then new techniques that go beyond current licensing practices are needed.

Accidents that result in substantial melting of the core are the most significant, in terms of public risk, of the events not included in the current licensing design basis. Even though core-melt accidents are believed to have a lower frequency than the design basis accidents, their much larger consequences make them the dominant contributors to overall risk from nuclear power plants. The larger consequences do not solely arise because of the large quantity of radioactivity that would be released from molten fuel rods. It is the potential failure of the containment, and thus the eventual release of large amounts of radioactivity to the atmosphere, that is a dominant contributor to the risk. There is a substantial body of knowledge and opinion that the consequences of

a core-melt accident (and therefore the risk) can be significantly reduced if an option exists in the design to control and delay failure of the containment. Delay of containment failure increases the probability of arresting the course of the accident, increases the effectiveness of emergency plans, and allows for additional decay of the radioactive fission products. Available studies indicate that controlled venting of the containment to prevent failure due to overpressure could be an effective means of delaying ultimate containment failure by melt through. If appropriately filtered to partially decontaminate the gases that would be released in order to avoid overpressurization, such venting may significantly reduce the consequences and risk from core-melt accidents.

To varying degrees, the risk from core-melt accidents is already an implicit factor in the requirements for nuclear power plant siting, emergency response plans, and containment leak rates. It also has been treated to varying degrees in environmental impact statements for some specific plants, was the primary subject of the Reactor Safety Study (WASH-1400), and is the focus for the NRC improved safety research program. However, an explicit consideration of core-melt accidents in the design and operation of light water nuclear power plants has not been a part of current and past licensing scrutiny. Because the accident at Three Mile Island exceeded many of the present design bases by a wide margin and was evidently a significant precursor of a core-melt accident, the Task Force has concluded that the NRC should begin to formulate requirements for design features that could mitigate the consequences of core-melt accidents. It is important to note that the word "mitigate" does not mean "contain or prevent" when we use it in this context. It is also important to note that, lacking definitive policy guidance on the desired safety objective of reactor regulation (a topic addressed in some detail in Chapters 1 and 4 of this report), it is very difficult to judge whether design modifications to mitigate core-melt consequences would be necessary or sufficient to achieve that goal. It appears to us that sufficient studies have been completed to support a preliminary conclusion that controlled filtered venting of containments is an effective and feasible means of mitigating the consequences of core melting. We do not recommend going beyond that degree of mitigation, at least for all currently approved designs, except for continued core-melt research. However, not all of the relevant information on the use of filtered venting of containment has been evaluated, and the issuance of a regulatory requirement within the next few months is impossible. Sufficient information can probably be generated within the next year, including information from the NRC's research program for improved reactor safety. An evaluation and a Commission decision could be made soon thereafter as to whether to require this specific design feature for core-melt accidents in light water reactor power plants. As discussed in Chapter 2, a decision to include training for unusual events such as core-melt accidents could be made now. The Task Force recommends that this be done (see Recommendation 1.2). An effective means of assuring that all of the relevant information is considered and a timely decision on the need for controlled, filtered venting of containments would be to publish, within the next few months, a notice of intent to conduct rulemaking. The Task Force recommends (see Recommendation 10) that a notice of intent to conduct rulemaking be issued to solicit comments on the issues and specific facts relating to the consideration of controlled, filtered venting for core-melt accidents in nuclear power plant design and that a decision on whether and how to proceed with this specific requirement be made within one year of the notice.

Although core-melt accidents have the most significant consequences and are apparently the dominant contributors to the overall risk from nuclear power plants, the public perception of the risk includes all potential exposure to radiation. Thus, even though the accident at TMI-2 resulted in offsite doses that had statistically small health effects, the public has been intense in its aversion to any radiation exposure. Even though this may be inconsistent with the public acceptance, either knowing or unknowing, of other more probable and detrimental hazards, the aversion is there and should be recognized. The accident at TMI-2 also raises the question as to whether the potential for large releases of radioactivity from a core that has suffered damage, but not substantial melting, is greater than previously perceived. The prevalent engineering judgment prior to the accident was that, once severe core damage and consequent large releases of fission products from the fuel began to occur, there was only a small probability of arresting the course of an accident before substantial melting of the core occurred. The TMI-2 accident was arrested after the core was severely damaged, but before substantial melting occurred, and a significant fraction of the fission products was released to the containment. The Task Force believes that events of this type (i.e., core damage beyond the current design basis acceptance criteria but not including substantial melting) should be considered in the design of nuclear power plants and that additional design features should be provided to assure that offsite exposure can be limited. Since the guidelines of 10 CFR Part 100 are already representative of such a situation, these guidelines are probably appropriate for this class of accidents. Furthermore, if the qualifications of some existing safety equipment and some non-safety equipment were upgraded, the current designs are apparently better able to assure cooling of badly damaged cores than previously credited. However, protection of containment integrity (primarily from potential hydrogen explosions), monitoring and control of radioactivity from leakage, and the operability of systems required for post-accident control and recovery under the expected conditions resulting from such events, would need to be much better specified than they are at present. The Task Force believes that the recommended notice of intent to conduct rulemaking on core-melt consequence mitigation should also include the topic of coping with the effects of a degraded core and its consequences.

The two short-term recommendations from NUREG-0578 concerning hydrogen control in the containment building, for which implementation was deferred pending the completion of a broader study, should also be included within the scope of the rulemaking. It appears from information that we have reviewed that hydrogen control measures, for degraded core events short of core melt, that might be feasible and effective in some containment designs would not be as effective or feasible in others. For some deisgns, tt might also be possible that strong engineering arguments can be presented to prove that their degree of prevention of degraded core events is sufficient to offset the reduction of risk attainable by hydrogen control measures in other designs. These should be considerations in the rulemaking.

Current emergency procedures do not go beyond on the current design basis events. The scope of the rulemaking should also include emergency procedures for core-damage and core-melt accidents. The training of the operating staff, emergency procedures, radiation control and monitoring, and contingency plans for the procurement and installation of auxiliary equipment for the storage or processing of radioactive wastes should be specified in any final requirements.

4. IMPROVEMENTS IN NUCLEAR POWER PLANT REGULATION

In addition to the areas previously discussed, the aftermath of the TMI-2 accident and the general self-examination process that has accompanied it have brought forth challenges to the approach and effectiveness of the NRC's methods of establishing safety criteria and conducting licensing reviews. We believe there are a number of concepts that should be explored regarding the policy basis for regulatory decisions and how the staff implements its safety reviews.

4.1 Policy Basis

It is apparent after TMI-2 that we regulate in an environment that is largely governed by perceptions and subjective judgments rather than the more objective considerations of engineering, science, and law. For example, the fundamental proposition of NRC's role in accidents is subject to substantially different interpretations, according to whether it is considered in theory (i.e., statutorily), as it occurred in fact at TMI-2, or as it is perceived by others. Similarly, although the NRC staff deals in concepts of safety and risk every day from a predominantly scientific and analytical perspective, the public, the Congress, and the media generally react to their perception of risk whether or not it comports with the best technical assessments of reality. Lacking a national consensus on the approach to making safety judgments, there is an acute need within NRC for policy guidance to flow from the highest levels of the agency to the technical staff on what is an acceptable safety goal of reactor regulation. Such guidance should reflect a synthesis of views and priorities and should provide a clear objective for the staff to aim for in its day-to-day decisionmaking.

Without such guidance, the NRC staff will, of course, inevitably chart its own policy course simply because it must fulfill its licensing responsibilities. The requirement to perform value impact assessments does very little to help with this problem because we lack guidance as to whether cost-effective improvements are necessary to meet the basic goal of regulation. Our charting of the policy course is ad hoc, attuned to the problem of the moment, parochial to segments of the staff, and only coincidentally directed to achieving a common safety goal. Evidence that this is currently the situation is provided even by the short-term recommendations of this Lessons Learned Task Force. Those recommendations were judged by the Task Force as providing substantial additional protection required for the public health and safety, i.e., pursuant to the language of 10 CFR 50.109. Implicitly, this judgment embodied a policy determination that some increased level of safety was required. The Commission, by its endorsement of those recommendations, again implicitly embraced a new policy objective, but without it being labeled as such or clearly articulated. Even though it is possible to evolve policy on a continuing ad hoc basis (nearly 20 years of this form of regulation bear witness to the fact that it is possible), the lack of a definitive statement of the safety objective or goal of this agency creates an ever-increasing residuum of uncertainty within the staff as to the safety objective itself, as well as to the level within the agency from which such policy should issue. This leads to an erosion of the staff's ability, once having identified a potential safety concern, to discern the appropriate action and to act decisively.

Although it is possible to arrive at an implied safety goal by integrating the body of regulatory criteria generated over the past 20 years, neither the staff nor the public is well served by such an approach. First, it amounts to

safety being what the staff says it is through its imposition of regulatory requirements. Second, reliance on this form of inductive reasoning results in regulatory decisions founded on the following rationale: a plant is acceptable because it meets the current list of prescribed regulatory requirements, rather than a plant is acceptable because it meets the enumerated criteria that the staff finds sufficient to achieve the level of safety specified by the Commission's regulations. Although the difference may be subtle, in the world of reactor regulation, it is the difference between debating the need for a specific component or procedure because the staff thinks it is a good idea, and debating whether a component or procedure is necessary to achieve a stated national safety goal. The Task Force believes that the latter provides a much-needed basis for reasoned decisionmaking and is at the core of the long- standing debate on how backfit decisions are to be made for operating plants and plants under construction.

There are a myriad of possible safety goals and equally as many ways to articulate an agreed-upon goal. The goal could be phenomenon oriented such as no core meltdowns; it could be consequence oriented in terms of offsite releases, health effects, or property damage; it could be approached from an optimization view in terms of "as safe as reasonably achievable" or best technology available; or it could be based on the comparison of risks with those of other energy technologies. Most, if not all, of the possible formulations of a safety goal could be expressed in qualitative or quantitative terms.

The Task Force feels that it cannot stress enough the importance of a safety goal in achieving a balanced regulatory perspective. Recognizing the nature of the decision involved in choosing such a goal and the wide variety of inputs that need to be considered, the Task Force does not feel compelled, or uniquely capable, to specify the goal itself. We are mindful, however, of the extensive debate within the nuclear community as to the form that regulatory criteria should take (i.e., qualitative versus quantitative), and we would offer the following thoughts.

Traditionally, regulatory judgments have been routinely made, and to some degree successfully, on the basis of inherently subjective concepts such as reasonable assurance, as low as reasonably achievable (ALARA), and safety margins. Even though individual views will vary as to what constitutes conformance to a particular criterion, the collective judgments of the staff, the reviews of management and oversight committees, and input from public comments tend to yield reasonably balanced judgments. In addition, qualitatively defined goals are particularly amenable to flexible interpretation as the technology of reactor safety evolves and as perceptions of risk necessitate changes in emphasis. Also as a practical matter, many, if not the bulk of, regulatory decisions cannot be reduced to quantifiable terms, given the state of the art today. These advantages are gained, of course, at the expense of a certain amount of uncertainty and unpredictability in the qualitative judgments themselves.

The specification of quantitative standards, on the other hand, has much to offer in selected areas. In circumstances such as systems analysis, where there are methods and a growing body of data to quantitatively analyze and measure performance parameters, the quantitative goal is a powerful tool in providing informed, balanced decisions. Also, the relative importance of various risk contributors can be evaluated and resources allocated in the most

productive manner using quantitative standards. The obvious danger, and one that both the industry and the staff must be admonished not to abuse, is the almost endless opportunity for debate and disagreement over the methods and assumptions required for quantitative analysis. To allow numbers games to supplant the root safety question would inevitably cripple this method of specifying a safety goal.

With these thoughts in mind, the Task Force recommends the exposition by the Commission of clear subjective criteria defining the safety goal of nuclear power plant regulation. This goal would be used by the staff in the development of any new regulatory requirements and as a threshold for backfitting of these or current requirements to existing plants. The Task Force also encourages the Commission to supplement the subjective goal with quantitative criteria where possible and to the extent that they do not impede the capability for timely decisionmaking (see Recommendation 11).

The type of safety goal we envision would not necessarily need to be perfectly prescriptive. The need is for a criterion that is at least connotative of a level of safety. An example of a criterion that would tend to maintain the current level of safety would be based on a concept of "required for safety" where this was defined to be equivalent to the aggregate of requirements, practices, and policies set forth in the regulations (including, presumably, any rule changes flowing from post-TMI activities). Even though a certain amount of subjectivity would still be inherent in staff decisions on new regulatory requirements or licensing actions (since the regulations are largely criteria oriented), the decisions would be anchored in the necessity to be consistent with and in furtherance of the regulations. This would mean, however, that further staff consideration of practicality, cost benefit, or various other impacts would not be relevant to the threshold finding of being required for safety. It would also alleviate pressures, in fact or implied, to constantly improve the level of safety of reactors. This is not to say that safety improvements cannot be or should not be considered under this example. They could be considered by proposed additions to the regulations through rulemakings or in periodic re-evaluations of the level of safety being provided by current regulations. In any event, it is a basic policy question that should not cloud individual licensing decisions but should instead be channeled to a generic policy forum.

As previously discussed, a byproduct of the specification of a safety goal would be the clarification of backfitting decisions. Under this example, a proposed backfit would not need to provide substantial additional protection (as currently inferred under 10 CFR 50.109); anything required for safety would be sufficient. Similarly, a decision to backfit would naturally precipitate the need to backfit all nuclear plants, since it was required for safety, without agonizing over value impact studies or case-by-case determinations. The specifics of implementation would still be tailored as necessary, of course, to individual plants and would be consistent with the overall design of each plant.

Although the above example is only one of many possible goals, it demonstrates the impressive gains that are possible with even a modest attempt at goal articulation.

4.2 Integrated Systems Reviews

Whatever our safety goal, in restructuring our reactor regulatory organization we must be sensitive to the need for optimum allocation of limited technical resources to assure efficiency and effectiveness. There is a need to improve the quality of regulation and licensing, especially as they are applied to operating reactors.

The licensing reviews conducted by the various technical branches in the Office of Nuclear Reactor Regulation are basically audits of an applicant's design and design methods and result from more than a decade of gradual evolution. Distinctly different review approaches, varying from review of criteria to detailed design and analysis audits, are used by the staff in different technical areas and depend on the stage in life of the plant (construction permit, operating license, or in operation). To a large extent, these differences reflect the developing background, experience, and interests of the staff in the different areas over the years, and the influence of changing interests and concerns expressed by Congress, the Advisory Committee on Reactor Safeguards (ACRS), the Licensing and Appeal Boards, the industry, and the public.

We believe that it is neither feasible nor practical for the staff to review every element of every design. The audit review performed in reactor licensing relies on a selected number of verifications of the system design to assure that it adequately conforms to the regulatory criteria. The Office of Inspection and Enforcement also performs a limited number of verifications in the field to assure that the plant is being built and operated in conformance with regulatory criteria. Ultimate reliance is placed on the licensee, its vendor, and its architect-engineers and their quality assurance programs to adequately and consistently implement the details of the design of the plant with knowledge that a large percentage of their work will never be reviewed by the regulating body. The bulk of design errors will be discovered by the licensee or its suppliers and contractors because of the nature of the limited verification review and inspection conducted by the NRC. This does not indicate a weakness in the audit concept; rather it is the natural and predictable result. However, recognition of these facts highlights the need for very close scrutiny by a conscientious industry with good quality assurance programs at all stages and levels of design, construction, and operation, and for continuing NRC evaluation of these programs.

The audit review is basically a workable system that is consistent with our present statutory mandate, provides reasonably good coverage of important safety issues, and is consistent with the amount of resources that can be expected to be available now and in the future. Part of this satisfaction, quite candidly, is the lack of suitable alternatives. A complete design verification or certification process would, for example, entail enormous resources as well as require a design-oriented staff composition. Another factor favoring the audit review is its flexibility to allow the staff to emphasize particular review areas and to update its emphasis as issues become better understood or resolved and new concerns arise. Finally, our role in nuclear safety regulation is primarily at the criteria-setting level rather than the component design level. The detailed system reviews that we perform on an audit basis are aimed more to obtain feedback of how well a license

applicant is applying our criteria and fulfilling his basic responsibility for safety, rather than to provide a comprehensive verification.

The TMI-2 accident brought into focus, however, the fact that the staff safety reviews may be too prescriptive in nature and do not promote awareness or incentive to pursue on a broader basis new areas of potential safety concerns. The technical reviewers are required to spend too much time verifying that safety analysis reports have addressed all required aspects of the design rather than concentrating and collecting their efforts to challenge the adequacy of the overall design, particularly across systems interfaces and the man-machine interface. This is not to say that component level reviews are never appropriate, but that the emphasis should be on system level reviews. The burden for the detailed system design must be on the applicant who is more familiar with the design and who has the basic responsibility for the safety of the facility during all aspects of design, construction, and operation. The role of NRC should be to assure that this basic responsibility of the applicant is being met and that the overall system meets minimum safety requirements. If detailed verification and validation of the design is not being adequately accomplished by the applicant, then the application review should be suspended until the applicant does it correctly. The NRC staff should not have to perform the detailed verification and validation function as it often has when that function was found to be lacking.

Consistent with emphasizing a system level of review, post-TMI-2 activities have focused attention on the concept of performing reviews under the direction of some form of technical overview group. The recent reviews of auxiliary feedwater systems in operating plants demonstrated that bringing together the various technical reviewers under the direction of a technical review integrator provided an overall technical perspective and uniformity across all cases that improved the quality and timeliness of the review. The Lessons Learned Task Force is another example of how the combined expertise of a multidisciplinary technical review group can significantly improve the overall system and safety perspective of the individual reviewers, thus contributing to a more efficient and effective performance of the individuals, and more balance in the team's collegial view of overall safety. We believe that implementation, on a trial basis, of interdisciplinary reviews of selected license applications or operating reactors would provide further insight as to their feasibility and utility for general and routine use (see Recommendation 12).

Another aspect of this approach to reviews should be an accident evaluation function within the Office of Nuclear Reactor Regulation. This function would provide the capability for effecting changes and improvements in licensing requirements based on evaluation of accidents from initiation through consequences, and from insights gained from operating experience (see Recommendation 12).

Finally, a better system level of review would require that greater emphasis be placed on reactor operations and the control room operator and process interface. To promote the regulatory emphasis and staff growth and improvement needed in these areas, we recommend that all activities concerning reactor operations be consolidated into a single organizational entity. These activities would include reactor operation evaluation, operational quality assurance, human factors evaluation, personnel qualifications standards, and personnel licensing and certification (see Recommendation 12).

4.3 Unresolved Safety Issues

Section 210 of the Energy Reorganization Act of 1974 requires the development of a plan for specification, analysis, and progress reports for unresolved safety issues. Consistent with satisfying this Congressional requirement and with the safety significance of unresolved safety issues, a permanent, dedicated group should be created to continue with the expeditious resolution of these issues (see Recommendation 12). This need was emphasized immediately after the TMI-2 accident by the creation of a task force responsible for the resolution of unresolved safety issues that were identified in NUREG-0510, "Identification of Unresolved Safety Issues Relating to Nuclear Power Plants" (Ref. 4). That is, despite other compelling demands for staff resources, the unresolved safety issues maintained their highest priority status. This function needs to be continued and formally institutionalized to arrive at a resolution of current unresolved safety issues as well as those unresolved safety issues that will likely be identified as a result of the TMI-2 accident, including some of our final recommendations in the appendix to this report, and as a result of future operating experience.

4.4 Operating Experience

Consistent with the goal of significantly improving the operational reliability of licensed power reactors, the Task Force concludes that the NRC's operational surveillance program should parallel and complement the improvements recommended for licensees' programs as discussed in Chapter 2.

In this regard, the Commission has established an agency-wide Office of Operational Data Analysis and Evaluation that has the responsibility to analyze and evaluate operational safety data associated with all NRC activities. The Commission has also directed that complementary groups be formed in some of its program offices.

This decision has the full support of the Task Force. We urge that consideration be given immediately to the problem of how safety problems identified from operating experience and elsewhere are to be resolved and fixed. There is need for a workable, reliable mechanism to ensure that solutions to these problems are identified and then implemented on operating plants, consistent with better articulated safety goals and backfit criteria, as previously discussed. We suggest that it is necessary to dedicate a body of resources to this task in a fashion similar to the Unresolved Safety Issues (see Recommendation 12).

In this regard, we have observed that there can be a tendency on the part of the NRR staff to view the efforts of the various TMI related task forces as all-inclusive or that any items not addressed by a task force will lack sufficient visibility to assure timely implementation. This goes to the core of our finding that the NRR organization must be able to assure adequate consideration of such items in its normal configuration and through established paths. We recognize that there are a number of additional specific recommendations that could be made to improve design or operations that are not covered by this report. This report was not intended to address all of these specific requirements, but to address more fundamental and general policy bases. As additional items are identified, and we encourage continuing reflection by all

members of the NRR staff, we believe that they should be channeled to the Office Director level for priority setting and resource planning. This will serve as an ongoing challenge to develop the appropriate mechanism within NRR to effectively deal with safety issues as they are normally and naturally identified.

4.5 Emergency Response

A final aspect of improved reactor regulation is the definition and recognition of the emergency response role of the Office of Nuclear Reactor Regulation. We recognize that the NRR emergency response role will ultimately be constrained by what is determined to be the appropriate overall agency role in emergency situations. This general question has already been considered in several aspects by the Emergency Planning Task Force. The question will also continue to be studied in the context of the Commission's Special Inquiry, by the President's Commission, and the Congressional oversight committees in their continuing study of the Three Mile Island accident and its implications. Eventually, the findings and conclusions of all these efforts will need to be synthesized into a "consensus" position regarding this important policy question; that position will determine finally the scope and the structure of NRR's emergency response role and capabilities. The entire process, however, could take many months to complete.

The Task Force believes that what is already known regarding the weaknesses and limitations in the agency's capability to respond immediately and effectively in the Three Mile Island accident demonstrates a need to begin improving that capability on a much more immediate and urgent schedule than that dictated by the long-term "consensus forming" process outlined above. These considerations suggest the institutionalization (and refinement) of many of the ad hoc arrangements established for dealing with the Three Mile Island accident as well as the identification of other emergency response measures that may be appropriate. There is considerable work ongoing within the staff to redefine and improve the role and capability of the Executive Management Team and its support group. Another ongoing effort is the identification of the information required by licensee and NRC personnel at the onsite Technical Support Center (as discussed in NUREG-0578) to assess plant status in off-normal conditions. Beyond these efforts, one of our specific recommendations in Appendix A would improve the readiness of the Office of Nuclear Reactor Regulation for emergency engineering and analysis support of the overall agency response (see Recommendation 13).

5. REFERENCES

1. U.S. Nuclear Regulatory Commission, "TMI-2 Lessons Learned Task Force Status Report and Short-term Recommendations," USNRC Report NUREG-0578, July 1979. Available for purchase from NRC Public Document Room, 1717 H Street, NW, Washington, DC 20555 or from National Technical Information Service, Springfield, Virginia 22161.

2. Memorandum from H. R. Denton, NRC, to Commissioners, Commission Action Paper, Subject: Qualification of Reactor Operators (SECY 79-330E), July 30, 1979. Available for inspection and copying for a fee at NRC Public Document Room, Washington, DC 20555.

3. U.S. Nuclear Regulatory Commission, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975. Available from National Technical Information Service, Springfield, Virginia 22161. [NOTE: See also NUREG/CR-0400, "Risk Assessment Review Group Report to the United States Nuclear Regulatory Commission," H. W. Lewis et al., September 1978, and the "NRC Statement on Risk Assessment and the Reactor Safety Study Report (WASH-1400) in Light of the Risk Assessment Review Group Report," January 18, 1978.]

4. U.S. Nuclear Regulatory Commission, "Identification of Unresolved Safety Issues Relating to Nuclear Power Plants," USNRC Report NUREG-0510, February 1979. Available from National Technical Information Service, Springfield, Virginia 22161.

APPENDIX A
FINAL RECOMMENDATIONS OF TMI-2 LESSONS LEARNED TASK FORCE

INTRODUCTION

This appendix provides specific recommendations for achieving goals and policy objectives discussed in the report. They have been developed so that early steps toward implementation can proceed promptly in coordination with results of studies still taking place inside and outside the Nuclear Regulatory Commission. Unless otherwise stated in a specific recommendation, they are intended to apply to all commercial nuclear power plants.

The recommendations are arranged generally in the order of the main sections of the report. They are numbered sequentially for ease of future reference.

The recommendations are classed in two categories, defined as follows:

> Category I - Decisions to implement these recommendations can and should be reached promptly to provide increased safety. We recommend that these decisions be reached within three months.
> Category II - Implementation requires further study or research to fully define the necessary scope and ultimate requirements, or it involves a fundamental change in policy (e.g., rulemaking). We recommend that decisions on whether, how, and on what time schedule to proceed with these recommendations should also be made within the next three months.

Table A-1 lists the main headings of the recommendations, identifies their categories, and cross-references them to the body of this report.

TABLE A-1. FINAL RECOMMENDATIONS OF TMI-2 LESSONS LEARNED TASK FORCE

	Recommendations	Category	Report Chapter and Section
1.	Personnel qualifications and training		
	1.1 Utility management involvement	I	2.3.1
	1.2 Training programs	I	2.3.3
	1.3 In-plant drills	I	2.3.3, 2.3.8
	1.4 Operator licensing	I	2.3.1, 2.3.2
	1.5 NRC staff coordination	I	2.3.1, 2.3.2, 2.3.3
	1.6 Licensed operator qualifications	I	2.3.1, 2.3.2
	1.7 Licensee technical and management support	I	2.3.2
	1.8 Licensing of additional operating personnel	I	2.3.1, 2.3.2
2.	Staffing of control room	I	2.3.5
3.	Working hours	I	2.3.5
4:	Emergency procedures	I	2.3.4
5.	Verification of correct performance of operating activities	I/II	2.3.6
6.	Evaluation of operating experience		
	6.1 Nationwide network	I	2.3.7
	6.2 Providing information to operators	I	2.3.7
7.	Man-machine interface		
	7.1 Control room reviews	I	2.3.5, 2.3.8
	7.2 Plant safety status display	I	2.3.5, 2.3.8
	7.3 Disturbance analysis systems	II	2.3.5, 2.3.8

TABLE A-1. FINAL RECOMMENDATIONS OF TMI-2 LESSONS LEARNED TASK FORCE (Cont'd)

	Recommendations	Category	Report Chapter and Section
	7.4 Manual versus automatic operations	II	2.1, 2.3.5
	7.5 Standard control room design	II	2.3.5, 2.3.8
8.	Reliability assessments of final designs	I	3.2
9.	Review of safety classifications and Qualifications	I	3.2
10.	Design features for core-damage and core-melt accidents	II	3.3
11.	Safety goal for reactor regulation	I	4.1
12.	Staff review objectives	II	4.2, 4.3, 4.4
13.	NRR Emergency Response Team	I	4.5

1. PERSONNEL QUALIFICATIONS AND TRAINING

1.1 Utility Management Involvement

The corporate management of each licensee should establish a definitive presence and involvement in the selection, training, and qualification of operations personnel. To assure that this has been accomplished, the NRC should require, as part of the application for operator and senior operator licenses, that corporate management certify the competence and fitness of the applicants. Such certification should be required by the highest level of corporate management responsible for plant operation (for example, the Vice-President for Operations). The Task Force recommends that, when the NRC staff judges the quality of applications from a particular utility to be deficient, the corporate official certifying the competence of the applicants be required to discuss the reasons for the decline in competence and planned corrective action with the Director of Nuclear Reactor Regulation.

1.2 Training Programs

Each licensee should be required to review, within one year, its training program for all operations personnel, including maintenance and technical personnel, and should justify the acceptability of training programs on the basis that these programs provide sufficient assurance that safety-related functions will be effectively carried out. Documentation of this review and justification should be retained on site for inspection, but need not be submitted to the NRC for review. The preferred method of fulfilling this recommendation is a position task analysis, in which the tasks performed by the person in each position are defined and the training, in conjunction with education and experience, is identified to provide assurance that the tasks can be effectively carried out. The position task analysis should include normal and emergency duties, including maintenance activities, placing emphasis on the role played by every member of an operations organization in assuring safe plant operations. All levels of the operations organization should be included. This action is regarded by the Task Force as an interim measure pending resolution of the question of licensing of additional operations personnel beyond reactor operators and senior reactor operators, as discussed in Recommendation 1.8 of this appendix.

The scope of emergency duties defined in the position task analysis should not be restricted to only the transients and accidents considered in the design basis. The training should recognize that events beyond the current licensing design basis events can occur.

The training should include the use of the systems already installed at the plant to control or mitigate the consequences of accidents in which the core is severely damaged. This training would be an interim measure pending completion of the rulemaking to determine what design features to mitigate these more severe accidents should be required.

1.3 In-Plant Drills

Each licensee should be required to review, within 90 days, its training program with respect to the conduct of in-plant drills. For tasks performed by shift operating personnel in response to off-normal or accident situations,

licensees should assure that sufficient in-plant drills are conducted to enable personnel to maintain proficiency in those tasks. The Task Force considers drills of a walk-through nature acceptable and does not mean to imply the actual manipulation of controls or equipment or initiation of an event (such as by the opening or closing of valves or tripping breakers or pumps). The Task Force considers that drills requiring the physical manipulation of controls are also important but can be more efficiently and safely conducted using an appropriate nuclear power plant simulator. With this in mind, each licensee should develop a schedule for in-plant drills. This schedule should be a part of a disciplined training program for each station. It need not be submitted to the NRC for review; however, it should be available at the site for inspection.

1.4 Operator Licensing

The first areas of personnel qualification that need to be upgraded are those pertaining to licensed senior reactor operators and reactor operators. NRR recommendations to the Commission for improvements in the operator licensing program were contained in Commission Paper SECY 79-330E (Ref. 2). We believe these recommendations should be treated as the first steps in a long-term program to upgrade operator proficiency. They are, however, necessary improvements in the program. The ultimate resolution of the issue of qualifications of reactor operators should take a broader perspective. Although the Task Force generally agrees with the recommendations contained in SECY 79-330E, we recommend implementation of the following additional items by the regulatory staff in conjunction with the implementation of the recommendations in SECY 79-330E.

(1) As part of the inspector training program of the Office of Inspection and Enforcement (IE), operator licensing program personnel of the Office of Nuclear Reactor Regulation should (a) provide information to IE inspectors on the operator licensing program and (b) identify the types of information the IE inspectors should provide to assist NRR in making decisions with regard to the renewal of operator licenses.

(2) The NRC staff should establish a mechanism whereby individuals committing operational errors are identified in Licensee Event Reports. Such a mechanism should include provisions for protection of the privacy of the individual. The intent of this recommendation is to provide additional information to operator licensing program personnel to assist them in determining the continued qualification of operators in the review of operator license renewal applications. Due consideration should be given to whether such reporting will affect the quality of reports received by the NRC.

(3) As part of the training program for all licensed operators, a one-week course should be conducted by the NRR operator licensing program personnel with assistance from other NRR technical personnel. Particulars of the course would include:

    (a) Safety analyses
    (b) Probabilistic assessments
    (c) Current safety issues and recent significant operating experience
    (d) NRC and industry responsibilities for safety

This recommendation would reinforce the knowledge of and respect for accident/transient sequences as well as providing a positive feedback for better decisions by NRC staff on reactor operations and design matters. Additional NRC staffing will be required to accomplish this objective.

(4) Prior to assuming initial assignment as shift supervisor or shift technical advisor and on a biennial basis thereafter, individuals should be interviewed by an interdisciplinary group of NRC staff. Such interviews should probe the individual's technical knowledge in the area of transient and accident response and, in the case of a shift supervisor, the managerial ability to command and control the activities of shift personnel.

These interviews should be conducted at NRC headquarters. Criteria for subjects to be covered and acceptable standards of performance of individuals should be developed by NRR operator licensing personnel prior to promulgation of this requirement. This action will require a considerable expenditure of resources and its phasing needs to be carefully considered.

(5) The NRR operator licensing program personnel should sponsor an annual workshop for licensed operators to be attended by at least one representative of the licensed shift personnel at each unit. The purpose of this workshop is to provide an opportunity for exchange of information on operating experiences between the NRC staff and the utility shift personnel. For example, such a seminar could lead to an exchange of information on (a) NRC safety concerns related to shift operations, (b) the impact of licensing on shift activities and personnel, and (c) recommendations from shift personnel concerning changes in reactor regulation that would improve safety.

(6) As a less prescriptive alternative to Recommendation 6 of SECY 79-330E that "Phase II, III, and IV cold training program instructors and all hot training program instructors that provide instruction in nuclear power plant operations hold senior operator licenses and be required to successfully participate in applicable requalification programs to maintain their instructor status," the following is considered acceptable: Such instructors should hold or have previously held a senior reactor operator (SRO) license on a comparable nuclear power plant and currently possess instructor certification from the Institute of Nuclear Power Operations, provided the INPO certification program has been examined and found acceptable to the NRC. Emphasis should be placed on an instructor's ability to instruct, in addition to his technical competence.

(7) Consideration should be given to placing resident operator licensing examiners in each of the major geographical areas in which there is a concentration of training centers using nuclear power plant simulators. The intent of this recommendation is to provide for greater interaction by operator licensing examiners in operator qualification and requalification programs.

1.5 NRC Staff Coordination

At the present time, several groups are addressing the subject of qualifications of personnel somewhat independently of one another. Even though each of the efforts is appropriate on a short-term basis, a coordinated approach must be developed for the long term. The NRC should increase the staff resources in this area, assure the hiring of needed professional disciplines to increase present staff capabilities, and designate responsibilities and organizational entities within the various offices.

1.6 Licensed Operator Qualifications

A program for raising the qualification requirements for shift supervisors and senior reactor operators should be established. The distinction being made in present practice between senior reactor operators (e.g., shift foreman in a multi-unit station) and shift supervisors should be recognized. As a short-term action pursuant to NUREG-0578 (until such time as staffing and qualification of shift personnel and the control room man-machine interface requirements are upgraded), each licensee has been required to provide an on-shift technical advisor to the shift supervisor. Within the next five years, it is recommended that the qualifications of senior reactor operators and shift supervisors be upgraded as indicated below. Qualification requirements for applicants for licensing prior to initial fuel loading may require special additional considerations, particularly with respect to experience.

(1) Shift Supervisor (person in charge of operations on shift at the station) - Shift Supervisors should have at least a Bachelor of Science degree or equivalent training and experience in engineering or the related physical sciences. The Shift Supervisor should also hold a senior reactor operator's license (issued under new proposed requirements defined below) and have served as a reactor operator for one year or senior reactor operator for six months. In establishing equivalency with a Bachelor of Science degree, consideration should be given not only to formal courses in engineering and related sciences, but also to education in the liberal arts. It is recommended that the use of the equivalency to a Bachelor of Science degree be exercised to only a limited degree and that most shift supervisors hold degrees. It is also recommended that shift supervisor qualifications include leadership training and experience.

(2) Senior Reactor Operator (e.g., shift foreman in a multi-unit station) - Senior Reactor Operators should have at least the same general technical education and specific training in transient and accident response characteristics of nuclear power plants as recently articulated for the shift technical advisor. Additional recommendations for upgrading senior reactor operator qualifications are identified in the Commission Paper SECY 79-330E on Qualification of Reactor Operators.

(3) At present, a basic fundamentals course of approximately twelve weeks is required as part of the operator training program. A prerequisite to satisfactory performance of nuclear power operation is the fundamental understanding of nuclear technology. The Task Force beieves twelve weeks to be insufficient time to provide a broad and comprehensive level of understanding in the fundamentals of nuclear technology. It is recommended

that the NRC, perhaps in consultation with INPO, examine the content of the basic fundamentals course and establish definitive instructional requirements for the course.

1.7 Licensee Technical and Management Support

The review and evaluation (being conducted by the Quality Assurance Branch) of the management and technical resources available to utilities who own and operate nuclear power plants to handle unusual events or accidents should be completed, and regulatory guidance should be developed that covers the capabilities and role of technical and management personnel in the normal operation of the plant and during an emergency. The criteria should contain a requirement for periodic verification of the licensee's technical and management support capability throughout the operating life of the plant. The present criteria for determining the acceptability of licensee technical and management support is very general and applies only to normal plant operations.

1.8 Licensing of Additional Operating Personnel

The staff should decide which plant personnel, other than reactor operators and senior reactor operators, should be licensed. NRC review of the training and qualifications of nonlicensed personnel has been very limited in the past, based on the assumption that it is the licensed operators who have the most important influence on plant safety. A number of examples from the TMI-2 accident indicate the degree to which plant safety can be greatly influenced by persons in many positions, including managers, engineers, auxiliary operators, maintenance personnel and technicians. All of these previously nonlicensed personnel may affect plant operation, and their roles should receive greater attention from a safety perspective. Answering the questions of how much independent examination of their qualifications and training is necessary and whether NRC licensing is appropriate is a significant undertaking. The prerequisites to an effective examination program are definitive qualification requirements and specific training programs. The current NRC guidelines addressing nonlicensed personnel training and qualification are very general and are not suitable for a licensing program.

The newly formed Institute of Nuclear Power Operations intends to develop standardized training requirements for technicians and nonlicensed operators and to provide certification for the training of these personnel. The Task Force believes this program, if properly implemented in a timely way, could substitute for detailed guidance from NRC, and could, under the right conditions, be endorsed by NRC as meeting its independent licensing requirements for additional operating personnel. A statement of understanding between INPO and the NRC should be established at an early date (within the next six months) so that both groups can decide whether and to what extent to proceed independently.

2. STAFFING OF CONTROL ROOM

The Commission's regulations should be revised to more clearly state present staff requirements (as described in the Standard Review Plan, Section 13.1.2) for minimum shift staffing of licensed reactor operators. The governing regulation, 10 CFR 50.54(k), states that "an operator or senior operator licensed pursuant to Part 55 of this chapter shall be present at the controls

at all times during operation of the facility." For single-unit power stations, the staff requires the shift crew to include at least one licensed senior reactor operator, two licensed reactor operators, and two additional operators (auxiliary operators) during reactor operation. For multiple-unit power stations with separate control rooms, the staff also requires the shift crew to include at least one licensed senior reactor operator and two licensed reactor operators for each operating reactor. For multiple-unit power stations with a common control room, the staff permits a reduction of licensed reactor operators to one per unit plus one additional reactor operator with the other requirements remaining the same. However, the staff does not require the presence in the control room at all times of two licensed operators and the senior reactor operator. In developing the revision to the regulations, consideration should be given to requiring the presence in the control room at all times during normal operations of two reactor operators and one senior reactor operator. Provisions for tours of the plant by operators will probably need to be made if this staffing proposal is adopted.

3. WORKING HOURS

Each licensee should be required to review and revise within 90 days the plant administrative procedures to assure that a sound policy is established covering working hours for reactor operators and senior reactor operators. It is recognized that this is a complex subject involving other interests (e.g., labor unions). The NRC staff should assure that the subject is addressed in a comprehensive manner by all licensees and that the other interests not be allowed to interfere with the basic safety interest. As general guidance, it is expected that licensees' administrative procedures will make it unlikely that personnel would have to be used for more than two consecutive work periods in excess of 12 hours and that a 12-hour rest period would be required between work periods. In the event that special circumstances arise that would cause extended periods of work in excess of 12 hours for more than two consecutive days, such work should be authorized by the Station Manager with appropriate documentation of the cause. Indications aside from Three Mile Island lead the Task Force to conclude that this step must be taken to reasonably assure that individuals are in proper physical condition to perform work at nuclear power plants.

4. EMERGENCY PROCEDURES

Emergency operating procedures for all nuclear power plants should be reviewed by the NRC. The review should be conducted by interdisciplinary review groups comprising I&E inspectors and NRR technical reviewers knowledgeable in system design, accident analysis, operator training, theories of education and crisis management, human factors, and the underlying technical bases for licensing. Special attention should be paid to the recent advice of the ACRS on the style and content of emergency procedures. A safety evaluation regarding the adequacy of the emergency procedures should be issued at the conclusion of the review. Previous NRR reviews and I&E reviews of emergency operating procedures did not specifically investigate their compatibility with the design bases of the systems involved nor was the discipline of human factors included.

This action will require a considerable expenditure of resources and its phasing needs to be carefully considered. It may be satisfactory to limit the general application of this recommendation to new operating licenses for the next year or so. These initial few reviews by the staff, with oversight by the ACRS, will provide the time and experience necessary for the staff and industry to develop and agree upon acceptance criteria for the development, formatting, and future review of all emergency operating procedures. Upon completion of these acceptance criteria, say within the next two years, a systematic effort by all licensees to review their emergency procedures and revise them as necessary could be conducted more productively than it could today.

5. VERIFICATION OF CORRECT PERFORMANCE OF OPERATING ACTIVITIES

A more effective system of verifying the correct performance of operating activities is needed to provide a means of reducing human errors and improving the quality of normal operations, thereby reducing the frequency of occurrence of situations that could result in or contribute to accidents. Such a verification system should include automatic system status monitoring and human verification of operations and maintenance activities independent of the people performing the activity.

The Task Force recommends that automatic status monitoring be required by a decision to backfit Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," to plants not already required to meet it. Furthermore, the design to satisfy the objectives of the guide should be flexible and capable of accepting additional monitoring functions at a later date.

The implementation of Regulatory Guide 1.47, although reducing the extent of human verification of operations and maintenance activities, does not eliminate the need for such verification in all instances. Therefore, each licensee should be required to review his procedures for maintenance, test, surveillance and other normal plant operations activities (1) to delineate each activity that requires independent verification because of its importance to safety, (2) to identify the personnel responsible for conducting the verification, and (3) to describe the method of documenting performance of the verification process. The results of this work should be submitted to NRC within six months for use in the development of minimum acceptance criteria for operations verification procedures, probably in the form of a Regulatory Guide. The procedures adopted by the licensees should contain two phases; namely, before and after installation of status monitoring equipment in conformance with Regulatory Guide 1.47.

6. EVALUATION OF OPERATING EXPERIENCE

6.1 Nationwide Network

An integrated NRC-utility program to evaluate operating experience should be established. Action within the NRC has been initiated to establish an Office of Operational Data Analysis and Evaluation to provide agency-wide coordination and an overview of all operational data analysis-related activities performed within the line offices of NRC. The nuclear industry, through NSAC and INPO,

has established its own operational evaluation program. Pursuant to the recommendations of NUREG-0578, each licensee is now required to have an operations experience evaluation group. The director of the new NRC Office of Operational Data Analysis and Evaluation should take the lead to assure that these diverse programs are formally tied together to the extent necessary to benefit from one anothers' viewpoint and analysis while recognizing their individual responsibilities.

6.2 Providing Information to the Operator

Each licensee should be required to review, within 90 days, its administrative procedures to assure that a mechanism exists through which lessons learned from operating experience contained in various publications (such as IE Bulletins, Circulars and Notices, and applicable Licensee Event Reports) and from the licensee's own operating experience evaluation group are conveyed to the reactor operators and other affected operations personnel.

Two ways of accomplishing this objective are (1) standard distribution lists or publications and (2) regularly scheduled lectures as part of operations staff retraining. This recommendation is intended to assure that operators and other operations personnel are continually provided with lessons learned from operating experience.

7. MAN-MACHINE INTERFACE

7.1 Control Room Reviews

All licensees should be required to conduct a one-year review of their control rooms. The safety review should consider control room design and control room operational procedures, including emergency operating procedures. In this review, the licensees should evaluate:

(1) The adequacy of information presented to the operator to reflect plant status for normal operation, anticipated operational occurrences, and accident conditions;

(2) The grouping of displays and the layout of panels;

(3) Improvements in the safety monitoring and human factors enhancement of controls and control displays;

(4) The communication from the control room to points outside the control room, such as the on-site Technical Support Center. (This communication link must also be coordinated with new requirements for transmission of plant systems data to NRC.);

(5) The use of direct rather than derived signals for the presentation of process and safety information to the operator;

(6) The operability of the plant from the control room with multiple failures of non-safety-grade and non-seismic systems and control room systems;

(7) The adequacy of operating procedures and operator training with respect to limitations of instrumentation displays in the control room;

(8) The categorization of alarms, with unique definition of safety alarms; and

(9) The modification of operating procedures and operator training programs as a function of control room modifications resulting from this review.

The purpose of this recommendation is to improve upon operator-process communications. Guidelines and criteria for the control room design review are now being drafted by the Division of Systems Safety, including consideration of the results of previous studies of this sort and existing technology outside of the nuclear industry. Explicit criteria can probably be developed by about February 1, 1980. Consideration is being given to a series of topical meetings with recognized experts in the field and affected licensees. Specific requirements for backfitting existing control rooms to correct deficiencies will be established in the course of the reviews by licensees.

7.2 Plant Safety Status Display

Each licensee should be required to define and adequately display in the control room a minimum set of plant parameters (in control terminology, a state vector) that defines the safety status of the nuclear power plant. The minimum set of plant parameters should be annotated for sensor limits, process limits, and sensor status. The annotated set of plant parameters should be presented to the operator in real time by a reliable, single-failure-proof system located in the control room. The annotated set of plant parameters should also be available in real time in the Onsite Technical Support Center.

The objective of this recommendation is to require a concise set of information that is easily available and assessed by the operator and the shift technical advisor to ascertain the safety status of the operating process. The implementation of this recommendation should be undertaken in conjunction with the year-long control room study previously described, but should be completed by January 1, 1981, in consonance with the final implementation date for the onsite technical support center recommended in NUREG-0578. As a further guideline for the development of the safety state vector, the status of the plant process should be designed and instrumented as a function of the various barriers against release of radioactivity. For example, the two primary barriers are the fuel cladding and the reactor coolant pressure boundary. Thus, parameters such as primary liquid inventory and coolant radioactivity levels would be principal components of the state vector for these levels of defense. Similarly, reactor coolant level, containment water level, containment hydrogen content, etc., would be principal components of the state vector for the engineered safety feature levels of defense.

7.3 Disturbance Analysis Systems

We recommend that the Office of Nuclear Regulatory Research establish a program to evaluate the safety effectiveness of designs of disturbance analysis systems. This program should consider the evaluation of all pertinent methodologies being used in disturbance analysis systems. The evaluations should be quantitative in

nature and include prototype assessments in operating power plant environments. Experience gained in this program should be used to consider whether regulatory requirements should be formulated for the use of disturbance analysis systems in operating plants.

7.4 Manual versus Automatic Operations

We recommend that the Office of Nuclear Regulatory Research formulate a program to establish a technical basis for definitive licensing criteria for manual and automatic operations for systems which execute plant safety functions and safety-related functions. The study should include examination of the feasibility of backfit of its conclusions and recommendations to operating plants. The role of the operator should be specifically examined. Complexity of the safety function, the rapidity of the initiating events, the response time available to diagnose the event and to implement corrective action, and verification of the corrective action should be considered in the program. The scope of the proposed study includes the operator, the control room, displays and instrumentation, in addition to the manual and automatic controls that execute safety functions. The research team should consist of human factors engineers, control engineers, and nuclear system engineers and analysts.

7.5 Standard Control Room Design

The Institute of Electrical and Electronic Engineers (IEEE) has established a standards development committee to define design requirements for the standard control room. The regulatory staff is represented on the committee. We recommend that this standards committee expeditiously complete its work of establishing standard design requirements for future control rooms. The design requirements should consider the lessons learned from the TMI-2 accident as well as the principles of human-factors engineering for the man-machine interface. Upon completion of the standard, the Office of Standards Development should evaluate the standard for its acceptability in the licensing process, including consideration of its partial applicability to plants under construction.

8. RELIABILITY ASSESSMENTS OF FINAL DESIGNS

The staff should initiate a systematic assessment of the reliability of safety systems in operating units and in units in the late stages of construction using simplified fault and event tree analyses. Since these assessments go beyond the requirements of current regulations, their completion should not be a condition of licensing for operation. The purposes of these assessments would be (1) to audit the implementation of the current NRC design requirements by searching for areas that have potential to seriously decrease reliability, and (2) to identify outliers in overall system safety compared with designs previously subjected to this type of review. Measures to correct any problem areas should be promptly referred to the cognizant licensing organization where, in consultation with the Regulatory Requirements Review Committee, backfit decisions are to be promptly reached. If a particular deficiency is identified and known to exist in several systems or plants, appropriate revisions to NRC design requirements should be made with all licensees and applicants being directed to implement the design revisions in their plants.

Possible approaches would be to assess all systems in one plant or several systems in all plants. An acceptable combined approach would be to do all systems in a few lead plants and then proceed plant by plant unless particular systems indicated possible generic problems. The suspect systems would then by assessed in all plants, in the manner employed with PWR auxiliary feedwater systems in the summer of 1979. This recommendation would apparently be satisfied by the Integrated Reliability Evaluation Program currently under development in the Office of Nuclear Regulatory Research with the previously expressed concurrence of the Office of Nuclear Reactor Regulation.

9. REVIEW OF SAFETY CLASSIFICATIONS AND QUALIFICATIONS

The owners of operating plants and all plants under construction should be required to evaluate the interaction of non-safety and safety-grade systems during normal operation, transients, and design basis accidents to assure that any interaction will not result in exceeding the acceptance criteria for any design basis event. The review should be systematic and include all non-safety components, equipment, systems, and structures under all conditions of normal operation, anticipated operational occurrences, and design basis accidents initiated both within the plant (such as pipe breaks) and from outside the plant (such as earthquakes, other natural phenomena, and offsite hazards). The interactions and effects should consider various failure modes including spurious operation, failure to operate upon demand, and any unusual or erratic operation that might result from exposure to the abnormal process or environmental conditions accompanying the event under study. As a necessary part of this evaluation, proper qualification of safety systems, including mechanical components, should be verified.

The number of simultaneous failures of non-safety equipment considered should reasonably reflect the expected number of non-safety systems simultaneously exposed during the event under study to conditions for which they were not designed or qualified.

Equipment identified as the potential cause of violation of the acceptance criteria for any design basis event should be appropriately modified to eliminate or significantly reduce the probability of the adverse interaction. Alternatively, the affected safety systems or structures should be modified to cope with the interaction. The results of the evaluations should be used to review, and modify as appropriate, the plant operating and emergency procedures and operator training. The Task Force recommends that these studies be completed within a year, at which time licensees should submit proposed schedules for making the modifications identified in the evaluations. Completion of this study would not be a condition of licensing new plants in the interim of one year if the basis for continued licensing in face of the present unresolved safety issue on systems interaction is judged by the staff to continue to be valid.

10. DESIGN FEATURES FOR CORE-DAMAGE AND CORE-MELT ACCIDENTS

The Task Force recommends that the Commission issue within three months a notice of intent to conduct rulemaking to solicit comments on the issues and facts relating to the consideration of design features to mitigate accidents that would

result in (a) core-melt and (b) severe core damage, but not substantial melting. Specific areas for comment should include, but not be limited to, the following:

(1) Are design features to mitigate the consequences of either or both of these types of accidents necessary to provide reasonable assurance that the health and safety of the public are protected?

(2) In lieu of such features, should additional and supplemental means of preventing core damage or core-melt accidents, through improved engineered safety features be required?

(3) What should be the objective of such design features? Should the design objectives be a set of specific acceptance criteria (e.g., some limitation on calculated offsite dose) or the reduction of potential offsite exposure that is reasonably achievable?

(4) What should be the characteristics and functions of such design features?

(5) What are the probabilities and consequences of the various event sequences that might result in releasing significant amounts of radioactivity to the environment? Which sequences are amenable to interdiction and by what means?

(6) What is the expected effectiveness and performance of suggested means of reducing the consequences of events in which severe damage or substantial melting of the core occurs, in particular, systems for controlled, filtered venting of the containment and for preventing the uncontrolled combustion of hydrogen?

(7) How should other requirements, and in particular those for siting, emergency plans and procedures, training or other related areas, be modified if such design features were required?

(8) What additional information is required or desirable before setting requirements? What information is available, and what information needs to be developed through experiment, test, analysis, or evaluation?

(9) What should be the final form of the requirement, if any? What should be the implementation schedule for new plants, plants under construction, and operating plants?

The Task Force recommends that a proposed rule be published for public comment within one year of the notice of intent.

11. SAFETY GOAL FOR REACTOR REGULATION

The Commission should undertake with the staff the development and articulation of clear criteria to define the basic safety goal for nuclear power plant regulation. Since this goal will be used as a benchmark by the staff in defining new regulatory requirements, definitive policy guidance should also be developed regarding the threshold for backfitting of new requirements to existing plants. The Task Force believes that the goal should be supplemented where possible with quantitative reliability or risk criteria, with limitations

being placed on their use to assure that such criteria do not impede the capability for timely decisionmaking.

12. STAFF REVIEW OBJECTIVES

The approach, methods, and organization of the NRC staff in performing licensing reviews of nuclear power plants should be revised to emphasize the following objectives:

(1) An overall system level, integrated review that gives full consideration to operational safety aspects and provides for a design basis accident assessment function from event initiation through consequence mitigation, including the review of emergency operating procedures.

(2) Timely analysis of operating experience and implementation of needed changes derived from operating experience.

(3) Discipline in the application of a single overall safety goal.

(4) Continuity of licensing cognizance and responsibility from initial plant licensing, throughout construction and into operation.

(5) Technical oversight of Safety Evaluation Reports to assure increased emphasis on safety while still satisfying the requirements of the administrative process of regulation.

(6) Assurance of adequate operations experience and training for the NRC technical review staff, especially those staff members assigned responsibility in accident response situations.

(7) Dedication of adequate resources to the three principal functions of the Office of Nuclear Reactor Regulation: reactor licensing, oversight of operating reactors, and resolution of generic safety issues.

(8) Use of a formal procedure for followup on questions and requests from the Advisory Committee on Reactor Safeguards and its individual members.

13. NRR EMERGENCY RESPONSE TEAM

The Task Force recommends the establishment of a designated NRR Emergency Response Team (ERT) to be on immediate call in the event of emergencies. The ERT should be a multi-disciplinary group composed of NRR personnel knowledgeable in reactor systems, instrumentation and control, core physics, accident analysis, radiation control, and health physics. In the selection of team members, emphasis should be given to applicable operations experience where possible, and the team should be trained and drilled regularly in emergency response. The Task Force recommends that the Emergency Response Team be identified and on call by November 15, 1979, and at least several members of that team be relieved temporarily of normal duties to devote full time to the initial ERT task (to be completed by February 1, 1980) of identifying resource requirements, procedures, training, and facilities, including deployment in the field, to enable effective emergency response by NRR in support of the Executive Management Team and the Incidence Response Action Coordination Team (IRACT) in

the NRC Incident Response Center. The Task Force further recommends that the Commission consider the potential for NRC involvement in nuclear emergencies in foreign countries and provide definitive groundrules for the NRC staff role in such response.

NRC FORM 335 (7-77) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*: NUREG-0585

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*: TMI-2 Lessons Learned Task Force Final Report

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)

5. DATE REPORT COMPLETED: MONTH October YEAR 1979

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*:
U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Washington, D.C. 20555

DATE REPORT ISSUED: MONTH October YEAR 1979

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*:
Same as 9 above

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.

13. TYPE OF REPORT

PERIOD COVERED *(Inclusive dates)*

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

In its final report reviewing the Three Mile Island accident, the TMI-2 Lessons Learned Task Force has suggested change in several fundamental aspects of basic safety policy for nuclear power plants. Changes in nuclear power plant design and operations and in the regulatory process are discussed in terms of general goals. The appendix sets forth specific recommendations for reaching these goals.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT: Unlimited availability

19. SECURITY CLASS *(This report)*: unclassified

21. NO. OF PAGES

20. SECURITY CLASS *(This page)*: unclassified

22. PRICE: $

NRC FORM 335 (7-77)

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION